**Fujitsu SPARC M12 and
Fujitsu M10/SPARC M10**

System Operation and Administration Guide

FUJITSU

ORACLE

Contents

Preface

This document describes methods of setting and managing the SPARC M12/M10 systems from Oracle or Fujitsu after installation. Read the necessary parts when operating any SPARC M12/M10 system.
We recommend you read the *Fujitsu SPARC M12 Quick Guide* or *Fujitsu M10/SPARC M10 Systems Quick Guide* before reading this document.

Fujitsu SPARC M12 is sold as SPARC M12 by Fujitsu in Japan.
Fujitsu SPARC M12 and SPARC M12 are identical products.

Fujitsu M10 is sold as SPARC M10 by Fujitsu in Japan.
Fujitsu M10 and SPARC M10 are identical products.

Audience

This document is designed for system administrators with advanced knowledge of computer networks and Oracle Solaris.

Related Documentation

All documents for your server are available online at the following locations.

- Sun Oracle software-related documents (Oracle Solaris, etc.)
  http://docs.oracle.com/en/

- Fujitsu documents
  Global site

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

  Japanese site

For a system using the SPARC M12, see the manuals listed in "Documentation Related to the SPARC M12."

For a system using the SPARC M10, see the manuals listed in "Documentation Related to the SPARC M10."

Documentation Related to the SPARC M12

Manual Names (*1)
Fujitsu SPARC M12 Product Notes
Fujitsu SPARC M12 Quick Guide
Fujitsu SPARC M12 Getting Started Guide (*2)
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information (*2)
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide
Software License Conditions for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security Guide
Fujitsu SPARC Servers/SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual
Fujitsu SPARC M12-1 Installation Guide
Fujitsu SPARC M12-2 Installation Guide
Fujitsu SPARC M12-2S Installation Guide
Fujitsu SPARC M12 PCI Card Installation Guide
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 System Operation and Administration Guide
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide (*3)
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists
Fujitsu SPARC M12-1 Service Manual
Fujitsu SPARC M12-2/M12-2S Service Manual
Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual
PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Glossary
External USB-DVD Drive user guide

*1 The listed manuals are subject to change without notice.
*2 Printed manuals are provided with the product.
*3 This document applies specifically to the SPARC M12/M10 and FUJITSU ETERNUS disk storage system.

Documentation Related to the SPARC M10

Manual Names (*1)
Fujitsu M10/SPARC M10 Systems Product Notes
Fujitsu M10/SPARC M10 Systems Quick Guide
Fujitsu M10/SPARC M10 Systems Getting Started Guide (*2)
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information (*2)
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide
Software License Conditions for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security Guide
Fujitsu SPARC Servers/SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual
Fujitsu M10-1/SPARC M10-1 Installation Guide
Fujitsu M10-4/SPARC M10-4 Installation Guide
Fujitsu M10-4S/SPARC M10-4S Installation Guide
Fujitsu M10/SPARC M10 Systems PCI Card Installation Guide
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 System Operation and Administration Guide
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide (*3)
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists
Fujitsu M10-1/SPARC M10-1 Service Manual
Fujitsu M10-4/Fujitsu M10-4S/SPARC M10-4/SPARC M10-4S Service Manual
Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual
PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual
Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Glossary
External USB-DVD Drive user guide

*1 The listed manuals are subject to change without notice.
*2 Printed manuals are provided with the product.
*3 This document applies specifically to the SPARC M12/M10 and FUJITSU ETERNUS disk storage system.

Notes on Safety

Read the following documents thoroughly before using or handling the SPARC M12/M10.

- *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information*

- *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide*

Text Conventions

This manual uses the following fonts and symbols to express specific types of information.

Font/Symbol	Meaning	Example
AaBbCc123	What you type, when contrasted with on-screen computer output. This font is used to indicate an example of command input.	XSCF> **adduser jsmith**
AaBbCc123	The names of commands, files, and directories; on-screen computer output. This font is used to indicate an example of command output in the frame.	XSCF> **showuser -P** User Name: jsmith Privileges: useradm auditadm
Italic	Indicates the name of a reference manual.	See the *Fujitsu M10-1/SPARC M10-1 Installation Guide*.
" "	Indicates the names of chapters, sections, items, buttons, or menus.	See "Chapter 2 Network Connection."

Command Syntax in the Text

While the XSCF commands have a section number of (8) or (1), it is omitted from the text.
For details on the commands, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Syntax of the Command-Line Interface (CLI)

The command syntax is as follows:

- A variable that requires the input of a value is in Italics.

- An optional element is enclosed in [].

- A group of options for an optional keyword is enclosed in [] and delimited by |.

Document Feedback

If you have any comments or requests regarding this document, please take a moment to share them with us. Along with the manual code, manual title, and page number, state your points specifically at one of the following websites:

- Global site
  http://www.fujitsu.com/global/contact/

- Japanese site
  http://www.fujitsu.com/jp/products/computing/servers/unix/sparc/contact/

Chapter 1

Understanding an Overview of the SPARC M12/M10

This chapter provides an overview of the SPARC M12/M10 systems and describes the software and firmware used with them.

- Basics of the SPARC M12/M10
- Basics of the XSCF Firmware
- Network Configuration
- Basics of Hypervisor
- Basics of Oracle VM Server for SPARC
- Basics of OpenBoot PROM

1.1 Basics of the SPARC M12/M10

This section provides an overview of the SPARC M12/M10 systems.

The SPARC M12/M10 is a UNIX server system that uses the SPARC processor and Oracle Solaris. CPU Activation allows the expansion of resources in units of one core in phases. The SPARC M12-2S/M10-4S uses a building block system so that the system can be configured as appropriate for the intended business use and the scale of business. The servers can be applied in many ways; as the database servers best-suited for data centers in an era of cloud computing, and as the Web servers or application servers for which high throughput is demanded.

The following models have been prepared to support various intended uses.

- SPARC M12-1
  This 1-CPU compact model with six cores at maximum is designed for space saving and high performance.

- SPARC M12-2
  This model consists of up to two CPUs, each of which has up to 12 cores.

- SPARC M12-2S
  This model consists of up to two CPUs, each of which has up to 12 cores. With the

building block (BB) system, the number of connected SPARC M12-2S units can be adjusted according to the performance required. A configuration can be expanded to up to four BBs by connecting the SPARC M12-2S units directly to one another. Moreover, a system that uses crossbar boxes supports a configuration of up to 16 BBs and scales up to 32 CPUs--the scalability is ensured.

- SPARC M10-1
  This 1-CPU compact model with 16 cores at maximum is designed for space saving and high performance.

- SPARC M10-4
  This model consists of up to four CPUs, each of which has up to 16 cores.

- SPARC M10-4S
  This model consists of up to four CPUs, each of which has up to 16 cores. With the building block (BB) system, the number of connected SPARC M10-4S units can be adjusted according to the performance required. A configuration can be expanded to up to four BBs by connecting the SPARC M10-4S units directly to one another. Moreover, a system that uses crossbar boxes supports a configuration of up to 16 BBs and scales up to 64 CPUs--the scalability is ensured.

Note - If the building block system is used, the SPARC M12-2S and SPARC M10-4S cannot be mixed in the same configuration.

System configuration

This section describes the system configuration.

Figure 1-1 shows an example of a system configuration where more than one SPARC M12-2S or more than one SPARC M10-4S is connected by the building block system. A single SPARC M12-2S/M10-4S unit that can have a building block configuration is one building block. A physical partition (PPAR) is configured by combining one or more building blocks.
Figure 1-2 shows an example of a system configuration of SPARC M12-1/M12-2/M10-1/M10-4. A single SPARC M12-1/M12-2/M10-1/M10-4 unit cannot have a building block configuration yet it is sometimes called a physical partition. Note that the SPARC M12-2S and SPARC M10-4S in a single unit configuration is also sometimes called a physical partition.

Figure 1-1   Example of a SPARC M12-2S/M10-4S System Configuration
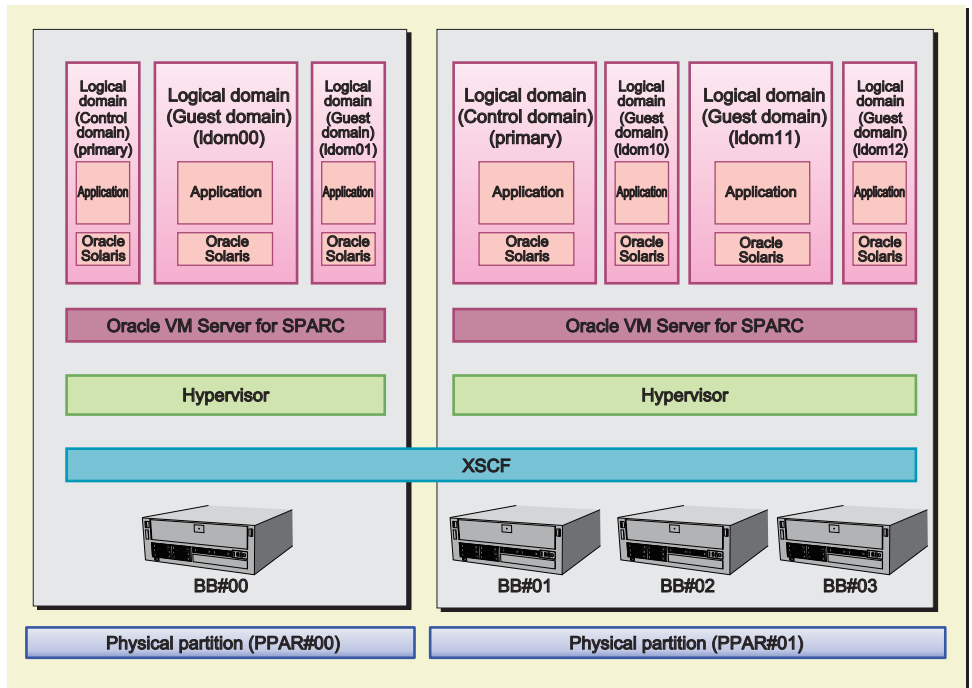
Figure 1-2   Example of a SPARC M12-1/M12-2/M10-1/M10-4 System Configuration
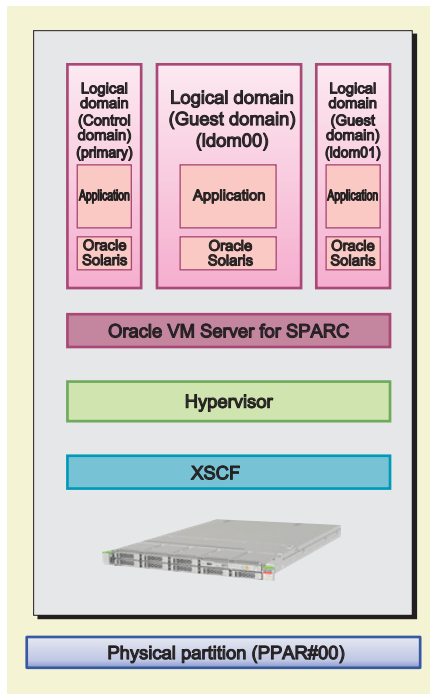
The following sections describe "physical partitions" and "logical domains," which are key to the system configuration.

Configuration of Physical Partitions

To configure a SPARC M12-2S or SPARC M10-4S system, configure a physical partition (PPAR) by combining one or more building blocks of the same model. Configuring physical partitions is called partitioning, and the resulting configured object is called a physical partition (PPAR). Physical partitions are configured using the XSCF firmware, which is the system management firmware.

In the example shown in Figure 1-1, PPAR#00 is one of the building blocks (BBs), and BB#00 is configured as the physical partition PPAR#00. Similarly, physical partition PPAR#01 is configured from BB#01, BB#02, and BB#03.

Once a physical partition is configured, hardware resources on the physical partition are assigned to logical domains.

Note that since the SPARC M12-1/M12-2/M10-1/M10-4 is a model consisting of a single unit, it can be configured with only one physical partition.

Configuration of Logical Domains

A physical partition has the CPUs, memory, I/O devices, and other hardware resources to be assigned to logical domains. A logical domain is configured using the Oracle VM Server for SPARC software.

A configured logical domain is handled as one UNIX system on the software side. Oracle Solaris and applications can be installed in logical domains and applied to tasks separately. In the example shown in Figure 1-1, the logical domains primary, ldom00, and ldom01 are configured with the assignment of hardware resources of the physical partition PPAR#00.

Similarly, the logical domains primary, ldom10, ldom11, and ldom12 are configured with the physical partition PPAR#01.

One of the logical domains, to which physical partition resources are assigned, serves as the domain controlling all the logical domains. It is called the control domain. The control domain, which is the logical domain controller, also serves to handle communication between the physical partition and logical domains.

Firmware/Software Required for the Systems

The physical partitions are implemented with the XSCF firmware and the logical domain, Oracle VM Server for SPARC. Even for a configuration of only the control domain, Oracle VM Server for SPARC is required.
Between the XSCF firmware and Oracle VM Server for SPARC, communication for monitoring and managing the whole system is handled inside the system. Users do not need to pay attention to that.

The interface between the XSCF firmware and Oracle VM Server for SPARC in the SPARC M12/M10 systems is implemented by firmware named Hypervisor.

"1.2   Basics of the XSCF Firmware" and subsequent sections describe firmware and software used in the systems.

1.2 Basics of the XSCF Firmware

This section provides an overview and describes the functions of the XSCF firmware.

1.2.1 XSCF Overview

The XSCF firmware is the standard built-in system control facility in the SPARC M12/M10. The XSCF firmware runs on a dedicated processor (service processor) independently of the server processors. The chassis of each SPARC M12/M10 system contains one complete package of the XSCF firmware for communicating with logical domains and managing the whole system. When multiple servers are combined using the building block (BB) system, the server is interconnected with other servers by means of crossbar boxes (XBBOX). In each of these crossbar boxes, there is a service processor that runs the XSCF firmware.

The XSCF firmware runs and constantly monitors the proper operation of the server as long as input power is supplied to the server, even if a logical domain is not running or the power of the physical partition is off. It also changes the server configuration and powers on/off the server, as required.

Moreover, the XSCF firmware includes a user interface to provide functions to monitor, manage, and control the system.

In this manual, the XSCF firmware may be referred to as the XSCF. The board containing the mounted service processor for running the XSCF firmware may be referred to as the XSCF unit.

1.2.2 XSCF Features

Built-in user interface used for daily server operation and maintenance

You can get a grasp of the server status, operate the server, and service the server by accessing the XSCF from the command line or a Web browser.

- **XSCF shell (command-line interface)**
  You can connect a user PC to the server directly through a serial cable, or connect an Ethernet connection with the XSCF LAN, and perform communications using the SSH service or Telnet service. As a result, the PC can be used as an XSCF shell terminal, which can execute XSCF shell commands. On the XSCF shell, you can switch to a console from which you can operate the control domain (referred to below as the control domain console).

  Figure 1-3 shows an example of the XSCF shell terminal.

Figure 1-3   Example of the XSCF shell terminal
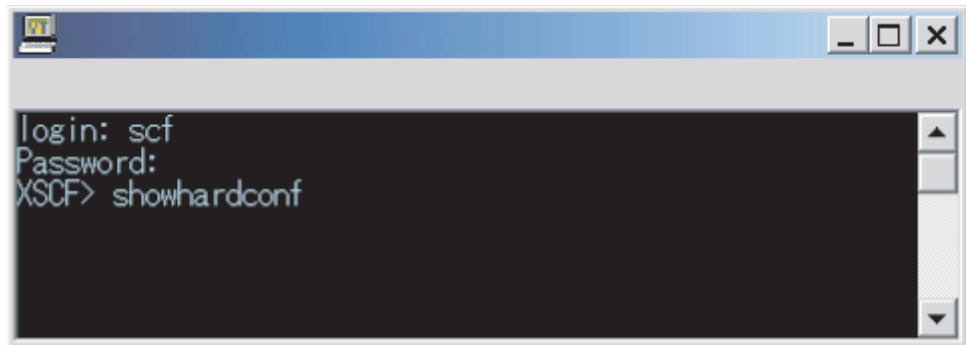
- ■ **XSCF Web (browser user interface)**
  This interface allows you to connect a user PC to the XSCF LAN via Ethernet and
  perform communications using the HTTPS and SSL/TLS protocols. As a result,
  you can use a Web browser on the PC for using the XSCF Web console. With XSCF
  Web, you can lessen the load of operations by users and reduce server management
  costs by displaying components in a hierarchical view and finding the operations
  for those purposes from a menu.

  Figure 1-4 shows an example of using the XSCF Web console.

Figure 1-4   Example of the XSCF Web Console
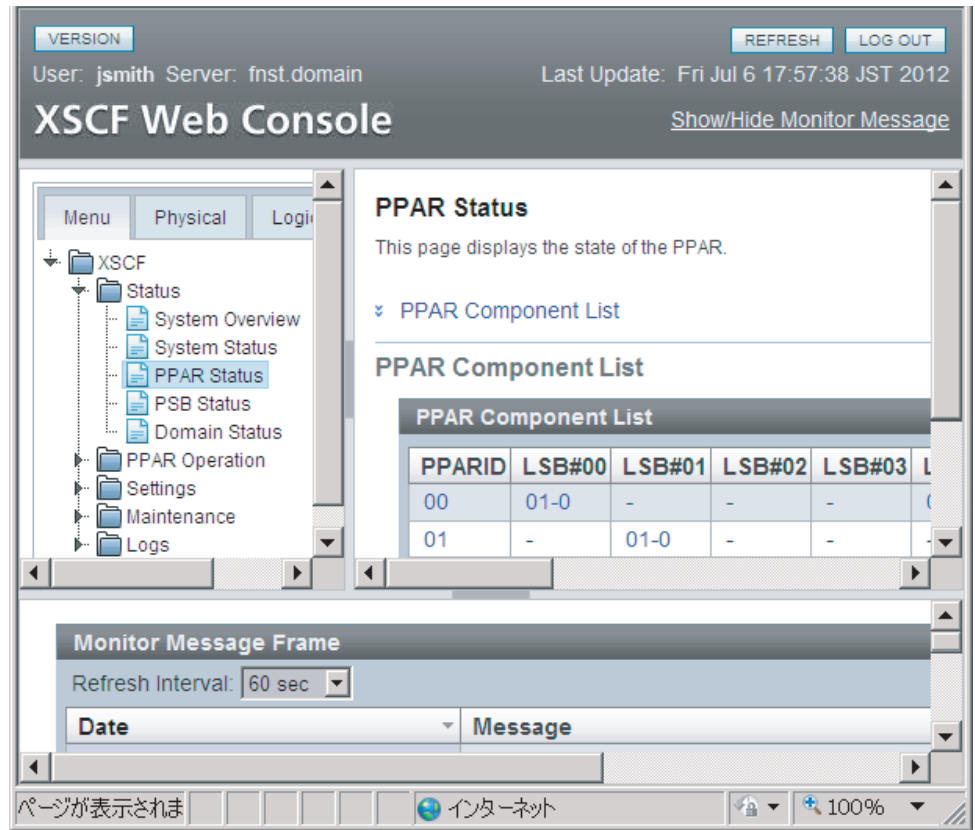
XSCF in the building block configuration

When the system is configured using the building block system, the crossbar box (XBBOX) also contains XSCF. Mounting the XSCF in the server and XBBOX implements a highly reliable system.

Note - If a system is configured using the building block system, SPARC M12-2S and SPARC M10-4S chassis cannot be mixed in the configuration.

Figure 1-5 shows an example of a SPARC M12-2S or SPARC M10-4S system in the 4BB configuration, with chassis directly interconnected.

Figure 1-5   Example of a SPARC M12-2S/M10-4S System XSCF Configuration (No
              Crossbar Box)
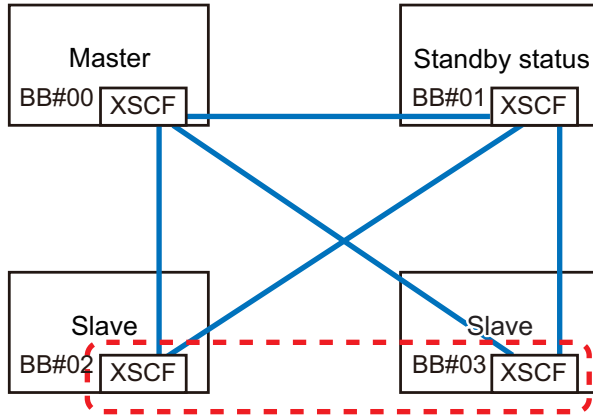
Figure 1-6 shows an example of a SPARC M12-2S or SPARC M10-4S in the 8BB
configuration with a crossbar box.

Figure 1-6   Example of a SPARC M12-2S/M10-4S System XSCF Configuration
              (With Crossbar Boxes)
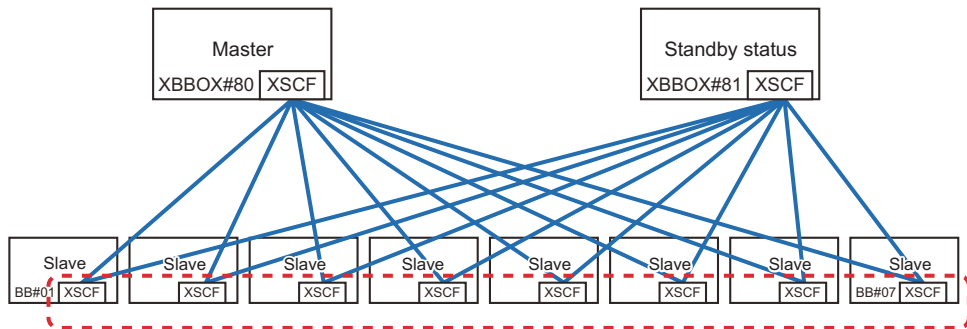
XSCFs in the building block configuration are classified into three roles: master,
standby, and slave. For details, see "1.2.4   Master/Standby/Slave XSCF Mechanism."

External Interfaces

The individual chassis and crossbar boxes in the SPARC M12/M10 have the following
XSCF-related connectors (ports) and LEDs mounted. Users, system administrators,
and field engineers can monitor and operate the servers by using these interfaces and
the XSCF firmware.
For the location of each interface and details on the connection method, see either of
the following.
- "Checking External Interface Port Specifications" in the *Installation Guide* for your
  server
- "Understanding the LED Indications" in the *Service Manual* for your server
■ Serial port
  The serial port is used with the XSCF shell to configure the server and display the

server status. The serial port (RS-232C) uses an RJ-45 connector. The connection between the serial port and a PC uses an RS-232C serial cross cable. If you connect with a LAN cable, the connection needs an RJ-45/RS-232C conversion cable or conversion connector.

- XSCF-LAN port (Ethernet port)
  The XSCF-LAN port is the port for the LAN connection used by the system administrator to operate the server via Ethernet. Through the XSCF-LAN port, the system administrator configures the server and displays the server status by using the XSCF shell or XSCF Web. There are two XSCF-LAN ports. Both ports use an RJ-45 connector. Each port supports only 10Base-T/100Base-TX/1000Base-T auto negotiation. The connection speed/connection mode of the XSCF-LAN cannot be set.

- USB ports
  The front panel has one USB port (Type-A) and the rear panel has two USB ports for connections with USB devices. Use these USB ports to, for example, connect a DVD drive to install Oracle Solaris. The XSCF-dedicated USB port on the rear panel supports the USB 1.1 or USB2.0 interface. Use it to save and restore XSCF hardware information and to collect log information.

- LEDs
  The following LEDs relate to the XSCF and XSCF-LAN.

  - READY LED (green)
    The READY LED goes on in green. The READY LED starts blinking immediately after the input power is turned on. The blinking indicates that the XSCF is starting and being initialized. Once the XSCF initialization ends, the LED stops blinking and stays on.

  - CHECK LED (amber)
    The CHECK LED goes on in amber. The CHECK LED goes on immediately after the input power is turned on. However, the CHECK LED stays off while the hardware operates normally. It goes on when the hardware has some kind of failure.

  - MASTER LED (green, only for the SPARC M12-2S/M10-4S system)
    The MASTER LED goes on in green. The MASTER LED indicates the SPARC M12-2S chassis, SPARC M10-4S chassis, or crossbar box that has the master XSCF, in a system with multiple XSCFs. It goes on for the master XSCF and stays off for the standby and slave XSCFs.

  - LINK SPEED (green or amber)
    Each XSCF-LAN port has the Link Speed LED, which goes on in green or amber. The Link Speed LED goes on in amber with a 1000-Mbps LAN connection and goes on in green with a 100-Mbps LAN connection. It goes out with a 10-Mbps LAN connection.

  - ACT LED (green)
    Each XSCF-LAN port has the ACT LED, which goes on in green. It blinks in green while data is being sent or received. It goes out while data is not being sent or received.

- Protocol for SP to SP communication port (SSCP port)
  In the system with a building block configuration and multiple XSCFs, the following connectors (ports) are mounted on each SPARC M12-2S or SPARC

M10-4S chassis and crossbar boxes because communications are made between service processors. For the configuration of connections between XSCFs, see "Chapter 4   Setting the SPARC M12-2S in a Building Block Configuration" in the *Fujitsu SPARC M12-2S Installation Guide* or "Chapter 4   Configuring Building Block Connections" in the *Fujitsu M10-4S/SPARC M10-4S Installation Guide*.

- SPARC M12-2S/M10-4S side
  XSCF DUAL control port: 1 port. This port connects the master and standby XSCFs together.
  XSCF BB control port: 3 ports. These ports connect the master and standby XSCFs to slave XSCFs.

- Crossbar box side
  XSCF DUAL control port: 1 port. This port connects the master and standby XSCFs together.
  XSCF BB control port: 19 ports. These ports connect the master and standby XSCFs to slave XSCFs.

1.2.3   XSCF Functions

XSCF shell and XSCF Web

The XSCF provides the XSCF shell and XSCF Web, enabling users to display the server status, operate the server, display the physical partition status, operate a physical partition, and display a console.

System Initialization and Initial Diagnosis

The XSCF performs an initial self-diagnosis at the input power-on time or XSCF reboot time, to detect and notify the user of any failure in the XSCF. It also makes the initial hardware settings of the XSCF and also initializes the required hardware for starting Oracle Solaris.

System Configuration Recognition and Physical Partition Configuration Management

The XSCF manages CPUs, memory, and I/O system resources by chassis, displays the state of the system configuration, and creates and changes a physical partition configuration.
In the SPARC M12-2S and SPARC M10-4S, users can configure a physical partition by connecting multiple chassis using the building block system with one chassis (1BB) as the minimum unit. Chassis (BBs), physical partition configuration units, are managed by logical numbers (LSB numbers), which are recognized by logical domains. In addition, in linkage with the Hypervisor firmware, the XSCF firmware monitors the memory, CPUs, and I/O resources used by the logical domains configured from Oracle VM Server for SPARC software.

Note - A system of one SPARC M12/M10 unit consists of one physical partition.

Failure Monitoring and RAS Functions

The XSCF batch controls/monitors the server so that the system operates stably. Upon detecting a system failure, it immediately starts collecting a hardware log, performs an analysis, identifies the failure location, and determines the failure status. The XSCF displays the status and performs parts degradation, physical partition degradation, and a system reset, as needed, to prevent another failure from occurring. The XSCF ensures high reliability, availability, and serviceability (RAS) of the whole system.

The target of monitoring is as follows.
- Hardware configuration management and monitoring
- Network configuration monitoring
- Monitoring of cooling units, such as the fan units, and the ambient temperature
- Monitoring of the physical partition status and logical domain status
- Monitoring of peripheral failures

Function to Notify the System Administrator of Failure Information

The XSCF constantly monitors system operation. The XSCF provides the following services to notify the system administrator of failure information.
- Server monitoring function without relying on Oracle Solaris operation
- Remote control of the server from a remote location
- E-mail notification when trouble occurs
- Trap notification using the SNMP agent function

Messaging and Logging

The XSCF collects and stores system failure information. Failures and failure locations are identified from hardware failure information, which also provides server failure predictions and accurate, easy-to-understand information to users immediately after failure occurrence. For details of error messages and logs, see "Chapter 12   Checking Logs and Messages."

The displayed messages are as follows.
- Initial diagnosis message at system startup
- Message displayed at the same time that network configuration monitoring detects a configuration failure
- Message displayed at the same time that the failure of a part is detected
  With information from monitoring of the status of the power supply unit, fan, system board, memory, CPU, and other components, the system administrator can quickly find out about a part to be replaced.
- Message displayed at the same time that an environmental failure is detected
  Monitoring of the server temperature and CPU temperature can prevent system instability due to a temperature rise.

The logs that are taken are as follows.

- Error log
- Monitor message log
- Power log
- Event log
- Console log
- Panic log
- IPL log
- Audit log
- COD log
- Temperature history log
- Active Directory log
- LDAP over SSL log

XSCF User Account Management

The XSCF manages the user accounts for using the XSCF. The types of privilege for user accounts managed by the XSCF are listed below. The available operations on the provided XSCF shell and XSCF Web depend on the user account type (referred to as a user privilege).

- System administrator
- Physical partition administrator
- Operator
- Field engineer

Security

The XSCF provides encryption and audit functions via SSH and SSL/TLS. Operational errors and invalid accesses are recorded in logs while the system is running. The system administrator can use the logs to investigate the causes of system failures and invalid accesses.

Assistance in Active Replacement of a Part

The XSCF assists maintenance work through the XSCF shell during active replacement of a part. When a maintenance command is executed, the maintenance menu appears. The user can then follow the menu to perform the maintenance.

Console Redirection Function

The XSCF provides a function to output to the OS console (control domain console) of Oracle Solaris in each physical partition. With an SSH (Secure Shell) or Telnet connection to the XSCF, the function can serve as the OS console.

CPU Activation registration/management function

Registering the CPU Activation key with the XSCF allows the permanent usage of server CPU resources. Before the server enters operation, one or more CPU

Activations must be purchased.

The XSCF performs the work of adding a CPU Activation key when additional CPU resources become necessary. The XSCF performs the work of removing a CPU Activation key when you want to decrease the CPU resources.
For details of CPU core resource use, see "Chapter 5   CPU Activation."

Firmware Update Function

Using XSCF Web and XSCF shell commands, you can download a new firmware (XSCF firmware, OpenBoot PROM firmware, POST firmware, or Hypervisor firmware) without powering off the physical partition. You can also update the firmware without powering off the other physical partitions.   Note that if you update the OpenBoot PROM firmware, POST firmware, or Hypervisor firmware when the physical partition is started, the update is applied when the physical partition is rebooted. For details of firmware updates, see "Chapter 16   Updating the XCP Firmware."

Green IT Function

Oracle Solaris, Hypervisor, and the XSCF stop power input to components not in operation to suppress power consumption. The XSCF can also control the upper limit value of power consumption to suppress system power consumption. If the upper limit value is exceeded, the XSCF immediately determines the system power operations and performs a shutdown or power-off operation.

Time Control

The SPARC M12/M10 sets the XSCF clock as the system reference time.
The physical partitions of the SPARC M12/M10 systems synchronize the time with the XSCF clock at physical partition startup. The XSCF manages time differences from the control domain in linkage with the Hypervisor firmware.

Physical Partition Dynamic Reconfiguration (PPAR DR) Function

In a building block configuration, the XSCF supports the work necessary to dynamically change the configuration of the physical partition while the system is running. The dynamic reconfiguration of the physical partition (PPAR DR) enables you to add or delete a building block (SPARC M12-2S or SPARC M10-4S) of the physical partition, with the physical partition being operated. For details of the PPAR DR function, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Note - In SPARC M12-1/M12-2/M10-1/M10-4, the PPAR DR function cannot be used.

1.2.4   Master/Standby/Slave XSCF Mechanism

In a system where the SPARC M12-2S or SPARC M10-4S is connected by the building block system, one XSCF is mounted in each SPARC M12-2S or SPARC M10-4S chassis and crossbar box. The XSCFs are classified into three types according to their

role.

- Master XSCF
  The system contains only one master XSCF. In addition to monitoring and managing the whole system, the master XSCF also manages the SPARC M12-2S, SPARC M10-4S, or crossbar box in which it is mounted. For duplication, a standby XSCF operates as the backup to the master XSCF.

- Slave XSCF
  The slave XSCF is an XSCF other than the master XSCF. The slave XSCF monitors and manages only the SPARC M12-2S, SPARC M10-4S, or crossbar box in which it is mounted.

- Standby XSCF
  This XSCF operates as the backup to the master XSCF. It is also called standby XSCF. One standby XSCF is included in the slave XSCF.

The master XSCF and standby XSCF monitor each other. If a failure occurs in the master XSCF, the master XSCF can switch with the standby XSCF, enabling continuous system operation and management without stopping business.

The master XSCF is connected to slave XSCFs by dedicated cables, and communication is made via the XSCF-dedicated protocol called the SP to SP communication protocol (SSCP). The settings made for the master XSCF are reflected on the slave XSCFs via SSCP. However, the settings made for a given physical partition are reflected only on the XSCFs belonging to that PPAR.

1.2.5 Differences in XSCF Configurations by Model

This section describes how XSCFs are configured and how the system is monitored and managed in the respective configurations of the SPARC M12/M10.

SPARC M12-1/M12-2/M10-1/M10-4, and SPARC M12-2S/M10-4S in a Single-Unit Configuration

The SPARC M12-1/M12-2/M10-1/M10-4 and the SPARC M12-2S/M10-4S in a single-unit configuration each have a configuration with only one XSCF. There is no standby XSCF or slave XSCF.

SPARC M12-2S/M10-4S in a Building Block Configuration (No Crossbar Box)

The SPARC M12-2S/M10-4S system in a building block configuration with no crossbar box is configured with up to four SPARC M12-2S or SPARC M10-4S chassis, so the configuration has up to four XSCFs accordingly. In this case, the XSCF in the BB#00 or BB#01 chassis is the master XSCF or standby XSCF. If a failure occurs in the master XSCF, the standby XSCF switches to the master XSCF. The BB#02 and BB#03 chassis are fixed as slave XSCFs.

- Forms of connection
  The XSCF BB control port of the master XSCF (BB#00 in Figure 1-7) is connected to the XSCF BB control port with network ID 0 (#0 port of BB#01 to BB#03 in Figure 1-7) on each slave XSCF.

The XSCF BB control port of the standby XSCF (BB#01 in Figure 1-7) is connected to the XSCF BB control port with network ID 1 (#1 port of BB#02 and BB#03 in Figure 1-7) on each slave XSCF. The master XSCF and standby XSCF are connected by the XSCF DUAL control ports. The slave XSCFs are connected only to the master XSCF and standby XSCF.

- XSCF control flow
  The master XSCF monitors and manages all the XSCFs. In principle, the various settings for XSCFs are made from the master XSCF. The settings made with the master XSCF are reflected on all slave XSCFs, including the standby XSCF, through the SSCP network. Also, the settings made with the master XSCF for a given SPARC M12-2S or SPARC M10-4S chassis are also reflected on the standby XSCF and the slave XSCFs in the intended SPARC M12-2S or SPARC M10-4S chassis.

Figure 1-7   XSCF Connections (for the SPARC M12-2S/M10-4S in a Building Block Configuration (No Crossbar Box))
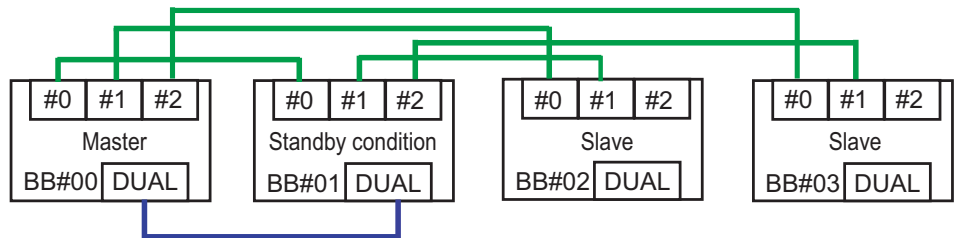
SPARC M12-2S/M10-4S in a Building Block Configuration (With Crossbar Boxes)

The SPARC M12-2S or SPARC M10-4S in a building block configuration (with crossbar boxes) is configured with up to 16 XSCFs, or the crossbar boxes with up to four XSCFs. In this case, the XSCF in the XBBOX#80 or XBBOX#81 crossbar box is the master XSCF or standby XSCF. The XSCFs in the XBBOX#82 and XBBOX#83 crossbar boxes and in all SPARC M12-2S or SPARC M10-4S chassis are fixed as slave XSCFs.

- Forms of connection

- Connections to crossbar boxes
  The master XSCF (XBBOX#80) is connected to the XSCF BB control port with network ID 16 (#16 port of XBBOX#81 to XBBOX#83 in Figure 1-8) on each slave XSCF. The standby XSCF (XBBOX#81) is connected to the XSCF BB control port with network ID 17 (#17 port of XBBOX#82 and XBBOX#83 in Figure 1-8) on each slave XSCF. The master XSCF and standby XSCF are connected by the XSCF DUAL control ports. Connection is not made to any XSCF other than the master XSCF and standby XSCF.

- Connections to the SPARC M12-2S/M10-4S
  The master XSCF (XBBOX#80) is connected to the XSCF BB control port with network ID 0 (#0 port of BB#00 to BB#15 in Figure 1-8) on each slave XSCF. The standby XSCF (XBBOX#81) is connected to the XSCF BB control port with network ID 1 (#1 port of BB#00 to BB#15 in Figure 1-8) on each slave XSCF. The XSCFs fixed

as slave XSCFs (BB#00 to BB#15) are connected only to the master XSCF and standby XSCF.

- XSCF control flow
  The master XSCF monitors and manages all the XSCFs. In principle, the various settings for XSCFs are made from the master XSCF. The settings made with the master XSCF are reflected on all slave XSCFs, including the standby XSCF, through the SSCP network. Also, the settings made with the master XSCF for a given SPARC M12-2S or SPARC M10-4S chassis are also reflected on the standby XSCF and the slave XSCFs in the intended SPARC M12-2S or SPARC M10-4S chassis.

Figure 1-8   XSCF Connections (for the SPARC M12-2S/M10-4S in a Building Block Configuration (With Crossbar Boxes))
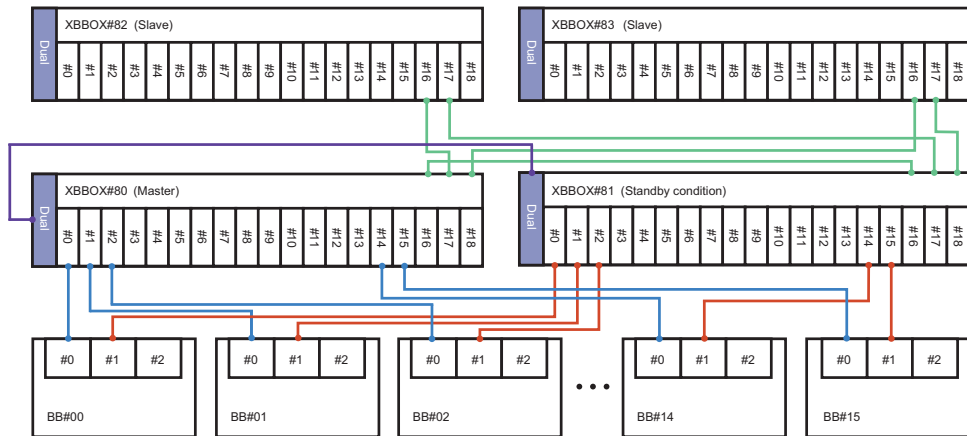
1.3   Network Configuration

1.3.1   Overview of Network Connections

This section provides an overview of the network connections for system operation.

The system consists of two major networks. One is the user network, and the other is the system control network.

- User network
  The user network is used to run the configured system in business. The user network is connected to other servers, other PCs, and peripherals as required for tasks, and configured accordingly.

  The user network environment is kept secure with the installation of a firewall and other security measures as needed when the network can be connected

externally to the Internet.

- System control network (XSCF network)

  The system control network (XSCF network) is used for system maintenance and management. Other uses of this network include operations of the XSCF firmware, which is used to monitor and manage the system, power-on/off operations, and component replacement operations. To perform operations for remote system control, the system control network is set up in an environment configured for the operations.

  Though the system control network can be connected to the user network too, security measures such as a firewall must be installed for higher security to prevent unauthorized external access to the system control network.

  The terminal used for system maintenance and management (system management terminal) is connected via a serial or LAN connection, according to the situation. For the forms of connection of the system management terminal, see "2.1 Connecting the System Management Terminal."

The following example shows a SPARC M12/M10 system configuration.

Figure 1-9 shows a configuration that uses one SPARC M12/M10.
The system management terminal is connected to the XSCF-LAN port via the serial port or the system control network. The remote storage is connected to the XSCF-LAN port via the system control network. The GbE LAN port or 10GbE LAN port is connected to the installation server and others via the user network. Moreover, the SAS ports are connected to external SAS interface devices, such as a tape unit, and the USB ports are connected to external USB interface devices, such as an external DVD drive.

Figure 1-9   Configuration Example of Connections of the Single-Unit Configuration of the SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S
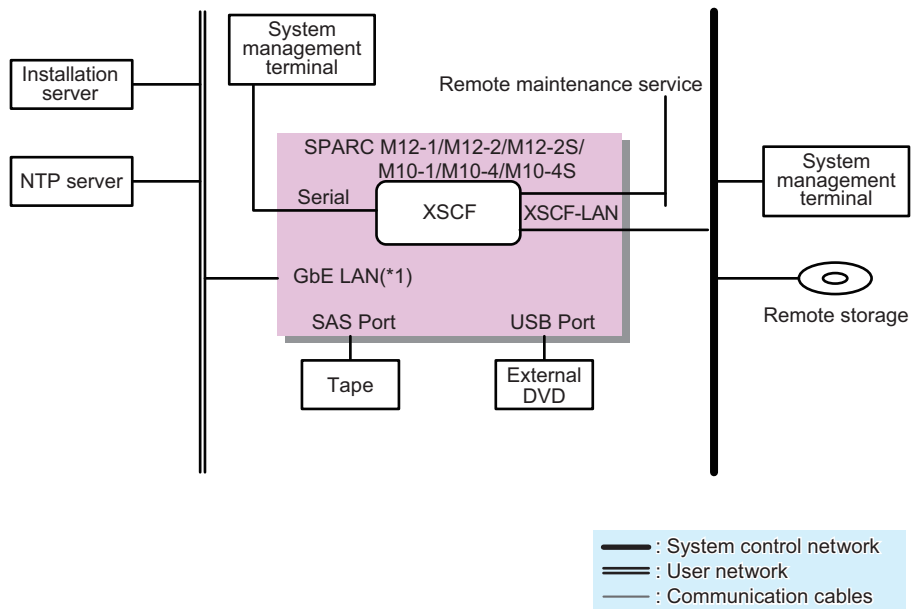
*1 10GbE LAN for SPARC M12-1/M12-2/M12-2S

Figure 1-10 shows a configuration that has four SPARC M12-2S or SPARC M10-4S units connected without using crossbar boxes.
The system management terminal is connected to the serial port of the master XSCF or to the XSCF-LAN ports of the master XSCF and standby XSCF via the system control network. The 10GbE LAN port of four SPARC M12-2S units or GbE LAN port of four SPARC M10-4S units is connected to the installation server and others via the user network. Moreover, the SAS ports are connected to external SAS interface devices, such as a tape unit, and the USB ports are connected to external USB interface devices, such as an external DVD drive.

Figure 1-10   Configuration Example of SPARC M12-2S/M10-4S Connections (No Crossbar Box)
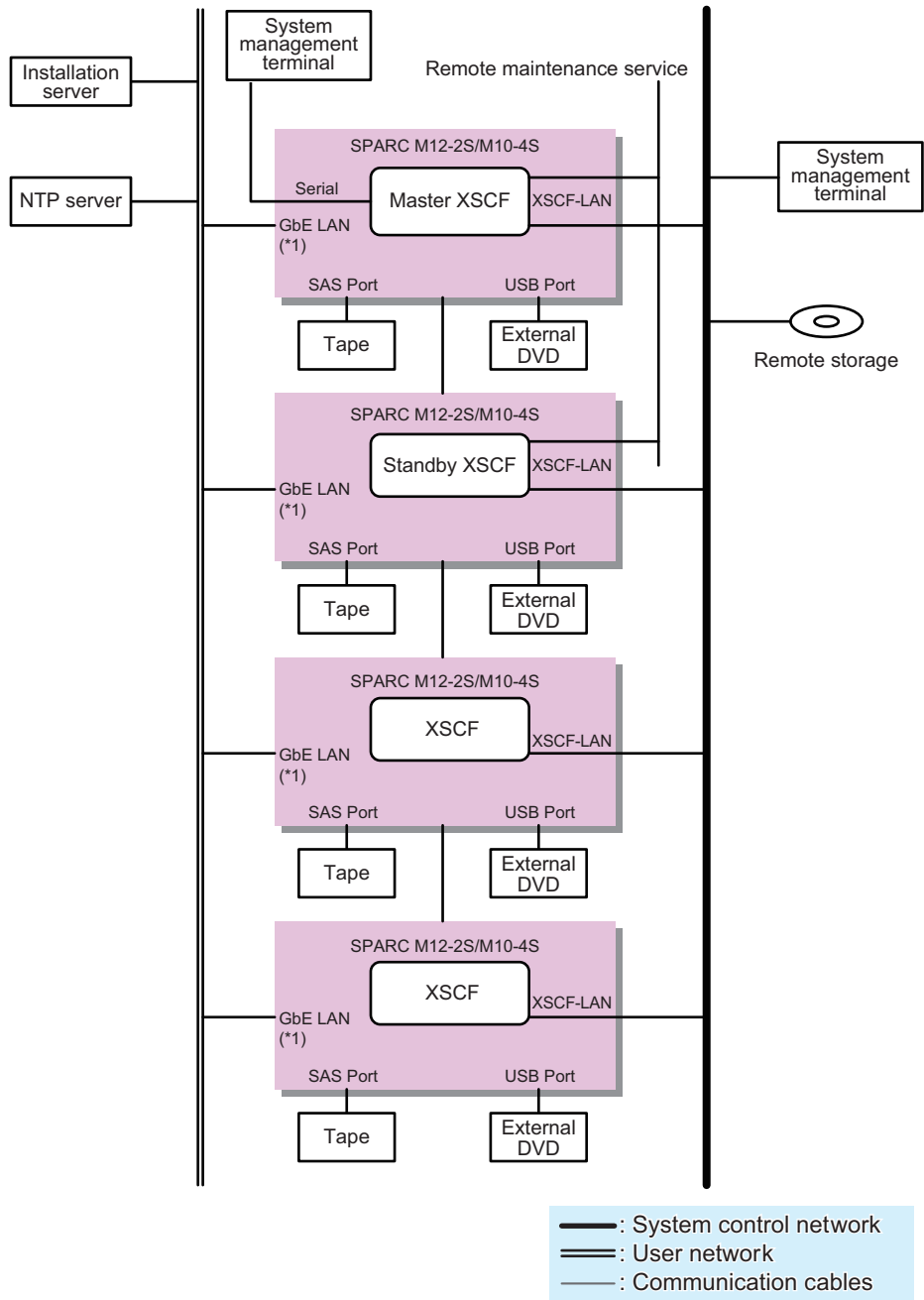
*1 10GbE LAN for SPARC M12-2S

Figure 1-11 shows a configuration that has multiple SPARC M12-2S or SPARC M10-4S units connected through crossbar boxes.

The system management terminal is connected to the serial port of the master XSCF in the crossbar box or to the XSCF-LAN ports of the master XSCF and standby XSCF via the system control network. The remote storage is connected to the XSCF-LAN of each SPARC M12-2S or SPARC M10-4S unit via the system control network.

The 10GbE LAN port of SPARC M12-2S or GbE LAN port of SPARC M10-4S is connected to the installation server and others via the user network. Moreover, the SAS ports of the SPARC M12-2S or SPARC M10-4S units are connected to external SAS interface devices, such as a tape unit, and the USB ports are connected to external USB interface devices, such as an external DVD drive.

Figure 1-11　　Configuration of SPARC M12-2S/M10-4S Connections (With Crossbar Boxes)
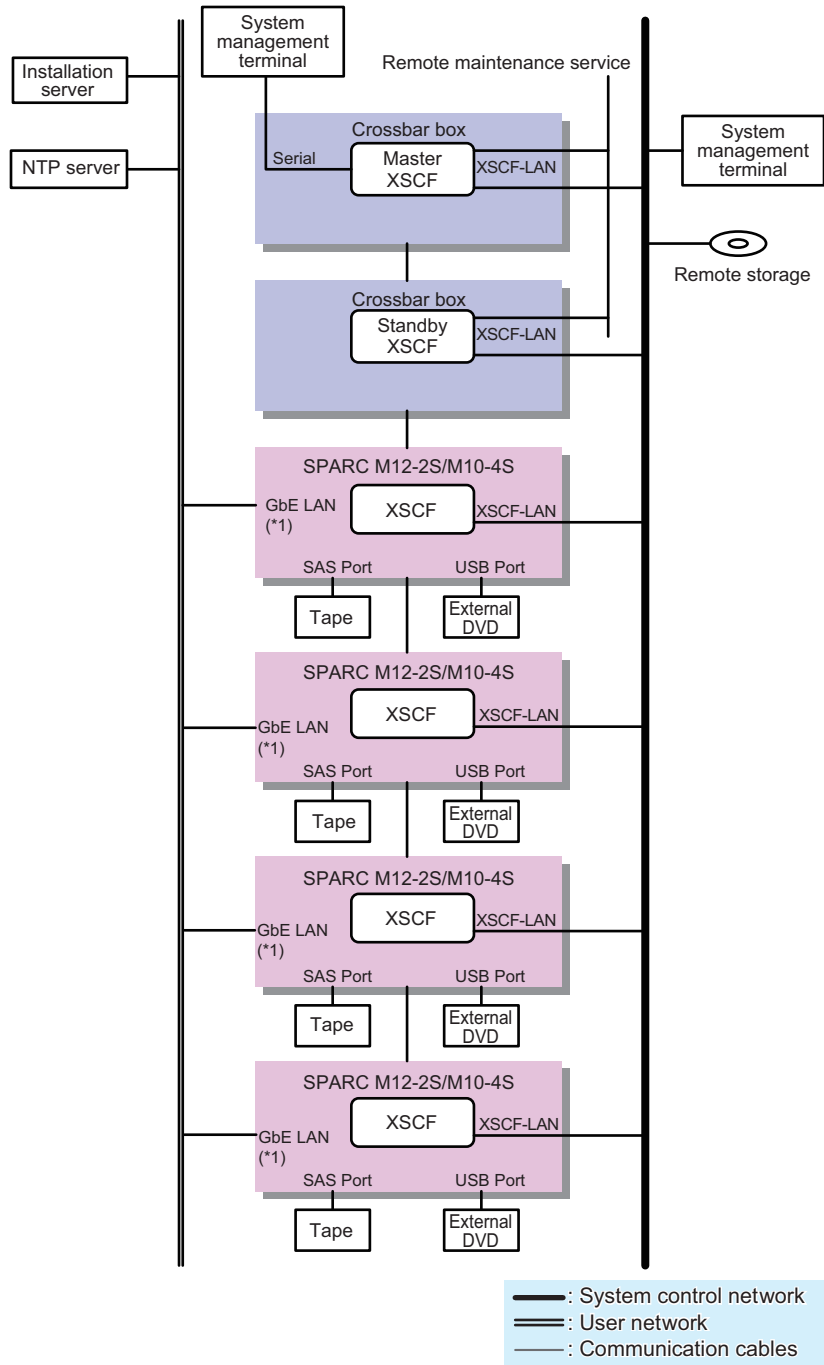
*1 10GbE LAN for SPARC M12-2S

Figure 1-12 shows a configuration that connects the system control network and user

network through the firewall.

Here, to use an NTP server to synchronize the time of the XSCFs, the NTP server on the user network is connected through the firewall. The connection through the firewall can protect the XSCFs from security threats on the user network.

For the remote storage placed on the user network, you can connect it to the XSCF-LAN while protecting it from security threats by configuring remote storage access in the firewall.

Figure 1-12   Configuration Connecting the System Control Network and User Network
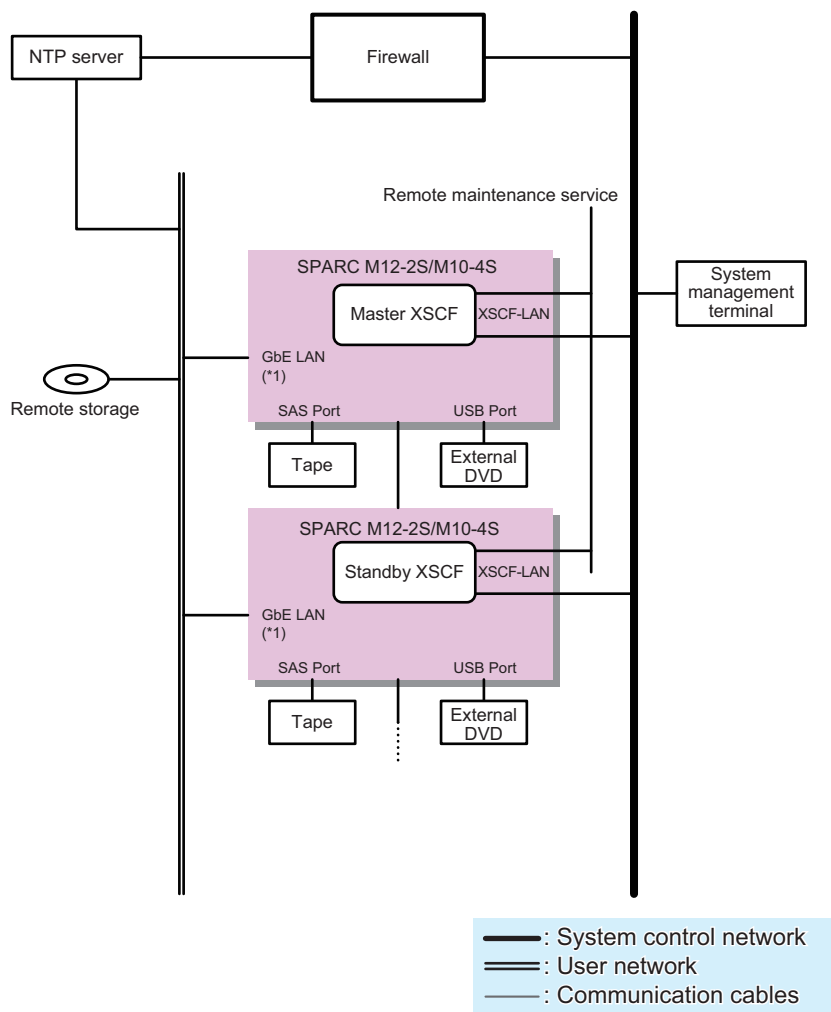
*1 10GbE LAN for SPARC M12-2S

Figure 1-13 shows a system in a building block configuration where each SPARC M12-2S or SPARC M10-4S unit is connected to a separate user network. Separating the user network segment connected to the 10GbE LAN of each SPARC M12-2S unit or the user network segment connected to the GbE LAN of each SPARC

M10-4S unit reduces the risk from security threats on the user networks.
The system control network cannot be separated for each SPARC M12-2S or SPARC
M10-4S unit in a building block configuration.

Figure 1-13   Configuration Separating the User Network Segment of Each Server
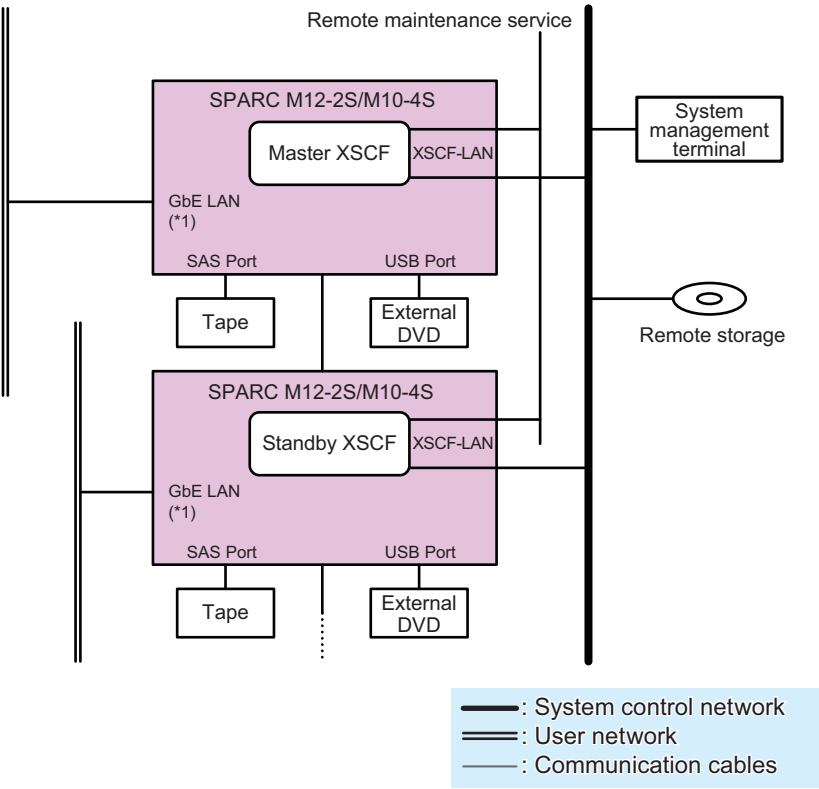
*1 10GbE LAN for SPARC M12-2S

1.3.2 XSCF-LAN Port Numbers and Functions, and Firewall

Table 1-1 lists the port numbers used with the XSCF-LAN ports and the functions
used by the XSCF. To protect the XSCF against unauthorized access and attacks
when it is connected to an external network, we recommend configuring a firewall. If
you install a firewall, you need to permit packets to pass through a port as required.

Table 1-1   XSCF-LAN Port Numbers, Functions, and Direction of Connections

Port Number/ Protocol	Function	Direction of Connection(*)
21/TCP	XSCF shell external transfer (FTP)	XSCF -> External network (21)
22/TCP	XSCF shell (SSH)	External network -> XSCF (22)

Table 1-1   XSCF-LAN Port Numbers, Functions, and Direction of Connections *(continued)*

Port Number/ Protocol	Function	Direction of Connection(*)
	XSCF shell external transfer (SSH)	XSCF -> External network (22)
23/TCP	XSCF shell (Telnet)	External network -> XSCF (23)
25/TCP	E-mail notification and remote maintenance service	XSCF -> External network (25)
53/TCP 53/UDP	DNS	XSCF (53) -> External network (53)
80/TCP	XSCF shell external transfer (HTTP)	XSCF -> External network (80)
110/TCP	E-mail notification by POP authentication, Remote maintenance service by POP authentication	XSCF -> External network (110)
123/UDP	Time synchronization with the NTP server	XSCF (123) -> External network (123)
	Time synchronization from the NTP client	External network (123) -> XSCF (123)
161/UDP	SNMP function	External network -> XSCF (161)
162/UDP	SNMP trap function	XSCF -> External network (162)
389/TCP	Authentication by LDAP and Active Directory	XSCF -> External network (389)
443/TCP	XSCF Web (HTTPS)	External network -> XSCF (443)
	XSCF shell external transfer (HTTPS)	XSCF -> External network (443)
465/TCP	Remote maintenance service (SMTP over SSL)	XSCF -> External network (465)
587/TCP	E-mail notification by SMTP authentication, Remote maintenance service by SMTP authentication	XSCF -> External network (587)
623/UDP	Remote power management function using IPMI	XSCF (623) < -> External network (623)
636/TCP	Authentication by LDAP over SSL, Active Directory	XSCF -> External network (636)
3260/TCP	Remote storage	XSCF -> External network (3260)
6481/TCP 6481/UDP	Auto Service Request (ASR) function (service tag) (*2)	External network (6481) -> XSCF (6481)

*1 Each symbol and number in parentheses has the following meaning:
     Symbol ->: Denotes the direction from left to right. <>: Denotes the direction from either left to right or right to left.
     Number in parentheses: Connection port number For a connection to an external network, the port number of the network can be changed on the XSCF. For details, see the section of the respective function in this document. For a connection to remote storage, the port number of the storage is fixed (3260).
*2 The ASR function is a remote maintenance service that uses the Oracle Auto Service Request software provided by Oracle Corporation. For details of the ASR function, see the *Oracle Auto Service Request Installation and Operations Guide* for the version of the software that you are using.

1.4 Basics of Hypervisor

This section provides an overview of the Hypervisor firmware built into the SPARC M12/M10 systems.

Hypervisor is firmware used to implement virtualization. It is built into the CPU memory unit.

Different firmware and software such as the XSCF firmware and Oracle Solaris, which is installed on logical domains, are running on each SPARC M12/M10 system. That firmware and software monitor and manage the whole system. The Hypervisor firmware is positioned between the XSCF firmware and Oracle Solaris to serve as an interface for transmitting setting information from the XSCF to logical domains and notifying the XSCF of the status of logical domains.

The Hypervisor firmware has the following main functions.

- Transmission of information between the physical partition managed by the XSCF and the logical domains managed by Oracle VM Server for SPARC
  Oracle VM Server for SPARC configures logical domains according to the PPAR configuration information (PCL) transmitted from the XSCF to the control domain. Also, logical domain configuration information and reconfigured hardware resource information are transmitted via Hypervisor to the XSCF firmware.

  For details on the PPAR configuration information, see "11.2.2　Checking the Physical Partition Configuration."

- Transmission of information related to a logical domain hang-up or failure
  If a logical domain hangs up or fails, Hypervisor notifies the XSCF of the status of the logical domain.

- Transmission of information related to the XSCF and logical domain dates and times
  Hypervisor notifies the XSCF of the set times of logical domains. The XSCF saves the time of each logical domain as its difference from the set time of the whole system.

1.5 Basics of Oracle VM Server for SPARC

This section provides an overview of the Oracle VM Server for SPARC software.

Oracle VM Server for SPARC is the software used to configure the logical domain environment. It is installed and used in the Oracle Solaris environment.

A logical domain is configured with the hardware resources, such as CPUs, memory, and I/O devices, flexibly distributed to it from the physical partition built by the XSCF firmware. The resources are assigned as a virtual hardware environment. The configured logical domain can run business applications, each of which is in an independent Oracle Solaris environment. Building more than one virtual hardware environment in one or more SPARC M12 or SPARC M10 units implements better server utilization and can lower costs when compared with server integration.

The typical logical domains are the control domain, which creates and controls other logical domains, and the guest domains, used for applications for business. In each SPARC M12/M10 system, one control domain is created per physical partition to manage other logical domains configured in the physical partition. Oracle VM Server for SPARC runs on the control domain and is used to configure and manage guest domains.
The control domain also serves to notify the XSCF firmware of logical domain information through the built-in Hypervisor firmware. Setting information from the XSCF is also transmitted to the control domain via the Hypervisor firmware.

The CPU, memory, I/O device, and other hardware resources of even the configured logical domains already applied to tasks can be reconfigured, depending on the logical domain operation status. Oracle VM Server for SPARC implements hardware resource reconfiguration too. Adding hardware resources for a task that temporarily increases the load can maintain high availability of the hardware resources and prevent tasks from overflowing.

For details about configuring and reconfiguring logical domains by using Oracle VM Server for SPARC in the SPARC M12/M10 systems, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*. For details of Oracle VM Server for SPARC, see the *Oracle VM Server for SPARC Administration Guide* of the version used.

1.6   Basics of OpenBoot PROM

This section provides an overview of OpenBoot PROM.

OpenBoot PROM provides the basic functions required for starting Oracle Solaris.

Under the OpenBoot PROM environment, the console screen displays an ok prompt. You can configure various functions related to starting Oracle Solaris by defining OpenBoot PROM environment variables. You can define OpenBoot PROM environment variables with either of the following commands.

- Execute the setenv command in the OpenBoot PROM environment (at the ok prompt).
- Execute the eeprom command in the Oracle Solaris environment.

Also, a number of the OpenBoot PROM environment variables can be overwritten using the setpparparam command of the XSCF firmware.

For details on the OpenBoot PROM environment variables and commands, see the *OpenBoot 4.x Command Reference Manual* of Oracle Corporation.
For details on the OpenBoot PROM environment variables and commands not supported by the SPARC M12/M10, see the "Appendix H OpenBoot PROM Environment Variables and Commands."

Chapter 2

Logging In/Out of the XSCF

This chapter describes the forms of connection for the system management terminal, and the method of logging in to the XSCF.

- Connecting the System Management Terminal
- Logging In to the XSCF Shell
- Logging Out from the XSCF Shell
- Logging In to XSCF Web
- Logging Out From XSCF Web
- Number of Connectable Users

2.1 Connecting the System Management Terminal

This section describes the forms of system management terminal connection with the system control network. For practical connection methods, see "2.2   Logging In to the XSCF Shell."

The forms of connection of the system control network are classified into the following two types according to the connected port.

- Serial connection
  A serial cable is connected to the serial port.

- LAN connection
  A LAN cable is connected to an XSCF-LAN port.

Usually, the system management terminal with a connection to the serial port is used to make the initial settings of the XSCF firmware. Upon completion of the XSCF network settings, either a serial connection or LAN connection can be selected.

The next sections describe the features of each type of connection.

2.1.1 Connection With the Serial Port

A serial connection is the form of connection with a serial cable to the serial port on the server. If the SPARC M12-2S or SPARC M10-4S is in a building block configuration, connect a serial cable to the chassis that has the master XSCF. The environment is secure because the system management terminal has a 1-to-1 connection with the master XSCF. When the system management terminal is connected by means of a serial connection, the login screen for the master XSCF appears.

Figure 2-1   Serial Port (SPARC M12-1)
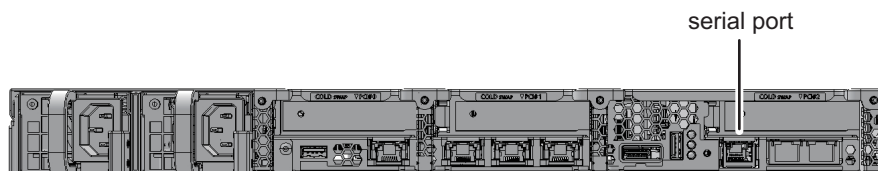
Figure 2-2   Serial Port (SPARC M12-2)
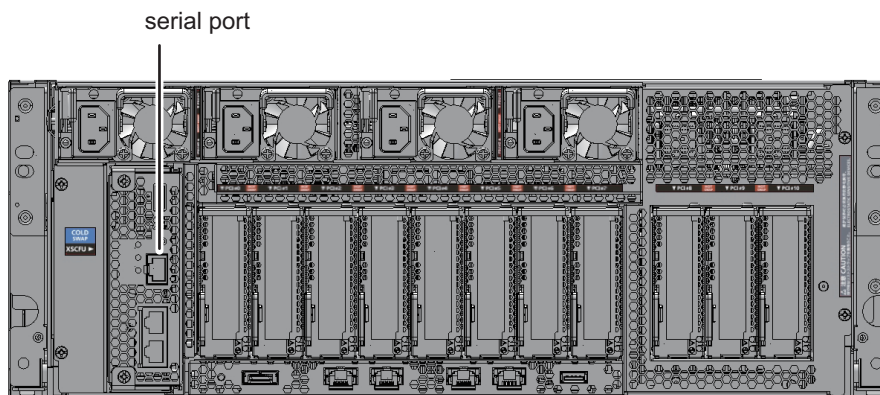
Figure 2-3   Serial Port (SPARC M12-2S)
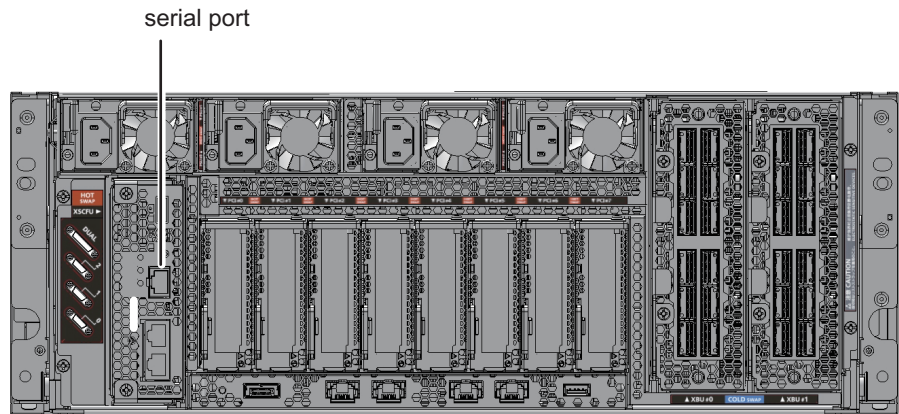
serial port

Figure 2-4   Serial Port (SPARC M10-1)
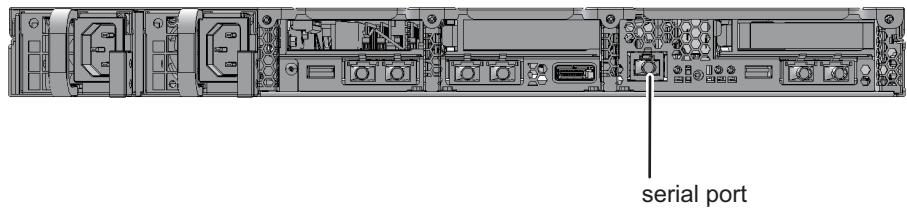
serial port

Figure 2-5   Serial Port (SPARC M10-4S)
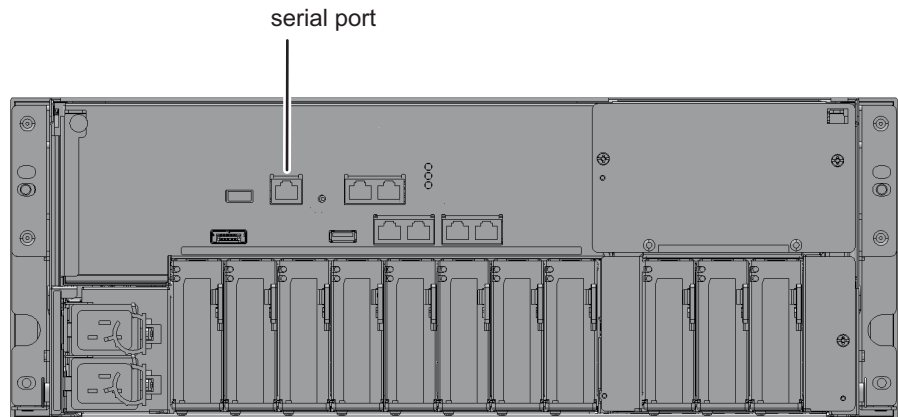
serial port

Figure 2-6   Serial Port (SPARC M10-4S)
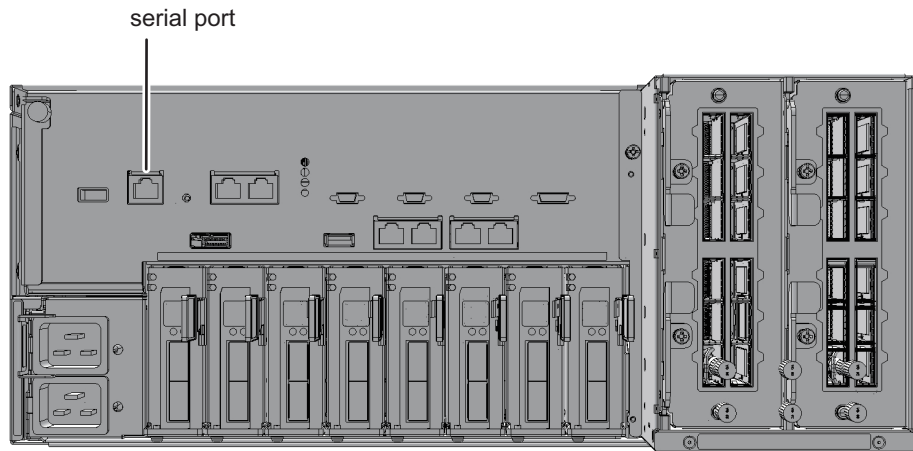
serial port

After logging in to the XSCF, you can use the XSCF shell. Use XSCF commands to monitor and manage the system. If you need to monitor or manage a logical domain, you can switch from the XSCF shell to the control domain console. For the switching method, see "8.3   Switching to the Control Domain Console From the XSCF Shell."

To connect the serial port, the following preparations must already be completed.

- Preparation of a serial cable
  Have the supplied D-Sub 9-pin RS-232C cable at hand. If the terminal being used has no serial port, an RJ-45/RS-232C conversion cable, a conversion connector, or a USB/serial conversion cable is required.

Figure 2-7   RC-232C D-Sub 9-pin Connector
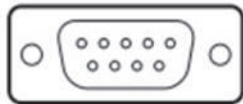
- Preparation of terminal software for connection
  When you use XSCF shell, set TERM=vt100 for the terminal software.

- Confirmation of the recognized serial port
  Connect the serial cable to the terminal, and confirm that the serial port is recognized. Specify the recognized serial port as the port for the serial connection with the XSCF.

  The serial port in the following example is the port recognized as COM6.

Figure 2-8   Serial Port Confirmation (With Device Manager)
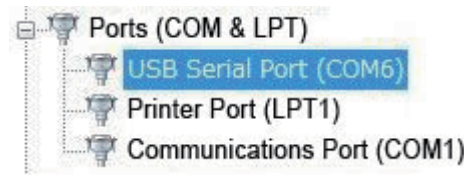
2.1.2   Available Functions for Terminals in Serial Connection

With a terminal connected to the serial port, you can use the XSCF shell and the console for the control domain (control domain console). XSCF Web is not available.

Table 2-1 lists the terminals and consoles for the serial connection and the available functions.

Table 2-1   Terminals and Consoles for the Serial Connection and the Available Functions

Terminal Type	Work	Cable
XSCF shell terminal	- You can use the XSCF shell terminal immediately after connecting it to the serial port. - You can switch the window to the control domain console by using the console command. - After you log in, if the XSCF shell is left unused for a specific duration, you are forcibly logged out. For details of the XSCF session timeout setting, see the setautologout(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.	An RS-232C serial cross cable is required. If you have only a LAN cable, a 9-pin conversion cable on the PC side is required.
Control domain console (RW console)	- This OS console can be used for input/output. Using the console command from the XSCF shell terminal, you can open the RW console by specifying the physical partition and the write-enabled console. - In one physical partition, only one user (one connection) can use the RW console at a time. - For details on the time setting for the session timeout when the control domain console is left unused, see the ttymon explanation in the reference manual of Oracle Solaris.	
Control domain console (RO console)	- This OS console is a reference-only console. Using the console command from the XSCF shell terminal, you can open the RO console by specifying the physical partition and the reference-only console.	

The maximum number of allowed concurrent connections to the RW console and RO console is as follows:
  - SPARC M12-1/M10-1: 20 consoles

- SPARC M12-2/M10-4: 40 consoles
- SPARC M12-2S/M10-4S (no crossbar box): 40 consoles
- SPARC M12-2S/M10-4S (with crossbar boxes): 70 consoles

2.1.3   Connection With an XSCF-LAN Port

An XSCF-LAN connection is the form of connection with a LAN cable to an XSCF-LAN port. In a building block configuration, connect the LAN cable to the SPARC M12-2S, SPARC M10-4S, or crossbar box that has the master XSCF or standby XSCF.

After the LAN cable is connected, configure the XSCF network settings and connect the system management terminal via the SSH service or Telnet service to display the login screen for the master XSCF.

Figure 2-9   XSCF-LAN Ports (SPARC M12-1)
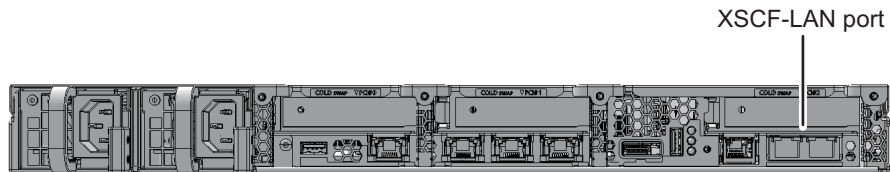
XSCF-LAN port

Figure 2-10   XSCF-LAN Ports (SPARC M12-2)
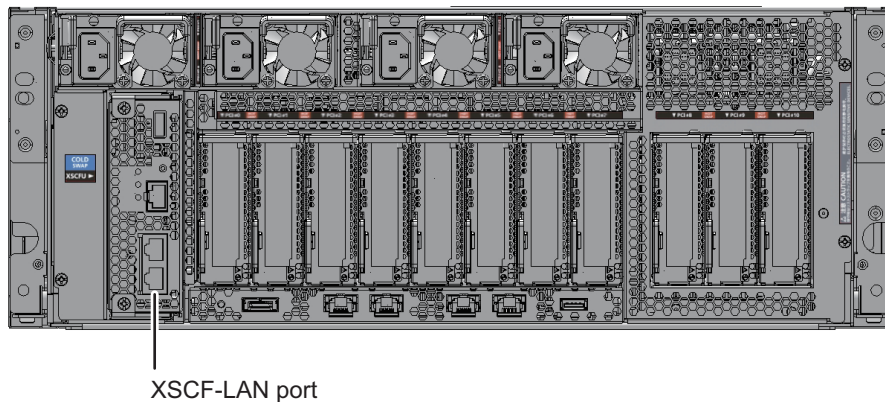
XSCF-LAN port

Figure 2-11   XSCF-LAN Ports (SPARC M12-2S)
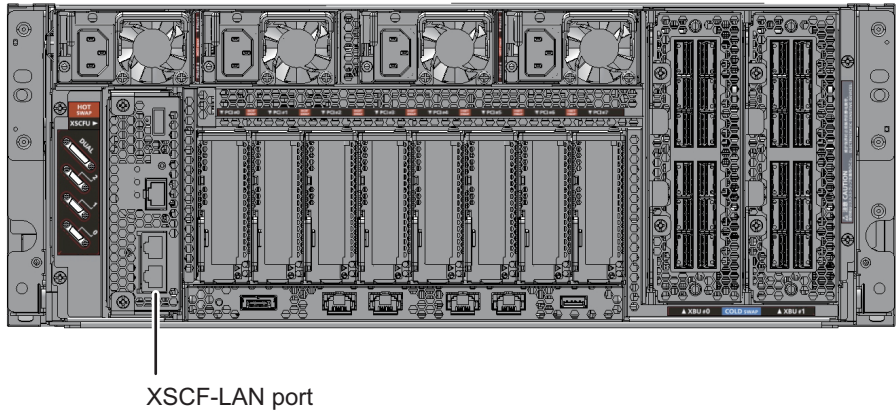
XSCF-LAN port

Figure 2-12   XSCF-LAN Ports (SPARC M10-1)
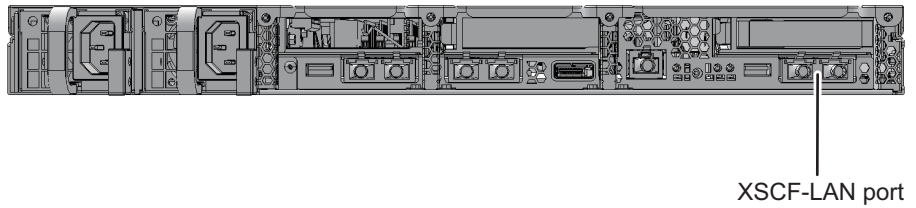
XSCF-LAN port

Figure 2-13   XSCF-LAN Ports (SPARC M10-4)
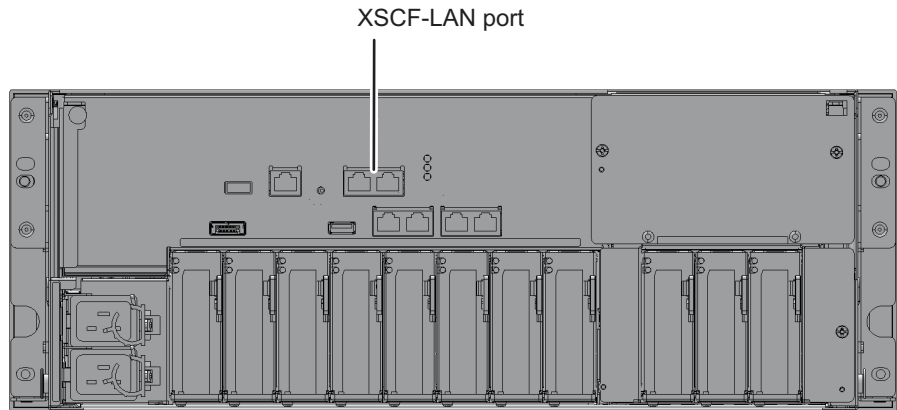
XSCF-LAN port

Figure 2-14   XSCF-LAN Ports (SPARC M10-4S)
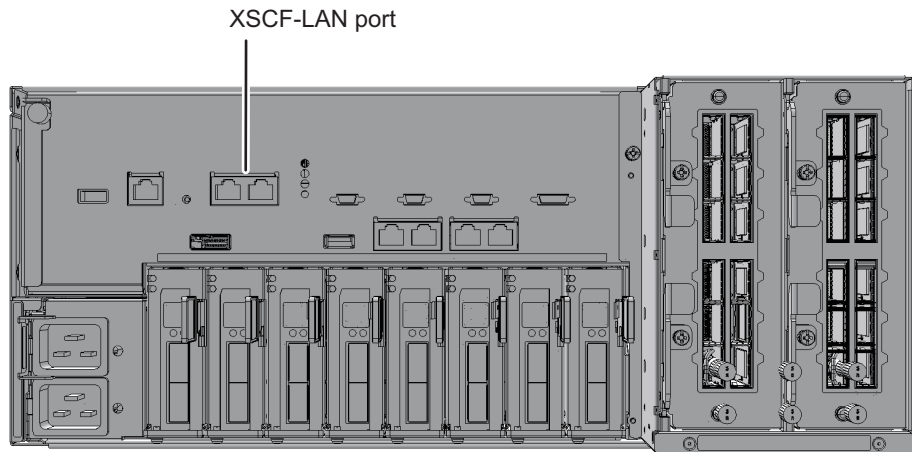
XSCF-LAN port

You can use the XSCF shell on the system management terminal with the connection to the XSCF-LAN port. Also, by configuring a Web browser, you can use XSCF Web. You can configure the system settings by using either XSCF commands or XSCF Web.

With the XSCF network configured and the system management terminal connected to the XSCF-LAN port, you can use the following functions that require a network environment:

- E-mail notification
- SNMP
- Remote maintenance service
- External NTP server connection and synchronization
- Remote XSCF monitoring and management

Two XSCF-LAN ports have been prepared in each system. You can use one of the ports only, use both ports, or split the use of the ports, such as using one port for an intranet and the other for the Internet, depending on the system operation.

After logging in to the XSCF, you can use the XSCF shell. Use XSCF commands to monitor and manage the server. If you need to monitor or manage a logical domain, you can switch from the XSCF shell to the control domain console. For the switching method, see "8.3   Switching to the Control Domain Console From the XSCF Shell."

To make a LAN connection, the following preparations must already be completed.

- Preparation of a LAN cable
  A LAN cable of Category 5 or higher is required.

- Configuration of the XSCF network
  The XSCF network and the SSH, Telnet, and other services must be configured.
  For details, see "3.9   Configuring the XSCF Network."

- Preparation of a Web browser (to use XSCF Web)
  Prepare a Web browser. For the supported Web browsers, see the latest *Product*

Notes for your server.

- Preparation of terminal software
  When you use XSCF shell, set TERM=vt100 for the terminal software.

2.1.4 Available Functions for Terminals in XSCF-LAN Connection

You can use the XSCF shell and control domain console via the SSH or Telnet service from a terminal connected to the XSCF-LAN.

Access through the XSCF-LAN makes available the e-mail notification function, the SNMP function, the remote maintenance service function, time synchronization by an external NTP server, and user authentication with the LDAP server, Active Directory server, or LDAP over SSL server. Depending on the Web browser settings, you can also use XSCF Web.

Table 2-2 lists the terminals and consoles for the XSCF-LAN connection and the available functions.

Table 2-2   Terminals and Consoles for the XSCF-LAN Connection and the Available Functions

Terminal Type	Work	Port number/ cable
XSCF shell terminal	- Once connected to the SSH service or Telnet service, the XSCF shell can be used. - You can switch the window to the control domain console in the same way as with the serial port. - After you log in, if the XSCF shell is left unused for a specific duration, you are forcibly logged out in the same way as with the serial port.	SSH:22 Telnet:23 A LAN cable is required.
Control domain console (RW console)	- This OS console can be used for input/output. Using the console command from the XSCF shell terminal, you can open the RW console by specifying the physical partition and the write-enabled console. - In one physical partition, only one user (one connection) can use the RW console at a time. - For details on the time setting for the session timeout when the control domain console is left unused, see the ttymon explanation in the reference manual of Oracle Solaris.	
Control domain console (RO console)	- This OS console is a reference-only console. Using the console command from the XSCF shell terminal, you can open the RO console by specifying the physical partition and the reference-only console.	
XSCF Web console	You can use the XSCF Web console by specifying the URL in a Web browser.	HTTPS:443 A LAN cable is required.

The maximum number of allowed concurrent connections to the RW console and RO console is as follows:

- SPARC M12-1/M10-1: 20 consoles
- SPARC M12-2/M10-4: 40 consoles
- SPARC M12-2S/M10-4S (no crossbar box): 40 consoles
- SPARC M12-2S/M10-4S (with crossbar boxes): 70 consoles

2.2   Logging In to the XSCF Shell

This section describes how to log in to the XSCF with the XSCF shell.

Using the default user account at the initial installation time, create a user account for login authentication. Log in with the new user account. For details on the login authentication method using the default account, see "Performing an Initial System Diagnosis" in the *Installation Guide* for your server. For details on how to create a new account, see "3.5   Creating/Managing XSCF Users."
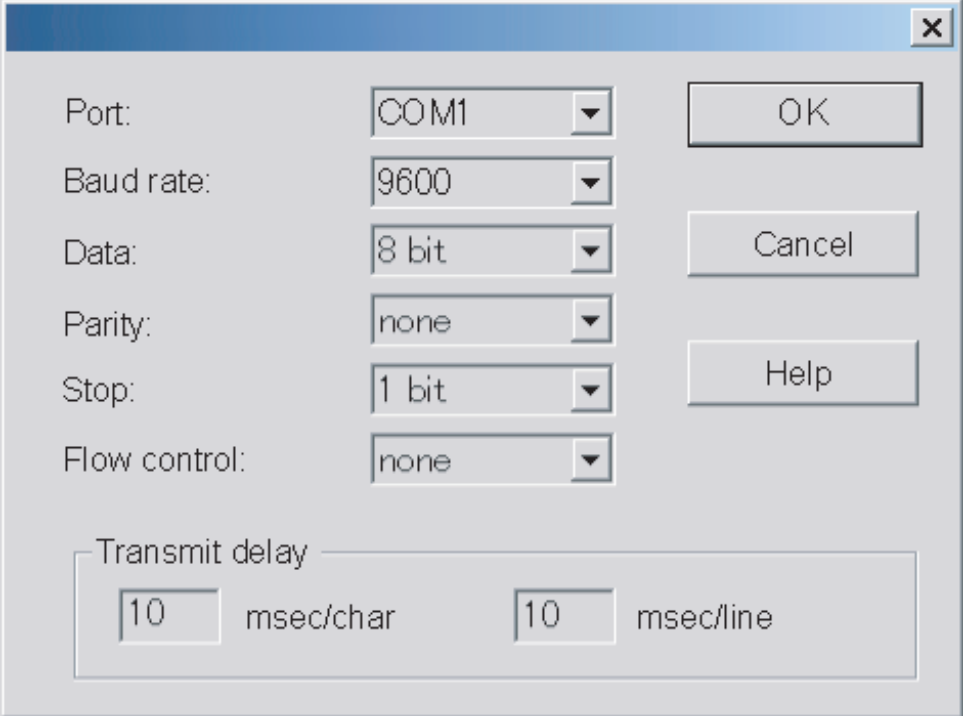
2.2.1   How to Log In to the XSCF Shell With a Serial Connection

This section describes how to connect a terminal to the serial port and log in to the XSCF shell.

1. **Confirm that the connected serial cable is inserted in the serial port of the master XSCF and correctly connected to the PC or workstation used.**

2. **Confirm that the following values are the terminal software settings:**
    Baud rate: 9600 bps

    Data length: 8 bits

    Parity: None

    Stop bit: 1 bit

    Flow control: None

    Transmission delay: Other than 0

    Figure 2-15 shows an example of configuring terminal software. If a connection cannot be established, increase the delay.

Figure 2-15   Example of Terminal Software Settings

3. **Establish the serial connection, and press the [Enter] key.**
    The terminal becomes the XSCF shell terminal, and the login prompt is output.

4. **Enter an XSCF user account and password to log in to the XSCF.**

```
login: jsmith
Password: xxxxxxxx
```

5. **Confirm that the XSCF shell prompt (XSCF>) appears.**
    You can now use the XSCF shell.

Note - If the user who logged in to the XSCF shell in the serial connection last time
terminated that connection while the console command was being executed, the XSCF shell
prompt may not appear.
If the XSCF shell prompt does not appear, enter "#.". The "XSCF>" prompt is displayed while
the console command was being executed.

```
XSCF>
```

2.2.2 How to Log In to the XSCF Shell Through an SSH Connection via the XSCF-LAN

The procedure described here assumes that the SSH service described in "3.7 Configuring the SSH/Telnet Service for Login to the XSCF" is enabled.

This section describes how to log in to the XSCF shell via SSH through an XSCF-LAN port.

1. **Confirm that the connected LAN cable is inserted in an XSCF-LAN port of the master XSCF and correctly connected to the PC or workstation used.**

2. **Before logging in via SSH, check the fingerprints that have been stored in advance.**
   If there is no stored fingerprint, establish a connection through the serial port, execute the showssh command, make a note of the fingerprint of the host public key, and then keep it at hand for reference.

3. **Start the SSH client, then specify the IP address (physical IP address) that is assigned to the XSCF-LAN or the host name, and if necessary, specify the port number and connect to the SSH service.**
   In systems with multiple XSCFs, specify the takeover IP address (virtual IP address) as necessary.

4. **Enter an XSCF user account and passphrase to log in to the XSCF shell.**

5. **A question may appear about the validity of the fingerprint of the host public key. Check the fingerprint you kept on hand for reference, and confirm that the correct XSCF is connected, and then enter "yes".**

6. **Confirm that the XSCF shell prompt (XSCF>) appears.**
   You can now use the XSCF shell.

   The following example performs a login.

```
[foo@phar foo]% ssh june@192.168.0.2
The authenticity of host '192.168.0.2 (192.168.0.2)' can't be
established.
RSA key fingerprint is
03:4b:b4:b2:3d:4d:0c:24:03:ca:f1:63:f2:a7:f3:35.
Are you sure you want to continue connecting? [yes|no] : yes
Warning: Permanently added '192.168.0.2' (RSA) to the list of
known
hosts.
foo@phar's password:xxxxxx
XSCF>
```

To establish the SSH connection with a user key, register the user public key with the XSCF in advance. For details on how to register a user public key, see "3.7 Configuring the SSH/Telnet Service for Login to the XSCF."

The following example performs login with a user public key.

```
[client]# ssh nana@192.168.1.12
Enter passphrase for key '/home/nana/.ssh/id_rsa': xxxxxxxx
Warning: No xauth data; using fake authentication data for X11
forwarding.
Last login: Mon Sep 1 10:19:37 2012 from client
XSCF>
```

Note - For details about starting SSH, see the respective SSH manuals.

2.2.3 How to Log In to the XSCF Shell Through a Telnet Connection via the XSCF-LAN

The procedure described here assumes that the Telnet service described in "3.7 Configuring the SSH/Telnet Service for Login to the XSCF" is enabled.

This section describes how to log in to the XSCF shell via Telnet through an XSCF-LAN port.

1. **Confirm that the connected LAN cable is inserted in an XSCF-LAN port of the master XSCF and correctly connected to the PC or workstation used.**

2. **Start terminal software, specify the IP address (physical IP address) assigned to the XSCF-LAN, or the host name and port number 23 to establish a Telnet service connection, and open the XSCF shell terminal.**
   In systems with multiple XSCFs, specify the takeover IP address (virtual IP address) as necessary.

   Figure 2-16 shows an example of configuring terminal software.

   Figure 2-16   Example of Terminal Software Settings
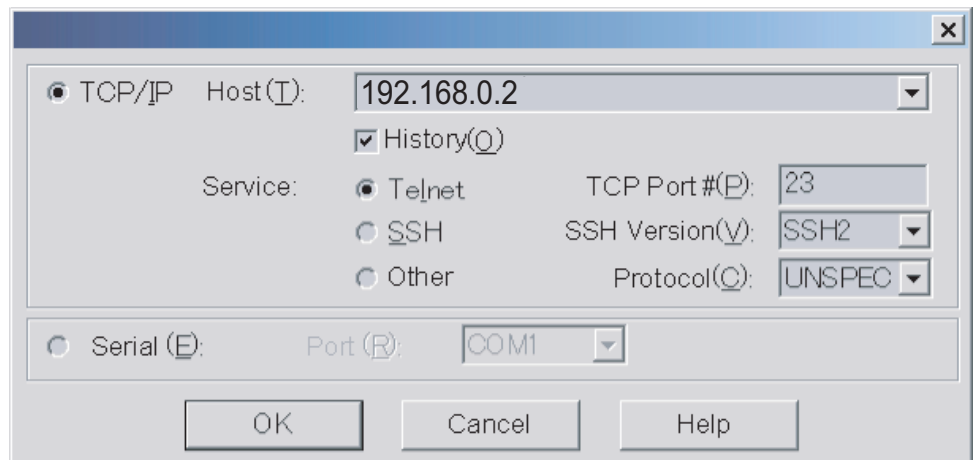
3. **Enter an XSCF user account and password to log in to the XSCF shell.**

4. **Confirm that the XSCF shell prompt (XSCF>) appears.**

You can now use the XSCF shell.

The following example shows a successful login.

```
login:jsmith
Password:xxxxxxxx
XSCF>
```

2.3 Logging Out from the XSCF Shell

This section describes how to log out from XSCF Web.

1. **Execute the exit command to log out.**

```
XSCF> exit
```

You are logged out of the XSCF, and the XSCF session is disconnected.

After you log in, if the XSCF shell is left unused for a specific duration, you are forcibly logged out. The timeout value of an XSCF session is set using the setautologout command. For details, see the setautologout(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

2.4 Logging In to XSCF Web

This section describes how to log in to the XSCF with XSCF Web.

Depending on the Web browser settings on the PC connected to the XSCF-LAN, you can use XSCF Web. XSCF Web cannot be connected from the serial port.

Access through the XSCF-LAN also makes available the e-mail notification function, the SNMP function, the remote maintenance service function, time synchronization by an external NTP server, and user authentication with the LDAP server, Active Directory server, or LDAP over SSL server.

XSCF Web is connected to a server connected with the user network via the HTTPS and SSL/TLS protocols. It displays the server status, exercises control to operate devices, and supports Web-based browsing of configuration information.

When a registered user connects to XSCF Web in a Web browser from a PC and logs in to the XSCF, the browser displays the available tree index and pages. For details of XSCF Web page information, see "Appendix C   List of the XSCF Web Pages."

2.4.1 Items That Must be Set in Advance

In the initial settings, XSCF Web is disabled. Before using XSCF Web, the following settings need to be made in advance.

- Registering an XSCF user account

- Enabling the HTTPS service to use XSCF Web

- Registering a Web server certificate with an HTTPS service setting

- Configuring e-mail notification (the recommended setting for notification in case of failure)

For the procedure to enable the HTTPS service, see "3.8   Configuring the HTTPS Service for Login to the XSCF."

2.4.2 Supported Browsers

XSCF Web supports the Web browsers listed in Table 2-3.

Table 2-3   Supported Web Browsers

Web Browser Name	Version
Microsoft Internet Explorer	8.0, 9.0, 10.0, and 11.0
Mozilla Firefox 32-bit version	10.0 to ESR 60

For details on the Web browsers used, see the latest *Product Notes* for your server.

2.4.3 Functions That Need to be Enabled in the Web Browser

The following functions will be used in the Web browser, so they need to be set so they are enabled.

- Transport Layer Security (TLS) Ver. 1.2

- JavaScript

- Cookies (for session management)

2.4.4 How to Log In With XSCF Web

This section describes how to log in to the XSCF with XSCF Web.

1. **Confirm that the connected LAN cable is inserted in an XSCF-LAN port of the master XSCF and correctly connected to the PC or workstation used.**

2. **For the URL in the Web browser, specify the IP address or host name of the XSCF to connect to the XSCF.**

- Example of URL input in a Web browser

```
https://192.168.111.111 (Enter the XSCF IP address <numbers>)/
Alternatively,
https://XSCF-host-name  (Note: Not the host name of the domain)/
```

Note - You may be asked to confirm the certificate when communication begins. Confirm the contents and accept the certificate at this time. Upon establishing an HTTPS connection, the Web browser keeps displaying a warning until the certificate is installed.

3. **Enter an XSCF user account and password on the login page to log in to the XSCF.**
   Figure 2-17 shows an example of the login page.

Figure 2-17   Example of the XSCF Web Login Page
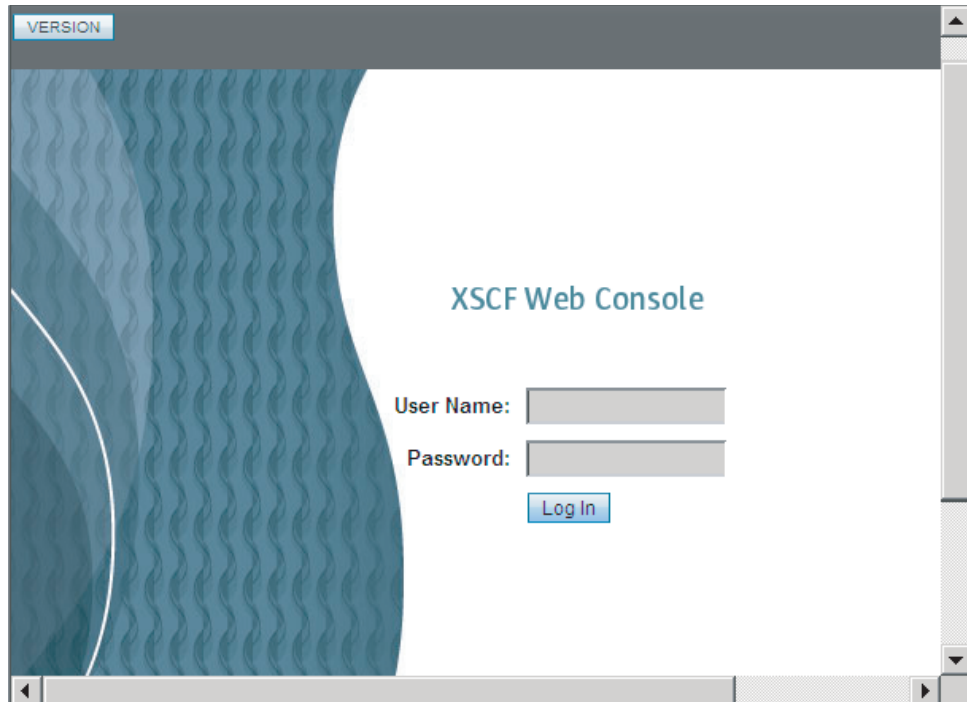
After a successful login, the default page is displayed. The default page displays a frame with a tree structure allowing selection of pages, and a single page.

Cases of Authentication Failure

If login fails, a login failure message appears. Furthermore, the login failure is logged in the event log and audit log.

2.5 Logging Out From XSCF Web

This section describes how to log out from XSCF Web.

1. **Click the [LOG OUT] button on the XSCF Web page to log out.**
   After you are logged out of the XSCF, the window returns to the XSCF Web login page.

Access Status Monitoring

XSCF Web monitors the use status of the logged-in XSCF user accounts. If there is no access from a logged-in account over a specific duration, XSCF Web recognizes that authentication has expired for the account. Therefore, if you attempt to access XSCF Web after your authentication has expired, a dialog box appears with a message about the expired authentication, followed by a transition to the top page. To continue to use XSCF Web, log in again.

You can change the monitoring time for authentication expiration on XSCF Web pages. The default monitoring time for authentication expiration is 10 minutes. The range for the monitoring time is 1 minute to 255 minutes. To set the monitoring time, select [Menu] - [Settings] - [Autologout].

2.6 Number of Connectable Users

This section describes the number of users that can be connected to the XSCF. Executing the who command lists the user accounts logged in to the XSCF.

- SPARC M12-1/M10-1
  The maximum is 20 users. While 20 users are concurrently connected to the XSCF, access is denied to any user who tries to establish a subsequent (21st) connection.

- SPARC M12-2/M12-2S/M10-4/M10-4S (no crossbar box) system
  The maximum is 40 users. While 40 users are concurrently connected to the XSCF, access is denied to any user who tries to establish a subsequent (41st) connection.

- SPARC M12-2S/M10-4S (with crossbar boxes) system
  The maximum is 70 users. While 70 users are concurrently connected to the XSCF, access is denied to any user who tries to establish a subsequent (71st) connection.

Chapter 3

Configuring the System

This chapter describes the setting procedures required for using the XSCF.

- Preliminary Work for XSCF Setup
- Understanding the Contents of the XSCF Firmware Settings
- Setting Up From the XSCF Shell
- Setting Up From XSCF Web
- Creating/Managing XSCF Users
- Setting the XSCF Time/Date
- Configuring the XSCF Network
- Configuring the SSH/Telnet Service for Login to the XSCF
- Configuring the HTTPS Service for Login to the XSCF
- Configuring Auditing to Strengthen XSCF Security

3.1 Preliminary Work for XSCF Setup

This section describes what to check and do before setting up the XSCF.

The descriptions assume that server installation, cable connection, initial diagnosis of the system, and other installation work have been completed.

3.1.1 Initial Work Before Setup

Before you start setting up the XSCF, cable connection, initial login authentication for the server, and other work must be done so that you can connect to the XSCF from any terminal capable of a serial connection or LAN connection.

The system administrator and field engineers are requested to set up the XSCF after they perform the following work.

Table 3-1 Work to be Done Before XSCF Setup

Work	See
Perform initial login authentication for the XSCF by using the default user account of the XSCF.	"Logging In to the XSCF" in the *Installation Guide* for your server.
Register at least one user account that has the platadm or useradm user privilege.	"3.5 Creating/Managing XSCF Users"

During regular operation, set the Mode switch to Locked to prevent operation mistakes. For the switching method of the Mode switch, see "13.2 Switching the Operating Mode."

3.1.2 Support Information

Before setting up the XSCF, be sure to read through the latest *Product Notes* for your server to check the software requirements and product support information.

3.1.3 User Interface for Setup and How to Access

To set up the XSCF, connect a PC to the master XSCF. To make various settings, access the XSCF from the XSCF shell, which is a command-line interface, or XSCF Web, which is a browser user interface.

Table 3-2 User Interfaces and How to Access the XSCF

User Interface	How to Access XSCF
XSCF shell (command-line interface)	Log in from a PC connected to the serial port.
	Log in from a PC connected to an XSCF-dedicated LAN (XSCF-LAN) port using the SSH or Telnet service.
XSCF Web (browser user interface)	Log in using the HTTPS service from a PC with an installed Web browser connected to the XSCF-LAN.

To use XSCF Web, you need to first configure it with the XSCF shell. Note also that settings for some functions, such as the altitude setting and dual power feed, are not supported with XSCF Web. When using such functions, use the XSCF shell to make the settings. For details of functions supported by XSCF Web, see "Appendix C List of the XSCF Web Pages."

Setting Procedure

The setting procedure varies depending on the connected user interface.
- Using the XSCF shell
  See "3.3 Setting Up From the XSCF Shell."

- Using XSCF Web

See "3.4   Setting Up From XSCF Web."

Setting Information

After the XSCF is configured, the set content is automatically saved on the XSCF and PSU backplane or crossbar backplane unit. Therefore, once the XSCF is configured, daily management is not required. However, considering the possibility of damage to information saved on the server, regularly save/restore XSCF settings information. For details on how to save/restore XSCF settings information, see "10.10   Saving/ Restoring XSCF Settings Information."

3.1.4   Proceeding Smoothly With Configuration

This section describes what you should understand before configuring the XSCF.

In many cases, the system can run with the settings and default values from the initial installation. However, the server needs to be configured to suit the customer's environment. You can reduce the time taken for configuration by checking the work already done with the *Installation Guide* for your server and the items determined in advance. For the settings, consider the following.

- List the items already configured during the initial installation, if any. For each item described below, display the setting information for the item, and confirm that nothing needs to be reconfigured.

- Ensure that the necessary user accounts are ready by checking the user accounts for maintenance, the system administrator, physical partitions, etc. You also have to decide whether to use the local account saved in the XSCF or to use the account data on a remote server as a user account in advance.

- Check the server configuration again. Confirm that no item for the network addresses, domain configurations, number of CPU Activations, etc. is undetermined or missing. Measures like examination must be taken for any settings, such as a network address, not suitable for the customer's environment in order to ensure suitability.

- You can use various services by connecting to the XSCF network. Determine in advance how to deal with unauthorized access and limit access to the host as well as the means of using the remote maintenance service, such as for notification, and what approach to take for standard time.

- The server operating environment is a necessary consideration to implement power-saving measures. According to the area and temperature of the server room and other attributes of the installation environment, determine the intervals at which the server is to be started. Also determine the maximum value for power consumption and other such values.

3.2 Understanding the Contents of the XSCF Firmware Settings

This section describes detailed procedures for configuring the XSCF firmware.

3.2.1 Setting Items for Using the XSCF

The various XSCF settings items have the following purposes:

- Settings for using the XSCF firmware
- Settings for configuring physical partitions and logical domains
- Settings for managing/controlling the system hardware
- Other settings, such as for event notification

This section describes the settings for using the XSCF firmware. For the settings to configure physical partitions and logical domains, see "Chapter 7 Controlling Physical Partitions" and "Chapter 8 Controlling Logical Domains" and also the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*. For the settings for the administration/control of hardware, such as those for the power supply, see "Chapter 4 Configuring the System to Suit the Usage Type" and "Chapter 15 Expanding the System Configuration." Additionally, concerning other settings, see the relevant chapter.

Table 3-3 shows the setting items for using the XSCF firmware. For details of individual items, see the sections indicated in the table.

Table 3-3 Setting Items for Using the XSCF

Setting Item	Required or Optional Setting	See
User management	Required	3.5
Time	Required	3.6
Network	Required	3.9
SSH/Telnet service	Optional	3.7
HTTPS service	Optional	3.8
Audit	Optional	3.10
LDAP service	Optional	3.5.12
Active Directory service	Optional	3.5.13
LDAP over SSL service	Optional	3.5.14

Note - Service related to the following setting items was enabled at factory shipment.
- User management

- Time
- Network
- Audit

3.2.2 Checking the Master XSCF

For the SPARC M12-1/M12-2/M10-1/M10-4, and the SPARC M12-2S/M10-4S in a single-unit configuration, the XSCF of that chassis is the master XSCF. For the SPARC M12-2S or the SPARC M10-4S in a building block configuration, only the master XSCF or standby XSCF is accessible to users. Configure the XSCF from the master XSCF. In principle, the master XSCF in a building block configuration is the XSCF mounted in the SPARC M12/M10 whose ID (BB-ID) is 0 or 1, or in the chassis of crossbar box 80 or 81. The standby XSCF is also the XSCF mounted in chassis with the same numbers.

If the master XSCF and the standby XSCF are switched while the system is in operation, the master XSCF changes from the unit in the chassis with a BB-ID of 0 to the unit in the ID 1 chassis. Likewise, the standby XSCF changes from the unit in the chassis with a BB-ID of 1 to the unit in the ID 0 chassis.

The master XSCF and standby XSCF in a system with multiple XSCFs has the following component mounting numbers:
- SPARC M12-2S or SPARC M10-4S system (no crossbar box)
  - Master XSCF: BB#00; Standby XSCF: BB#01

  Alternatively,

  - Master XSCF: BB#01; Standby XSCF: BB#00

- SPARC M12-2S or SPARC M10-4S system (with crossbar boxes)
  - Master XSCF: XBBOX#80; Standby XSCF: XBBOX#81

  Alternatively,

  - Master XSCF: XBBOX#81; Standby XSCF: XBBOX#80

The method of checking and connecting the master XSCF in a system with multiple XSCFs is as follows.
- Checking the MASTER LED and establishing a serial connection
  With power supplied to the SPARC M12-2S or SPARC M10-4S or crossbar boxes, the completion of master XSCF initialization turns on the MASTER LED on the rear panel of the XSCF unit. By connecting a PC to the serial port on the same panel, you can log in to the master XSCF.

- Specifying the takeover IP address or master XSCF IP address to establish a connection
  The master XSCF and standby XSCF have the XSCF LAN#0 and LAN#1 ports, respectively. LAN#0 and LAN#1 are duplicated as they are connected to each other through the same subnet.

  To connect to the master XSCF, specify the LAN#0 takeover IP address or LAN#1 takeover IP address. Even when the master and standby XSCFs have been

switched, you can connect to the master XSCF by specifying the same takeover IP address.

An alternative method of connecting to the master XSCF is to specify the master XSCF LAN#0 or LAN#1 IP address. This method of connecting can be used when the system has only one XSCF, or when, due to maintenance operations, the standby XSCF cannot be accessed.

After connecting and successfully logging in to the master XSCF at the specified IP address, execute the showhardconf command. You can check which chassis of the SPARC M12-2S, SPARC M10-4S, or crossbar box has the master XSCF.

The following example shows that BB-ID 0 is the master XSCF.

```
XSCF> showhardconf
SPARC M10-4S;
        + Serial: 2081208013; Operator_Panel_Switch:Locked;
:
        BB#00 Status:Normal; Role:Master Ver: 0101h; Serial:
        7867000297;
                + FRU-Part-Number: CA20393-B50X A2 ;
:
        BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:
        7867000297;
                + FRU-Part-Number: CA20393-B50X A2 ;
:
```

The following example shows that crossbar box 80 is the master XSCF.

```
XSCF> showhardconf
SPARC M10-4S;
        + Serial:PAxxxxxxxx; Operator_Panel_Switch:Locked;
:
        XBBOX#80 Status:Normal; Role:Master Ver:0101h; Serial:
        7867000297;
                + FRU-Part-Number:CA20393-B50X A2 ;
:
        XBBOX#81 Status:Normal; Role:Standby Ver:0101h; Serial:
        7867000297;
                + FRU-Part-Number:CA20393-B50X A2 ;
:
```

Note - The settings made on the master XSCF are reflected by the standby XSCF.

3.2.3 Executable Functions on the Standby XSCF

This section describes the functions and commands that can be executed on the standby XSCF.

Table 3-4   Executable Functions on the Standby XSCF

Function	Command
Exiting the XSCF	exit
Displaying a man page	man
Rebooting the XSCF	rebootxscf
Setting a user privilege	setprivileges
Displaying the chassis status	showbbstatus
Displaying the command end status	showresult
Displaying user information	showuser
Getting a firmware dump	snapshot
Switching the XSCF	switchscf
Displaying an audit	viewaudit
Displaying logged-in users	who

For details of each command, see its man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.2.4 Checking Command Options in Detail on the man Pages

By using the man(1) command on the XSCF, you can check the command man pages about the operands, options, etc. of XSCF commands, when configuring the XSCF. The displayed man page contents consist of the same detailed command information as that in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

```
XSCF> man showhardconf
System Administration                        showhardconf(8)
NAME
     showhardconf - display information about field replaceable
     unit (FRU) installed in the system

SYNOPSIS
     showhardconf [-u] [-M]
     showhardconf -h

DESCRIPTION
     showhardconf(8) command displays information about each
FRU.
:
```

3.3 Setting Up From the XSCF Shell

This section describes the flow of setup from the XSCF shell.

For details of each step, see the section indicated by the title enclosed in double quotation marks. Also, depending on the customer's environment, select whether to enable or disable setting (optional) items.

1. **Connect to the XSCF shell from any terminal capable of a serial connection.**
   Set up a secure environment with a serial connection to the server.

   For details, see "2.2.1   How to Log In to the XSCF Shell With a Serial Connection."

2. **Log in to the XSCF shell.**
   Log in to the XSCF shell with a new user account created at the initial login authentication time.

   For details of login, see "2.2   Logging In to the XSCF Shell."

   For details about creating a new user account at the initial login authentication time, see "3.5   Creating/Managing XSCF Users."

3. **Set the password policy.**
   Specify the password attributes, such as the password expiration time and number of characters, of XSCF user accounts.

   For details, see "3.5   Creating/Managing XSCF Users."

4. **Configure items for auditing (optional).**
   The audit function records XSCF logins and logouts and various other events in the audit log. The audit function is enabled by default. The auditadm user privilege is required for audit settings.

   For details, see "3.10   Configuring Auditing to Strengthen XSCF Security."

5. **Set the time.**
   Set the XSCF time, which is the system standard time. After the system time is updated, the XSCF is rebooted, and the XSCF session is disconnected. Log in again.

   For details, see "3.6   Setting the XSCF Time/Date."

Note - The work for this setting has been done during initial installation. If the value needs to be changed, set it again.

---

6. **Configure the SSH/Telnet service.**
   SSH and Telnet can be concurrently enabled. However, connections using the Telnet service do not provide a secure communication protocol. We recommend disabling the Telnet service when an SSH service is enabled.

   The SSH/Telnet service is disabled by default.

   For details, see "3.7   Configuring the SSH/Telnet Service for Login to the XSCF."

7. **Confirm the XSCF host public key.**
   To use an SSH service with an XSCF-LAN connection, execute the showssh

command, and make a note of the fingerprint. Step 11 refers to the contents of the noted fingerprint during login to the XSCF shell via an SSH service. Copy the text data of the host public key to a file in a given directory on the client.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtpWI9bay6CK0nrFRok+z54ez7B
rDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBmW9pqa/WxC21Ja4RQVN3009km
VwAAAIAON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSzvfzzFFj5XUzQBdabh5p5Rwz+
1vriawFIZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T/uFwP8yqtJf6Y9GdjBAhWuH8
F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64FL0YYBSwfbwLIz6PSA/yKQe23
dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCAOvVlMhqHuPNpX+hE19nPdBFG
zQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

For details, see "3.7   Configuring the SSH/Telnet Service for Login to the XSCF."

8. **Register a user public key.**
   To use a user key of an SSH service through an XSCF-LAN connection, create a user secret key and user public key for a registered XSCF user account on the PC, and register the user public key with the XSCF.

   For details, see "3.7   Configuring the SSH/Telnet Service for Login to the XSCF."

9. **Configure the XSCF-dedicated network.**
   Configure the XSCF network, including the XSCF-LAN IP address and SSCP. Multiple users can access the XSCF concurrently via SSH, Telnet, or HTTPS.

   Execute the applynetwork command to reflect the network settings. Then, execute the rebootxscf command to reboot the XSCF and complete configuration work. After the XSCF is rebooted, the XSCF session is disconnected. Log in again.

   For details, see "3.9   Configuring the XSCF Network."

10. **Connect to the XSCF shell from any terminal capable of an XSCF-LAN connection (optional).**
    The setting work from this step can be done through an XSCF-LAN connection too. Here, connect to the XSCF by specifying its IP address on a PC connected to

the XSCF-LAN, and log in again.

To keep using the serial connection for settings, go to step 12.

The Telnet service should not be considered as being a secure form of communication. We recommend using an SSH service. In login via an SSH service, there may be a question about the validity of the fingerprint of the host public key. Confirm that the fingerprint is the same as the one noted in step 7, and reply "yes". If the fingerprints do not match, the IP address may not be correct or unique to the connection destination, or may imply "spoofing." Check the IP address again.

```
RSA key fingerprint is xxxxxx
Connecting? [yes|no] : yes
```

To use an SSH service with user key authentication when a passphrase has been set, enter the passphrase.

```
Enter passphrase for key '/home/nana/.ssh/id_rsa' :xxxxxxxx
Warning: No xauth data; using fake authentication data for X11
forwarding.
Last login: Fri Sep 1 10:19:37 2011 from client
```

11. **Configure NTP (optional).**
    Configure NTP such that the XSCF operates as an NTP server or NTP client. You may also be configuring NTP after configuring a domain.

    For details, see "3.6   Setting the XSCF Time/Date."

The following configures the settings to manage a user account. To manage a user account, determine in advance whether to configure a local user account saved in the XSCF or to set the account data saved in a directory database on a network using the Lightweight Directory Access Protocol (LDAP), Active Directory, or LDAP over SSL. To configure a directory database on a network, set the user accounts to authenticate against the directory database.
To use the LDAP, Active Directory, or LDAP over SSL server, you need to download a certificate, create a public key, and complete user registration to the directory database in your environment in advance.
Since an Active Directory or LDAP over SSL user cannot upload a user public key to the XSCF, you must login after connecting to the XSCF via SSH, using password authentication.
This manual does not provide details on the LDAP, Active Directory, and LDAP over SSL. See the available LDAP, Active Directory, and LDAP over SSL manuals.

Note - For the XCP firmware version that supports the LDAP, Active Directory, and LDAP over SSL service, see the latest *Product Notes* for your server.

12. **Configure LDAP service settings (optional).**
    Configure the XSCF as an LDAP client. For details, see "3.5.12   Managing XSCF User Accounts Using LDAP."

13. **Configure Active Directory service settings (optional).**

Configure the XSCF as an Active Directory client. For details, see "3.5.13 Managing XSCF User Accounts Using Active Directory."

14. **Configure LDAP over SSL service settings (optional).**
Configure the XSCF as an LDAP over SSL client. For details, see "3.5.14 Managing XSCF User Accounts Using LDAP over SSL."

15. **Configure XSCF user accounts.**
Register the XSCF user accounts retained locally on the server, according to the user environment.

   - To add a user account, execute the showuser command with the -l option specified, and confirm that the user account list has no invalid user account.

   - Considering maintenance work, be sure to prepare a field engineer (FE) user account that has the fieldeng user privilege.

   For details, see "3.5   Creating/Managing XSCF Users."

16. **Configure SMTP (optional).**
Configure SMTP to use the XSCF e-mail notification function.

   For details, see "10.2   Receiving Notification by E-mail When a Failure Occurs."

17. **Configure SNMP protocol-related items for using the SNMP agent function (optional).**
For details, see "10.3   Monitoring/Managing the System Status With the SNMP Agent."

18. **Configure items for using the remote maintenance service (optional).**
This document does not describe the remote maintenance service function in detail. For information on the remote maintenance service function, see the latest *Product Notes* for your server.

The following steps configure items for management of hardware in the whole system.

19. **Set the altitude.**
For details, see "4.1   Setting/Checking the System Altitude."

Note - The work for this setting has been done during initial installation. If the value needs to be changed, set it again.

---

20. **Configure power capping (optional).**
For details, see "4.4   Reducing Power Consumption."

21. **Configure memory mirror mode (optional).**
For details, see "14.1   Configuring Memory Mirroring."

22. **Set the air-conditioning wait time (optional).**
Set the time so that power-on processing waits until the air conditioning facilities adjust the environment to room temperature.

   For details, see "4.2.2   Setting/Checking the Wait Time for Air Conditioning."

Note - The SPARC M12/M10 does not support the wait time setting for air conditioning.

The following steps configure items for management of physical partitions.

23. **Configure physical partitions (optional).**
Set domain configuration management information.

For details, see "11.2   Checking a Physical Partition" and *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide.*

24. **Set the physical partition mode (optional).**
For details, see "7.2   Setting the Physical Partition Operation Mode" and *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide.*

25. **Perform the settings for CPU Activation.**
For details, see "Chapter 5   CPU Activation."

26. **Set the warmup time (optional).**
Set a time to delay power-on processing for a specific elapsed time immediately before Oracle Solaris starts running. The set time applies after the start of server power-on processing. This setting is used to wait until the server has warmed up and peripheral devices are powered on.

If the setpowercapping command has set the upper limit value of power consumption, the power consumed by all physical partitions operating concurrently may exceed the upper limit value. To prevent this, you can use this setting to stagger operating times for each physical partition.

For details, see "4.2.1   Setting/Checking the Warmup Time."

27. **Set the power schedule (optional).**
Set power schedule information for each physical partition.

To set a power schedule, use the setpowerschedule, addpowerschedule, and deletepowerschedule commands of the XSCF firmware. For details of each command, see the man page of the command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

3.4   Setting Up From XSCF Web

This section describes the flow of setup required from XSCF Web. For details of each step, see the section indicated by the title enclosed in double quotation marks.

To use XSCF Web, the HTTPS service must already be enabled in settings with the XSCF shell.

1. **Connect to the XSCF shell from any terminal capable of a serial connection.**
For details, see "2.2   Logging In to the XSCF Shell."

2. **Perform steps 2 to 11 in "3.3   Setting Up From the XSCF Shell." If you have already performed steps 2 to 11 in Section 7.2 with the XSCF shell, go to the next step in this section.**

3. **Configure HTTPS.**
For details, see "3.8   Configuring the HTTPS Service for Login to the XSCF."

4. **Connect from a Web browser to the XSCF.**
Connect to XSCF Web from a PC with an installed Web browser connected to the

XSCF-LAN, by specifying the host name or IP address.

- Example of URL input in a Web browser

```
https://192.168.111.111 (Enter the XSCF IP address <numbers>)/
Alternatively,
https://XSCF-host-name (Note: Not the host name of the domain)/
```

5. **Log in to the XSCF from the XSCF Web console.**
   Log in with a created user account.

```
<Example showing login authentication input in a Web browser>
login:yyyy
Password:xxxxxxxx
```

The XSCF Web browser window is called the XSCF Web console.

For details, see "2.4   Logging In to XSCF Web."

6. **The setting items are the same as those with the XSCF shell. Configure them from the XSCF Web console in the same way as in step 12 and later in "3.3 Setting Up From the XSCF Shell."**
   For details of the XSCF Web menu, see "Appendix C   List of the XSCF Web Pages."

Note - For settings not included in the XSCF Web menu, such as the altitude setting and dual power feed, use the XSCF shell.

3.5   Creating/Managing XSCF Users

This section describes how to create/manage the user accounts, passwords, user privileges, and password policy used for XSCF login. To manage user accounts, you can either configure an XSCF local user account or a user account to authenticate to a directory database on a network using the LDAP, Active Directory, or LDAP over SSL.

3.5.1   XSCF User Accounts

Use Scenarios

XSCF user accounts are used to log in with the XSCF shell via SSH or Telnet or with XSCF Web.

Users Who Can Register an XSCF User Account

To register an XSCF user account, you need to log in with a user account that has the useradm user privilege.

Available XSCF User Account Names

None of the following XSCF user account names are available because they are reserved for the system:
root, bin, daemon, adm, operator, nobody, sshd, rpc, rpcuser, ldap, ntp, admin, default, proxyuser

If the XSCF user account is managed using the LDAP, Active Directory, or LDAP over SSL service, the user account name and (if specified) user identifier (UID) must not already be in use in the XSCF, LDAP, Active Directory, or LDAP over SSL. For details of the available characters, see the adduser(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Number of User Accounts

The number of user accounts that can be specified is 100, assuming an average of 10 characters per user account. The adduser command, when executed, registers a user account with an ID, called a UID, automatically assigned. The UID is an integer equal to or greater than 100. An arbitrary number can also be specified as the UID. In this case, specify a UID in a range of 100 to 60000.

Cases of Login Authentication Failure

If login authentication fails, the user account can be locked out for a specific length of time. The function for locking out such an account is called the XSCF user account lockout function. The system administrator can disable and enable the XSCF user accounts in use.

3.5.2   Passwords and Password Policy

When registering an XSCF user account, also register a password. A newly created user account does not have a set password. Therefore, until a password by the password command or a public key by Secure Shell (SSH) is set for the user, the user account cannot be used for login.

Passwords have limitations such as length and character type. Those password attributes conform to rules called the password policy. After you create a user account, the current password policy applies to the created user account. When you set the password policy again, the password policy applies to users added later. You can check the current password policy by executing the showpasswordpolicy command.

Table 3-5 shows the password policy setting items.

Table 3-5   Password Policy Items

Setting Item	Meaning
Mindays	Minimum number of days after a password change before the next time that the password can be changed. 0 indicates that the password can be changed anytime.
Maxdays	Maximum number of days that a password is valid
Warn	Number of days after a password expiration warning is issued before the password actually expires
Inactive	Number of days after the password expiration time before the account is locked out
Expiry	Number of days that the account remains valid The default is 0. 0 means that the account will never expire.
Retry	Number of permitted retries to change a password
Difok	Number of characters not included in the old password but to be included in the new password
Minlen	Minimum acceptable password length
Dcredit	A password that contains numeric characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of numeric characters included in the password. Here, you can set the maximum value for this decrease.
Ucredit	A password that contains uppercase characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of uppercase characters included in the password. Here, you can set the maximum value for this decrease.
Lcredit	A password that contains lowercase characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of lowercase characters included in the password. Here, you can set the maximum value for this decrease.
Ocredit	A password that contains non-alphanumeric characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of non-alphanumeric characters included in the password. Here, you can set the maximum value for this decrease.
Remember	Number of passwords to be stored in the password history

3.5.3 Types of User Privilege

When adding an XSCF user account, set a user privilege for the account. The purposes of granting user privileges to user accounts are to:

- Provide the system administrator with operational privileges for the whole server
- Limit operations to a given physical partition
- Manage user accounts
- Configure auditing
- Limit server operations by field engineers

Multiple user privileges can be set for one user account. Grant user privileges to accounts according to the user environment and purpose. Table 3-6 lists the user privileges.

Table 3-6 User Privileges

User Privilege	Outline	Description of Privilege
pparop@n	Reference all statuses of a specific physical partition.	- Allowed to reference all statuses of the hardware mounted on a specific physical partition (PPAR-ID:n). - Allowed to reference all statuses of a specific physical partition (PPAR-ID:n).
pparmgr@n	Allowed to operate power supply and reference only status of a specific physical partition.	- Allowed to power on/off and reboot a specific physical partition (PPAR-ID:n). - Allowed to reference all statuses of the hardware mounted on a specific physical partition (PPAR-ID:n). - Allowed to reference all statuses of a specific physical partition (PPAR-ID:n).
pparadm@n	Allowed only to manage a specific physical partition.	- Allowed to control all hardware mounted on a specific physical partition (PPAR-ID:n). - Allowed to reference all statuses of the hardware mounted on a specific physical partition (PPAR-ID:n). - Allowed to control all specific physical partitions (PPAR-ID:n). - Allowed to reference all statuses of a specific physical partition (PPAR-ID:n).
platop	Refer to the status of the whole system.	Can refer to all the statuses of the server but cannot change any of them.

Table 3-6   User Privileges *(continued)*

User Privilege	Outline	Description of Privilege
platadm	Manage the whole system.	- Can perform all hardware operations for the system. - Can manipulate all XSCF settings except those requiring the useradm and XSCF audit privileges. - Can add/delete hardware in the physical partition. - Can perform power operations for the physical partition. - Can refer to all of the statuses of the server.
useradm	Manage user accounts.	- Can create, delete, enable, and disable user accounts. - Can change user passwords and password profiles. - Can change user privileges.
auditop	Refer to the audit status.	Can refer to the XSCF audit status and audit methods.
auditadm	Control auditing.	- Can control XSCF auditing. - Can delete XSCF audit methods.
fieldeng	Allow use by field engineers.	Permits field engineers to only be able to perform maintenance work and change device configurations.
none	You do not have user privilege.	When a user account stored in the XSCF is set to none, the user privilege of the user account is not looked up in the LDAP. Therefore, even if a user privilege has been set to the user account in the LDAP, the privilege is regarded as "none."

A user privilege for a target physical partition has "@PPAR number" appended after the user privilege name. (e.g., pparadm for PPAR-ID 01 becomes pparadm@1)

One user account can have privileges to multiple physical partitions, including the intended physical partition. For details of user privilege settings, see the setprivileges (8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.5.4   Checking the Setting Items and Commands Related to XSCF User Accounts

Table 3-7 lists the setting items related to XSCF user accounts and the corresponding XSCF shell commands.

Table 3-7　　Setting Items Related to XSCF User Accounts

Setting Item	Required or Optional Setting	Related Command
Adding/Deleting a user account	Required	showuser(8), adduser(8), deleteuser(8)
Enabling/Disabling a user account	Required	enableuser(8), disableuser(8)
Setting the password policy	Optional	setpasswordpolicy(8), showpasswordpolicy(8)
Setting a password	Required	password(8)
Assigning a user privilege	Required	setprivileges(8), showuser(8)
Configuring the lockout function	Optional	setloginlockout(8), showloginlockout(8)

Table 3-8　　Setting Items Related to User Accounts for Directory Service

Setting Item	Required or Optional Setting	Related Command
LDAP client setting	Optional	showldap(8), setldap(8)
Active Directory client setting	Optional	showad(8), setad(8)
LDAP over SSL client setting	Optional	showldapssl(8), setldapssl(8)

Note - For the XCP firmware version that supports the LDAP, Active Directory, and LDAP over SSL service, see the latest *Product Notes* for your server.

3.5.5　　XSCF User Account Registration Flow

The default user account that was set at factory shipment is named "default." To employ any other user account for system operation, register it with the XSCF.

The user account "default" has the following privileges:

- "default" privileges: useradm and platadm

Upon logging in with this default account during initial installation, register at least one user account that has the useradm or platadm user privilege. For details on login authentication with the default user account, see "Logging In to the XSCF" in the *Installation Guide* for your server.

Registration Flow

To manage the XSCF user account through a directory service on a network using the LDAP, Active Directory, or LDAP over SSL service, see "3.5.12　Managing XSCF User Accounts Using LDAP," "3.5.13　Managing XSCF User Accounts Using Active Directory," or "3.5.14　Managing XSCF User Accounts Using LDAP over SSL."

The system administrator registers a user account in the following steps. For details,

see the respective sections indicated.

1. **Log in to the XSCF with a user account that has the useradm privilege (see Section 3.5.6).**
   The default user account "default" has the useradm privilege.

2. **Check the registered users (see showuser(8) in Section 3.5.6).**
   When adding a user account, execute the showuser command with the -l option specified, and confirm the user account list does not show an invalid user account.

3. **Check/Change the password policy (see showpasswordpolicy(8) or setpasswordpolicy(8) in Section 3.5.7).**

4. **Register the XSCF user account (see adduser(8) in Section 3.5.8).**
   Using the adduser command, register the user account as appropriate to the user environment.

5. **Set a password (see password(8) in Section 3.5.8).**

6. **Register a user privilege (see setprivileges(8) in Section 3.5.9).**

For details of each command, see its man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.5.6 Confirming Registered Users

To confirm the users registered with the system, use the showuser command. To display information on other user accounts, a user account having useradm privileges must be used to execute the command.

1. **Execute the showuser command to display information on an XSCF user account.**
   In the following example, all information for an XSCF user account is displayed by specifying the -l option.

```
XSCF> showuser -l
User Name:          user001
UID:                101
Status:             Enabled
Minimum:            0
Maximum:            99999
Warning:            7
Inactive:           -1
Last Change:        Jul 11, 2012
Password Expires:   Never
Password Inactive:  Never
Account Expires:    Never
Privileges:         platadm
```

In the following example, information on the user privileges is displayed by specifying the -p option.

```
XSCF> showuser -p
User Name:          jsmith
Privileges:         pparadm@1,3-6,8,9
                    platadm
```

3.5.7 Checking/Changing the Password Policy

Once the password policy is set, the password policy applies to users added later. Use the showpasswordpolicy command to check the password policy that is currently set. After checking the password policy, if you want to change it, use the setpasswordpolicy command. Execute the setpasswordpolicy command with a user account that has the useradm privilege.

The setpasswordpolicy command sets the password policy with the following options.

Table 3-9   setpasswordpolicy command options

Option	Password Policy	Content of Setting
-n	Mindays	Minimum number of days after a password change before the next time that the password can be changed. 0 indicates that the password can be changed anytime.
-M	Maxdays	Maximum number of days that a password is valid
-w	Warn	Number of days after a password expiration warning is issued before the password actually expires
-i	Inactive	Number of days after the password expiration time before the account is locked out
-e	Expiry	Number of days that the account remains valid
-y	Retry	Number of permitted retries to change a password
-k	Difok	Number of characters not included in the old password but to be included in the new password
-m	Minlen	Minimum acceptable password length
-d	Dcredit	A password that contains numeric characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of numeric characters included in the password. Here, you can set the maximum value for this decrease.

Table 3-9   setpasswordpolicy command options *(continued)*

Option	Password Policy	Content of Setting
-u	Ucredit	A password that contains uppercase characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of uppercase characters included in the password. Here, you can set the maximum value for this decrease.
-l	Lcredit	A password that contains lowercase characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of lowercase characters included in the password. Here, you can set the maximum value for this decrease.
-o	Ocredit	A password that contains non-alphanumeric characters can be shorter than the minimum acceptable password length (Minlen). The decreased number of characters is up to the number of non-alphanumeric characters included in the password. Here, you can set the maximum value for this decrease.
-r	Remember	Number of passwords to be stored in the password history

Operation Procedure

1. **Execute the showpasswordpolicy command to check the password policy.**

```
XSCF> showpasswordpolicy
Mindays:           0
Maxdays:           90
Warn:              7
Inactive:          -1
Expiry:            0
Retry:             5
Difok:             1
Minlen:            8
Dcredit:           0
Ucredit:           0
Lcredit:           0
Ocredit:           0
Remember:          4
```

2. **As necessary, execute the setpasswordpolicy command to make changes in the settings for the password policy.**
   The example below specifies the following:

   - A retry count of up to 3

- A password length of 6 characters or more when the password contains 2 numeric characters. A password length of 8 characters or more when the password does not contain numeric characters
- An expiration time of 60 days
- 15 days ahead as the start date for warnings before the password expires
- 3 as the number of passwords to remember

```
XSCF> setpasswordpolicy -y 3 -m 8 -d 2 -u 0 -l 0 -o 0 -M 60 -w 15 -r 3
```

3. **Execute the showpasswordpolicy command, and confirm the settings.**

```
XSCF> showpasswordpolicy
Mindays:            0
Maxdays:            60
Warn:               15
Inactive:           -1
Expiry:             0
Retry:              3
Difok:              1
Minlen:             8
Dcredit:            2
Ucredit:            0
Lcredit:            0
Ocredit:            0
Remember:           3
```

Note - The system password policy does not apply when a password is changed by the password command with another user specified in the user operand. When changing the password of another user, be sure to specify a password conforming to the system password policy.

3.5.8 Adding an XSCF User Account and Setting a Password

To add a user account, use the adduser command.
Execute the command with a user account that has the useradm privilege. For information on the names that can be used for user accounts, see "3.5.1 XSCF User Accounts."

For the user account that was added, use the password command to set the password. The password command sets the validity period of the password with the following options.

Table 3-10 password Command Options

Option	Content of Setting
-e	Sets the user account validity period, or sets the expiration date. When set to NEVER, the expiration date for the user account is eliminated.
-i	Sets the number of days after the password expiration date before the account is locked out
-M	Sets the maximum number of days that a password is valid
-n	Sets the minimum number of days that a password is valid
-w	Sets the number of days after a password expiration warning is issued before the password actually expires

Operation Procedure

1. **Execute the adduser command to add a user account.**
   The following example specifies jsmith for the user account name. If the UID specification is omitted, a UID is automatically assigned.

   ```
   XSCF> adduser jsmith
   ```

   The following example adds a user account with a UID specified, using the -u option.

   ```
   XSCF> adduser -u 359 jsmith
   ```

2. **Execute the password command, and specify a password.**

   ```
   XSCF> password jsmith
   Password:
   Retype new password:
   passwd: password updated successfully
   XSCF>
   ```

   The following example specifies 60 days for the expiration time and 15 days ahead for the start date for warnings before the password expires.

   ```
   XSCF> password -M 60 -w 15 jsmith
   ```

3.5.9   Setting a User Privilege

To set user privileges, use the setprivileges command. Execute the setprivileges command with a user account that has the useradm privilege. For the types of user

privileges, see Table 3-6.

1. **Execute the showuser command to display information on an enabled user account.**

```
XSCF> showuser -p jsmith
User Name:        jsmith
Privileges:       None
```

2. **Execute the setprivileges command to assign a user privilege to the user account.**
   The following example assigns the user privileges useradm and auditadm to the jsmith user account.

```
XSCF> setprivileges jsmith useradm auditadm
```

Note - The setprivileges command assigns the user privilege of the specified operand. To add a new user privilege to a user account already assigned a user privilege, specify the existing user privilege too.

3. **Execute the showuser command, and confirm the user privileges.**

```
XSCF> showuser -p jsmith
User Name:        jsmith
Privileges:       useradm
                  auditadm
```

3.5.10 Enabling/Disabling a User Account

The user accounts registered with the adduser command are enabled immediately after they are registered. You can disable registered XSCF user accounts when necessary, and then you can also enable them again.

To disable a user account, use the disableuser command. To enable a user account that was disabled, use the enableuser command. Execute the disableuser command and enableuser command with a user account that has the useradm privilege.

1. **Execute the showuser command to display information on an enabled user account.**

```
XSCF> showuser -p jsmith
User Name:        jsmith
 :
```

2. **Execute the disableuser command to disable a user account.**
   The following example specifies the user account to be disabled.

```
XSCF> disableuser jsmith
```

3. **To use the user account again, execute the enableuser command to enable the account.**
   The following example specifies the user account to be enabled.

```
XSCF> enableuser jsmith
```

4. **Execute the showuser command to check information on an enabled user account.**

```
XSCF> showuser -p jsmith
User Name:           jsmith
 :
```

3.5.11   Enabling/Disabling the Login Lockout Function

When the login lockout function is enabled, and a user fails three times in succession when attempting to log in, that user will not be able to log in until after a predetermined amount of time has passed. In the default settings, the login lockout function is disabled.

To set a lockout time and enable the login lockout function, use the setloginlockout command. To enable the lockout function, set the lockout time to a time other than 0 minutes. Any value from 0 to 1,440 minutes can be set as the lockout duration. To disable the lockout function after it has been activated, specify a lockout time of 0 minutes. Use the showloginlockout command to confirm the lockout time that is set. Execute the setloginlockout command and showloginlockout command with a user account that has the useradm privilege.

1. **Execute the showloginlockout command to display the lockout function setting.**

```
XSCF> showloginlockout
90 minutes
```

2. **Execute the setloginlockout command to configure the lockout function.**
   The following example specifies a lockout duration of 20 minutes and enables the lockout function.

```
XSCF> setloginlockout -s 20
```

   The following example disables the lockout function.

```
XSCF> setloginlockout -s 0
```

The set lockout duration applies from the next login. If the specified time is 0 minutes, the lockout function is disabled beginning at the next login.
The lockout function is enabled on both the master and standby XSCFs. If a user account is locked out, a message is saved in the audit log.
If the lockout function is disabled, there is no limit on the number of permitted login attempts by users.
If you need to use a locked-out user account before the lockout duration expires, the system administrator can disable the lockout function. After a successful login to that user account, the system administrator should set the lockout duration and enable the lockout function again.

3.5.12 Managing XSCF User Accounts Using LDAP

Lightweight Directory Access Protocol (LDAP) is a protocol that is used to access a directory service on a network. Normally, user authentication and user privilege of an XSCF user account on SPARC M12/M10 systems are managed by the local master XSCF. However, by using LDAP, they can be managed by a directory service (LDAP server) on a network. In addition, if multiple SPARC M12/M10 systems are installed, the XSCF user account common to all systems can be used with LDAP.
To manage the XSCF user account settings, such as user authentication and user privileges, using LDAP, configure the XSCF as an LDAP client.
This section describes how to manage the XSCF user account settings through a directory service on a network using LDAP.

Note - This section does not describe the configuration and management of the LDAP server. An administrator who is familiar with the LDAP server should design the LDAP server.

Note - For the XCP firmware version that supports LDAP, see the latest *Product Notes* for your server.

In the LDAP settings, items related to an LDAP client are set. The settings cover the LDAP Server, bind ID, password, search base, and so on. In the LDAP server, the XSCF user information is managed.

Table 3-11 lists terms related to the LDAP settings.

Table 3-11   Terms Related to LDAP

Term	Description
LDAP	Abbreviation for Lightweight Directory Access Protocol. LDAP is a protocol used to access a directory service on a network.
baseDN	Abbreviation for base Distinguished name. Under LDAP, directory information is organized in a hierarchical structure. To perform a search, specify the subtree to be searched in the hierarchical structure. At this time, specify the distinguished name (DN) of the top of the target subtree. This DN is referred to as the search base (baseDN).

Table 3-11	Terms Related to LDAP *(continued)*
Term	**Description**
Certificate chain	List of certificates, including a user certificate and certification authority certificate. OpenSSL and TLS certificates must be downloaded in advance.
TLS	Abbreviation for Transport Layer Security. This is a protocol for encrypting information for transmission/reception via the Internet.

LDAP setting flow

This section describes the flow to configure the XSCF as an LDAP client.

1. **Enable LDAP.**

2. **Enter the configuration information of the LDAP server.**
   - The IP address or the host name and port number of the primary LDAP directory
   - Option: Up to two IP addresses or the host name and port of alternate LDAP directories
   - The search base distinguished name (DN) for reference
   - Whether or not to use the Transport Layer Security (TLS)

3. **Check whether or not the LDAP operates normally.**

Settings required on LDAP server

■ Add descriptions related to user privileges to an LDAP schema file.
To configure the XSCF as an LDAP client, create an LDAP schema related to the user privileges of the XSCF on an LDAP server. Add the following descriptions to the schema file.

```
attributetype ( 1.3.6.1.1.1.1.40 NAME 'spPrivileges'
    DESC 'Service Processor privileges'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
    SINGLE-VALUE )
objectclass ( 1.3.6.1.1.1.2.13 NAME 'serviceProcessorUser' SUP top
AUXILIARY
    DESC 'Service Processor user'
    MAY spPrivileges )
```

■ Add attributes required for users to an LDIF file.
Add the following attributes that are required for each user to an LDIF (LDAP Data Interchange Format) file on an LDAP server.

Table 3-12 Required Attributes for an LDIF File

Field Name	Description
spPrivileges	User privilege that is valid on the XSCF
uidNumber	User ID number that is valid on the XSCF uidNumber must be a numeric value larger than 100. Use the showuser command to display a UID.

The following shows an input example of an LDAP schema file.

```
spPrivileges: platadm
uidNumber: 150
```

User authentication mechanism when configuring the XSCF as an LDAP client

If LDAP clients are configured on the XSCF and enabled, the user authentication is first performed locally and then on the LDAP server. If the setprivileges command is executed without specifying a privilege to the user, all local privilege data of the user is deleted. After that, if the privilege reference is enabled in LDAP, then the user privilege is referenced in LDAP. When none is specified for the user privilege, the user does not have user privilege even if there is privilege data on LDAP.

The following commands are used to manage LDAP on the XSCF.
- setlookup
- setldap
Unix crypt or MD5 encryption method is used for the passwords saved in the LDAP repository.
Once you have configured the XSCF to use LDAP, it requires no day-to-day management.

LDAP setting items and shell commands to be used

Table 3-13 lists the LDAP setting items and the corresponding shell commands.

Table 3-13 LDAP Setting Items and Commands to be Used

Setting Item	Function Description	Shell Command	Remarks
LDAP usage display	Displays the status regarding whether an LDAP server is used for authentication and user privilege lookup.	showlookup	

Table 3-13   LDAP Setting Items and Commands to be Used *(continued)*

Setting Item	Function Description	Shell Command	Remarks
LDAP usage enable/disable	Enables or disables the use of an LDAP server for authentication and user privilege lookup.	setlookup	If this specifies that authentication data and user privilege data be placed on an LDAP server, the system first searches the local area. If the target data is not found locally, then it searches the LDAP server.
Client display	Displays LDAP client setting information.	showldap	
Bind ID	Registers an ID for connecting to (bind: authenticate) an LDAP server.	setldap	The maximum length of a bind ID is 128 characters.
Password	Sets a password used to connect to an LDAP server.		A password can consist of 8 to 16 characters.
Search base	Sets an LDAP tree search base (baseDN).		- If this item is omitted, the command searches the tree, beginning from the top. - The maximum length allowed for the search base is 128 characters.
Certificate chain	Imports the certificate chain of an LDAP server. Imports the certificate chain (scp) from a remote file by using a secure copy.		- The certificate chain must be in the PEM format. (*1) - A password may need to be entered to import the certificate from a remote file by using scp.
LDAP server/port	Specifies the IP addresses and port numbers of the primary and secondary LDAP servers. Specifies IP addresses or host names for the addresses. (e.g. ldap://foobar.east, ldaps://10.8.31.14:636)		The default LDAP port number is 636 for ldaps:// and 389 for ldap:// when the port number is not specified.
Timeout	Sets the maximum time (seconds) allowed for an LDAP search.		
LDAP test	Tests the connection to an LDAP server.		

*1 PEM: Abbreviation for Privacy Enhanced Mail. Mail to be sent is encrypted for increased privacy.

Enabling or Disabling the use of an LDAP Server

1. **Execute the showlookup command to display the lookup method of authentication and user privileges.**
   In the following example, lookup is executed only for the XSCF server for user

authentication, and XSCF and LDAP servers for user privileges.

```
XSCF> showlookup
Privileges lookup: Local only
Authentication lookup: Local and LDAP
```

2. **Execute the setlookup command to enable/disable the use of an LDAP server.**
   In the following example, an LDAP server is enabled for both user authentication and user privileges.

```
XSCF> setlookup -a ldap
XSCF> setlookup -p ldap
```

3. **Execute the showlookup command, and confirm the lookup method.**

```
XSCF> showlookup
Privileges lookup: Local and LDAP
Authentication lookup: Local and LDAP
```

Setting LDAP server, port number, bind ID, bind password, search base (baseDN), and search time (timeout period)

1. **Execute the showldap command to display LDAP client settings.**

```
XSCF> showldap
Bind Name:              Not set
Base Distinguished Name: Not set
LDAP Search Timeout:    0
Bind Password:          Not set
LDAP Servers:           Not set
CERTS:                  None
```

2. **Execute the setldap command to configure LDAP client settings.**
   In the following example, a bind ID and search base (baseDN) are specified.

```
XSCF> setldap -b "cn=Directory Manager" -B "ou=People,dc=users,
dc=apl,dc=com,o=isp"
```

In the following example, a bind password is specified.

```
XSCF> setldap -p
Password:xxxxxxxx
```

In the following example, the primary and secondary LDAP servers and port

numbers are specified.

```
XSCF> setldap -s ldap://onibamboo:389,ldaps://company2.com:636
```

In the following example, the timeout time for the LDAP search is specified.

```
XSCF> setldap -T 60
```

3. **Execute the showldap command, and confirm the setting.**

```
XSCF> showldap
Bind Name:              cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:    60
Bind Password:          Set
LDAP Servers:           ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                  None
```

Installing the certificate chain of an LDAP server

1. **Execute the showldap command to display the LDAP setting.**

```
XSCF> showldap
Bind Name:              cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:    60
Bind Password:          Set
LDAP Servers:           ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                  None
```

2. **Execute the setldap command to import the certificate chain.**

```
XSCF> setldap -c hhhh@example.com:Cert.pem
```

3. **Execute the showldap command, and confirm that the certificate chain has been imported.**

```
XSCF> showldap
Bind Name:              cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:    60
Bind Password:          Set
LDAP Servers:           ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                  Exists
```

Testing a connection to an LDAP server

1. **Execute the setldap command to perform the test.**

```
XSCF> setldap -t sysadmin
onibamboo:389      PASSED
```

2. **Log in as the user registered to the LDAP server. Confirm the authentication using the entered password.**

```
login: sysadmin
Password:xxxxxxxx
```

3. **Execute the showuser command, and confirm whether the displayed user privilege is the same as the one created in the LDAP server.**

```
XSCF> showuser
User Name:    sysadmin (nonlocal)
UID:          110
Privileges:   platadm
```

3.5.13   Managing XSCF User Accounts Using Active Directory

In the Active Directory settings, items related to an Active Directory client are set. The settings cover the Active Directory server, loading of a server certificate, group name, user privilege, user domain, log, DNS locator query, and so on. In the Active Directory server, the XSCF user information is managed.

Note - This section does not describe the configuration and management of the Active Directory server. An administrator who is familiar with the Active Directory server should design the Active Directory server.

Note - For the XCP firmware version that supports Active Directory, see the latest *Product Notes* for your server.

Table 3-14 lists terms related to the Active Directory settings.

Table 3-14   Terms Related to Active Directory

Term	Description
Active Directory	Active Directory is a distributed directory service that was developed by Microsoft Corporation and is available in Windows operating systems. Like LDAP directory service, it is used for user authentication.
User domain	User domain is the authentication domain used to authenticate a user.
DNS locator query	The query is used to query a DNS server about the Active Directory server for user authentication.

The Active Directory provides both user certificate authentication and authorization of a user access level to network resources. The Active Directory uses the authentication to identify specific users before they access the system resources, and to grant specific access privileges to users in order to control their rights to access network resources.

User privileges are either configured on the XSCF or obtained from a server in a network domain based on each user's group membership. A user can belong to more than one group. User domain is the authentication domain used to authenticate a user. The Active Directory authenticates users in the order in which the user domains are configured.

Once authenticated, user privileges can be determined in the following ways:

- In the simplest case, user privileges are determined by the Active Directory settings on the XSCF. There is a defaultrole parameter for the Active Directory. If the defaultrole parameter is configured or set, all users that are authenticated via the Active Directory are assigned the user privileges set in the parameter. Users that are set on the Active Directory server require only a password regardless of their group membership.

- If the defaultrole parameter is not configured or set, a user privilege is obtained from the Active Directory server based on the user's group membership. On the XSCF, the group parameter must correspond to the group name of an Active Directory server. Each group has a user privilege that is configured on the XSCF and is associated with the group. Once a user is authenticated, the user's group membership is used to determine the user privilege.

Active directory setting items and shell commands to be used

Table 3-15 lists the setting items and the corresponding shell commands.

Table 3-15   Active Directory Related Setting Items and Commands to be Used

Setting Item	Function Description	Shell Command	Remarks
Active Directory status display	Displays the current status of the Active Directory, such as enable/disable of the Active Directory and DNS locator mode.	showad	

Table 3-15   Active Directory Related Setting Items and Commands to be Used *(continued)*

Setting Item	Function Description	Shell Command	Remarks
Active Directory usage enable/disable	Specifies whether to enable or disable the use of the Active Directory server for managing authentication and user privileges.	setad	It is disabled by default.
Active Directory server display	Displays the configuration of the primary Active Directory server or up to five alternate Active Directory servers.	showad	A port number "0" indicates that the default port for the Active Directory is used.
Active Directory server/port	Specifies IP addresses and port numbers of the primary and up to five alternate Active Directory servers. Specifies IP addresses or host names for the addresses. To specify host names for the Active Directory servers, the server names must be resolvable by the DNS server.	setad	When a port number is not specified, the default port is used.
Server certificate load/delete	Loads or deletes the certificates of the primary and up to five alternate servers.	setad	The strictcertmode must be in the disabled state for a certificate to be removed.
DNS locator mode enable/disable	Enables or disables the DNS locator mode.	setad	It is disabled by default.
DNS locator query display	Displays the configuration of up to five DNS locator queries.	showad	
DNS locator query	Configures the DNS locator query. The DNS locator query is used to query a DNS server to determine an Active Directory server to use for user authentication.	setad	DNS and DNS locator mode must be enabled for the DNS locator query to work.
Expanded search mode enable/disable	Enables or disables the expanded search mode. The expanded search mode is only enabled when addressing a specific environment where the user account is not in the UserPrincipalName (UPN) format.	setad	It is disabled by default.
strictcertmode enable/disable	Enables or disables the strictcertmode. If the strictcertmode is enabled, the certificate of a server must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.	setad	It is disabled by default.
Server certificate display	Displays the following: - Certificate information for the primary and up to five alternate servers. - Entire contents of the certificate	showad	
User domain display	Displays user domains.	showad	

Table 3-15 Active Directory Related Setting Items and Commands to be Used *(continued)*

Setting Item	Function Description	Shell Command	Remarks
User domain	Configures up to five specified user domains. Specify a user domain in the UPN format, where a user name and domain name are connected using the "@" symbol, or in the Distinguished Name (DN) format, which is defined as "uid = user name, ou = organization unit, and dc = domain name."	setad	If a user domain is directly specified using the UPN form at the login prompt, such as "login: ima.admin@dc01.example.com", the user domain is used only for this login.
defaultrole display	Displays the defaultrole setting.	showad	
defaultrole	Specifies the user privileges assigned to all users that are authenticated via Active Directory.	setad	
Group display	Displays the configuration of administrator group, operator group, and custom group.	showad	
Administrator group	Assigns group names for up to five administrator groups. The administrator group has platadm, useradm, and auditadm privileges. These privileges cannot be changed.	setad	
Operator group	Assigns group names for up to five operator groups. The operator group has platop and auditop privileges. These privileges cannot be changed.	setad	
Custom group	Assigns group names and user privileges for up to five groups.	setad	
Timeout	Configures transaction timeout in seconds. You can specify a numeric value from 1 to 20.	setad	The default value is 4 seconds. If a specified timeout is too short for the configuration, the login process or retrieval of the user privilege setting could fail.
Log enable/disable	Enables or disables the logging of Active Directory authentication and authorization diagnosis messages.	setad	This log is cleared when the XSCF is rebooted.
Log display	Displays Active Directory authentication and authorization diagnosis messages.	showad	
Log clear	Clears the logs of Active Directory authentication and authorization diagnosis messages.	setad	
Default	Resets the Active Directory settings to their factory defaults.	setad	

Before configuring the Active Directory settings

Note the following before configuring the Active Directory settings.

- Confirm that the XCP version that supports Active Directory is used. For the XCP that supports Active Directory, see the latest *Product Notes*.
- The useradm user privilege is required for the Active Directory settings.
- If the XSCF is configured to use LDAP, Active Directory, or LDAP over SSL for user account data, then the user account name and user identifier (if specified) must not already be in use in the XSCF, LDAP, Active Directory, or LDAP over SSL.
- To use a host name for an Active Directory server, DNS settings need to be configured properly before setting Active Directory.
- In Active Directory, the system account called proxyuser is used. Verify that no user account with that name already exists. If a user account with the name proxyuser exists, then delete the account with the deleteuser command. After deleting the account, reboot the XSCF before using Active Directory.
- If Active Directory is enabled and you try to login via telnet, inquiries to the second and subsequent alternate servers may time out, causing the login to fail.
- If the value set by the timeout operand is small, and you log in to the XSCF, user privilege may not be assigned to you. In this case, increase the timeout setting value and try again.
- If you are an Active Directory user, you cannot upload a user public key to the XSCF. The Active Directory users can login by connecting to the XSCF via SSH using password authentication.

Enabling or disabling the use of an Active Directory Server

1. **Execute the showad command to display the usage of the Active Directory server.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Execute the setad command to enable/disable the use of the Active Directory server.**
   In the following example, the use of the Active Directory server is enabled.

```
XSCF> setad enable
```

In the following example, the use of the Active Directory server is disabled.

```
XSCF> setad disable
```

3. **Execute the showad command, and confirm whether Active Directory is enabled or disabled.**
   In the following example, the Active Directory is enabled.

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Setting Active Directory servers and port numbers

1. **Execute the showad command to display the Active Directory server settings.**

```
XSCF> showad server
Primary Server
    address: (none)
    port: 0
XSCF> showad server -i
Alternate Server 1
    address: (none)
    port: 0
Alternate Server 2
    address: (none)
    port: 0
Alternate Server 3
    address: (none)
    port: 0
Alternate Server 4
    address: (none)
    port: 0
Alternate Server 5
    address: (none)
    port: 0
```

2. **Execute the setad command to set Active Directory servers.**
   In the following example, the primary server and port number are specified.

```
XSCF> setad server 10.24.159.150:8080
```

In the following example, alternate servers are specified.

```
XSCF> setad server -i 1 10.24.159.151
```

3. **Execute the showad command, and confirm the Active Directory settings.**

```
XSCF> showad server
Primary Server
    address: 10.24.159.150
    port: 8080
XSCF> showad server -i
Alternate Server 1
    address: 10.24.159.151
    port: 0
Alternate Server 2
    address: (none)
    port: 0
Alternate Server 3
    address: (none)
    port: 0
Alternate Server 4
    address: (none)
    port: 0
Alternate Server 5
    address: (none)
    port: 0
```

Loading/Deleting the Server Certificate

1. **Execute the showad command to display the server certificate information.**

```
XSCF> showad cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

XSCF> showad cert -i
Alternate Server 1:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

Alternate Server 2:
```

```
... <snip>

Alternate Server 5:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

2. **Execute the setad command to load the server certificate to the XSCF.**
   In the following example, the server certificate of the primary server is loaded using the user name and password.

```
XSCF> setad loadcert -u yoshi http://domain_2/UID_2333/testcert
Warning: About to load certificate for Primary Server.
Continue? [y|n]: y
Password:
```

In the following example, the content of the certificate is copied and pasted on the screen, and then the certificate for the alternate server 1 is loaded from a console. After pressing the [Enter] key, press the [Ctrl] and [D] keys to complete loading.

```
XSCF> setad loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:
-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
[Enter]
[Ctrl]+[D]
```

3. **Execute the showad command, and confirm that the server certificate is loaded.**

```
XSCF> showad cert
Primary Server:
certstatus = certificate present
issuer = DC = local, DC = xscf, CN = apl
serial number = 55:1f:ff:c4:73:f7:5a:b9:4e:16:3c:fc:e5:66:5e:5a
subject = DC = local, DC = xscf, CN = apl
valid from = Mar 9 11:46:21 2010 GMT
valid until = Mar 9 11:46:21 2015 GMT
version = 3 (0x02)

XSCF> showad cert -i 1
```

```
Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = aplle, CN = aplle.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = aplle, CN = aplle.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)
```

4. **Execute the setad command to delete the primary server certificate.**

```
XSCF> setad rmcert
Warning: About to delete certificate for Primary Server.
Continue? [y|n]: y
```

5. **Execute the showad command, and confirm that the server certificate has been deleted.**

```
XSCF> showad cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

The strictcertmode must be in the disabled state for a certificate to be removed.

Enabling/disabling the DNS locator mode

1. **Execute the showad command to display that the DNS locator mode is enabled/disabled.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Execute the setad command to enable/disable the DNS locator mode.**
   In the following example, the DNS locator mode is enabled.

```
XSCF> setad dnslocatormode enable
```

In the following example, the DNS locator mode is disabled.

```
XSCF> setad dnslocatormode disable
```

3. **Execute the showad command, and confirm that the DNS locator mode is enabled/disabled.**
   In the following example, the DNS locator mode is enabled.

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Configuring the DNS locator query

Note - Before setting DNS locator query, enable DNS locator mode.

1. **Execute the showad command to display the configuration of the DNS locator query.**

```
XSCF> showad dnslocatorquery -i 1
service 1: (none)
XSCF> showad dnslocatorquery -i 2
service 2: (none)
```

2. **Execute the setad command to configure the DNS locator query.**

```
XSCF> setad dnslocatorquery -i 1 '_ldap._tcp.gc._msdcs..'
```

3. **Execute the showad command, and confirm the DNS locator query.**

```
XSCF> showad dnslocatorquery -i 1
service 1: _ldap._tcp.gc._msdcs..
```

DNS and DNS locator mode must be enabled for the DNS locator query to work.

Enabling/disabling the expanded search mode

1. **Execute the showad command to display whether the expanded search mode is enabled or disabled.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Execute the setad command to enable/disable the expanded search mode.**
   In the following example, the expanded search mode is enabled.

```
XSCF> setad expsearchmode enable
```

In the following example, the expanded search mode is disabled.

```
XSCF> setad expsearchmode disable
```

3. **Execute the showad command, and confirm that the expanded search mode is enabled/disabled.**
   In the following example, the expanded search mode is enabled.

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Enabling/Disabling the strictcertmode

1. **Execute the showad command to display whether the strictcertmode is enabled or disabled.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
```

```
logdetail: none
```

2. **Execute the setad command to enable/disable the strictcertmode.**
   In the following example, the strictcertmode is enabled.

```
XSCF> setad strictcertmode enable
```

   In the following example, the strictcertmode is disabled.

```
XSCF> setad strictcertmode disable
```

3. **Execute the showad command, and confirm that the strictcertmode is enabled/disabled.**
   In the following example, the strictcertmode is enabled.

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

   To enable the strictcertmode, the server certificate must have already been loaded to the XSCF.

Setting a User Domain

1. **Execute the showad command to display user domains.**

```
XSCF> showad userdomain
domain 1: (none)
domain 2: (none)
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

2. **Execute the setad command to set user domains.**
   In the following example, user domain 1 is set.

```
XSCF> setad userdomain -i 1 '@davidc.example.aCompany.com'
```

   In the following example, user domain 2 is set.

```
XSCF> setad userdomain -i 2 'CN=<USERNAME>,CN=Users,DC=davidc,DC=example,
DC=aCompany,DC=com'
```

3. **Execute the showad command, and confirm the user domains.**

```
XSCF> showad userdomain
domain 1: <USERNAME>@davidc.example.aCompany.com
domain 2: CN=<USERNAME>,CN=Users,DC=davidc,DC=example,
DC=aCompany,
DC=com
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

If a user domain is directly specified at the login prompt, such as "login: ima.admin@dc01.example.com", the user domain is used only for this login.

Setting the Default Privilege

1. **Execute the showad command to display the default privilege.**

```
XSCF> showad defaultrole
Default role: (none)
```

2. **Execute the setad command to set a default privilege.**

```
XSCF> setad defaultrole platadm platop
```

3. **Execute the showad command, and confirm the default privilege.**

```
XSCF> showad defaultrole
Default role: platadm platop
```

Setting Group Names and Privileges

1. **Execute the showad command to display group names.**
   The following example shows administrator groups.

```
XSCF> showad group administrator
Administrator Group 1
    name: (none)
Administrator Group 2
    name: (none)
Administrator Group 3
```

```
      name: (none)
Administrator Group 4
      name: (none)
Administrator Group 5
      name: (none)
```

The following example shows operator groups.

```
XSCF> showad group operator
Operator Group 1
      name: (none)
Operator Group 2
      name: (none)
Operator Group 3
      name: (none)
Operator Group 4
      name: (none)
Operator Group 5
      name: (none)
```

The following example shows custom groups.

```
XSCF> showad group custom
Custom Group 1
      name: (none)
      roles: (none)
Custom Group 2
      name: (none)
      roles: (none)
Custom Group 3
      name: (none)
      roles: (none)
Custom Group 4
      name: (none)
      roles: (none)
Custom Group 5
      name: (none)
      roles: (none)
```

2. **Execute the setad command to set the group names and privileges.**
   In the following example, administrator group 1 is set.

```
XSCF> setad group administrator -i 1 name CN=SpSuperAdmin,OU=Groups,DC=davidc,
DC=example,DC=aCompany,DC=com
```

In the following example, operator group 1 is set.

```
XSCF> setad group operator -i 1 name CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
```

In the following example, custom group 1 is set.

```
XSCF> setad group custom -i 1 name CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
```

In the following example, the privilege of the custom group 1 is set.

```
XSCF> setad group custom -i 1 roles platadm,platop
```

3. **Execute the showad command, and confirm the group names and privileges.**
   In the following example, the administrator groups are confirmed.

```
XSCF> showad group administrator
Administrator Group 1
    name: CN=<USERNAME>,CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,
DC=aCompany,DC=com
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)
```

In the following example, the operator groups are confirmed.

```
XSCF> showad group operator
Operator Group 1
    name: CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)
```

In the following example, the custom groups are confirmed.

```
XSCF> showad group custom
Custom Group 1
    name: CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
    roles: platadm platop
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
```

```
     roles: (none)
Custom Group 5
     name: (none)
     roles: (none)
```

The administrator group has platadm, useradm, and auditadm privileges. These privileges cannot be changed. The operator group also has platop and auditop privileges. These privileges cannot be changed.

Setting a Timeout

1. **Execute the showad command to display the timeout time.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

2. **Execute the setad command to set the timeout.**
   In the following example, 10 seconds are set as the timeout time.

```
XSCF> setad timeout 10
```

3. **Execute the showad command, and confirm the timeout time.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

Enabling/disabling the logs of Active Directory authentication and authorization diagnosis messages.

1. **Execute the showad command to display the log detail level.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
```

```
strictcertmode: enabled
timeout: 10
logdetail: none
```

2. **Execute the setad command to set the log detail level.**
   In the following example, the log is enabled and the log detail level is set to trace.

```
XSCF> setad logdetail trace
```

In the following example, the log is disabled.

```
XSCF> setad logdetail none
```

3. **Execute the showad command, and confirm the log detail level.**
   In the following example, the log detail level is set to trace.

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

Displaying the Log of Diagnosis Messages and Clearing the Log File

1. **Execute the showad command to display the log detail level.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Execute the showad command to display the diagnosis messages.**
   In the following example, diagnosis messages are displayed in real time.

```
XSCF> showad log -f
Mon Nov 16 14:47:53 2009 (ActDir): module loaded, OPL
Mon Nov 16 14:47:53 2009 (ActDir): --error-- authentication
status:
```

```
auth-ERROR
Mon Nov 16 14:48:18 2009 (ActDir): module loaded, OPL
...
```

3. **Execute the setad command to clear the log file of diagnosis messages.**

```
XSCF> setad log clear
Warning: About to clear log file.
Continue? [y|n]: y
```

Resetting the Active Directory Settings to Their Defaults

1. **Execute the showad command to display the setting status of the Active Directory.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Execute the setad command to reset the Active Directory settings to their defaults.**

```
XSCF> setad default -y
Warning: About to reset settings to default.
Continue? [y|n]: y
```

3. **Execute the showad command, and confirm that the Active Directory settings are reset to their defaults.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Logging In With the Active Directory User Account

After completing each setting, confirm whether login with the user account of Active Directory is possible.

3.5.14 Managing XSCF User Accounts Using LDAP over SSL

In the LDAP over SSL settings, items related to an LDAP over SSL client are set. The settings cover the LDAP over SSL server, loading of server certificate, group name, user privilege, user domain, log, DNS locator query, and so on. In the LDAP over SSL server, the XSCF user information is managed.

Note - This section does not describe the configuration and management of the LDAP over SSL server. An administrator who is familiar with the LDAP over SSL server should design the LDAP over SSL server.

Note - For the XCP firmware version that supports LDAP over SSL, see the latest *Product Notes*.

Table 3-16 lists terms related to the LDAP over SSL settings.

Table 3-16   Terms Related to LDAP over SSL

Term	Description
LDAP over SSL	LDAP over SSL is a distributed directory service like Active Directory. LDAP over SSL offers enhanced security to LDAP users by using Secure Socket Layer (SSL)/Transport Layer Security (TLS) technology. Like LDAP directory service, LDAP over SSL is used for user authentication.

LDAP over SSL provides both user certificate authentication and authorization of a user access level to network resources. LDAP over SSL uses the authentication to identify specific users before they access the system resources, and to grant specific access privileges to users in order to control their rights to access network resources.

User privileges are either configured on the XSCF or obtained from a server in a network domain based on each user's group membership. A user can belong to more than one group. User domain is the authentication domain used to authenticate a user. LDAP over SSL authenticates users in the order in which the user domains are configured.

Once authenticated, user privileges can be determined in the following ways:
- In the simplest case, user privileges are determined by the LDAP over SSL settings on the XSCF. There is a defaultrole parameter for the LDAP over SSL. If the defaultrole parameter is configured or set, all users that are authenticated via LDAP over SSL are assigned the user privileges set in the parameter. Users that are set on the LDAP over SSL server require only a password regardless of their group membership.
- If the defaultrole parameter is not configured or set, user privilege is obtained from the LDAP over SSL server based on the user's group membership. On the XSCF, the group parameter must correspond to the group name of an LDAP over

SSL server. Each group has a user privilege that is configured on the XSCF and is associated with the group. Once a user is authenticated, the user's group membership is used to determine the user privilege.

LDAP over SSL setting items and shell commands to be used

Table 3-17 lists the setting items and the corresponding shell commands.

Table 3-17   LDAP over SSL Setting Items and Commands to be Used

Setting Item	Function Description	Shell Command	Remarks
LDAP over SSL status display	Displays the current status of LDAP over SSL, such as enable/disable of LDAP over SSL and usemapmode.	showldapssl	
LDAP over SSL usage enable/disable	Specifies whether to enable/disable the use of the LDAP over SSL server for managing authentication and user privileges.	setldapssl	It is disabled by default.
LDAP over SSL server display	Displays the configuration of the primary LDAP over SSL server or up to five alternate LDAP over SSL servers.	showldapssl	A port number "0" indicates that the default port for LDAP over SSL is used.
LDAP over SSL server/port	Specifies IP addresses and port numbers of the primary and up to five alternate LDAP over SSL servers. Specifies IP addresses or host names for the addresses. To specify host names for the LDAP over SSL servers, the server names must be resolvable by the DNS server.	setldapssl	When a port number is not specified, the default port is used.
Server certificate load/delete	Loads or deletes the certificates of the primary and up to five alternate servers.	setldapssl	The strictcertmode must be in the disabled state for a certificate to be removed.
usermapmode enable/disable	Enables/disables the usermapmode. When enabled, user attributes specified with the usermap operand, rather than user domain, are used for user authentication.	setldapssl	It is disabled by default.
usermap display	Displays the usermap setting.	showldapssl	
usermap	Configures the usermap. The usermap is used for user authentication.	setldapssl	The usermapmode must be enabled to use the usermap.
strictcertmode enable/disable	Enables or disables the strictcertmode. If the strictcertmode is enabled, the certificate of a server must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.	setldapssl	It is disabled by default.

Table 3-17 LDAP over SSL Setting Items and Commands to be Used *(continued)*

Setting Item	Function Description	Shell Command	Remarks
Server certificate display	Displays the following: - Certificate information for the primary and up to five alternate servers. - Entire contents of the certificate	showldapssl	
User domain display	Displays user domains.	showldapssl	
User domain	Configures up to five specified user domains. User domain is specified in the Distinguished Name (DN) format.	setldapssl	
defaultrole display	Displays the defaultrole setting.	showldapssl	
defaultrole	Specifies the user privilege assigned to all users that are authenticated via LDAP over SSL.	setldapssl	
Group display	Displays the configuration of administrator group, operator group, and custom group.	showldapssl	
Administrator group	Assigns group names for up to five administrator groups. The administrator group has platadm, useradm, and auditadm privileges. These privileges cannot be changed.	setldapssl	
Operator group	Assigns group names for up to five operator groups. The operator group has platop and auditop privileges. These privileges cannot be changed.	setldapssl	
Custom group	Assigns group names and user privileges for up to five groups.	setldapssl	
Timeout	Configures transaction timeout in seconds. You can specify a numeric value from 1 to 20.	setldapssl	The default value is 4 seconds. If a specified timeout is too short for the configuration, the login process or retrieval of the user privilege setting could fail.
Log enable/disable	Enables/disables the logs of LDAP over SSL authentication and authorization diagnosis messages.	setldapssl	This log is cleared when the XSCF is rebooted.
Log display	Displays LDAP over SSL authentication and authorization diagnosis messages.	showldapssl	
Log clear	Clears the logs of LDAP over SSL authentication and authorization diagnosis messages.	setldapssl	
Default	Resets the LDAP over SSL settings to their factory defaults.	setldapssl	

Before Configuring the LDAP over SSL Settings

Note the following before configuring the LDAP over SSL settings.

- Confirm that the XCP version that supports LDAP over SSL is used. For the XCP that supports LDAP over SSL, see the latest *Product Notes*.
- The useradm privilege is required for the LDAP over SSL settings.
- If the XSCF is configured to use LDAP, Active Directory, or LDAP over SSL for user account data, then the user account name and user identifier (if specified) must not already be in use in the XSCF, LDAP, Active Directory, or LDAP over SSL.
- To use a host name for the LDAP over SSL server, DNS settings need to be configured properly before setting LDAP over SSL.
- In LDAP over SSL, the system account called proxyuser is used. Verify that no user account with that name already exists. If a user account with the name proxyuser exists, then delete the account with the deleteuser command. After deleting the account, reboot the XSCF before using LDAP over SSL.
- If the value set by the timeout operand is small, and you log in to the XSCF, user privilege may not be assigned to you. In this case, increase the timeout setting value and try again.
- LDAP over SSL users cannot upload a user public key to the XSCF. LDAP over SSL users can login by connecting to the XSCF via SSH using password authentication.

Enabling/Disabling the Use of the LDAP over SSL Server

1. **Execute the showldapssl command to display the usage of the LDAP over SSL server.**

```
XSCF> showldapssl
usermapmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Execute the setldapssl command to enable/disable the use of the LDAP over SSL server.**
   In the following example, the use of the LDAP over SSL server is enabled.

```
XSCF> setldapssl enable
```

In the following example, the use of the LDAP over SSL server is disabled.

```
XSCF> setldapssl disable
```

3. **Execute the showldapssl command, and confirm whether LDAP over SSL is enabled or disabled.**
   In the following example, the LDAP over SSL is enabled.

```
XSCF> showldapssl
usermapmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Setting LDAP over SSL Servers and Port Numbers

1. **Execute the showldapssl command to display the LDAP over SSL server settings.**

```
XSCF> showldapssl server
Primary Server
    address: (none)
    port: 0
XSCF> showldapssl server -i
Alternate Server 1
    address: (none)
    port: 0
Alternate Server 2
    address: (none)
    port: 0
Alternate Server 3
    address: (none)
    port: 0
Alternate Server 4
    address: (none)
    port: 0
Alternate Server 5
    address: (none)
    port: 0
```

2. **Execute the setldapssl command to set LDAP over SSL servers.**
   In the following example, the primary server and port number are specified.

```
XSCF> setldapssl server 10.18.76.230:4041
```

   In the following example, alternate servers are specified.

```
XSCF> setldapssl server -i 1 10.18.76.231
```

3. **Execute the showldapssl command, and confirm the LDAP over SSL server settings.**

```
XSCF> showldapssl server
Primary Server
address: 10.18.76.230
port: 4041

XSCF> showldapssl server -i
Alternate Server 1
    address: 10.18.76.231
    port: 0
Alternate Server 2
    address: (none)
    port: 0
Alternate Server 3
    address: (none)
    port: 0
Alternate Server 4
    address: (none)
    port: 0
Alternate Server 5
    address: (none)
    port: 0
```

Loading/Deleting the Server Certificate

1. **Execute the showldapssl command to display the server certificate information.**

```
XSCF> showldapssl cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

XSCF> showldapssl cert -i
Alternate Server 1:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

Alternate Server 2:
... <snip>
```

```
Alternate Server 5:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

2. **Execute the setldapssl command to load the serve certificate to the XSCF.**
   In the following example, the server certificate of the primary server is loaded using the user name and password.

```
XSCF> setldapssl loadcert -u yoshi http://domain_3/UID_2333/testcert
Warning: About to load certificate for Primary Server.
Continue? [y|n]: y
Password:
```

In the following example, the content of the certificate is copied and pasted on the screen, and then the certificate for the alternate server 1 is loaded from a console. After pressing the [Enter] key, press the [Ctrl] and [D] keys to complete loading.

```
XSCF> setldapssl loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:
-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
[Enter]
[Ctrl]+[D]
```

3. **Execute the showldapssl command, and confirm that the server certificate is loaded.**

```
XSCF> showldapssl cert
Primary Server:
certstatus = certificate present
issuer = DC = local, DC = xscf, CN = apl
serial number = 55:1f:ff:c4:73:f7:5a:b9:4e:16:3c:fc:e5:66:5e:5a
subject = DC = local, DC = xscf, CN = apl
valid from = Mar 9 11:46:21 2010 GMT
valid until = Mar 9 11:46:21 2015 GMT
version = 3 (0x02)

XSCF> showldapssl cert -i 1
```

```
Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = aplle, CN = aplle.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = aplle, CN = aplle.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)
```

4. **Execute the setldapssl command to delete the primary server certificate.**

```
XSCF> setldapssl rmcert
Warning: About to delete certificate for Primary Server.
Continue? [y|n]: y
```

5. **Execute the showldapssl command, and confirm that the server certificate has been deleted.**

```
XSCF> showldapssl cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

The strictcertmode must be in the disabled state for a certificate to be removed.

Enabling/Disabling the usermapmode

1. **Execute the showldapssl command to display whether the usermapmode is enabled or disabled.**

```
XSCF> showldapssl
usermapmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Execute the setldapssl command to enable/disable the usermapmode.**
   In the following example, the usermapmode is enabled.

```
XSCF> setldapssl usermapmode enable
```

In the following example, the usermapmode is disabled.

```
XSCF> setldapssl usermapmode disable
```

3. **Execute the showldapssl command to confirm that the usermapmode is enabled/disabled.**
   In the following example, the usermapmode is enabled.

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Setting or Clearing the usermap

1. **Execute the showldapssl command to display the configuration of the usermap.**

```
XSCF> showldapssl usermap
attributeInfo: (none)
binddn: (none)
bindpw: (none)
searchbase: (none)
```

2. **Execute the setldapssl command to configure the usermap.**
   In the following example, attribute information is set.

```
XSCF> setldapssl usermap attributeInfo '(&(objectclass=person)(uid=))'
```

   In the following example, the bind DN is set.

```
XSCF> setldapssl usermap binddn CN=SuperAdmin,DC=aCompany,DC=com
```

   In the following example, the bind password is set.

```
XSCF> setldapssl usermap bindpw b.e9s#n
```

   In the following example, the search base is set.

```
XSCF> setldapssl usermap searchbase OU=yoshi,DC=aCompany,DC=com
```

3. **Execute the showldapssl command, and confirm the usermap.**

```
XSCF> showldapssl usermap
attributeInfo: (&(objectclass=person)(uid=))
binddn: CN=SuperAdmin,DC=aCompany,DC=com
bindpw: Set
searchbase: OU=yoshi,DC=aCompany,DC=com
```

4. **Execute the setldapssl command to clear the usermap.**
   In the following example, attribute information is cleared.

```
XSCF> setldapssl usermap attributeInfo
```

   In the following example, the bind DN is cleared.

```
XSCF> setldapssl usermap binddn
```

   In the following example, the bind password is cleared.

```
XSCF> setldapssl usermap bindpw
```

   In the following example, the search base is cleared.

```
XSCF> setldapssl usermap searchbase
```

5. **Execute the showldapssl command, and confirm that the usermap is cleared.**

```
XSCF> showldapssl usermap
attributeInfo: (none)
binddn: (none)
bindpw: (none)
searchbase: (none)
```

   The usermapmode must be enabled to use the usermap.

Enabling/Disabling the strictcertmode

1. **Execute the showldapssl command to display whether the strictcertmode is enabled or disabled.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
```

```
logdetail: none
```

2. **Execute the setldapssl command to enable/disable the strictcertmode.**
   In the following example, the strictcertmode is enabled.

```
XSCF> setldapssl strictcertmode enable
```

   In the following example, the strictcertmode is disabled.

```
XSCF> setsetldapssl strictcertmode disable
```

3. **Execute the showldapssl command, and confirm that the strictcertmode is enabled/disabled.**
   In the following example, the strictcertmode is enabled.

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

   To enable the strictcertmode, the server certificate must have already been loaded to the XSCF.

Setting a User Domain

1. **Execute the showldapssl command to display user domains.**

```
XSCF> showldapssl userdomain
domain 1: (none)
domain 2: (none)
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

2. **Execute the setldapssl command to set user domains.**
   In the following example, user domain 1 is set.

```
XSCF> setldapssl userdomain -i 1 '@davidc.example.aCompany.com'
```

   In the following example, user domain 2 is set.

```
XSCF> setldapssl userdomain -i 2 'CN=<USERNAME>,CN=Users,DC=davidc,DC=example,
DC=aCompany,DC=com'
```

3. **Execute the showldapssl command, and confirm the user domains.**

```
XSCF> showldapssl userdomain
domain 1: <USERNAME>@davidc.example.aCompany.com
domain 2: CN=<USERNAME>,CN=Users,DC=davidc,DC=example,
DC=aCompany,
DC=com
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

Setting the Default Privilege

1. **Execute the showldapssl command to display the default privilege.**

```
XSCF> showldapssl defaultrole
Default role: (none)
```

2. **Execute the setldapssl command to set a default privilege.**

```
XSCF> setldapssl defaultrole platadm platop
```

3. **Execute the showldapssl command, and confirm the default privilege.**

```
XSCF> showldapssl defaultrole
Default role: platadm platop
```

Setting Group Names and Privileges

1. **Execute the showldapssl command to display group names.**
   The following example shows administrator groups.

```
XSCF> showldapssl group administrator
Administrator Group 1
    name: (none)
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
```

```
Administrator Group 5
    name: (none)
```

The following example shows operator groups.

```
XSCF> showldapssl group operator
Operator Group 1
    name: (none)
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)
```

The following example shows custom groups.

```
XSCF> showldapssl group custom
Custom Group 1
    name: (none)
    roles: (none)
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
Custom Group 5
    name: (none)
    roles: (none)
```

2. **Execute the setldapssl command to set group names and privileges.**
   In the following example, administrator group 1 is set.

```
XSCF> setldapssl group administrator -i 1 name CN=SpSuperAdmin,OU=Groups,
DC=davidc,DC=example,DC=aCompany,DC=com
```

In the following example, operator group 1 is set.

```
XSCF> setldapssl group operator -i 1 name CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
```

In the following example, custom group 1 is set.

```
XSCF> setldapssl group custom -i 1 name CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
```

In the following example, the privilege of the custom group 1 is set.

```
XSCF> setldapssl group custom -i 1 roles platadm,platop
```

3. **Execute the showldapssl command, and confirm the group names and privileges.**
   In the following example, the administrator groups are confirmed.

```
XSCF> showldapssl group administrator
Administrator Group 1
    name: CN=<USERNAME>,CN=SpSuperAdmin,OU=Groups,DC=davidc,
DC=example,DC=aCompany,DC=com
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)
```

In the following example, the operator groups are confirmed.

```
XSCF> showldapssl group operator
Operator Group 1
    name: CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)
```

In the following example, the custom groups are confirmed.

```
XSCF> showldapssl group custom
Custom Group 1
    name: CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
    roles: platadm platop
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
```

```
Custom Group 5
    name: (none)
    roles: (none)
```

The administrator group has platadm, useradm, and auditadm privileges. These privileges cannot be changed. The operator group also has platop and auditop privileges. These privileges cannot be changed.

Setting a Timeout

1. **Execute the showldapssl command to display the timeout time.**

```
XSCF> showldapssl
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

2. **Execute the setldapssl command to set the timeout time.**
   In the following example, the timeout time is set to 10 seconds.

```
XSCF> setldapssl timeout 10
```

3. **Execute the showldapssl command, and confirm the timeout time.**

```
XSCF> showldapssl
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

Enabling or Disabling the Logs of LDAP over SSL Authentication and Authorization Diagnosis Messages

1. **Execute the showldapssl command to display the log detail level.**

```
XSCF> showldapssl
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
```

```
timeout: 10
logdetail: none
```

2. **Execute the setldapssl command to set the log detail level.**
   In the following example, the log is enabled and the log detail level is set to trace.

```
XSCF> setldapssl logdetail trace
```

In the following example, the log is disabled.

```
XSCF> setldapssl logdetail none
```

3. **Execute the showldapssl command, and confirm the log detail level.**
   In the following example, the log detail level is set to trace.

```
XSCF> showldapssl
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

Displaying the Log of Diagnosis Messages and Clearing the Log File

1. **Execute the showldapssl command to display the log detail level.**

```
XSCF> showldapssl
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Execute the showldapssl command to display the diagnosis messages.**
   In the following example, diagnosis messages are displayed in real time.

```
XSCF> showldapssl log -f
Mon Nov 16 14:47:53 2009 (LdapSSL): module loaded, OPL
Mon Nov 16 14:47:53 2009 (LdapSSL): --error-- authentication status:
auth-ERROR
Mon Nov 16 14:48:18 2009 (LdapSSL): module loaded, OPL
```

3. **Execute the setldapssl command to clear the log file of diagnosis messages.**

```
XSCF> setldapssl log clear
Warning: About to clear log file.
Continue? [y|n]: y
```

Resetting the LDAP over SSL Settings to Their Defaults

1. **Execute the showldapssl command to display the setting status of the LDAP over SSL.**

```
XSCF> showldapssl
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Execute the setldapssl command to reset the LDAP over SSL settings to their defaults.**

```
XSCF> setldapssl default -y
Warning: About to reset settings to default.
Continue? [y|n]: y
```

3. **Execute the showldapssl command, and confirm that the LDAP over SSL settings are reset to their defaults.**

```
XSCF> showldapssl
dnslocatormode: disabled
expsearchmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Logging In With the LDAP over SSL User Account

After completing each setting, confirm whether login with the user account of LDAP over SSL is possible.

3.6 Setting the XSCF Time/Date

This section describes how to set the time of this system. The system uses the XSCF clock as the reference time for all physical partitions.

The XSCF can be configured to operate as an NTP server or NTP client too. If the XSCF is not configured as an NTP client, the built-in Realtime Clock (RTC) of each chassis of the SPARC M12/M10 is used for the XSCF time. To change the XSCF time in this case, use the setdate command.

Figure 3-1 shows some examples of operating schemes related to the time on this system. In example 1, the XSCF and the logical domain are running as NTP clients. In example 2, the XSCF is operating as an NTP client and as an NTP server.

Figure 3-1   Examples of Operating Schemes Related to Time
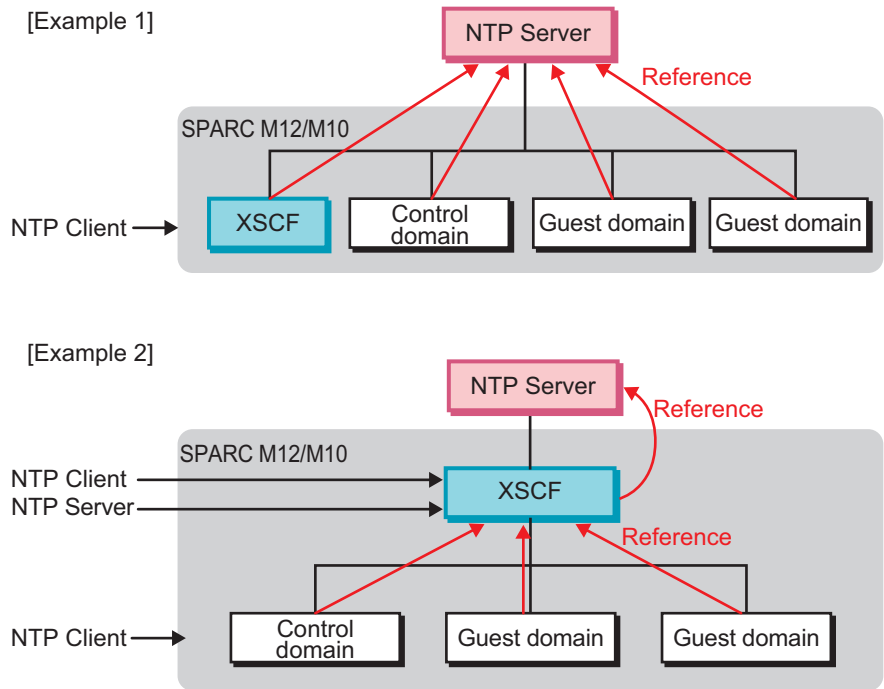
Note - The customer is requested to determine the NTP server operating scheme. For details of NTP, see NTP-related manuals.

3.6.1 Understanding the Relationship Between the XSCF and Physical Partition Times

The XSCF maintains the time difference between XSCF and the physical partition. This prevents the time difference between the logical domains and XSCF from changing, even when the physical partition is reset. Even if the time of the XSCF is changed by executing the setdate command on the XSCF firmware, the time difference between the physical partition and XSCF is maintained.

The XSCF time and physical partition time are managed in the following manner.

- When the power of the physical partition is on, the information on the time difference between the XSCF and physical partition is added to the XSCF time, and this value is set as the physical partition hardware time (TOD).

- At Oracle Solaris boot, the logical domain time is set based on the physical partition hardware time (TOD).

Figure 3-2   Setting the Time for the XSCF and the Logical Domain

TOD: Time Of Day
OVM: Oracle VM Server for SPARC
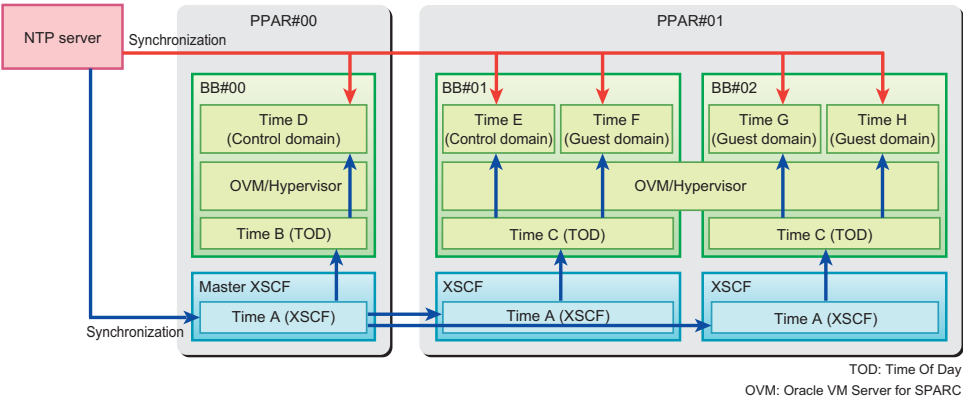
Note - Do not use the resetdateoffset command, except at the initial configuration of a physical partition, because it affects the time control mentioned above. The resetdateoffset command is used at the initial configuration of the physical partition only.
For the usage of the resetdateoffset command at the initial configuration of a physical partition, see the *Installation Guide* for your server.

3.6.2 Time Management Policy of a Logical Domain

You can set individual time management policies for logical domains. As a result, time can be managed in different ways by logical domain. Domain time management policies are described below.

- The time at logical domain startup is set based on the XSCF time.

- A logical domain can be configured as an NTP client of an external NTP server. In this case, after the initial time of the logical domain is set based on the XSCF time, it is synchronized with the NTP server.

- A logical domain can be configured as an NTP client of the XSCF that is acting as an NTP server. In this case, the time at logical domain startup synchronizes with the XSCF time.

- If the time is set on a logical domain by the date command of Oracle Solaris, the time difference between the logical domain and physical partition is maintained after a reboot.

Note - To synchronize time by using NTP, specify the same NTP server for the logical domains that are in the same physical partition. For details on how to specify the NTP server in a domain, see the *Oracle Solaris Administration: Network Services* (Oracle Solaris 10) or *Introduction to Oracle Solaris 11 Network Services* (Oracle Solaris 11).

3.6.3 Checking the Time-related Setting Items and Commands

Table 3-18 lists the time-related setting items and the corresponding XSCF shell commands.

Table 3-18   Time-related Setting Items

Setting Item	Required or Optional Setting	Related Command
Time zone	Optional	settimezone(8), showtimezone(8)
Daylight saving time	Optional	settimezone(8), showtimezone(8)
System time	Required	setdate(8), showdate(8)
NTP server	Optional	setad(8), showad(8)
DNS round-robin	Optional	setad(8), showad(8)
Prefer, stratum	Optional	setad(8), showad(8)
Local clock	Optional	setad(8), showad(8)

3.6.4 Setting the Time Zone

To check the time zone that is set, execute the showtimezone command with the -c tz option specified. To set the time zone, use the settimezone command. By specifying the -a option with the settimezone command, you can list the standard time zones that can be set. Execute the settimezone command with a user account that has the platadm or fieldeng privilege.

The time zones prepared as standard comply with the POSIX standard. The standard

time zone list may be modified annually.

1. **Execute the showtimezone command to display the time zone.**

```
XSCF> showtimezone -c tz
America/Chicago
```

2. **Execute the settimezone command to set the XSCF time zone.**
   In the following example, the -c settz and -a options are specified to display a list of time zones.

```
XSCF> settimezone -c settz -a
Africa/Abidjan
Africa/Accra
:
Asia/Thimphu
Asia/Tokyo
Asia/Ujung_Pandang
:
Europe/Lisbon
Europe/Ljubljana
Europe/London
 :
```

The following example sets Asia/Tokyo as the time zone.

```
XSCF> settimezone -c settz -s Asia/Tokyo
Asia/Tokyo
```

3. **Execute the showtimezone command, and confirm the setting.**

Note - The time zone (region/geographical name) supported by XSCF may be changed to support the latest time zone information.
If the previously-set time zone becomes unavailable on the system, XSCF operates by switching from the unavailable time zone to the coordinated universal time (UTC).
If the set time zone is changed to operate with UTC, execute the settimezone -c settz -a command to check which time zones can be specified. If the time zone list does not include the time zone you previously set, reset the time zone.

3.6.5 Setting Daylight Saving Time

To check or set daylight saving time information, use the showtimezone and settimezone commands.

1. **Execute the showtimezone command to display the time zone.**
   The following example displays the time zone.

```
XSCF> showtimezone -c tz
Asia/Tokyo
```

The following example displays the set daylight saving time information. In this example, the time zone is JST, the offset from GMT is +9 hours, the daylight saving time name is JDT, daylight saving time is 1 hour ahead, and the period is from 2:00 (JST) on the last Sunday in March to 2:00 (JDT) on the last Sunday in October.

```
XSCF> showtimezone -c dst -m custom
JST-9JDT,M3.5.0,M10.5.0
```

2. **Execute the settimezone command to set daylight saving time information for the XSCF.**
   The following example sets the following daylight saving time information: the time zone abbreviation is JST, the offset from GMT is +9 hours, the daylight saving time name is JDT, the offset from GMT daylight saving time is +10 hours, and the period is from 0:00 (JST) on the first Sunday in April to 0:00 (JDT) on the first Sunday in September.

```
XSCF> settimezone -c adddst -b JST -o GMT-9 -d JDT -p GMT-10 -f
M4.1.0/00:00:00 -t M9.1.0/00:00:00
JST-9JDT-10,M4.1.0/00:00:00,M9.1.0/00:00:00
```

The following example deletes the currently set daylight saving time information.

```
XSCF> settimezone -c deldst -b JST -o GMT-9
```

To apply the daylight saving time information changed by the -c adddst or -c deldst option, log out and then log in again.

3. **Execute the showtimezone command, and confirm the setting.**

3.6.6 Setting the System Time

Set the local time or coordinated universal time (UTC) for the XSCF clock date and time. After the time is set, the XSCF is rebooted.
To confirm the date and time of the XSCF clock, use the showdate command. Use the setdate command to set the date and time of the XSCF clock. Execute the setdate command with a user account that has the platadm or fieldeng privilege.

Note - The system time is set during initial installation.

---

1. **Execute the showdate command to display the XSCF time.**
   The following example displays the current time in the local time.

```
XSCF> showdate
Mon Jan 23 14:53:00 JST 2012
```

In the following example, the -u option is specified to display the current time in UTC.

```
XSCF> showdate -u
Mon Jan 23 05:56:15 UTC 2012
```

2. **Execute the setdate command to set the time.**
   The following example specifies the current time as local time 16:59:00 January 27, 2012.

```
XSCF> setdate -s 012716592012.00
Fri Jan 27 16:59:00 JST 2012
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2012
```

The following example specifies the current time as UTC 07:59:00 January 27, 2012.

```
XSCF> setdate -u -s 012707592012.00
Fri Jan 27 07:59:00 UTC 2012
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2012
```

The XSCF is rebooted when the time is set. The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

Note - If the input power was turned off and maintenance work was done, be sure to confirm the XSCF time with the showdate command after the input power is turned on. If it does not match the current time, set it to the current time with the setdate command.

3.6.7 Synchronizing the Control Domain Time and XSCF Time

This section describes the following two methods of synchronizing the control domain time and XSCF time after the control domain time has been set by the date command of Oracle Solaris:

- Setting the XSCF as the NTP server of the control domain
- Setting the same NTP server for the control domain and the XSCF

Setting the XSCF as the NTP Server of the Control Domain

1. **Set the XSCF to be the NTP server.**
   For details, see "3.6.8   Specifying the XSCF as an NTP Server."

2. **Specify the ID of the target physical partition and execute the console command to switch to the control domain console of the target physical partition.**

```
XSCF> console -p xx
```

3. **Specify the XSCF as the NTP server of the control domain.**
   For details of the NTP server settings of Oracle Solaris, see the *Oracle Solaris Administration: Network Services* (Oracle Solaris 10) or *Introduction to Oracle Solaris 11 Network Services* (Oracle Solaris 11).

4. **Reboot the control domain.**

5. **Execute the date command of Oracle Solaris to display the time of the control domain.**

6. **From the control domain console of the physical partition, press #. or another escape command to return to the XSCF shell.**

7. **Execute the showdate command to display the XSCF time, and confirm that the time of the control domain of the target physical partition is the same as the XSCF time.**

Specifying the Same NTP Server for the Control Domain and the XSCF

1. **Configure the XSCF as an NTP client.**
   For details, see "3.6.9   Specifying the XSCF as an NTP Client."

2. **Register an external NTP server with the XSCF.**
   For details of the NTP server settings of the XSCF, see "3.6.10   Configuring the NTP Servers Used by the XSCF."

3. **Specify the ID of the target physical partition and execute the console command to switch to the control domain console of the target physical partition.**

```
XSCF> console -p xx
```

4. **Specify the same external NTP server for the control domain as that of the XSCF.**
   For details of the NTP server settings of Oracle Solaris, see the *Oracle Solaris Administration: Network Services* (Oracle Solaris 10) or *Introduction to Oracle Solaris 11 Network Services* (Oracle Solaris 11).

5. **Reboot the control domain.**

6. **Execute the date command of Oracle Solaris to display the time of the control domain.**

7. **From the control domain console of the physical partition, press #. or another escape command to return to the XSCF shell.**

8. **Display the XSCF time with the showdate command, and confirm that the time of the control domain of the target physical partition is the same as the XSCF time.**

Note - By also specifying the same NTP server for guest domains as that of the XSCF and control domain, you can synchronize the times of all domains with the XSCF.

3.6.8 Specifying the XSCF as an NTP Server

Configure the XSCF as the NTP server providing the NTP service to other clients. By default, the XSCF does not act as an NTP server providing the service to other clients.

Use the showntp command to check the NTP information of an XSCF network. To have the XSCF act as an NTP server and provide the NTP service, use the setntp command with the -s server option specified. Execute the setntp command with a user account that has the platadm privilege.

1. **Execute the showntp command to display the NTP service status of the XSCF.**

```
XSCF> showntp -a
client : disable
server : disable
```

2. **Execute the setntp command to configure the XSCF as an NTP server to provide the service to other clients.**
   In the following example, the -s server and -c enable options are specified so that the XSCF is configured to act as an NTP server and provide the NTP service.

```
XSCF> setntp -s server -c enable
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Execute the rebootxscf command to reboot the XSCF.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

4. **Execute the showntp command, and confirm that the XSCF is configured as the NTP server.**

```
XSCF> showntp -a
client : disable
server : enable
```

3.6.9   Specifying the XSCF as an NTP Client

To have the XSCF use an NTP server, configure the XSCF as an NTP client. By default, the XSCF does not act as an NTP client obtaining the time from an NTP server. To configure the XSCF as an NTP client, use the setntp command with the -s client option specified.

1. **Execute the showntp command to display the XSCF status as an NTP client.**

```
XSCF> showntp -a
client : disable
server : enable
```

2. **Execute the setntp command to configure the XSCF as an NTP client.**

```
XSCF> setntp -s client -c enable
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Execute the rebootxscf command to reboot the XSCF.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

4. **Execute the showntp command, and confirm that the XSCF is configured as the NTP client.**

```
XSCF> showntp -a
client : enable
server : enable
```

Note - If the time difference between the XSCF and the NTP server reaches 1000 seconds (about 17 minutes) or more, the ntp daemon of the client XSCF stops. As a result, time synchronization with the NTP server becomes impossible. To check whether the ntp daemon is stopped, execute the showntp -l command. If "NTP is unavailable." appears, then the daemon is stopped.
To restart the ntp daemon, execute the rebootxscf command, which reboots the XSCF.

■ **When the ntp daemon is stopped**

```
XSCF> showntp -l
XSCF> NTP is unavailable.
```

■ **When the ntp daemon is operating**

```
XSCF> showntp -l
remote          refid     st t when poll reach delay  offset jitter
==============================================================================
*192.168.10.10 10.0.20.20 4 u 805 1024  377   19.429 0.083  0.917
127.127.1.0    .LOCL.     5 l 7   64     377   0.000  0.000  0.008
XSCF>
```

3.6.10　Configuring the NTP Servers Used by the XSCF

Up to three NTP servers can be registered to obtain the XSCF time from a high-level NTP server. To register an NTP server, use the setntp command with the -c add option specified.
At this time, the XSCF must be configured as an NTP client. For details on how to configure the XSCF as an NTP client, see "3.6.9　Specifying the XSCF as an NTP Client."
When an NTP server is registered, existing settings are deleted or overwritten with those of the specified NTP server. To specify an NTP server by its host name, DNS servers must be able to resolve the server name.

1. **Execute the showntp command to display the NTP servers used with the XSCF network.**

```
XSCF> showntp -a
client : disable
server : enable

server ntp1.example.com prefer
server ntp2.example.com
```

2. **Execute the showntp command to check synchronization and display the status.**

```
XSCF> showntp -l
remote          refid      st t when poll reach delay offset jitter
=====================================================================
*192.168.0.27 192.168.1.56 2 u  27   64  377 12.929 -2.756  1.993
+192.168.0.57 192.168.1.86 2 u  32   64  377 13.030  2.184 94.421
127.127.1.0    .LOCL.      5 l  44   64  377  0.000  0.000  0.008
```

3. **Execute the setntp command to add an NTP server.**
   The following example adds the following three IP addresses as high level NTP servers for the XSCF: 192.168.1.2, 130.34.11.111, and 130.34.11.117.

```
XSCF> setntp -c add 192.168.1.2 130.34.11.111 130.34.11.117
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

The following example adds the following two host names as high level NTP servers for the XSCF: ntp1.red.com and ntp2.blue.com.

```
XSCF> setntp -c add ntp1.red.com ntp2.blue.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

4. **Execute the setntp command to delete an NTP server of XSCF.**
   The following example deletes ntp2.example.com, which is an NTP server for the XSCF.

```
XSCF> setntp -c del ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

5. **Execute the rebootxscf command to reboot the XSCF to reflect the settings made.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

6. **Execute the showntp command, and confirm the NTP servers.**

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.red.com prefer
server ntp2.blue.com
```

3.6.11   Configuring the DNS Round-Robin of the NTP Server

If you have registered the NTP server by using the host name, you can use DNS round-robin with that host name. To use DNS round-robin, use the setntp command with the -c pool option specified. In advance of this time, the NTP server that you want to configure must be registered with the XSCF. For details on how to register the NTP server, see "3.6.10   Configuring the NTP Servers Used by the XSCF."

1. **Execute the showntp command to display the DNS round-robin settings.**

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.example.com prefer
server ntp2.example.com
```

2. **Execute the setntp command to configure DNS round-robin.**
   The following example shows the NTP server with DNS round-robin enabled.

```
XSCF> setntp -c pool ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

   The following example shows the NTP server with DNS round-robin disabled.

```
XSCF> setntp -c server ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Execute the rebootxscf command to reboot the XSCF to reflect the settings made.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

   The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

4. **Execute the showntp command to display the DNS round-robin settings.**
   The following example shows the ntp2.example.com with DNS round-robin enabled.

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.example.com prefer
pool ntp2.example.com
```

3.6.12 Specifying/Canceling prefer for an NTP Server

If multiple NTP servers are configured, the -m prefer=on specification gives priority to the NTP server registered first by the setntp command when synchronizing the NTP servers. From this point in time, the registered server with DNS round-robin enabled will be excluded from synchronization. By default, the prefer option is set to "on (enabled)."

1. **Execute the showntp command to display the prefer setting.**

```
XSCF> showntp -m
prefer : on
localaddr : 0
```

2. **Execute the setntp command to set prefer.**
   The following example specifies prefer for the NTP servers.

```
XSCF> setntp -m prefer=on
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

   The following example cancels the prefer specification for the NTP servers.

```
XSCF> setntp -m prefer=off
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Execute the rebootxscf command to reboot the XSCF to reflect the settings made.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

   The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

4. **Execute the showntp command, and confirm the prefer setting.**
   The following example cancels the prefer specification.

```
XSCF> showntp -m
prefer : off
localaddr : 0
```

   The following example does not specify prefer.

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.red.com
server ntp2.blue.com
```

3.6.13   Setting the stratum Value of the XSCF

To set a stratum value for the XSCF, use the setntp command with the -c stratum option specified. Any value from 1 to 15 can be specified as the stratum value. The default is 5.

1. **Execute the showntp command to display the set stratum value for the XSCF network.**

```
XSCF> showntp -s
stratum : 5
```

2. **Execute the setntp command to change the stratum value.**
The following example sets 7 as the stratum value used in the XSCF network.

```
XSCF> setntp -c stratum -i 7
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Execute the rebootxscf command to reboot the XSCF to reflect the settings made.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The session is disconnected at this time. Reconnect with a new interface, and log in again.

4. **Execute the showntp command, and confirm the stratum value.**

```
XSCF> showntp -s
stratum : 7
```

3.6.14 Changing the Clock Address of the XSCF Local Clock

Set the clock address of the local clock of the XSCF itself. You can specify a value from 0 to 3 for the least significant byte of the clock address of the local clock. The default clock address of the local clock is 127.127.1.0.

1. **Execute the showntp command to display the clock address of the local clock of the XSCF itself.**

```
XSCF> showntp -m
prefer : on
localaddr : 0

XSCF> showntp -l
remote          refid        st t when poll reach  delay  offset  jitter
==============================================================================
*192.168.0.27 192.168.1.56   2 u   27   64   377 12.929  -2.756   1.993
+192.168.0.57 192.168.1.86   2 u   32   64   377 13.030   2.184  94.421
127.127.1.0    .LOCL.         5 l   44   64   377  0.000   0.000   0.008
```

2. **Execute the setntp command to change the clock address of the local clock of the XSCF itself.**
   The following example sets 1 as the least significant byte of the clock address.

```
XSCF> setntp -m localaddr=1
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Execute the rebootxscf command to reboot the XSCF to reflect the settings made.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF session is disconnected at this time. Reconnect to the XSCF, and log in again.

4. **Execute the showntp command to display the clock address of the local clock of the XSCF.**

```
XSCF> showntp -m
prefer : on
localaddr : 1

XSCF> showntp -l
remote           refid        st t when poll reach  delay  offset  jitter
==========================================================================
*192.168.0.27 192.168.1.56    2 u   27   64   377 12.929  -2.756   1.993
+192.168.0.57 192.168.1.86    2 u   32   64   377 13.030   2.184  94.421
127.127.1.1   .LOCL.          5 l   44   64   377  0.000   0.000   0.008
```

Notes About NTP Servers Referencing the Local Clock

Suppose the XSCF refers to an NTP server that refers to the system time (local clock) of the server itself, and "127.127.1.0" is the set address of this local clock. In this case, time synchronization with the XSCF may be not be possible.

The address of the local clock of the XSCF itself is fixed at "127.127.1.0." So if the XSCF refers to an NTP server whose local clock has the set address of "127.127.1.0," the address of the clock source (refid) is the same as that of the local clock of the XSCF itself. Such an NTP server is not subject to XSCF time synchronization.

By executing the showntp -l command, you can display the address of the clock source of each NTP server itself as configured on the XSCF, and the address of the local clock of the XSCF itself.

```
XSCF> showntp -l
remote           refid        st t when poll reach  delay  offset  jitter
==========================================================================
192.168.1.2   LOCAL(0)        3 u   10 1024   377  0.000   0.000   0.000
```

```
*127.127.1.0   .LOCL.        5 l   28   64   377  0.000   0.000   0.008
```

Of the two NTP servers in the output, the first server (192.168.1.2) is the NTP server configured by the setntp command. The refid of this NTP server is LOCAL(0), so the set clock source of the NTP server is the local clock whose address is "127.127.1.0." The source of the second server is the local clock of the XSCF itself. The address of the local clock of the XSCF itself is fixed at "127.127.1.0." Since the NTP server (192.168.1.2) is not subject to XSCF time synchronization, the result is that the XSCF synchronizes the time to its own local clock.

By taking any of the following measures to prevent problems, you can have the time correctly synchronized with the NTP servers configured by the setntp command.

- Change the clock sources referenced by the NTP servers configured for the XSCF.
  Use the showntp -l command to check the clock sources of the NTP servers configured for the XSCF. The NTP server whose refid is LOCAL(0), as output above, refers to the local clock whose address is "127.127.1.0." Therefore, make a change such that the server refers to another clock source. Before changing the clock source of an NTP server, confirm that the change does not affect other NTP clients.

- Change the address of the local clock of the NTP server.
  Change the address of the local clock of the NTP server referenced by the XSCF to "127.127.1.1," "127.127.1.2," or "127.127.1.3." Modify /etc/inet/ntp.conf of Oracle Solaris. To apply the changes, restart the ntp daemon. Before changing the address of the local clock of an NTP server, confirm that the change does not affect other NTP clients.

- Change the stratum value of an NTP server.
  Change the stratum value of the NTP server referenced by the XSCF to 1. The NTP server with the stratum value of 1 is the most significant clock source and has no refid. Therefore, its address is never the same as the address of the local clock of the XSCF itself. Before changing the stratum value of an NTP server, confirm that the change does not affect other NTP clients.

- Change the address of the local clock of the XSCF itself.
  Use the setntp -m localaddr=value command to change the address of the local clock of the XSCF itself. For value, specify the least significant byte of the local clock address "127.127.1.x." You can specify a numeric value from 0 to 3. If the value specified for value is between 1 and 3, the address of the NTP server that refers to the local clock no longer matches the address of the XSCF internal local clock. As a result, even a server that refers to the local clock can be configured as an NTP server for the XSCF.

3.7 Configuring the SSH/Telnet Service for Login to the XSCF

This section describes how to configure the SSH service and Telnet service. To use the

XSCF shell terminal and the control domain console of the specified physical partition, use SSH or Telnet. Enable/Disable SSH and Telnet, set the SSH host key, and set the auto timeout time for logged-in users. Also, register the SSH user public key with the XSCF.

SSH and Telnet can be concurrently enabled. However, communications that use the Telnet service cannot be considered as being secure. We recommend disabling the Telnet service when an SSH service is enabled.

SSH Client

This system can use the SSH function with the following client software:

- Oracle Solaris Secure Shell
- OpenSSH
- PuTTY
- UTF-8 TeraTerm Pro with TTSSH2

For the software terms of use, see the respective software manuals.

Port Number

The SSH port number is 22, and the Telnet port number is 23.

User Public Key

To use an SSH user key through an XSCF-LAN connection, create a user secret key and user public key for a registered XSCF user account on the client PC, and register the user public key with the XSCF.
To display, register, or delete an SSH user public key after specifying a user name, the useradm user privilege is required.

Note - For UTF-8 TeraTerm Pro with TTSSH2 4.66 or later, 2048-bit DSA is not supported for user public keys.

Console

The SPARC M12/M10 systems can be used with a writable (RW) or reference only (RO) control domain console for a physical partition. You can use one RW console per physical partition. Use the console command to use the control domain console. For details on the console, see "Chapter 2   Logging In/Out of the XSCF."

3.7.1   Checking the Setting Items and Commands Related to SSH and Telnet

Table 3-19 lists the setting items related to SSH and Telnet and the corresponding XSCF shell commands.

Table 3-19	Setting Items Related to SSH and Telnet		
Setting Item	Required or Optional Setting	Related Command	
Enabling/Disabling SSH	Optional	setssh(8), showssh(8)	
Generating a host key	Optional	setssh(8), showssh(8)	
Registering/Deleting a user public key	Optional	setssh(8), showssh(8)	
Enabling/Disabling Telnet	Optional	settelnet(8), showtelnet(8)	
Timeout time	Optional	setautologout(8), showautologout(8)	

3.7.2 Enabling/Disabling the SSH and Telnet Services

To confirm the SSH service and Telnet service set for the XSCF network, use the showssh command and showtelnet command. Also, to set the SSH service or Telnet service, use the setssh command or settelnet command.

When using the setssh command or settelnet command to enable/disable the SSH service or Telnet service, the setting is reflected immediately after the command is executed.

1. **Execute the showssh command to display the SSH settings, or execute the showtelnet command to display the Telnet settings.**
   The following example displays the SSH service settings.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
W9pqa/WxC21Ja4RQVN3009kmVwAAAIAON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzzFFj5XUzQBdabh5p5Rwz+1vriawFIZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
```

```
/etc/ssh/ssh_host_dsa_key.pub
```

The following example displays the Telnet service settings.

```
XSCF> showtelnet
Telnet status: disabled
```

2. **Execute the setssh command to configure the SSH service, or execute the settelnet command to configure the Telnet service.**
   The following example specifies that the SSH service be enabled.

```
XSCF> setssh -c enable
Continue? [y|n] :y
```

The following example specifies that the Telnet service be disabled.

```
XSCF> settelnet -c disable
Continue? [y|n] :y
```

3.7.3 Setting an SSH Service Host Key

To enable and start using the SSH service, first generate a host key.
When using the SSH service through an XSCF-LAN connection, make a note of the fingerprint. Copy the text data of the generated host public key to a file in a given directory on the client.

1. **Execute the showssh command to display the host key and fingerprint.**
   A host key is generated when enabling the SSH service for the first time.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
```

```
W9pqa/WxC21Ja4RQVN3009kmVwAAAIAON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzzFFj5XUzQBdabh5p5Rwz+1vriawFIZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

2. **Execute the setssh command to generate a host key.**
   In the following example, a host key is generated and used to replace the
   existing one.

```
XSCF> setssh -c genhostkey
Host key already exits. The key will be updated. Continue? [y|n]
 : y
```

3.7.4   Registering/Deleting a User Public Key for the SSH Service

To use an SSH service user key through an XSCF-LAN connection, create a user
secret key and user public key for a registered XSCF user account on the client PC,
and register the user public key with the XSCF.

1. **Execute the showssh command to display user public keys.**
   In the following example, the -c pukey option is specified to display the user
   public key. However, no response is returned because no user key has been
   registered.

```
XSCF> showssh -c pubkey
```

2. **Create a user secret key and user public key for a registered XSCF user**
   account on the client.
   For details on how to create the user key and how to specify a passphrase on the
   client, see the manual of the client software being used. We recommend setting a
   passphrase.

3. **To register the user public key, execute the setssh command with the -c**
   addpubkey option specified, copy the user public key created in step 2, and
   paste it in the window.
   After pressing the [Enter] key, press the [Ctrl] and [D] keys to complete
   registration.

   The following example registers the user public key for user efgh.

```
XSCF> setssh -c addpubkey -u efgh
Please input a public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
```

```
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
<Press the [Ctrl] and [D] keys>
XSCF>
```

4. **Execute the showssh command, and confirm the user public key and user public key number.**
   The following example shows a user key registered with the number 1.

```
XSCF> showssh -c pubkey
Public key:
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

At the next XSCF shell login, establish an SSH connection from the client PC by using an XSCF user account. Confirm that you can log in to the XSCF shell with authentication using the user key.

5. **To delete a user public key, execute the setssh command with the user public key number specified.**
   In the next example, the -c delpubkey option is specified along with the user public key number specified with the -s option, to delete the user public key.

```
XSCF> setssh -c delpubkey -s 1
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

6. **Execute the showssh command, and confirm that the user public key was deleted.**

```
XSCF> showssh -c pubkey
```

3.7.5   Setting the SSH/Telnet Service Timeout Time

1. **Execute the showautologout command to display the timeout time.**

```
XSCF> showautologout
30min
```

2. **Execute the setautologout command to set the timeout time.**
   The following example sets 255 minutes as the timeout time.

```
XSCF> setautologout -s 255
255min
```

The set timeout time applies from the next login.

3.8 Configuring the HTTPS Service for Login to the XSCF

This section describes how to configure the HTTPS service.
The HTTPS service settings are configured for use of XSCF Web with a connection to the XSCF-LAN and for use of a Web browser window. Use the settings described here to enable/disable HTTPS and use HTTPS. HTTPS is disabled by default in these systems. The XSCF Web console can be a secure console.

Selecting a Certificate Authority

Considering the customer's system and Web browser environment, select one of the following certificate authorities:

- External certificate authority
- Intranet certificate authority
- Self-signed certificate authority

If the customer's environment has neither an external certificate authority nor an intranet certificate authority, use the XSCF self-signed certificate authority. (See "3.8.2 Flow When Using a Self-Signed Certificate Authority.")
The XSCF self-signed certificate authority is a self-signed certificate authority configured with the XSCF, and it cannot be used as an external certificate authority for other systems.

Expiration Time of a Self-Signed Certificate

A self-signed certificate has the following fixed expiration time:

- Server certificate: 10 years

After the expiration time of the Web server certificate has elapsed or the Web server certificate has been changed, configure the HTTPS service again.

Distinguished Name (DN)

To create a Web server certificate signing request (CSR), specify the Distinguished Name (DN) as follows:

Note - In the XSCF self-signed certificate authority, the key length for the self-signed certificate used for the signature for a Web server certificate is 2048-bit. The key length cannot be changed.

- 2-letter country code (e.g., US or JP)

- Region
- City
- Organization (company) name, division or section name
- Common name (user name, Web server host name)
- Administrator e-mail address

Except the country code, the above entries have up to 64 characters. For details on the DN, see the sethttps(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.8.1 Flow When Using an External or Intranet Certificate Authority

This section describes the setting flow when using an external certificate authority or intranet certificate authority.

1. **Create an XSCF Web server secret key.**
2. **Create a Web server certificate signing request (CSR) on the XSCF.**
3. **Ask the certificate authority to publish a certificate for the XSCF Web server certificate signing request.**
4. **Import the Web server certificate signed by the certificate authority to the XSCF.**
5. **Enable HTTPS.**

In the above steps 1 to 5, specify their respective options in the sethttps command. If XSCF Web is used for the settings, select the respective setting items.

If the system has multiple XSCFs, the settings are automatically reflected by the standby XSCF.

3.8.2 Flow When Using a Self-Signed Certificate Authority

This section describes the setting flow when using a self-signed certificate authority.

If there is neither a Web server secret key nor a self-signed Web server certificate, you can specify the option "enable" for self-signing in the sethttps command to automatically complete all the settings from steps 1 to 4 at one time.
If there is a Web server secret key and a self-signed Web server certificate, perform the following steps 1 to 4.

1. **Configure the XSCF self-signed certificate authority.**
2. **Generate an XSCF Web server secret key.**
3. **Create a self-signed Web server certificate on the XSCF.**
4. **Enable HTTPS.**

If the system has multiple XSCFs, the settings are automatically reflected by the

standby XSCF.

3.8.3 Checking the HTTPS-related Setting Items and Commands

Table 3-20 lists the HTTPS-related setting items and the corresponding XSCF shell commands.

Table 3-20   HTTPS-related Setting Items

Setting Item	Required or Optional Setting	Related Command
Enabling/Disabling HTTPS	Optional	sethttps(8), showhttps(8)
External certificate - Creating a Web server secret key on the XSCF - Creating a Web server CSR on the XSCF and asking the authority to issue a certificate - Importing a Web server certificate to the XSCF	Optional	sethttps(8), showhttps(8)
Self-signing - Configuring a self-signed certificate authority - Creating a Web server secret key - Creating a self-signed Web server certificate	Optional	sethttps(8), showhttps(8)

3.8.4 Enabling/Disabling the HTTPS Service

To confirm the HTTPS service that is set for the XSCF network, use the shownetwork command. Also, to set the HTTPS service, use the sethttps command. Execute the sethttps command with a user account that has the platadm privilege.

1. **Execute the showhttps command to display the HTTPS service settings.**
    The following example displays the HTTPS service settings.

```
XSCF> showhttps
HTTPS status: enabled
Server key: installed in Apr 24 12:34:56 JST 2006
CA key: installed in Apr 24 12:00:34 JST 2006
CA cert: installed in Apr 24 12:00:34 JST 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIBwjCCASsCAQAwgYExCzAJBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTERMA8G
A1UEBxMIbG9jYWxpdHkxFTATBgNVBAoTDG9yZ2FuaXphdGlvbjEPMA0GA1UECxMG
b3JnYW5pMQ8wDQYDVQQDEwZjb21tb24xFjAUBgkqhkiG9w0BCQEWB2VlLm1haWww
```

```
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5D57X/k42LcipTWBWzv2GrxaVM
5GEyx3bdBW8/7WZhnd3uiZ9+ANlvRAuw/YYy7I/pAD+NQJesBcBjuyj9x+IiJl9F
MrI5fR8pOIywVOdbMPCar09rrU45bVeZhTyi+uQOdWLoX/Dhq0fm2BpYuh9WukT5
pTEg+2dABg8UdHmNAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAux1jH3dyB6Xho
PgBuVIakDzIKEPipK9qQfC57YI43uRBGRubu0AHEcLVue5yTu6G5SxHTCq07tV5g
38UHSg5Kqy9QuWHWMri/hxm0kQ4gBpApjNb6F/B+ngBE3j/thGbEuvJb+0wbycvu
5jrhB/ZV9k8X/MbDOxSx/U5nF+Zuyw==
-----END CERTIFICATE REQUEST-----
```

2. **Execute the sethttps command to configure HTTPS.**
   The following example enables the HTTPS service.

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

   If there is neither a Web server secret key nor a self-signed Web server certificate, this command with "enable" specified automatically configures self-signing, generates a Web server secret key, creates a Web server certificate, and enables HTTPS to complete this work at one time.

   The following example disables the HTTPS service.

```
XSCF> sethttps -c disable
Continue? [y|n] : y
```

3.8.5 Importing a Web Server Certificate Using an External or Intranet Certificate Authority

1. **Execute the sethttps command to generate a Web server secret key.**
   The following example specifies the -c genserverkey to generate a Web server secret key.

```
XSCF> sethttps -c genserverkey
Server key already exists. Do you still wish to update? [y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. **Execute the sethttps command with the DN specified to generate a CSR.**
   The following example specifies the -c gencsr option along with the DN (JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com) to generate a CSR.

```
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example
development scfhost abc@example.com
```

3. **Execute the showhttps command to display the CSR. Copy and save the displayed CSR (BEGIN to END) to a text file.**

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2006
CA key: installed in Jul 11 06:33:21 UTC 2006
CA cert: installed in Jul 11 06:33:21 UTC 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAOBgNVBAoTB0ZVSklUU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IImqKg==
-----END CERTIFICATE REQUEST-----
```

4. **Send the copied CSR to the certificate authority to ask it to publish a Web server certificate.**

5. **To perform the import, execute the sethttps command with -c importca option specified, copy the Web server certificate signed in step 4, and paste it in the window.**
   Press the [Enter] key to import it, and press the [Ctrl] and [D] keys to complete this step.

```
XSCF> sethttps -c importca
Please import a certificate:
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgTELMAkGA1UEBhMCamox
:
R+OpXAVQvb2tjIn3kO99dq+begECo4mwknW1t7QI7A1BkcW2/MkOolIRa6iP1Zwg
JoPmwAbrGyAvGUtdzUoyIH0jl7dRQrVIRA==
-----END CERTIFICATE-----
<Press [Ctrl] and [D] keys>
```

6. **Execute the sethttps command to enable HTTPS.**

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

7. **From the client, access XSCF Web with HTTPS specified. Confirm that no security warning dialog box appears on the screen and the certificate is correct.**

3.8.6 Configuring a Self-Signed Certificate Authority and Creating a Web Server Certificate

With Neither a Web Server Secret Key nor a Self-Signed Web Server Certificate

1. **Execute the sethttps command with the -c enable option specified to start the HTTP service.**

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

The command automatically configures self-signing, generates a Web server secret key, creates a Web server certificate, and enables HTTPS to complete this processing at one time.

With a Web Server Secret Key and Self-Signed Web Server Certificate

The existing Web server secret key and certificate will be overwritten.

1. **Execute the sethttps command with the DN specified to create a self-signed Web server certificate.**
   The following example specifies the -c selfsign option along with the DN (JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com) to create a self-signed Web server certificate.

```
XSCF> sethttps -c selfsign JP Kanagawa Kawasaki Example
development scf-host abc@example.com
CA key and CA cert already exist. Do you still wish to update?
[y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. **Execute the showhttps command with the -t option specified, and confirm that the Web server certificate was created.**

```
XSCF> showhttps -t
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cb:92:cc:ee:79:6c:d3:09
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=JP, ST=Kanagawa, O=Fujitsu, OU=Fujitsu, CN=XSCF
        Validity
            Not Before: May 24 07:15:17 2017 GMT
            Not After : May 22 07:15:17 2027 GMT
        Subject: C=JP, ST=Kanagawa, O=Fujitsu, OU=Fujitsu, CN=XSCF/
```

```
emailAddress=hoge@hoge
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c7:5f:f1:61:ad:ba:4b:64:25:7e:49:ba:7a:6c:
                    d4:5c:b1:8c:2d:15:9f:8a:2f:70:c8:cc:4a:3d:2c:
                    bd:0a:b7:f8:1d:4a:12:93:ea:22:d5:be:85:69:d7:
                    0b:31:a8:1a:ae:34:c6:f6:e8:a1:c8:cc:02:08:be:
                    bc:2b:e9:34:8f:f2:ee:4a:93:26:a0:47:93:7e:b7:
                    f8:3f:73:24:55:45:02:14:f7:c2:d8:56:f7:a1:cf:
                    2f:2d:3e:d4:ff:05:1a:82:25:34:1f:f2:1a:83:91:
                    a7:35:98:7d:2a:92:53:6b:19:75:91:86:b5:2e:ef:
                    :
                    :
```

3. **Execute the sethttps command to enable HTTPS.**

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

If the system has multiple XSCFs, the settings are automatically reflected by the standby XSCF.

3.9 Configuring the XSCF Network

This section describes how to configure the XSCF network for this system.

The XSCF network settings consist of XSCF network interface settings, such as for the XSCF-LAN and the protocol for SP to SP communication (SSCP), routing settings, and DNS-related settings.

3.9.1 Using Services Through the XSCF Network

With a connection to the XSCF network, you can use various server information and services through the XSCF shell and XSCF Web interfaces. For details of each service, see the respective sections indicated below:

- Server operation, status display, and configuration change (See Chapter 10 and Chapter 11.)
- NTP service (See Section 3.6.)
- Telnet service (See Section 3.7.)
- SSH service (See Section 3.7.)
- HTTPS service (See Section 3.8.)

- SMTP service (See Section 10.2.)
- SNMP service (See Section 10.3.)
- Remote maintenance service (See the *Product Notes*.)
- LDAP service (See Section 3.5.12.)
- Active Directory service (See Section 3.5.13.)
- LDAP over SSL service (See Section 3.5.14.)

3.9.2 Understanding the XSCF Network Interfaces

XSCF Ethernet Port

Each SPARC M12/M10 chassis and crossbar box has two XSCF Ethernet ports. The ports are named XSCF-LAN#0 and XSCF-LAN#1.
Both use an RJ-45 connector, supporting 10Base-T/100Base-TX/1000Base-T. The XSCF-LAN ports are ports for the LAN connection used by the system administrator to perform operations using the XSCF shell or XSCF Web. The operations include displaying the server status, operating a domain, and displaying a console.
To connect to the XSCF network, specify the IP addresses of these Ethernet ports. Users can maintain/manage the server using the two LAN paths.
For a system that has multiple XSCFs, the XSCF-LAN ports of the slave XSCFs are not used for the purpose of server maintenance/management. The XSCF-LAN ports of the slave XSCFs are connected to the network only when remote storage is used. For details on remote storage, see "4.6   Using Remote Storage."

Takeover IP Address Between the Master XSCF and Standby XSCF

If the system has multiple XSCFs, XSCF-LAN#0 and XSCF-LAN#1 on the master XSCF and standby XSCF are respectively grouped together so that one takeover IP address (virtual IP address) can be set for the groups. As a result, even if the chassis housing the master XSCF and standby XSCF are switched, users need not be concerned about the IP addresses of the master XSCF and standby XSCF. By continuing to use the takeover IP address, they can access the master XSCF even after the switchover.

Protocol for SP to SP Communication (SSCP)

If the system has multiple XSCFs, a network is configured between the XSCFs. The protocol for the network interface between these XSCFs is referred to as the protocol for SP to SP communication (SSCP) or the SSCP link network. Through its communication paths, the XSCFs are connected to one another, mutually monitor one another's status, and exchange system information.

Figure 3-3 shows an SSCP link network using a SPARC M12-2S or SPARC M10-4S system in the 4BB configuration, with chassis directly interconnected.

Figure 3-3   SSCP Link Network
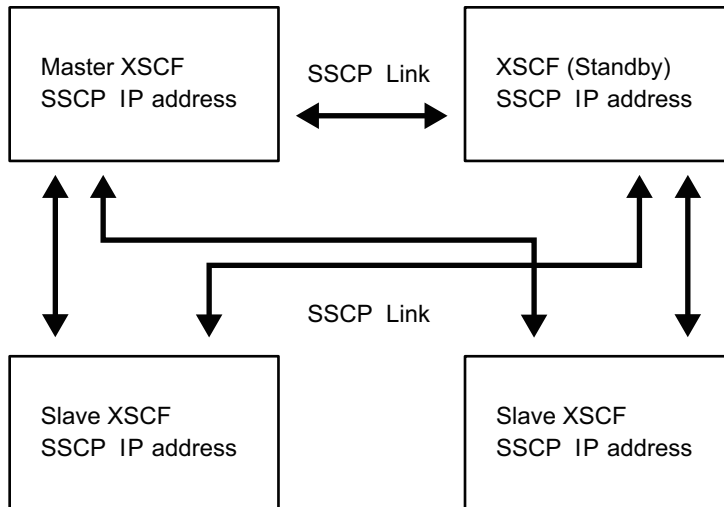
For configuring SSCP, the respective cables connect the master XSCF to the standby XSCF, the master XSCF to the slave XSCFs, and the standby XSCF to the slave XSCFs. For the connection between the master XSCF and the standby XSCF, the XSCF DUAL control ports are connected to each other. The SSCP port for connecting the master or standby to each slave is called the XSCF BB control port. The slave XSCFs are not mutually connected. For details on cable connections to configure SSCP, see "Chapter 4   Setting the SPARC M12-2S in a Building Block Configuration" in the *Fujitsu SPARC M12-2S Installation Guide* or "Chapter 4   Configuring Building Block Connections" in the *Fujitsu M10-4S/SPARC M10-4S Installation Guide*.

The SSCP IP address was set at factory shipment beforehand. If you want to set a different SSCP IP address, the setting needs to be made at the same time that the initial settings for the system are made. For details on the SSCP IP addresses, see "3.9.5   Understanding the IP Addresses that are Set with SSCP."

3.9.3   XSCF Network Interface Configuration

This section describes the following XSCF network interfaces:
- The system control network that provides users with access to the XSCF (XSCF-LAN)
- Link network for communication between XSCFs (SSCP) (in a system with multiple XSCFs)

With a system consisting of only one SPARC M12/M10, two IP addresses are set for XSCF-LAN in order to access the XSCF. The XSCF-LAN can use only one LAN port. With SPARC M12-2S systems consisting of four chassis or SPARC M10-4S systems consisting of four chassis that are directly connected, four IP addresses are set for XSCF-LAN, two are set as takeover IP addresses, and 10 are set for SSCP, for a total of 16 IP addresses.
With SPARC M12-2S systems consisting of 16 chassis or SPARC M10-4S systems consisting of 16 chassis that are connected by four crossbar boxes, four IP addresses

are set for XSCF-LAN, two are set as takeover IP addresses, and 44 are set for SSCP, for a total of 50 IP addresses.

Note - If the system has multiple XSCFs, the XSCFs cannot be configured from the standby XSCF. Commands for configuring all the XSCFs are executed only from the master XSCF.

Figure 3-4 shows the necessary network interfaces for configuring the XSCF network for the SPARC M12-2S or SPARC M10-4S system in the 4BB configuration, with chassis directly interconnected.

Figure 3-4   XSCF Network in the 4BB Configuration
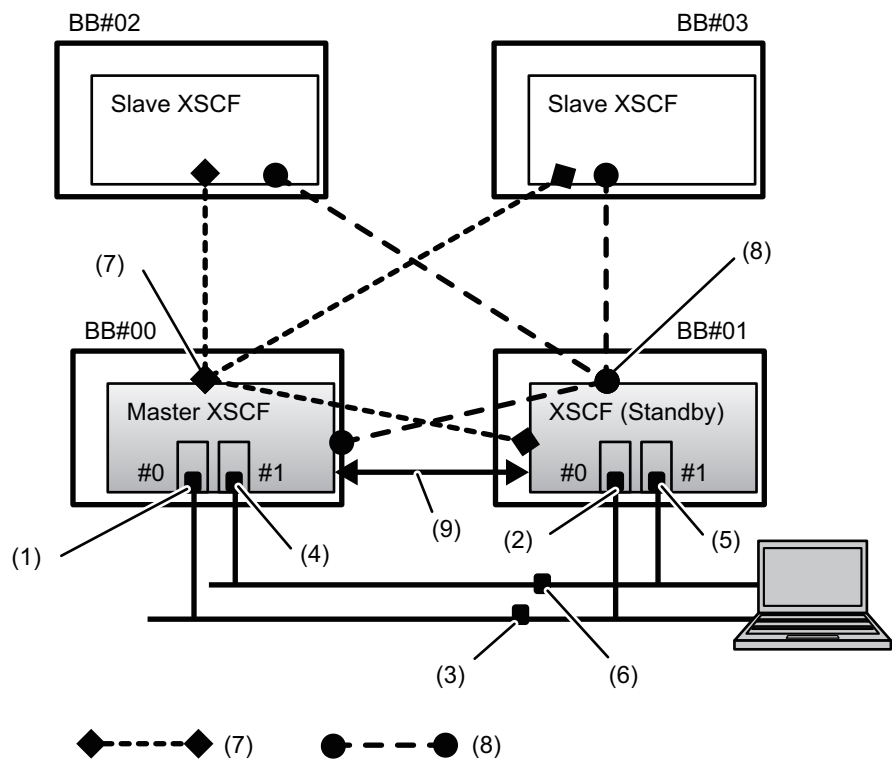
No.	Address Setting	No.	Address Setting
1	XSCF-LAN#0 address (on master XSCF side)	6	Inter-XSCF-LAN#1 takeover IP address
2	XSCF-LAN#0 address (on standby XSCF side)	7	SSCP address (master XSCF and XSCF in each BB#xx): 4 addresses
3	Inter-XSCF-LAN#0 takeover IP address	8	SSCP address (standby XSCF and XSCF in each BB#xx): 4 addresses
4	XSCF-LAN#1 address (on master XSCF side)	9	SSCP address for duplication (master XSCF and standby XSCF): 2 addresses

No.	Address Setting	No.	Address Setting
5	XSCF-LAN#1 address (on standby XSCF side)		

Figure 3-5 shows an example of the necessary network interfaces for configuring the XSCF network for the SPARC M12-2S or SPARC M10-4S system with crossbar boxes.

Figure 3-5   XSCF Network in a System Configuration with Crossbar Boxes
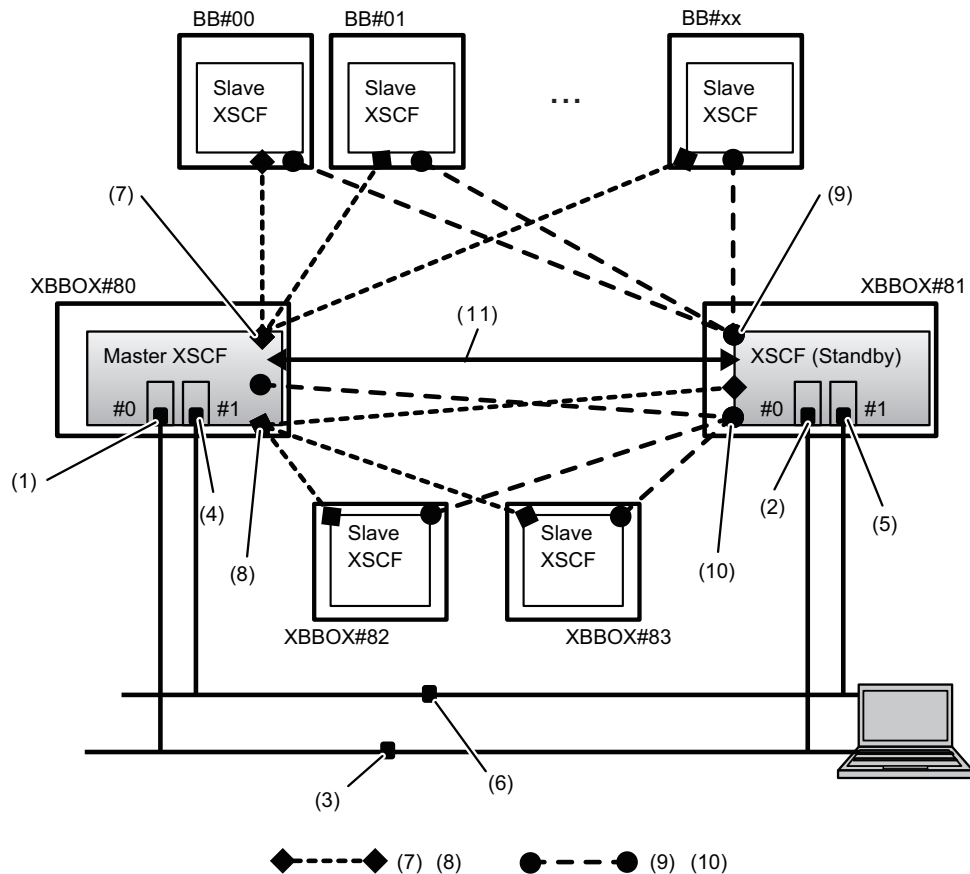
No.	Address Setting	No.	Address Setting
1	XSCF-LAN#0 address (on master XSCF side)	7	SSCP address (master XSCF and XSCF in each BB#xx): 17 addresses
2	XSCF-LAN#0 address (on standby XSCF side)	8	SSCP address (master XSCF and XSCFs in each XBBOX#xx): 4 addresses
3	Inter-XSCF-LAN#0 takeover IP address	9	SSCP address (standby XSCF and XSCF in each BB#xx): 17 addresses

No.	Address Setting	No.	Address Setting
4	XSCF-LAN#1 address (on master XSCF side)	10	SSCP address (standby XSCF and XSCF in each XBBOX#xx): 4 addresses
5	XSCF-LAN#1 address (on standby XSCF side)	11	SSCP address for duplication (master XSCF and standby XSCF): 2 addresses
6	Inter-XSCF-LAN#1 takeover IP address		

3.9.4   Understanding Network Group Subnets

The network addresses of the IP addresses in the following group of XSCF network connections must be set as different addresses:

- XSCF-LAN#0
- XSCF-LAN#1
- SSCP link between the master XSCF and each BB
- SSCP link between the standby XSCF and each BB
- SSCP link between the master XSCF and the XSCF of each XBBOX
- SSCP link between the standby XSCF and the XSCF of each XBBOX
- SSCP link between the master XSCF and standby XSCF (DUAL)

With SPARC M12-2S or SPARC M10-4S systems in the 4BB configuration, with chassis directly interconnected, three types of subnets are necessary as SSCP network addresses (SSCP link network ID 0-2). The SSCP links indicated by the numbers 7, 8, and 9 in Figure 3-4 must be configured with different subnet IP addresses.

A system with crossbar boxes needs up to five types of subnet. (Each subnet has an SSCP link network ID from 0 to 4.) The five types of SSCP links indicated by the numbers 7 to 11 in Figure 3-5 must be configured with different subnet IP addresses.

3.9.5   Understanding the IP Addresses that are Set with SSCP

The IP addresses used with SSCP are classified and set in the following groups. These groups are distinguished by SSCP link network ID. At least two IP addresses need to be set per SSCP port. (See Figure 3-4 and Figure 3-5.)

- Group consisting of the master XSCF and the XSCF of each BB (Figure 3-4, No. 7, Figure 3-5, No. 7)
- Group consisting of the standby XSCF and the XSCF of each BB (Figure 3-4, No. 8, Figure 3-5, No. 9)
- Group consisting of the master XSCF and the XSCF of each XBBOX (Figure 3-5, No. 8)

- Group consisting of the standby XSCF and the XSCF of each XBBOX (Figure 3-5, No. 10)
- Group consisting of the master XSCF and standby XSCF (Figure 3-4, No. 9, Figure 3-5, No. 11)

The SPARC M12-1/M12-2/M10-1/M10-4 system in a configuration with one XSCF does not have SSCP settings.

Table 3-21 lists the location, quantity, ID, and default IP address value of each SSCP IP address that is set for the SPARC M12-2S or SPARC M10-4S in the 4BB configuration, with chassis directly interconnected. Execute the showsscp command to check the currently set IP addresses.

Table 3-21   SSCP IP Addresses (in the 4BB Configuration)

Location	Quantity	SSCP Link Network ID	Default IP Address
Connection between master XSCF and XSCF of each BB#xx	4	0	
BB#00 (master)			169.254.1.1
BB#01			169.254.1.2
BB#02			169.254.1.3
BB#03			169.254.1.4
Connection between standby XSCF and each BB#xx	4	1	
BB#00			169.254.1.9
BB#01 (standby)			169.254.1.10
BB#02			169.254.1.11
BB#03			169.254.1.12
Connection for duplication between master XSCF and standby XSCF	2	2	
BB#00 (master)			169.254.1.17
BB#01 (standby)			169.254.1.18
Total	10		

Table 3-22 lists the location, quantity, ID, and default IP address value of each SSCP IP address that is set for the SPARC M12-2S or SPARC M10-4S in the maximum configuration (16BB and 4-XBBOX configuration).

Table 3-22 SSCP IP Address (in the 16BB and 4-XBBOX Configuration)

Location	Quantity	SSCP Link Network ID	Default IP Address
Connection between master XSCF and XSCF of each BB#xx	17	0	
XBBOX#80 (master)			169.254.1.1
From BB#00 to BB#15			169.254.1.2 to 169.254.1.17
Connection between standby XSCF and XSCF of each BB#xx	17	1	
XBBOX#81 (standby)			169.254.1.33
From BB#00 to BB#15			169.254.1.34 to 169.254.1.49
Connection between master XSCF and XSCF of each XBBOX#xx	4	2	
XBBOX#80 (master)			169.254.1.65
XBBOX#81			169.254.1.66
XBBOX#82			169.254.1.67
XBBOX#83			169.254.1.68
Connection between standby XSCF and XSCF of each XBBOX#xx	4	3	
XBBOX#80			169.254.1.73
XBBOX#81 (standby)			169.254.1.74
XBBOX#82			169.254.1.75
XBBOX#83			169.254.1.76
Connection for duplication between master XSCF and standby XSCF	2	4	
XBBOX#80 (master)			169.254.1.81
XBBOX#81 (standby)			169.254.1.82
Total	44		

3.9.6 Checking the Setting Items and Commands Related to the XSCF Network

Table 3-23 lists the setting items related to the XSCF network and the corresponding XSCF shell commands.

An XSCF reboot is necessary for the completion of configuration of the network. Use the rebootxscf command to reboot the XSCF. The XSCF reboot disconnects the XSCF session, so log in to the XSCF again.

Table 3-23   Setting Items Related to the XSCF Network

Setting Item	Required or Optional Setting	Related Command
XSCF network IP address - XSCF-LAN - Takeover IP address - SSCP	Required	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
Enabling/Disabling the network	Optional	setnetwork(8), shownetwork(8)
Net mask	Required	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
Host name/domain name	Optional	sethostname(8), showhostname(8)
Adding/Deleting a network route - Destination IP address - Gateway - Net mask	Required	setroute(8), showroute(8)
Adding/Deleting a DNS - Name server - Search path	Optional	setnameserver(8), shownameserver(8)
IP packet filtering rule	Optional	setpacketfilters(8), showpacketfilters(8)
Applying the network	Required	applynetwork(8)

3.9.7   Flow of Configuring the XSCF Network

This section describes the procedure for configuring the XSCF network. References to detailed procedures are shown in the respective steps.

1. **Set an Ethernet (XSCF-LAN) IP address (physical IP address).**
   Two XSCF-LAN ports can be used, depending on the network configuration.

   In systems with one XSCF, set either or both of the following IP addresses:

   - XSCF-LAN#0 of BB#00 (master XSCF)

   - XSCF-LAN#1 of BB#00 (master XSCF)

   In systems with multiple XSCFs, first set each XSCF-LAN IP address on the master XSCF side, and then set the XSCF-LAN IP address on the standby XSCF (see shownetwork(8), setnetwork(8), and 3.9.8).

   To be able to connect either XSCF in case of XSCF failover, set the same network address for the LAN ports with the same number on each XSCF.

   Different network addresses must be set for the IP addresses of XSCF-LAN#0 and XSCF-LAN#1.

2. **If the system has multiple XSCFs, set the takeover IP address (virtual IP address).**
   The setting of the takeover IP address enables takeover of the IP address after switching of the master and standby sides in cases of XSCF failover. Users can

always connect to the master XSCF by accessing the takeover IP address, with no need to pay attention to XSCF switching.

After setting the respective IP addresses of XSCF-LAN#0 and XSCF-LAN#1, set one takeover IP address for the respective LAN ports of XSCF-LAN#0 and XSCF-LAN#1, which are redundant (see shownetwork(8), setnetwork(8), and 3.9.9).

3. **If the system has multiple XSCFs, specify SSCP IP addresses.**
SSCP is used in networks for communication between duplicated XSCFs, so the IP address settings are necessary. The value of the SSCP IP address was set beforehand at factory shipment (see Table 3-21 and Table 3-22).

If the XSCF-LAN IP address settings conflict with the SSCP default network addresses, the SSCP IP addresses need to be set again. The SSCP IP addresses must be addresses within the same network in the same group or different network addresses outside of the group. For details on subnets, see "3.9.4 Understanding Network Group Subnets." Users cannot access the SSCP network (see showsscp(8), setsscp(8), and 3.9.10).

4. **Set the host name, routing, and DNS.**
In the systems with multiple XSCFs, first set the host name and routing on the master XSCF side, and then set them on the standby XSCF side (see showhostname(8), sethostname(8), showroute(8), setroute(8), shownameserver (8), setnameserver(8), 3.9.11, 3.9.12, and 3.9.13).

5. **Set IP packet filtering rules.**
Set IP packet filtering rules for the XSCF-LAN (see showpacketfilters(8), setpacketfilters(8), and 3.9.14).

For the settings for connecting remote storage to a slave XSCF, see "4.6.10 Configuring the XSCF-LAN Used with Remote Storage."

6. **Apply the network settings.**
To complete configuration of the network, settings must be reflected and the XSCF must be rebooted. The XSCF reboot disconnects the XSCF session, so log in again (see applynetwork(8), rebootxscf(8), and 3.9.15).

Note - If an XSCF reboot or failover occurs during execution of a setting command involving all the XSCFs, configuration may not complete successfully. Log in to the master XSCF again, and check whether the settings are correct. If they are incorrect, make the settings again.

3.9.8 Enabling/Disabling the XSCF Network and Setting an XSCF-LAN IP Address and Net Mask

To confirm the network interface information that is set for the XSCF, use the shownetwork command. Also, to configure the network interface used by the XSCF, use the setnetwork command. Execute the setnetwork command with a user account that has the platadm privilege.

1. **Execute the shownetwork command to display information on all XSCF network interfaces.**

```
XSCF> shownetwork -a
bb#00-lan#0
          Link encap:Ethernet HWaddr 00:00:00:12:34:56
          inet addr: 192.168.11.10 Bcast: 192.168.11.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12241827 (11.3 MiB) TX bytes:1189769 (0.9 MiB)
          Base address:0x1000
lan#0     Link encap:Ethernet HWaddr 00:00:00:12:34:56
          inet addr:192.168.11.11 Bcast:192.168.11.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          Base address:0xe000
bb#00-lan#1
 :
```

2. **Display XSCF-LAN#0 or XSCF-LAN#1 information.**
   The following example displays the XSCF-LAN#1 network interface information
   for BB#00 (master XSCF).

```
XSCF> shownetwork bb#00-lan#1
bb#00-lan#1
          Link encap:Ethernet HWaddr 00:00:00:12:34:57
          inet addr:192.168.10.10 Bcast: 192.168.10.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20241827 (19.3 MiB) TX bytes:2089769 (1.9 MiB)
          Base address:0x1000
```

3. **Execute the setnetwork command with network interface information specified.**
   The following example sets the IP address 192.168.1.10 and the net mask
   255.255.255.0 for XSCF-LAN#0 of BB#00 to enable the XSCF-LAN.

```
XSCF> setnetwork bb#00-lan#0 -m 255.255.255.0 192.168.1.10
```

   The following example disables XSCF-LAN#1 of BB#00.

```
XSCF> setnetwork bb#00-lan#1 -c down
```

   The following example deletes the set IP address and net mask of XSCF-LAN#1
   of BB#00.

```
XSCF> setnetwork -r bb#00-lan#1
You specified '-r' interface remove option.
So, we delete routing information that interface corresponds.
Continue? [y|n] :y
```

```
If you choose 'y'es, you must execute 'applynetwork' command for application.
Or you choose 'y'es, but you don't want to apply, you execute 'rebootxscf' for
 reboot.
```

4. **Execute the applynetwork and rebootxscf commands to reflect the settings made for the XSCF network interface.**

Note - You can also reflect the takeover IP address, SSCP IP address, XSCF host name, XSCF domain name, XSCF routing, DNS for the XSCF, and other settings made, by executing the applynetwork and rebootxscf commands.

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname   :hostname-0
  bb#01 hostname   :hostname-1
  DNS domain name  :example.com
  nameserver       :10.23.4.3

  interface        :bb#00-lan#0
  status           :up
  IP address       :10.24.144.214
  netmask          :255.255.255.0
  route            : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omitted)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF reboot disconnects the XSCF session, so log in again.

5. **Execute the shownetwork command, and confirm the XSCF network interface information.**

3.9.9 Setting the Takeover IP Address

To set the takeover IP address (virtual IP address) for the master XSCF and standby XSCF, use the setnetwork command.

1. **Execute the shownetwork command to display information on all XSCF network interfaces.**

```
XSCF> shownetwork -a
```

2. **Display information on the takeover IP address of XSCF-LAN#0 or XSCF-LAN#1.**
   The following example displays information on the takeover IP address of XSCF-LAN#0.

```
XSCF> shownetwork lan#0
lan#0 Link encap:Ethernet HWaddr 00:00:00:12:34:56
inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Base address:0xe000
```

3. **Set the takeover IP address of XSCF-LAN#0 or XSCF-LAN#1.**
   The following example sets the takeover IP address 192.168.11.10 and net mask 255.255.255.0 for XSCF-LAN#0.

```
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.11.10
```

4. **Execute the applynetwork and rebootxscf commands to reflect the settings made for the XSCF network interface.**

   Note - You can also reflect the SSCP IP address, XSCF host name, XSCF domain name, XSCF routing, DNS for the XSCF, and other settings made, by executing the applynetwork and rebootxscf commands.

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname    :hostname-0
  bb#01 hostname    :hostname-1
  DNS domain name   :example.com
  nameserver        :10.23.4.3

  interface         :bb#00-lan#0
  status            :up
  IP address        :10.24.144.214
  netmask           :255.255.255.0
  route             : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omitted)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

   The XSCF reboot disconnects the XSCF session, so log in again.

5. **Execute the shownetwork command, and confirm the XSCF network interface information.**

3.9.10 Setting an SSCP IP Address

To confirm the IP address that is assigned to the protocol for communication (SSCP) between service processors, use the showsscp command. The setsscp command is used to set the SSCP IP address. Execute the setsscp command with a user account that has the platadm or fieldeng privilege.

1. **Execute the shownetwork command to display information on all XSCF**

network interfaces.

```
XSCF> shownetwork -a
```

2. **Execute the showsscp command to display SSCP address information.**
   The following example displays information on all SSCP addresses on the
   SPARC M10-4S system in the 4BB configuration, with chassis directly
   interconnected.

```
XSCF> showsscp -a
SSCP network ID:0 address 169.254.1.0
SSCP network ID:0 netmask 255.255.255.248
Location     Address
------------ ---------------
bb#00-if#0 169.254.1.1
bb#01-if#0 169.254.1.2
bb#02-if#0 169.254.1.3
bb#03-if#0 169.254.1.4
SSCP network ID:1 address 169.254.1.8
SSCP network ID:1 netmask 255.255.255.248
Location     Address
------------ ---------------
bb#00-if#1 169.254.1.9
bb#01-if#1 169.254.1.10
bb#02-if#1 169.254.1.11
bb#03-if#1 169.254.1.12
SSCP network ID:2 address 169.254.1.16
SSCP network ID:2 netmask 255.255.255.252
Location     Address
------------ ---------------
bb#00-if#2 169.254.1.17
bb#01-if#2 169.254.1.18
```

The following example displays the set information for the master XSCF with
SSCP network ID 0 in BB#00.

```
XSCF> showsscp -b 0 -N 0
SSCP network ID:0 address 169.254.1.0
SSCP network ID:0 netmask 255.255.255.248

Location     Address
------------ ---------------
bb#00-if#0 169.254.1.1
```

The following example displays the set information on the SSCP standby XSCF
side.

```
XSCF> showsscp -b 1 -N 1
SSCP network ID:1 address 169.254.1.8
SSCP network ID:1 netmask 255.255.255.248
```

```
Location Address
------------- ---------------
bb#01-if#1 169.254.1.10
```

The following example displays the set information for the SSCP link for master and standby duplication.

```
XSCF> showsscp -N 2
SSCP network ID:2 address 169.254.1.16
SSCP network ID:2 netmask 255.255.255.252

Location Address
------------- ---------------
bb#00-if#2 169.254.1.17
bb#01-if#2 169.254.1.18
```

3. **Set the IP address of SSCP (when setting is required).**
   The IP address used in the SSCP network is set as the default. However, when the IP address of XSCF-LAN and the network address of the SSCP default IP address are the same, change the IP address of SSCP using the setsscp command. The following example sets, in interactive mode, the SSCP addresses and net masks of the SSCP link network for the SPARC M12-2S or SPARC M10-4S system in the 4BB configuration, with chassis directly interconnected.

```
XSCF> setsscp
How many BB[4] > 4
SSCP network ID:0 address [169.254.1.0 ] > 10.1.1.0
SSCP network ID:0 netmask [255.255.255.248] > 255.255.255.0
bb#00-if#0 address [10.1.1.1 ] >
bb#01-if#0 address [10.1.1.2 ] >
bb#02-if#0 address [10.1.1.3 ] >
bb#03-if#0 address [10.1.1.4 ] >

SSCP network ID:1 address [169.254.1.8 ] > 10.2.1.0
SSCP network ID:1 netmask [255.255.255.248] > 255.255.255.0
bb#00-if#1 address [10.2.1.1 ] >
bb#01-if#1 address [10.2.1.2 ] >
bb#02-if#1 address [10.2.1.3 ] >
bb#03-if#1 address [10.2.1.4 ] >

SSCP network ID:2 address [169.254.1.16 ] >
SSCP network ID:2 netmask [255.255.255.252] >
bb#00-if#2 address [169.254.1.17 ] >
bb#01-if#2 address [169.254.1.18 ] >
```

4. **Execute the applynetwork and rebootxscf command to reflect the settings made for the IP addresses and net masks.**

Note - You can also reflect the XSCF host name, XSCF domain name, XSCF routing, DNS for

the XSCF, and other settings made, by executing the applynetwork and rebootxscf commands.

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname    :hostname-0
  bb#01 hostname    :hostname-1
  DNS domain name   :example.com
  nameserver        :10.23.4.3

  interface         :bb#00-lan#0
  status            :up
  IP address        :10.24.144.214
  netmask           :255.255.255.0
  route             : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omitted)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF reboot disconnects the XSCF session, so log in again.

5. **Execute the showsscp command, and confirm the SSCP address information.**

3.9.11 Setting an XSCF Host Name and Domain Name

To confirm the host names set for the chassis of the master XSCF and standby XSCF, use the showhostname command. Also, to set the host names and domain names for the chassis of the master XSCF and standby XSCF, use the sethostname command. Execute the sethostname command with a user account that has the platadm privilege.

1. **Execute the showhostname command to display host names.**

```
XSCF> showhostname -a
bb#00: scf-hostname0.example.com
bb#01: scf-hostname1.example.com
```

2. **Execute the sethostname command to set a host name.**
   The following example sets the host name scf0-hostname for BB#00.

```
XSCF> sethostname bb#00 scf0-hostname
```

The following example sets the domain name example.com for the master XSCF and standby XSCF.

```
XSCF> sethostname -d example.com
```

3. **Execute the sethostname command, and then execute the applynetwork and rebootxscf commands to reflect the settings made for the host name and**

domain name.

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname   :hostname-0
  bb#01 hostname   :hostname-1
  DNS domain name  :example.com
  nameserver       :10.23.4.3

  interface        :bb#00-lan#0
  status           :up
  IP address       :10.24.144.214
  netmask          :255.255.255.0
  route            : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omitted)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF reboot disconnects the XSCF session, so log in again.

4. **Execute the showhostname command, and confirm the host name and domain name.**

3.9.12   Setting XSCF Routing

This section shows an example of data for routing by subnet in a system with multiple XSCFs.

- Configuring one default gateway

```
XSCF of BB#00                                      XSCF of BB#01

bb#00-lan#0              +------------------+       bb#01-lan#0
[192.168.11.10]                                     [192.168.11.20]

bb#00-lan#1              +------------------+       bb#01-lan#1
[10.12.108.10]                                      [10.12.108.20]
```

Destination	Gateway	Netmask	Interface
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

Note - How the routing of each interface of the XSCF is determined changes depending on the network environment at the installation location. The network environment must be appropriately configured for system operation.

Note - No route can be set for a takeover IP address.

- Configuring two default gateways

```
XSCF of BB#00                                      XSCF of BB#01

bb#00-lan#0              +------------------+       bb#01-lan#0
[192.168.11.10]                                     [192.168.11.20]

bb#00-lan#1              +------------------+       bb#01-lan#1
[10.12.108.10]                                      [10.12.108.20]
```

Destination	Gateway	Netmask	Interface
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[default]	[192.168.11.1]	[0.0.0.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[default]	[192.168.11.1]	[0.0.0.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

Note - If two default gateways are configured, one of them is automatically selected. In their settings, the network must be configured such that the gateways operate correctly as the default gateway.

Use the showroute command to check the routing information of an XSCF network. Furthermore, to set routing information, use the setroute command. Execute the setroute command with a user account that has the platadm privilege.

Operation Procedure

1. **Execute the showroute command to display the routing environment.**

```
XSCF> showroute -a
Destination      Gateway          Netmask          Flags   Interface
192.168.11.0     *                255.255.255.0    U       bb#00-lan#0
10.12.108.0      *                255.255.255.0    U       bb#00-lan#1
default          10.12.108.1      0.0.0.0          UG      bb#00-lan#1

Destination      Gateway          Netmask          Interface
192.168.11.0     *                255.255.255.0    bb#01-lan#0
10.12.108.0      *                255.255.255.0    bb#01-lan#1
default          10.12.108.1      0.0.0.0          bb#01-lan#1
```

2. **Execute the setroute command with the network interface routing environment specified.**
   The following example adds routing defined as the destination 192.168.11.0 and the net mask 255.255.255.0 for XSCF-LAN#0 of BB#00.

```
XSCF> setroute -c add -n 192.168.11.0 -m 255.255.255.0 bb#00-lan#0
```

   The following example adds routing defined as the default gateway 10.12.108.1 for XSCF-LAN#1 of BB#00.

```
XSCF> setroute -c add -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

   The following example deletes routing to the destination 192.168.11.0 for XSCF-LAN#0 of BB#00.

```
XSCF> setroute -c del -n 192.168.11.0 bb#00-lan#0
```

   The following example deletes routing defined as the destination 192.168.1.0 and the net mask 255.255.255.0 for XSCF-LAN#0 of BB#00.

```
XSCF> setroute -c del -n 192.168.1.0 -m 255.255.255.0 bb#00-lan#0
```

   The following example deletes routing defined as the default gateway 10.12.108.1 for XSCF-LAN#1 of BB#00.

```
XSCF> setroute -c del -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

3. **Execute the applynetwork and rebootxscf commands to reflect the settings made with the setroute command.**

Note - You can also reflect the DNS for the XSCF and other settings made, by executing the applynetwork and rebootxscf commands.

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname   :hostname-0
  bb#01 hostname   :hostname-1
  DNS domain name  :example.com
  nameserver       :10.23.4.3

  interface        :bb#00-lan#0
  status           :up
  IP address       :10.24.144.214
  netmask          :255.255.255.0
  route            : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omitted)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF reboot disconnects the XSCF session, so log in again.

4. **Execute the showroute command, and confirm the routing settings.**

3.9.13   Setting the DNS for the XSCF

Use the shownameserver command to confirm the name server and search path used by the XSCF network. Also, to set the name server and search path, use the setnameserver command. Execute the setnameserver command with a user account that has the platadm privilege.
When specifying a search path, you also have to set a name server.

1. **Execute the shownameserver command to display name servers and search paths.**
    If multiple name servers and search paths are registered, each appears on a separate line.

    The following example checks what is registered and finds three name servers and one search path.

```
XSCF> shownameserver
nameserver   10.0.0.2
namaserver   172.16.0.2
nameserver   192.168.0.2
search       sub.example.com
```

The following example checks what is registered and finds no name server and no search path.

```
XSCF> shownameserver
nameserver ---
search    ---
```

2. **Execute the setnameserver command with a name server and search path specified.**
   The following example adds the following three IP addresses as name servers: 10.0.0.2, 172.16.0.2, and 192.168.0.2.

```
XSCF> setnameserver 10.0.0.2 172.16.0.2 192.168.0.2
```

The following example deletes all set name servers.

```
XSCF> setnameserver -c del -a
```

The following example deletes two of the three duplicate settings of a registered DNS server.

```
XSCF> shownameserver
nameserver 10.24.1.2
nameserver 10.24.1.2
nameserver 10.24.1.2
XSCF> setnameserver -c del 10.24.1.2 10.24.1.2
XSCF> shownameserver
nameserver 10.24.1.2
```

The following example adds one domain name, sub.example.com, as a search path.

```
XSCF> setnameserver -c addsearch sub.example.com
```

The following example deletes all set search paths.

```
XSCF> setnameserver -c delsearch -a
```

3. **Execute the applynetwork and rebootxscf commands to reflect the name server and search path settings made with the setnameserver command.**

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname    :hostname-0
  bb#01 hostname    :hostname-1
  DNS domain name   :example.com
```

```
  nameserver        :10.23.4.3

  interface         :bb#00-lan#0
  status            :up
  IP address        :10.24.144.214
  netmask           :255.255.255.0
  route             : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omitted)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The XSCF reboot disconnects the XSCF session, so log in again.

4. **Execute the showroute command, and confirm the routing settings.**

3.9.14 Setting the IP Packet Filtering Rules for the XSCF Network

To confirm the IP packet filtering rules that are set for the XSCF network, use the showpacketfilters command. Also, to set the IP packet filtering rules, use the setpacketfilters command. Execute the setpacketfilters command with a user account that has the platadm or fieldeng privilege.
You can set the XSCF network IP filtering rules for input packets only. No such rules can be set for output packets.

1. **Execute the showpacketfilters command to display the IP packet filtering rules for the XSCF-LAN.**
   The following example displays the set IP packet filtering rules for the XSCF network.

```
XSCF> showpacketfilters -a
-i bb#00-lan#0 -j ACCEPT
-i bb#01-lan#1 -j ACCEPT
-s 173.16.0.0/255.255.0.0 -j ACCEPT
-s 205.168.148.100/255.255.255.255 -j ACCEPT
```

The following example displays the applied IP packet filtering rules.

```
XSCF> showpacketfilters -l
pkts   bytes target    prot   in            source
124     102K ACCEPT    all    bb#00-lan#0 0.0.0.0/0.0.0.0
  0        0 ACCEPT    all    bb#00-lan#1 0.0.0.0/0.0.0.0
  0        0 ACCEPT    all    *             173.16.0.0/255.255.0.0
  0        0 ACCEPT    all    *             205.168.148.100
```

The following example shows that no IP packet filtering rules are set.

```
XSCF> showpacketfilters -a
XSCF>
```

2. **Execute the setpacketfilters command to set an IP packet filtering rule.**
   The priority among the IP packet filtering rules follows the order in which they were set.

   The following example permits packets to pass through the IP addresses 192.168.100.0/255.255.255.0.

```
XSCF> setpacketfilters -y -c add -i bb#00-lan#0 -s
192.168.100.0/255.255.255.0 -j ACCEPT
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

   The following example permits packets to pass through the IP addresses 192.168.100.0/255.255.255.0 for XSCF-LAN#0 of BB#00.

```
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
XSCF>
XSCF> setpacketfilters -y -c add -i bb#00-lan#0 -j DROP
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
-i bb#00-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
-i bb#00-lan#0 -j DROP
```

   The following example deletes a setting for discarding communication from 10.10.10.10.

```
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
-s 10.10.10.10 -j DROP
XSCF>
XSCF> setpacketfilters -y -c del -s 10.10.10.10 -j DROP
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
```

   The following example clears all the set IP packet filtering rules.

```
XSCF> setpacketfilters -c clear
(none)
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

3.9.15 Reflecting the XSCF Network Settings

After completing settings with the setnetwork, setsscp, sethostname, setroute, and setnameserver commands, reflect their network settings.

1. **Execute the applynetwork command.**
   The network settings are displayed, and their application is confirmed.

```
XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname    :hostname-0
  bb#01 hostname    :hostname-1
  DNS domain name   :example.com
  nameserver        :10.23.4.3

  interface         :bb#00-lan#0
  status            :up
  IP address        :10.24.144.214
  netmask           :255.255.255.0
  route             : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1

  interface         :bb#00-lan#1
  status            :down
  IP address        :
  netmask           :
  route             :

  interface         :bb#01-lan#0
  status            :up
  IP address        :10.24.144.215
  netmask           :255.255.255.0
  route             : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1

  interface         :bb#01-lan#1
  status            :down
  IP address        :
  netmask           :
  route             :

  interface         :lan#0
  status            :down
  IP address        :
  netmask           :

  interface         :lan#1
  status            :down
  IP address        :
  netmask           :

  SSCP network ID:0 netmask  :255.255.255.248

  interface                   :bb#00-if#0
  IP address                  :192.168.1.1
```

```
   interface                    :bb#01-if#0
   IP address                   :192.168.1.2

   interface                    :bb#02-if#0
   IP address                   :192.168.1.3

   interface                    :bb#03-if#0
   IP address                   :192.168.1.4

   SSCP network ID:1 netmask    :255.255.255.248

   interface                    :bb#00-if#1
   IP address                   :192.168.1.10

   interface                    :bb#01-if#1
   IP address                   :192.168.1.9

   interface                    :bb#02-if#1
   IP address                   :192.168.1.11

   interface                    :bb#03-if#1
   IP address                   :192.168.1.12

   SSCP network ID:2 netmask    :255.255.255.252

   interface                    :bb#00-if#2
   IP address                   :192.168.1.17

   interface                    :bb#01-if#2
   IP address                   :192.168.1.18

Continue? [y|n] : y
```

2. **Execute the rebootxscf command to reboot the XSCF and complete the settings.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

The session is disconnected at this time. Reconnect with a new interface, and log in again.

3. **Execute the shownetwork, showsscp, showhostname, showroute, and shownameserver commands to display the network settings, and confirm the new network information.**

4. **Execute the nslookup command, and confirm the host name information.**
   The following example displays information on the host name scf0-hostname.

```
XSCF> nslookup scf0-hostname
Server: server.example.com
Address: 192.168.1.3
```

```
Name: scf0-hostname.example.com
Address: 192.168.10.10
```

3.9.16 Checking the XSCF Network Connection Status

To check the response of network devices, use the ping command. Also, to confirm the network route, use the traceroute command.

1. **Execute the shownetwork command to display the network connection status.**

```
XSCF> shownetwork -i
Active Internet connections (without servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 xx.xx.xx.xx:telnet xxxx:1617 ESTABLISHED
```

2. **Execute the ping command to check for a response from a network device.**
   The following example sends a packet three times to the host named scf0-hostname.

```
XSCF> ping -c 3 scf0-hostname
PING scf0-hostname (XX.XX.XX.XX): 56 data bytes
64 bytes from XX.XX.XX.XX: icmp_seq=0 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=64 time=0.1 ms

--- scf0-hostname ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

3. **Execute the traceroute command to check the network path to a network device.**
   The following example displays the network paths to the host named server. example.com.

```
XSCF> traceroute server.example.com
traceroute to server.example.com (XX.XX.XX.XX), 30 hops max, 40
byte packets
1 XX.XX.XX.1 (XX.XX.XX.1) 1.792 ms 1.673 ms 1.549 ms
2 XX.XX.XX.2 (XX.XX.XX.2) 2.235 ms 2.249 ms 2.367 ms
3 XX.XX.XX.3 (XX.XX.XX.3) 2.199 ms 2.228 ms 2.361 ms
4 XX.XX.XX.4 (XX.XX.XX.4) 2.516 ms 2.229 ms 2.357 ms
5 XX.XX.XX.5 (XX.XX.XX.5) 2.546 ms 2.347 ms 2.272 ms
6 server.example.com (XX.XX.XX.XX) 2.172 ms 2.313 ms 2.36 ms
```

3.10 Configuring Auditing to Strengthen XSCF Security

This section describes how to configure the XSCF to use auditing.
The audit settings are intended for auditing of network operations by users and keeping detailed access records of who logged in to the XSCF, when they logged in, and what operations were performed. The audit settings are enabled by default in this system. The audit settings mainly set whether auditing is enabled or disabled and how to manage the audit policy and audit log (audit trails).

3.10.1 Auditing

The SPARC M12/M10 systems can record all the XSCF events that may be related to security, such as user login and logout and changes to user privileges, as well as all operations, including system start and stop. After auditing is configured, auditing starts and information on a single event, cause of occurrence, date of occurrence, and other related information are recorded as an audit record. The system has an audit log (audit trails), which is a collection of audit records. The system administrator can refer to an audit log to check for suspicious or abnormal operation or to identify the person who did a specific event.
Figure 3-6 provides an overview of how login event information is recorded in an audit log.

Figure 3-6   Recording in an Audit Log
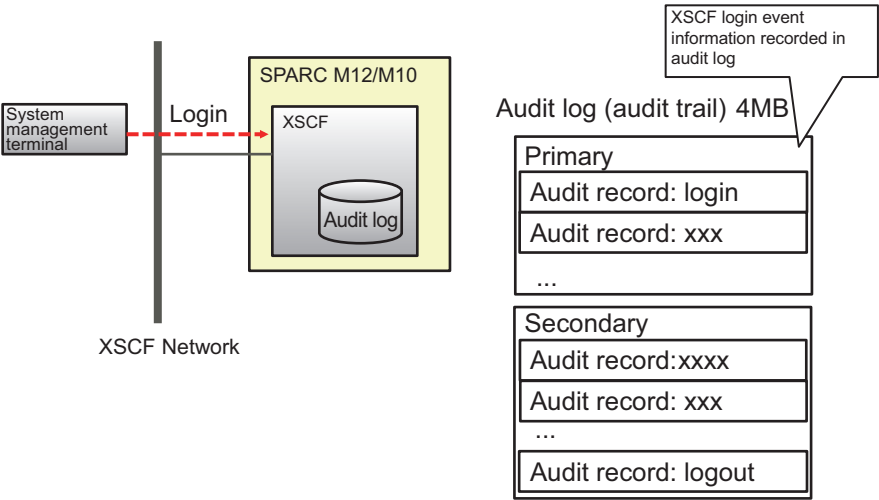
3.10.2　Understanding Audit Terms

Table 3-24 lists terms related to the XSCF audit settings.

Table 3-24　　Audit-related Terms

Term	Description
Audit	Audit is the function of auditing system access. It is also referred to as auditing.
Audit event	An audit event is a security-related system action that can be audited. Multiple audit events can be specified by numeric value or name. (e.g., AEV_LOGIN_SSH, LOGIN_SSH, 0, and all)
Audit class	An audit class is a group of relevant audit events. (e.g., audit events of login audit class: SSH login, Telnet login, HTTPS login, and logout) Multiple audit classes can be specified. (e.g., CS_AUDIT, AUDIT, 2, and all)
Audit record	One audit record is information identifying one audit event. That includes event, event time, and other relevant information. Audit records are stored in an audit file.
Audit log	An audit log is the log files that store multiple audit records. An audit log has two areas: primary and secondary.
Audit trail	An audit trail is also referred to as an audit log. Users use the viewaudit command to analyze the content of each audit record in an audit log.
Audit policy	The policy sets the type of audit records to be generated by specifying an audit event, audit class, or user. It also specifies other settings, such as e-mail notification settings used when an audit log reaches full capacity.
Audit token	An audit token is one field of an audit record. The audit token has a description of an audit event attribute, such as the user or privilege.

3.10.3　Managing Auditing

The system administrator determines which audit class, audit event, or user to use for auditing before performing auditing. The system administrator also determines at which audit log usage level a warning is generated and what action is taken when the capacity becomes full. These determinations are referred to as the audit policy, which is configured on the XSCF before auditing. The system administrator refers to each audit record in the audit log collected based on the audit policy to check the audit information for any abnormal or suspicious access.

The following provides details on the audit events, audit policy, and audit record,

and audit log used for auditing.

Audit event

An audit event is a security-related system operation that can be audited.
Audit events are described below.

- XSCF configuration changes, such as an IP address change
- Physical partition-related setting changes, operations, and status display
- Use of any authentication
- Changes to user security attributes, such as the password and user privileges
- Reading of audit record information (including failed attempts)
- Audit policy changes
- Change of the destination of e-mail to be sent when the audit log capacity threshold is exceeded
- Changes by the system administrator to an audit log.
- Time changes

Audit policy

The audit policy determines how to execute the audit function. The following audit function settings can be configured:

- Whether to enable/disable the audit function
- Types of events to be audited
- An auditor for events
- The audit log capacity threshold at which a warning is generated and the destination of e-mail to be sent when the threshold is exceeded
- Operation performed when an audit log reaches full capacity (Use this setting with the default value.)

Note - If you want to use e-mail to report that the audit log capacity threshold is exceeded, configure the SMTP server using the setsmtp command.

Audit record and audit log

Audit records are saved in the 4-MB audit log in the XSCF. An audit log is saved in binary format, but can be exported in XML format.
An audit log has two areas: primary and secondary. When these areas become full and a new audit record is generated, the record is not saved but discarded (dropped). To prevent new audit records from being discarded, the system administrator deletes secondary area data before the audit log reaches full capacity. After the deletion of the secondary area, the primary area becomes a new secondary area and a new primary area is created. When a new audit record is generated, the record is written to the new primary area.

Note - "count" (default) is set as the operation performed when an audit log reaches full

capacity. With this setting, new audit records are discarded (dropped) when the audit log reaches full capacity, and the number of discarded records is counted (drop count).

Note - If you specify "suspend," degradation due to an error may occur or the XSCF may be rebooted. Specify "count," which is the default, as the policy for writing to the audit log. Also note that, in XCP 2250 and later, specifying "suspend" results in the same operation as when "count" is specified.

Use the audit policy to set the threshold of the file capacity (such as 50%, 75%, or 80%) so that a warning appears before an audit log reaches full capacity. Upon this warning, the system administrator manually archives the audit log and deletes audit records to secure sufficient new storage. Or, he/she disables the audit function. The older file of the two audit log areas is deleted. If this deletion is performed twice in succession, all the data of the audit log will be deleted.

Note - For XSCF auditing in a configuration with multiple SPARC M12-2S/M10-4S systems, both audit logs on the master and standby XSCFs need to be referred to. For details, see "3.10.10   Managing the Audit Log of the Standby XSCF."

3.10.4   Checking the Audit-related Setting Items and Commands

Table 3-25 lists the audit-related setting items and the corresponding XSCF shell commands.

Table 3-25   Audit-related Setting Items

Setting Item	Required or Optional Setting	Related Command
Enabling/Disabling auditing	Optional	setaudit(8), showaudit(8)
Archiving an audit log (*1), deleting data	Optional	setaudit(8), showaudit(8)
Audit policy - Specifying enable/disable for the specified users or application of a global policy - Enabling/Disabling an audit class - Enabling/Disabling an audit event - Enabling/Disabling auditing for all users (global policy) - Warning threshold for the audit log amount (%) - Destination e-mail address used when the audit log amount reaches the threshold - Suspending writing/Discarding data when the audit log reaches full capacity (*2)	Optional	setaudit(8), showaudit(8) setsmtp(8), showsmtp(8)

Table 3-25   Audit-related Setting Items *(continued)*

Setting Item	Required or Optional Setting	Related Command
Displaying an audit log - Records after the specified time - Records before the specified time - Records in the specified time range - Records on a certain date (for 24 hours on a certain date in local time) - Audit class - Audit event - Audit session ID - User privileges - Return value (success, failure, or none) - User (name or numeric UID value) Display an audit trail by specifying the format as described below: - Outputting the data on a line-by-line basis - Specifying a delimiter character (default: comma) - Suppressing conversion from UIDs to user names and conversion from IP addresses to host names - Outputting the data in XML format	Optional	viewaudit(8)

*1 Audit log archiving is not currently supported.
*2 When an audit log reaches full capacity, only the default audit policy "count," which discards audit records, is currently supported. Do not specify "suspend."

3.10.5   Auditing Flow

Figure 3-7 shows the flow for configuring audit settings and displaying an audit log.

Figure 3-7   Audit Setting and Log Display Flow
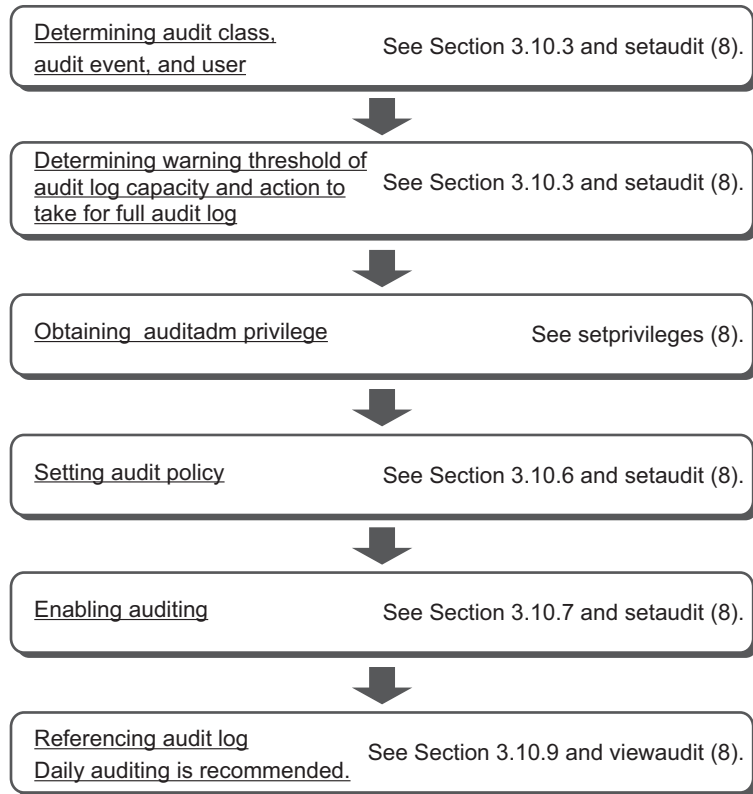
Figure 3-8 shows the flow for deleting audit log data.

Figure 3-8   Deleting Audit Log data

Checking audit log amount
Routinely monitor/check the amount when a warning message appears on the console or a warning e-mail arrives.

See Section 3.10.10 and showaudit (8).

Referencing audit log
Check if the auditing for the data is completed.

See Section 3.10.9 and viewaudit (8).

Deleting audit log data
The older area (2 MB) is deleted.
Before deleting, copy and save the audit log data as required.

See Section 3.10.8 and setaudit (8).

3.10.6   Displaying/Setting the Audit Policy

1. **Execute the showaudit command to display the audit policy settings.**

```
XSCF> showaudit all
Auditing:            enabled
Audit space used:    13713 (bytes)
Audit space free:    4180591 (bytes)
Records dropped:     0
Policy on full trail: count
User global policy:  enabled
Mail:
Thresholds:          80% 100%
User policy:
Events:
        AEV_AUDIT_START enabled
        AEV_AUDIT_STOP enabled
```

2. **Execute the setaudit command to set the audit policy.**
   The following example specifies three users (yyyyy, uuuuu, and nnnnn), with AUDIT and LOGIN enabled for the audit class, the version enabled for audit events, and the global policy disabled for the users.

```
XSCF> setaudit -a yyyyy,uuuuu,nnnnn=enabe -c
ACS_AUDIT,ACS_LOGIN=enable -e AEV_version=enable -g disable
```

The following example specifies a warning destination e-mail address, the deleting of new audit records and counting of the deleted records when the amount of audit trails reaches full capacity, and file amount warning thresholds (50%, 75%, and 90%).

```
XSCF> setaudit -m yyyy@example.com -p count -t 50,75,90
```

3. **Execute the showaudit command, and confirm the settings.**

```
XSCF> showaudit all
Auditing:              enabled
Audit space used:      13713 (bytes)
Audit space free:      4180591 (bytes)
Records dropped:       0
Policy on full trail: count
User global policy:    enabled
Mail:                  yyyy@example.com
Thresholds:            50% 75% 90%
User policy:
Events:
     AEV_AUDIT_START      enabled
     AEV_AUDIT_STOP       enabled
      :
     AEV_LOGIN_BUI        enabled
     AEV_LOGIN_CONSOLE    enabled
     AEV_LOGIN_SSH        enabled
     AEV_LOGIN_TELNET     enabled
     AEV_LOGOUT           enabled
     AEV_AUTHENTICATE     enabled
      :
     AEV_version          enabled
      :
```

With -p count specified, new audit record data is discarded (dropped) when the audit log reaches full capacity, and the number of times that records are dropped is counted (drop count).

Note - When an audit log reaches full capacity, only the default audit policy "count," which discards audit records, is currently supported. Therefore, do not specify "suspend."

If the audit log amount exceeds the threshold, a warning message appears on the console. If a warning destination e-mail address is specified, a warning can also be sent in a secure format.
The following example shows a warning message.

```
WARNING: audit trail is 91% full
```

3.10.7 Enabling/Disabling Auditing

To confirm the current status of auditing, use the showaudit command. Also, to set the items to audit, use the setaudit command. Execute the setaudit command with a user account that has the auditadm privilege.
Audit is enabled by default. Writing to the audit log stops when auditing is disabled. Writing resumes when auditing is enabled. In the processing after a reboot, auditing is disabled before being enabled.

1. **Execute the showaudit command to display the audit settings.**
   The following example displays the entire status of current system auditing.

```
XSCF> showaudit all
Auditing:            enabled
Audit space used:    13713 (bytes)
Audit space free:    4180591 (bytes)
Records dropped:     0
Policy on full trail: count
User global policy:  enabled
Mail:
Thresholds:          80% 100%
User policy:
Events:
        AEV_AUDIT_START enabled
        AEV_AUDIT_STOP enabled
 :
```

2. **Execute the setaudit command to set enable/disable.**
   The following example specifies that audit data writing be enabled.

```
XSCF> setaudit enable
```

   The following example specifies that audit data writing be disabled.

```
XSCF> setaudit disable
```

3.10.8 Deleting Audit Log Data

Audit log data can be deleted by executing the setaudit command in the following cases: when the audit log capacity threshold is exceeded, when a warning message appears on the console or a warning e-mail arrives, or when the audit log reaches full capacity.

1. **Execute the showaudit command to check audit settings and the audit log amount.**
   The following example fully displays the current status of auditing in the system.

The example shows that the audit log amount is 3.5 MB and that the warning-level capacity threshold of 80% is exceeded.

```
XSCF> showaudit all
Auditing:             enabled
Audit space used:     3670016 (bytes)
Audit space free:     524288 (bytes)
Records dropped:      0
Policy on full trail: count
User global policy:   enabled
Mail:
Thresholds:           80% 100%
User policy:
Events:
        AEV_AUDIT_START enabled
        AEV_AUDIT_STOP enabled
:
```

2. **Execute the setaudit command to delete audit log data.**
    The older 2-MB area (secondary) is deleted.

```
XSCF> setaudit delete
```

Note - Before deleting audit log data, check whether auditing of the data has been finished by using the viewaudit command.

3. **Execute the showaudit command to check the setaudit command execution results.**
    The following example shows that the older area of the audit log is deleted and an available capacity of about 2 MB is created.

```
XSCF> showaudit all
Auditing:             enabled
Audit space used:     2097152 (bytes)
Audit space free:     2097152 (bytes)
Records dropped:      0
Policy on full trail: count
User global policy:   enabled
Mail:
Thresholds:           80% 100%
User policy:
Events:
        AEV_AUDIT_START enabled
        AEV_AUDIT_STOP enabled
:
```

> **Note** - After the deletion of the secondary area, the primary area becomes secondary and a new primary area is created.
> The system then recognizes the amount of the new secondary area as 2 MB, regardless of the actual remaining amount of the area.
> Therefore, even after audit log data has been deleted, 2 MB always appears to be in use when the audit log amount is referred to by using the showaudit command.
> If this deletion is performed twice in succession, all information in the audit log will be deleted.
> Even in this case, 2 MB appears to be in use in the audit log amount shown for reference by the showaudit command.

3.10.9 Referencing an Audit Log

Use the viewaudit command to display audit records. Execute the viewaudit command with a user account that has the auditadm or auditop privilege.

1. **Execute the viewaudit command to view an audit trail.**

```
XSCF> viewaudit
file,1,2015-06-29 13:42:59.128 +09:00,20150629044259.
0000000000.localhost
header,20,1,audit - start,localhost.localdomain,2015-06-29 13:
42:59.131 +09:00
header,31,1,login - console,localhost.localdomain,2015-06-29
13:45:03.755
+09:00subject,1,default,normal,console
header,60,1,command - showpasswordpolicy,localhost.localdomain,
2015-06-29
13:45:33.653 +09:00
subject,1,default,normal,console
command,showpasswordpolicy
platform access,granted
return,0
:
```

For details on how to refer to audit records, see "Chapter 12   Checking Logs and Messages."

3.10.10 Managing the Audit Log of the Standby XSCF

Audit data of the master/standby XSCF is saved to an area of the audit log in the master/standby XSCF.
The audit log can be referred to by using the viewaudit command from each XSCF. However, only the master XSCF can be used to display the status of auditing or to delete audit log data.
Therefore, to manage the audit log of the standby XSCF, switch the XSCF from standby to master .

The following describes how to manage the audit log saved to the standby XSCF.

Referencing an audit log

Execute the viewaudit(8) command from the standby XSCF. For details of the reference method, see "3.10.9 Referencing an Audit Log."

Deleting audit log data

1. **Execute the switchscf(8) command to switch between the master and standby XSCFs.**
2. **Execute the showaudit(8) command to check the audit log amount for the former standby XSCF.**
3. **Execute the setaudit(8) command to delete audit log data.**
   For details on deleting the data, see "3.10.8 Deleting Audit Log Data."
4. **Execute the showaudit(8) command to confirm that the audit log has free space.**
5. **Execute the switchscf(8) command to switch between the master and standby XSCFs again.**

Chapter 4

Configuring the System to Suit the Usage Type

This chapter describes items for configuring the system appropriate to the usage type, with a focus on power control and drive connections.

- Setting/Checking the System Altitude
- Controlling System Start
- Enabling/Disabling Dual Power Feed
- Reducing Power Consumption
- Connecting a DVD Drive
- Using Remote Storage

4.1 Setting/Checking the System Altitude

This section describes how to set/check the system altitude.

The SPARC M12/M10 systems control the speed of the cooling fans inside the systems according to the altitude and temperature of the installation location. Therefore, the altitude needs to be set during initial system installation.

Note - Set the system altitude during initial installation. If the value needs to be changed, set it again.

For details of the XSCF commands executed in the following procedure, see their man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

4.1.1 Setting the System Altitude

Use the setaltitude command of the XSCF firmware to set the system altitude. Execute the command with a user account that has the platadm or fieldeng privilege.

```
XSCF> setaltitude -s altitude=value
```

For value, specify the altitude in meters for the installed server. You can specify a
value ranging from 0, in increments of 100.

Note - After setting the system altitude, you need to reboot the XSCF to apply the setting, so
execute the rebootxscf command.

Operation Procedure

1. **Execute the setaltitude command to set the altitude.**
   The following example sets 1,000 m as the altitude.

```
XSCF> setaltitude -s altitude=1000
1000m
```

2. **Execute the rebootxscf command to reboot the XSCF to reflect the setting
   made.**

Note - When continuing with other settings, you can perform this task after all the settings
are competed.

```
XSCF> rebootxscf -a
```

4.1.2   Checking the System Altitude Settings

Use the showaltitude command of the XSCF firmware to check the altitude currently
set for the system.
Execute the command with a user account that has the platadm or fieldeng privilege.

```
XSCF> showaltitude
```

The command displays the currently set system altitude in meters.

Operation Procedure

1. **Execute the showaltitude command to display the altitude.**
   In the following example, you can see that the set altitude is 1,000 m.

```
XSCF> showaltitude
1000m
```

4.2 Controlling System Start

This section describes the warmup time and the wait time for air conditioning (startup wait time) for controlling system start.

The warmup time and the wait time for air conditioning are used for the following purposes.

- You can keep the system from starting until peripherals are powered on. You can keep the system from starting until it warms up.
  Also, you can set a different operating time for each physical partition. When the upper limit value of power consumption is set, simultaneous power-on may cause power consumption to exceed the limit. So, set a different time for each physical partition. (See "4.2.1   Setting/Checking the Warmup Time.")

- You can start the system after the air conditioning in the data center has adjusted the temperature. (See "4.2.2   Setting/Checking the Wait Time for Air Conditioning.")

4.2.1 Setting/Checking the Warmup Time

If the warmup time is set, OpenBoot PROM starts after the set warmup time elapses following server power-on and the beginning of power-on processing.

Setting the Warmup Time

Use the setpowerupdelay command of the XSCF firmware to set the warmup time. Execute the command with a user account that has the platadm or fieldeng privilege.

```
XSCF> setpowerupdelay {-a|-p ppar-id} -c warmup -s time
```

If all physical partitions are to be targeted, specify -a. To target a specific physical partition, specify -p.

For time, specify the warmup time in minutes. You can specify an integer from 0 to 255. The default is 0.

Note - If you turn on the power by pressing the POWER switch on the operation panel, the set warmup time is ignored.

Operation Procedure

1. **Execute the setpowerupdelay command to set the warmup time.**
   The following example sets 5 minutes as the warmup time for physical partition 0.

```
XSCF> setpowerupdelay -p 0 -c warmup -s 5
```

If the warmup time is set while the system is running, the set time becomes valid at the next system startup.

Checking the Warmup Time

Use the showpowerupdelay command of the XSCF firmware to check the warmup time.
Execute the command with a user account that has the platadm, platop, or fieldeng privilege. Alternatively, you can also execute it with a user account that has the pparadm, pparmgr, or pparop privilege for the target physical partition.

```
XSCF> showpowerupdelay
```

In the results output by the showpowerupdelay command, "warmup time" shows the currently set warmup time in minutes. "wait time" shows the currently set wait time for air conditioning in minutes.

Operation Procedure

1. **Display the warmup time with the showpowerupdelay command.**
   In the following example, you can see that the set warmup time is 10 minutes.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

4.2.2 Setting/Checking the Wait Time for Air Conditioning

If the wait time for air conditioning is set, the system waits until the set amount of time has passed before starting. This can be a useful control to, for example, start the system after the air conditioning in the data center has adjusted the temperature.

Note - The SPARC M12/M10 does not support the wait time setting for air conditioning.

Setting the Wait Time for Air Conditioning

Use the setpowerupdelay command of the XSCF firmware to set the wait time for air conditioning.
Execute the command with a user account that has the platadm or fieldeng privilege.

```
XSCF> setpowerupdelay -c wait -s time
```

For time, specify the wait time for air conditioning in minutes. You can specify an integer from 0 to 255. The default is 0.

> **Note -** If you turn on the power by pressing the POWER switch on the operation panel, the set wait time for air conditioning is ignored.

Operation Procedure

1. **Set the wait time for air conditioning with the setpowerupdelay command.**
   The following example sets 5 minutes as the wait time for air conditioning.

```
XSCF> setpowerupdelay -c wait -s 5
```

   If the wait time for air conditioning is set while the system is running, the set time becomes valid at the next system startup.

Checking the Wait Time for Air Conditioning

Use the showpowerupdelay command of the XSCF firmware to check the wait time for air conditioning.
Execute the command with a user account that has the platadm, platop, or fieldeng privilege. Alternatively, you can also execute it with a user account that has the pparadm, pparmgr, or pparop privilege for the target physical partition.

```
XSCF> showpowerupdelay
```

In the results output by the showpowerupdelay command, "warmup time" shows the currently set warmup time in minutes. "wait time" shows the currently set wait time for air conditioning in minutes.

Operation Procedure

1. **Display the wait time for air conditioning with the showpowerupdelay command.**
   In the following example, you can see that the set wait time for air conditioning is 20 minutes.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

4.3 Enabling/Disabling Dual Power Feed

Four power supply units are mounted on the SPARC M12-2/M12-2S. For dual power systems, each system has two power supply units.
e.g., PSU#0/PSU#1 for power system 0, PSU#2/PSU#3 for power system 1
When the dual power feed is enabled/disabled, the PSU status and system operation are as shown in Table 4-1.

Table 4-1   Dual Power Feed Settings and Power Supply Unit (PSU) Status Enabling System Operation for the SPARC M12-2/M12-2S

Dual Power Feed Setting	PSU Status	System Operation
Disabled	2 or more operating PSUs	Operable
	No more than 1 operating PSU	Non-operable
Enabled	2 operating PSUs on at least 1 of power systems	Operable
	No more than 1 operating PSU on both power systems	Non-operable

Two power supply units (PSUs) are mounted on the SPARC M10 and SPARC M12-1. Since PSUs are redundant, the system can operate as long as at least one PSU is operating. Therefore, even if the dual power feed function is enabled/disabled, it does not affect the system operation.

4.3.1   Enabling Dual Power Feed

Use the setdualpowerfeed command of the XSCF firmware to enable dual power feed.

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s enable
```

To target all chassis in the system, specify -a.
To target only a given chassis in the system, specify -b bb_id. For bb_id, specify the BB-ID of the chassis. You can specify an integer from 0 to 15 or 80 to 83, depending on the system configuration.

Operation Procedure

1. **Enable dual power feed with the setdualpowerfeed command.**
    The following example enables dual power feed for BB-ID 1.

```
XSCF> setdualpowerfeed -b 1 -s enable
BB#01:disable -> enable
NOTE: Dual power feed will be enabled the next time the platform is powered on.
```

4.3.2   Disabling Dual Power Feed

Use the setdualpowerfeed command of the XSCF firmware to disable dual power feed.

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s disable
```

To target all chassis in the system, specify -a.
To target only a given chassis in the system, specify -b bb_id. For bb_id, specify the BB-ID of the chassis. You can specify an integer from 0 to 15 or 80 to 83, depending on the system configuration.

Operation Procedure

1. **Disable dual power feed with the setdualpowerfeed command.**
   In the following example, the target is all chassis.

```
XSCF> setdualpowerfeed -a -s disable
BB#00:enable -> disable
BB#01:enable -> disable
NOTE: Dual power feed will be change the next time the platform is powered on.
```

4.3.3 Checking the Dual Power Feed Setting

Use the showdualpowerfeed command of the XSCF firmware to check the dual power feed setting.

```
XSCF> showdualpowerfeed
```

The output is any of the following, depending on the status.
- **Output when dual power feed is enabled**

```
BB#00: Dual power feed is enabled.
```

- **Output when dual power feed is disabled**

```
BB#00: Dual power feed is disabled.
```

- **Output when dual power feed was changed from enabled to disabled**

```
BB#00:enable -> disable
NOTE: Dual power feed will be change the next time the platform is powered on.
```

- **Output when dual power feed was changed from disabled to enabled**

```
BB#00:disable -> enable
NOTE: Dual power feed will be change the next time the platform is powered on.
```

Operation Procedure

1. **Check the dual power feed setting with the showdualpowerfeed command.**
   In the following example, you can see a change from disabled to enabled in a
   system configuration with BB-ID 0 and BB-ID 1.

```
XSCF> showdualpowerfeed
BB#00:disable -> enable
BB#01:disable -> enable
NOTE: Dual power feed will be change the next time the platform is powered on.
```

4.4   Reducing Power Consumption

This section describes various prepared functions for reducing the power consumption
of the SPARC M12/M10.

4.4.1   Setting the Upper Limit Value of Power Consumption

In the SPARC M12/M10, you can set the upper limit value of power consumption
and the operation to perform when the upper limit value is exceeded.

Use the setpowercapping command of XSCF firmware to set the upper limit value of
power consumption.
Execute the command with a user account that has the platadm or fieldeng privilege.
Immediately after the command is executed, the set value is reflected by the XSCF.

```
XSCF> setpowercapping -s option=value [[-s option=value]...]
```

You can set the following items for option and value.

- Enabling/Disabling power capping function (activate_state)
  Specify either enabled or disabled. The default is disabled.

- Setting the upper limit value of power consumption
  Specify it in either of the following ways.
  - Number in watts (powerlimit_w)

    You can specify a numeric value from 0 to 999999.

  - Percentage (powerlimit_p)

    You can specify a numeric value from 0 to 100.

- Extension time when the upper limit value is exceeded (timelimit)
  You can specify an extension time in seconds, with a numeric value from 10 to

99999. You can also specify the following values for the extension time:

- default: 30 seconds

- none: No extension time

- Operation to perform for a violation (violation_actions)
  Specify the operation to perform when the extension time is exceeded after the upper limit value is exceeded. Specify any of the following operations. The default is none.

  - none

    Output the message.

  - shutdown

    Output the message and shut down physical partitions until power consumption falls below the upper limit value. An ordered shutdown is carried out on the physical partitions in decreasing order of PPAR-ID.

  - poff

    Output the message and forcibly power off physical partitions until power consumption falls below the upper limit value. The physical partitions are forcibly stopped in decreasing order of PPAR-ID.

Note - If the setting of the upper limit value of power consumption is based on the average power consumption during operation, the rush current generated in the power-on process, self-diagnosis test, etc. at SPARC M12/M10 system startup may be a problem. You can prevent exceeding the upper limit value of power consumption by using the setpowerupdelay command, which is an XSCF command, to stagger the power-on times of multiple physical partitions to even out the rush current.

Note - When the burden on the server suddenly increases due to the customer's operation, power consumption may also increase sharply. As a result, power consumption may exceed the designated upper limit over a long period of time. Therefore, before starting system operation for your business, set the value for violation_actions to "none" (default) to avoid affecting the continuity of system operation. Next, after executing an environment test on the customer's side, make sure that the upper limit for power consumption (powerlimit_w, powerlimit_p) is not too low, and the extension time (timelimit) for the upper limit to be exceeded is not too short. Then, set the value for violation_actions.

For details of the setpowercapping command, see the man page of the setpowercapping(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operation Procedure

1. **Execute the showenvironment power command to check the system power information.**
   Using the values for [Peak Permitted] and [Actual AC power consumption], set the upper limit for power consumption.

```
XSCF> showenvironment power
Power Supply Maximum      :5000W
Installed Hardware Minimum:1268W
Peak Permitted            :2322W
BB#00
    Permitted AC power consumption:5000W
    Actual AC power consumption   :1719W
```

Each item shows the following:

- Power Supply Maximum: Maximum power consumption of the power supply unit (PSU) for the entire system

- Installed Hardware Minimum: The minimum value that can be set with setpowercapping

- Peak Permitted: Reference value for assumed peak power

- Permitted AC power consumption: Maximum power consumption of the PSU (*1)

- Actual AC power consumption: Actual power consumption value in the chassis

*1 In the SPARC M12, "Available AC power consumption" is displayed. The rated power consumption of the PSU is also displayed.

2. **Execute the setpowercapping command.**
   The following example sets 1800 W as the upper limit value for power consumption and 90 seconds as the extension time when the upper limit value is exceeded.

```
XSCF> setpowercapping -s powerlimit_w=1800 -s timelimit=90
activate_state      : enabled -> -
powerlimit          : 2322w -> 1800w
timelimit           : 30 -> 90
violation_actions   :none -> -
The specified options will be changed.
Continue? [y|n]      :y
configured.
activate_state      :enabled
powerlimit          :1800w
timelimit           :90
violation_actions   :none
```

3. **Enable the limit for power consumption.**

```
XSCF> setpowercapping -s activate_state=enabled
activate_state      :disabled -> enabled
powerlimit          :1800w -> -
timelimit           :90 -> -
violation_actions   :none -> -
The specified options will be changed.
Continue? [y|n]      :y
configured.
activate_state      :enabled
```

```
powerlimit              :1800w
timelimit               :90
violation_actions       :none
```

4.4.2 Handling of Abnormal Temperature/Burden Due to Abnormal Power

One function prepared in the SPARC M12/M10 reduces the CPU frequency to continue operation when a burden caused by abnormal temperature, abnormal power, or some other problem is detected. This function is controlled for each CPU on the SPARC M12/M10. When the problem involving the temperature or power abnormality burden is resolved, the CPU frequency automatically returns to its original value.

4.4.3 Reducing the Power Consumption of Hardware That is Unused or Has a Low Utilization

In the SPARC M12/M10, you can set the operation for each physical partition to reduce the power consumption of the hardware that is unused or has a low utilization (power-saving operation).

When a setting that reduces the power consumption is made, the target hardware operates at a power-saving level according to its utilization. Therefore, power to hardware with a low utilization is reduced, and with an increase to the utilization, the power supply to the hardware increases.

In the SPARC M12, the power consumption can also be reduced with nearly no affect on the CPU processing performance through use of the Solaris Power Aware Dispatcher.
For software requirements of the XCP firmware and Oracle Solaris for using the Solaris Power Aware Dispatcher to reduce power consumption, see the latest version of the *Fujitsu SPARC M12 Product Notes*.

To set the above power-saving operation for hardware, use the setpparmode command of the XSCF firmware. Execute the command with a user account that has the platadm or pparadm privilege.

- **SPARC M12**
  To set the power-saving operation for SPARC M12, use the -m powermgmt_policy option.

```
XSCF> setpparmode -p ppar_id -m powermgmt_policy={elastic|performance|disabled}
```

With the powermgmt_policy option, you can enable (elastic or performance) or disable (disabled) the power-saving operation. The default is disabled. The setting

is reflected immediately after the command is executed.

The meaning of each option setting value is as follows.

- elastic
  Enables power-saving operation of CPU and memory. Changes system power usage according to the current utilization levels of CPUs and memory. This can reduce system power consumption.

- performance
  Enables power-saving operation of CPU. This can save power without much of an effect on performance because unused, idle CPUs in the system operate at slower speeds or may have entered the sleep state.

- disabled (default)
  Disables power-saving operation of CPU and memory. All CPUs and memory in the system will continuously operate at the highest performance.

Note - When the power-saving operation is enabled with the elastic option specified, power consumption can be reduced, but the CPU performance may be degraded. Specifying the performance value reduces the power consumption with nearly no affect on the CPU processing performance.

If the firmware is updated from a version earlier than XCP3040 to XCP3040 or later, the Power Aware Dispatcher function (PAD function) to use the Solaris Power Aware Dispatcher is disabled (off).
When you specify performance for the powermgmt_policy option, you need to change the PAD function to enabled (on).
When you specify disabled or elastic for the powermgmt_policy option, whether the setting of the PAD function is on or off makes no difference in the power-saving operation.
To change the setting of the PAD function, use the -m pad option.

```
XSCF> setpparmode -p ppar_id -m pad={off|on}
```

With pad, you can enable (on) or disable (off) the PAD function. The default is enabled (on).

The meaning of each option setting value is as follows.

- on (default)
  Enables the PAD function.

- off
  Disables the PAD function.
  When you set this option to off, the powermgmt_policy option must be disabled or elastic.

Make the setting of the PAD function when the PPAR is stopped.
When the setting of the PAD function is changed from the disabled state to the enabled state or vice versa, the configuration information of the logical domain is restored to factory-default after the PPAR starts. In this case, the logical domains need to be reconfigured. Save the configuration information in an XML file in advance.

- **SPARC M10**

To set the power-saving operation for SPARC M10, use the -m elastic option.

```
XSCF> setpparmode -p ppar_id -m elastic={on|off}
```

With elastic, you can enable (on) or disable (off) the power-saving operation. It is disabled (off) by default. The setting is reflected immediately after the command is executed.

The meaning of each option setting value is as follows.
- on
  Enables power-saving operation of CPU and memory. Changes system power usage according to the current utilization levels of CPUs and memory. This can reduce system power consumption.
- off (default)
  Disables power-saving operation of CPU and memory. All CPUs and memory in the system will continuously operate at the highest performance.

Note - When the power-saving operation is enabled, power consumption can be reduced, but the CPU performance may be degraded.

For details on the setpparmode command, see the man page of the setpparmode(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operation Procedure

- **SPARC M12**

Note -
- When the PAD function is disabled, you cannot change the setting of the power-saving operation to performance. After enabling the PAD function (on), change the setting to performance.
- When the power-saving operation is set to performance, you cannot disable the PAD function (off). After setting the power-saving operation to disabled or elastic, disable the function.

The following is an example for setting the power-saving operation to performance.

1. **Execute the showpparmode command to confirm the settings of the power-saving operation and PAD function. The following example indicates that the power-saving operation is disabled and the PAD function is enabled.**

```
XSCF> showpparmode -p 0
Host-ID                 :90060027
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
```

```
Power Aware Dispatcher    :on
Power Management Policy  :disabled
IOreconfigure           :false
CPU Mode                :-
PPAR DR(Current)        :-
PPAR DR(Next)           :off
```

2. **Execute the setpparmode command to set the power-saving operation to performance.**

```
XSCF> setpparmode -p 0 -m powermgmt_policy=performance
Diagnostic Level        :min          -> -
Message Level           :normal       -> -
Alive Check             :on           -> -
Watchdog Reaction       :reset        -> -
Break Signal            :on           -> -
Autoboot(Guest Domain)  :on           -> -
Power Aware Dispatcher   :on           -> -
Power Management Policy  :disabled     -> performance
IOreconfigure           :false        -> -
CPU Mode                :-
PPAR DR                 :off          -> -
The specified modes will be changed.
Continue? [y|n] :y
configured.
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on (alive check:available)
Watchdog Reaction       :reset (watchdog reaction:reset)
Break Signal            :on (break signal:non-send)
Autoboot(Guest Domain)  :on
Power Aware Dispatcher   :on
Power Management Policy  :performance
IOreconfigure           :false
CPU Mode                :-
PPAR DR                 :off
```

3. **Execute the showpparmode command, and confirm the setting.**

```
XSCF> showpparmode -p 0
Host-ID                 :90060027
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
Power Aware Dispatcher   :on
Power Management Policy  :performance
IOreconfigure           :false
CPU Mode                :-
PPAR DR(Current)        :-
```

```
PPAR DR(Next)             :off
```

- For SPARC M10

The following is an example for enabling the power-saving operation.

1. **Execute the showpparmode command to check whether the power-saving operation is enabled/disabled for hardware that is unused or has a low utilization.**

```
XSCF> showpparmode -p 0
Host-ID                   :0f010f10
Diagnostic Level          :min
Message Level             :normal
Alive Check               :on
Watchdog Reaction         :reset
Break Signal              :on
Autoboot(Guest Domain)    :on
Elastic Mode              :off
IOreconfigure             :true
CPU Mode                  :auto
PPAR DR(Current)          :-
PPAR DR(Next)             :off
```

2. **Execute the setpparmode command to enable the power-saving operation.**

```
XSCF> setpparmode -p 0 -m elastic=on
Diagnostic Level          :min      -> -
Message Level             :normal   -> -
Alive Check               :on       -> -
Watchdog Reaction         :reset    -> -
Break Signal              :on       -> -
Autoboot(Guest Domain)    :on       -> -
Elastic Mode              :off      -> on
IOreconfigure             :true     -> -
CPU Mode                  :auto     -> -
PPAR DR                   :off      -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level          :min
Message Level             :normal
Alive Check               :on (alive check:available)
Watchdog Reaction         :reset (watchdog reaction:reset)
Break Signal              :on (break signal:non-send)
Autoboot(Guest Domain)    :on
Elastic Mode              :on
IOreconfigure             :true
CPU Mode                  :auto
PPAR DR                   :off
```

3. **Execute the showpparmode command, and confirm the setting.**

```
XSCF> showpparmode -p 0
Host-ID                    :0f010f10
Diagnostic Level           :min
Message Level              :normal
Alive Check                :on
Watchdog Reaction          :reset
Break Signal               :on
Autoboot(Guest Domain)     :on
Elastic Mode               :on
IOreconfigure              :true
CPU Mode                   :auto
PPAR DR(Current)           :-
PPAR DR(Next)              :off
```

4.5 Connecting a DVD Drive

The SPARC M12/M10 does not have an internal DVD drive. To install Oracle Solaris and business applications from a DVD drive, use a DVD drive connected in either of the following ways:
- External DVD drive connected to a USB port
- DVD drive mounted on a terminal connected to the XSCF-LAN

This section describes the external DVD drive connected to a USB port. To use the DVD drive mounted on a terminal, see "4.6   Using Remote Storage."

4.5.1 Using an External DVD Drive

The SPARC M12/M10 chassis has been prepared with USB ports at the front and rear. To use an external DVD drive, connect it to one of the USB ports. Use a dedicated AC adapter to supply power to the connected external DVD drive.

Figure 4-1   USB Port (SPARC M12-1) that can be Connected to a DVD Drive
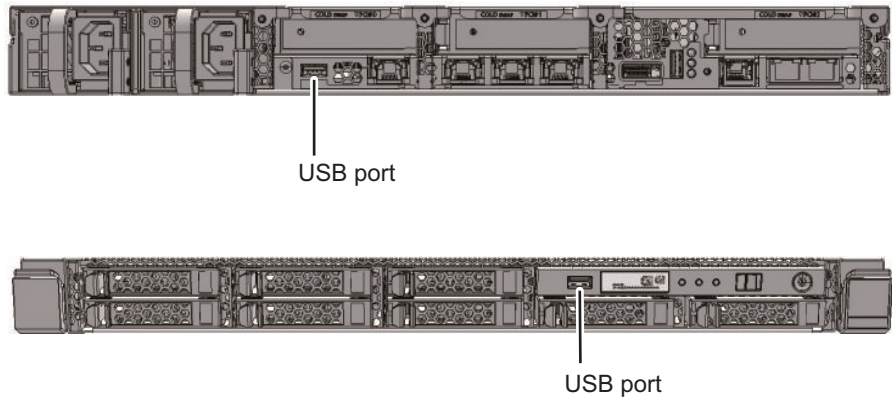
USB port

USB port

Figure 4-2   USB Port (SPARC M12-2) that can be Connected to a DVD Drive
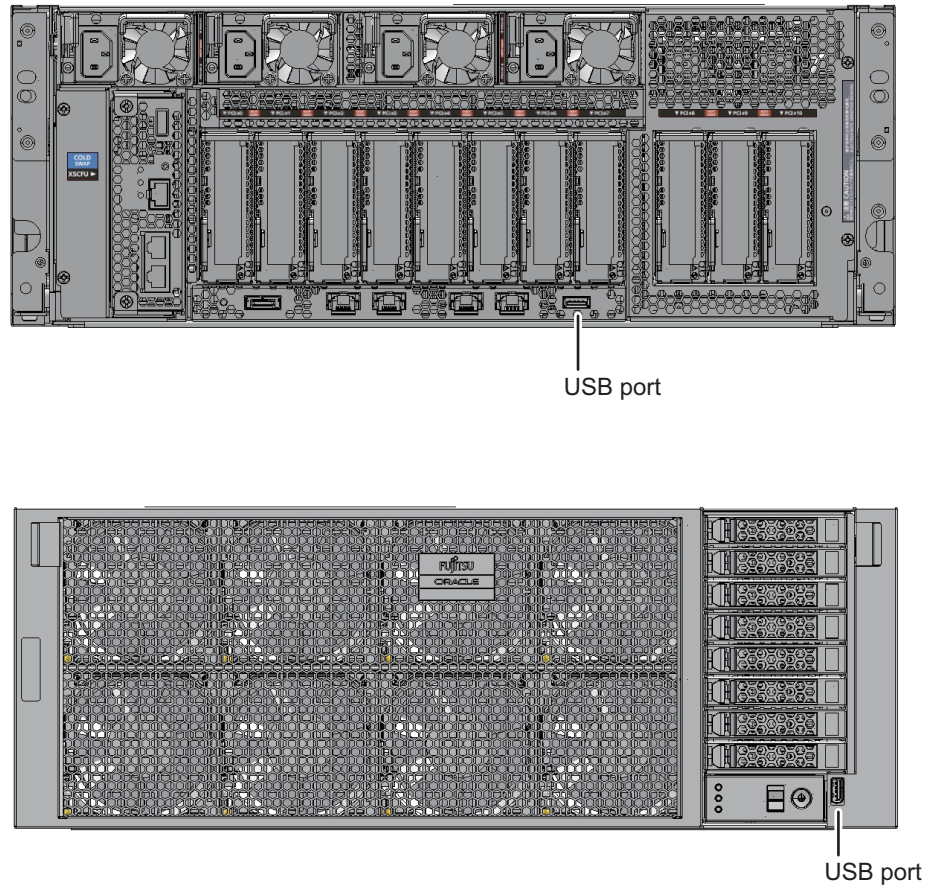
USB port

USB port

Figure 4-3   USB Port (SPARC M12-2S) that can be Connected to a DVD Drive
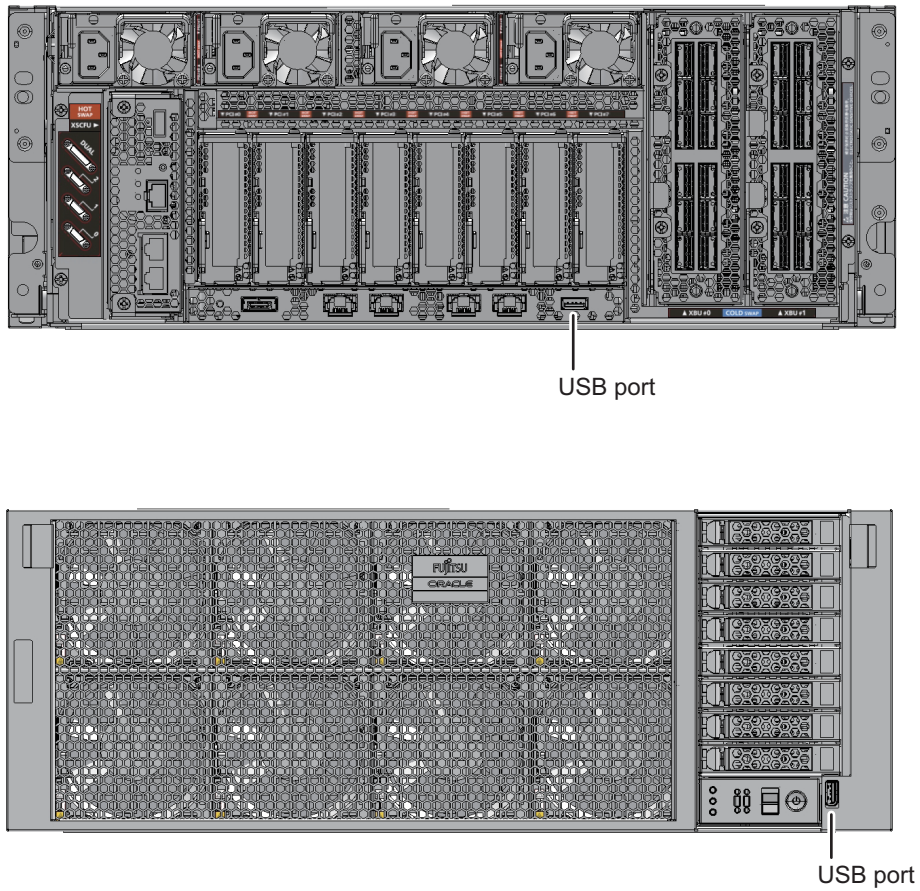
USB port

USB port

Figure 4-4   USB Port (SPARC M10-1) that can be Connected to a DVD Drive
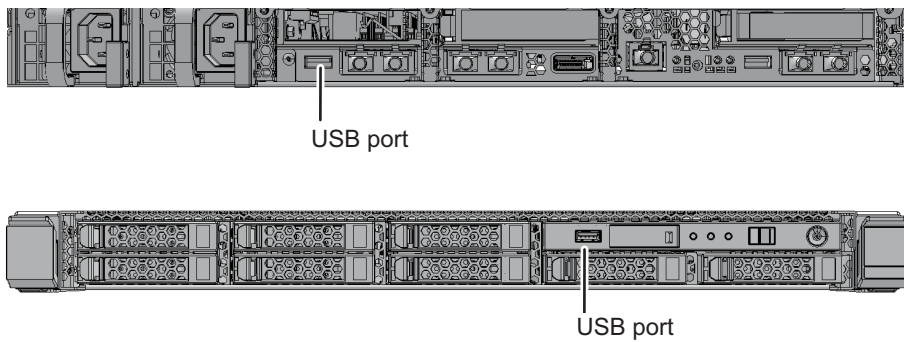
USB port

USB port

Figure 4-5   USB port (SPARC M10-4/M10-4S) that can be connected to a DVD
             drive

USB port

USB port
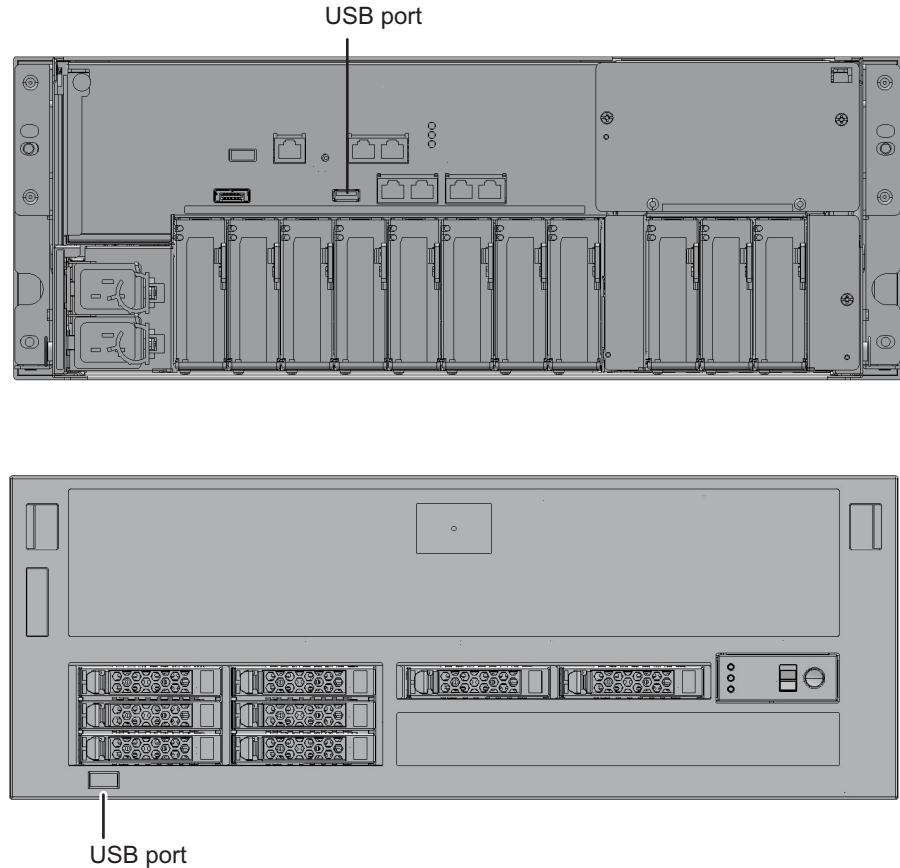
4.5.2 Using the External DVD Drive to Install Oracle Solaris

When installing Oracle Solaris on OpenBoot PROM from a CD/DVD-ROM drive,
specify the device path that is suitable for the model of SPARC M12/M10 that you are
using. For details of the device path for each model, see "Appendix A   Lists of
SPARC M12/M10 System Device Paths." For details of DVD drive aliases, see
"Appendix J   Lists of DVD Drive Aliases."

The following shows the procedure for specifying a device path and installing Oracle
Solaris.

1. **Connect a USB DVD drive to a USB port on the front or rear of the chassis.**
   If multiple DVD drives are connected, disconnect every USB DVD drive that will
   not to be used for installation.

2. **From the ok prompt of OpenBoot PROM, execute the show-disks command**

and confirm the device path.

- Example of connecting a USB DVD drive on the front panel in the SPARC M12-1

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive (USB 3.0) on the rear panel in the SPARC M12-1

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive (USB 2.0/1.1) on the rear panel in the SPARC M12-1

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive on the front panel in the SPARC M12-2/M12-2S

  When two CPUs are mounted

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive (USB 3.0) on the rear panel in the SPARC M12-2/ M12-2S

Note - If USB 3.0 is used, it works as USB 2.0.

When two CPUs are mounted

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive (USB 2.0/1.1) on the rear panel in the SPARC M12-2/ M12-2S

  When two CPUs are mounted

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive on the front panel in the SPARC M10-1

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive on the rear panel in the SPARC M10-1

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive on the front panel in the SPARC M10-4/M10-4S

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
```

```
Enter Selection, q to quit: q
```

- Example of connecting a USB DVD drive on the rear panel in the SPARC
  M10-4/M10-4S

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

3. **Specify the device path that was shown in a) of Step 2, execute the boot
   command, and install Oracle Solaris.**

- Example of specifying a USB DVD drive connected on the front panel in the
  SPARC M12-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk
```

- Example of specifying a USB DVD drive (USB 3.0) connected on the rear panel in
  the SPARC M12-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk
```

- Example of specifying a USB DVD drive (USB 2.0/1.1) connected on the rear panel
  in the SPARC M12-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk
```

- Example of specifying a USB DVD drive connected on the front panel in the
  SPARC M12-2/M12-2S when two CPUs are mounted

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
```

- Example of specifying a USB DVD drive (USB 3.0) connected on the rear panel in
  the SPARC M12-2/M12-2S when two CPUs are mounted

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk
```

- Example of specifying a USB DVD drive (USB 2.0/1.1) connected on the rear panel
  in the SPARC M12-2/M12-2S when two CPUs are mounted

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk
```

- Example of specifying a USB DVD drive connected on the front panel in the SPARC M10-1

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk
```

- Example of specifying a USB DVD drive connected on the rear panel in the SPARC M10-1

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk
```

- Example of specifying a USB DVD drive connected on the front panel in the SPARC M10-4/M10-4S

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk
```

- Example of specifying a USB DVD drive connected on the rear panel in the SPARC M10-4/M10-4S

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk
```

Note - Depending on the type of CD/DVD drive being used, "/cdrom@x" may instead be "/storage@x."

Note - Suppose that only a USB DVD drive on the front panel is connected with the SPARC M10-4/M10-4S and you specify the drive path to a USB DVD drive on the rear panel to execute the boot command. Even though the specified device path is incorrect, the boot is performed from the USB DVD connected to the front panel. When executing the boot command, always confirm that the specified device is correct.

4.6 Using Remote Storage

This section describes the remote storage that enables access to the mounted storage (media) in terminals. For remote storage, use the XSCF network interface Ethernet (XSCF-LAN).

4.6.1 What is Remote Storage?

Remote storage is a function for accessing the storage in terminals, such as the system management terminal or a user PC, via the XSCF-LAN. Remote storage supports only reading from storage to a SPARC M12/M10. Figure 4-6 is a conceptual diagram showing how the remote storage function is used from OpenBoot PROM or Oracle Solaris to access media in a terminal.

Figure 4-6   Conceptual Diagram of Remote Storage
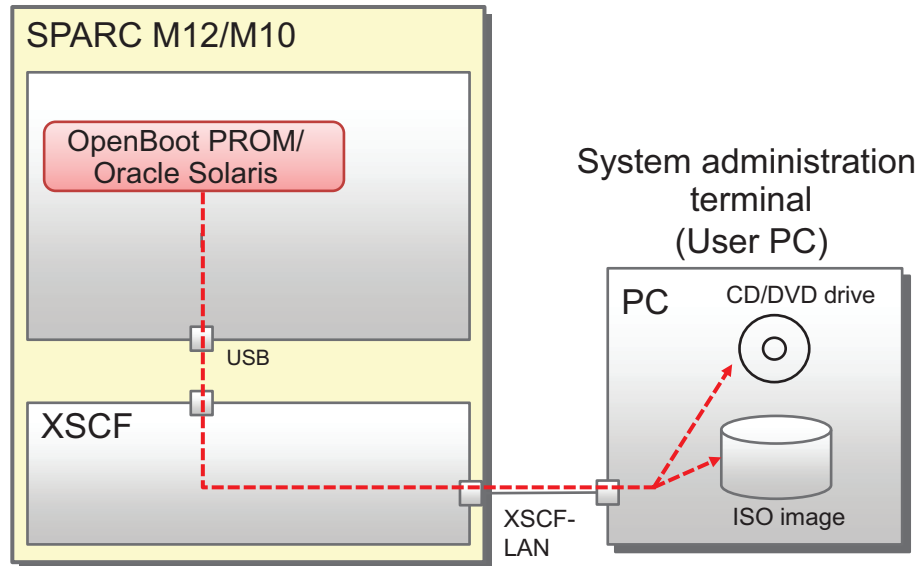
Remote storage enables connections from logical domains to the following media:
- Media inserted into the CD/DVD drive mounted on/connected to a terminal
- ISO image on a terminal

Also, if all of the following environments are in place, you can use remote storage through the required settings with the XSCF:
- Environment required for the SPARC M12/M10 system
  - The XSCF-LAN network can be used.
  - The HTTPS service is enabled and XSCF Web can be used. (In case of settings from XSCF Web.)
- Environment required for terminals
  The Java Runtime Environment software can be used.

For details on the XSCF network settings, see "3.9   Configuring the XSCF Network." For details of the XSCF Web operating requirement and the procedure for enabling the XSCF HTTPS service, see "3.8   Configuring the HTTPS Service for Login to the XSCF." Also, for details of the operating requirements of the Java Runtime Environment software on terminals, see "4.6.4   Operating Requirement of Terminals and Browsers."

As Seen From Oracle Solaris

When media in terminals are accessible from logical domains using remote storage, the remote storage devices are recognized as USB devices from OpenBoot PROM and Oracle Solaris, as shown below.

- An example of Oracle Solaris

```
# cfgadm -al
Ap_Id Type Receptacle Occupant Condition
...
usb1/3 usb-storage connected configured ok
```

- An example of OpenBoot PROM

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

For details on how to connect media, see "4.6.12   Connecting to Media When Using Remote Storage." For details on how to access media, see "4.6.13   Using Remote Storage From Oracle Solaris."

4.6.2　Remote Storage Network Configuration

Network Configuration

Remote storage uses the XSCF-LAN network of the SPARC M12/M10 to implement access to media in terminals.
Figure 4-7 shows the network configuration when using remote storage, where the system is configured with only one SPARC M12/M10.

Figure 4-7   System Configured With Only One SPARC M12/M10
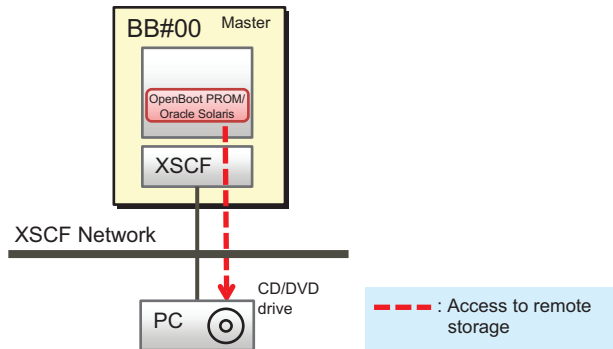
Figure 4-8 shows the network configuration when using remote storage in the system in a building block configuration (with no crossbar boxes). The LAN of the master XSCF and system management terminal, the XSCF-LAN used with remote storage, and the LAN of terminals are connected in the same subnet.

Figure 4-8   Remote Storage Network Configuration (No Crossbar Box)
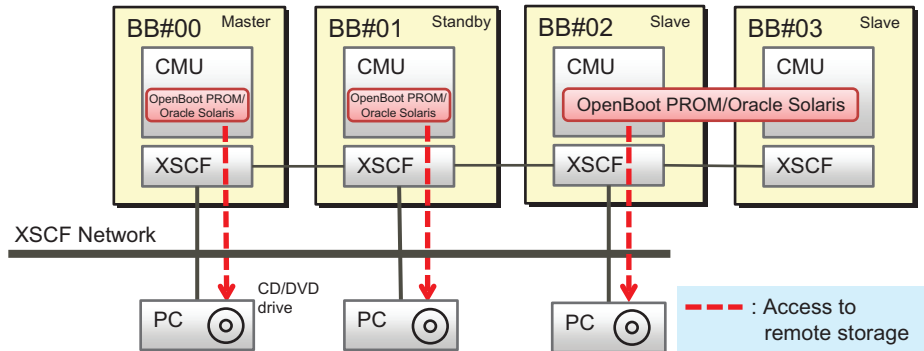
Note - If there is only one PC, you can even use the remote storage from each SPARC M12/M10 by switching the connecting SPARC M12/M10 system chassis each time.

Figure 4-9 shows the network configuration when using remote storage, where the system in a building block configuration is connected to a crossbar box. When using remote storage, do not use the XSCF-LAN of the crossbar box chassis to connect to media. Use the XSCF-LAN of the SPARC M12/M10, which is a slave chassis. In Figure 4-9, the LAN of the master XSCF and system management terminal, the XSCF-LAN used with remote storage, and the LAN of terminals are connected in the same subnet.

Figure 4-9   Remote Storage Network Configuration (When Connected to a Crossbar Box)
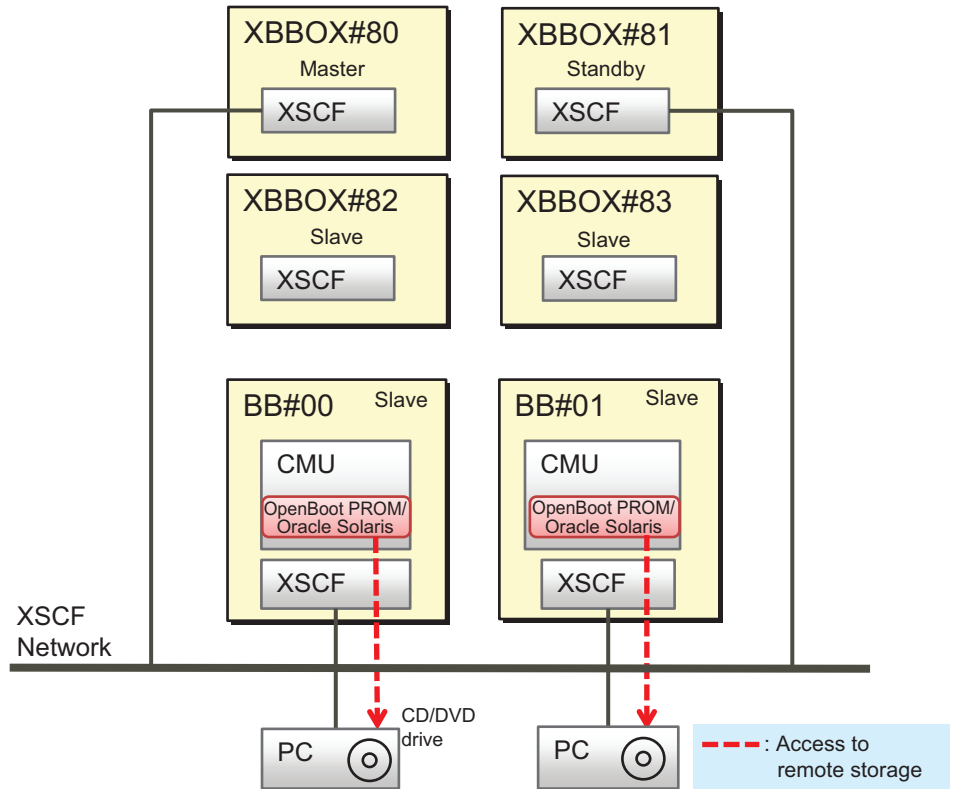
Note - If there is only one PC, you can even use the remote storage from each SPARC M12/M10 by switching the connecting SPARC M12/M10 system chassis each time.

Rules on 1-to-1 connection between a SPARC M12/M10 and a PC

As shown in Figure 4-10, the SPARC M12/M10 chassis is connected to terminal (PC) media on a 1-to-1 basis. The same SPARC M12/M10 chassis cannot be connected to two or more terminals, and multiple SPARC M12/M10 chassis cannot be connected to the same terminal at the same time.

For a connection from the BB#00 logical domain to media in a terminal via the XSCF of BB#01, note that BB#00 and BB#01 must belong to the same physical partition.

Figure 4-10   Rules on Connection With a SPARC M12/M10 Chassis
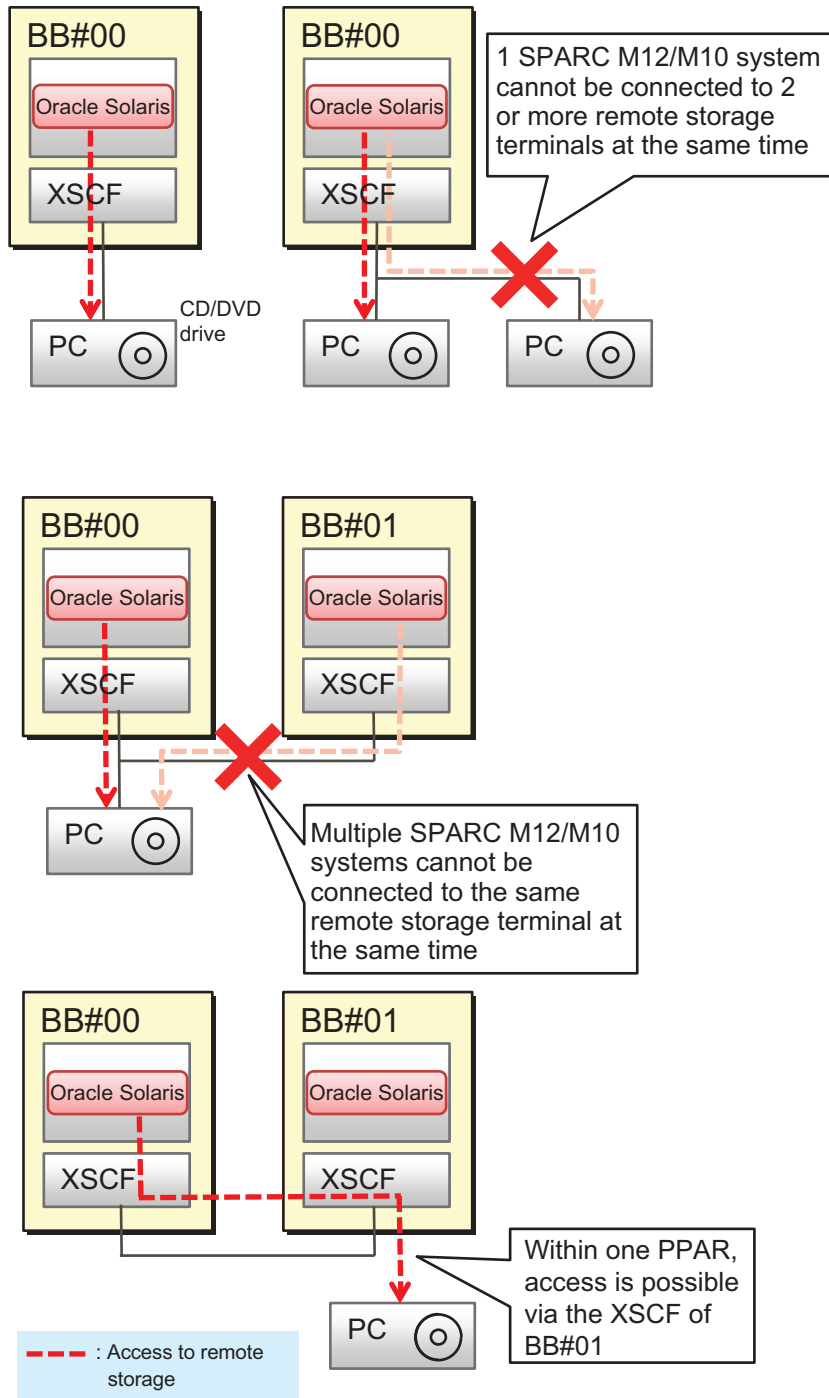
As shown in Figure 4-11, in a system configuration with multiple SPARC M12-2S systems or multiple SPARC M10-4S systems, a terminal may be installed for each

SPARC M12-2S/M10-4S system on a 1-to-1 basis. Of these installed terminals, multiple terminals can be connected at the same time. Likewise, in a configuration of physical partitions with multiple SPARC M12-2S systems or multiple /M10-4S systems, as many terminals as the number of configured chassis can be connected at the same time.

Figure 4-11   Forms of Simultaneous Connection for Multiple SPARC M12-2S or SPARC M10-4S Systems
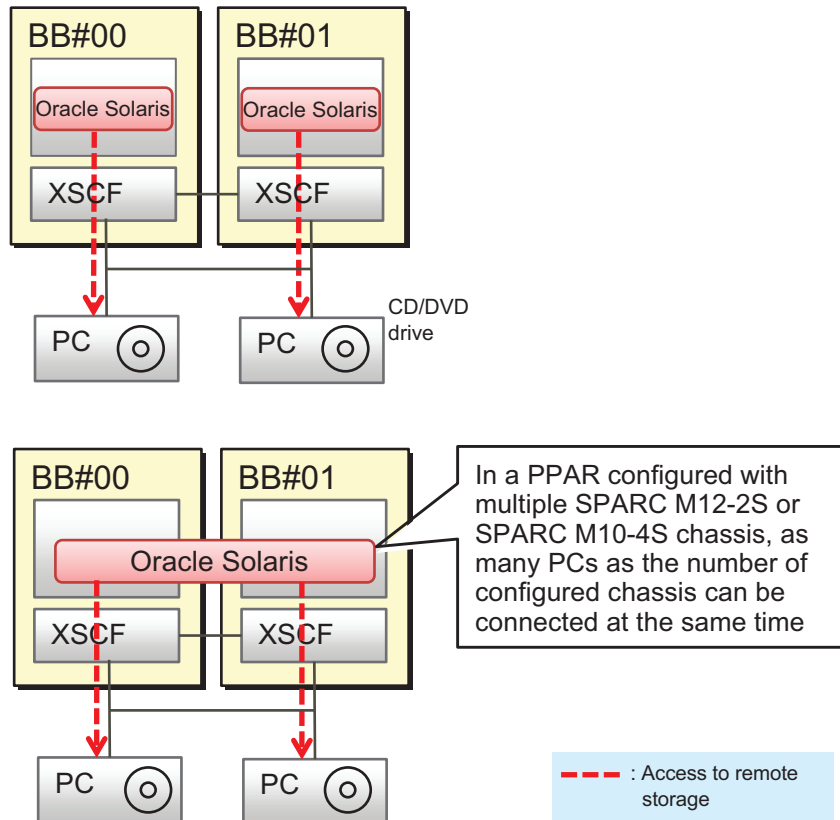
Connection via a Slave XSCF

As shown in Figure 4-12, the remote storage of SPARC M12/M10 can even be connected via a slave XSCF.

Note - The XSCF-LAN of the slave XSCF can be used only for remote storage. It cannot be used for services such as Telnet, SSH, XSCF Web, and SNMP.

Note - The XSCF-LAN of the slave crossbar box cannot be used for remote storage.

Figure 4-12　Connection to Remote Storage via a Slave XSCF
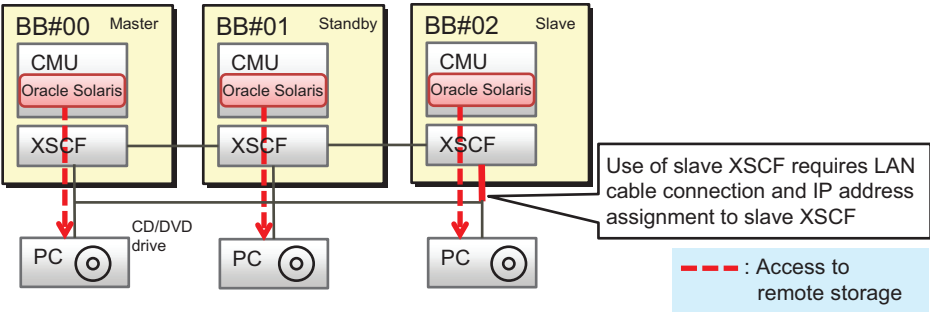
Note - If there is only one PC, you can even use the remote storage from each SPARC M12/M10 by switching the connecting SPARC M12/M10 system chassis each time.

Before starting to configure remote storage

Before starting to configure remote storage, you need to have completed the network settings of the master/standby XSCF. This is because the XSCF must be rebooted when the master/standby XSCF network has been configured. Also, to make settings and perform operations from XSCF Web, the network settings of the master XSCF and the HTTPS service settings must already be done to enable the HTTPS service. This allows XSCF Web to be used.

For connection via a slave XSCF, you need to connect an XSCF-LAN cable and set the XSCF-LAN IP address. Also, for the network settings of the slave XSCF, configure remote storage from XSCF Web or the XSCF shell, not with the setnetwork command or the [Network] menu on the XSCF Web.

If the crossbar box is connected, the XSCF-LAN IP address of the SPARC M12/M10 (slave chassis) connected to the crossbar box must be set to prevent the XSCF-LAN of the crossbar box from being used for remote storage.

Table 4-2 lists XSCF network setting differences between using remote storage via the master/standby XSCF and using it via a slave XSCF.

Table 4-2　Differences of XSCF Network Settings for Using Remote Storage

XSCF	XSCF-LAN Network Settings
SPARC M12/M10 chassis of master/standby XSCF	[Network] page of XSCF Web Alternatively, setnetwork, setroute, and applynetwork commands **Note -** An XSCF reboot is required.

XSCF	XSCF-LAN Network Settings
SPARC M12/M10 chassis of slave XSCF	[Remote Storage] page of XSCF Web Alternatively, setremotestorage and showremotestorage commands **Note -** An XSCF reboot is not required.

Note - If no gateway is set in the routing settings, the terminal and XSCF-LAN must be connected in the same subnet.

In a system configuration with multiple SPARC M12-2S systems or multiple SPARC M10-4S systems, the physical IP address is used as the XSCF-LAN IP address to access media in a terminal with remote storage. The takeover IP address (virtual address) is not used.
For details on the XSCF network settings, see "4.6.10   Configuring the XSCF-LAN Used with Remote Storage."

4.6.3   Means of Using Remote Storage

Two types of screen are used in the settings and operations for using remote storage. One is the XSCF Web console or XSCF shell. The other is the [XSCF Remote Storage Server] screen on a terminal (PC).
Figure 4-13 shows the [Remote Storage] page of XSCF Web. On the page, you can configure remote storage. You can also configure it by using the setremotestorage command from the XSCF shell.

Figure 4-13   [Remote Storage] Page of XSCF Web
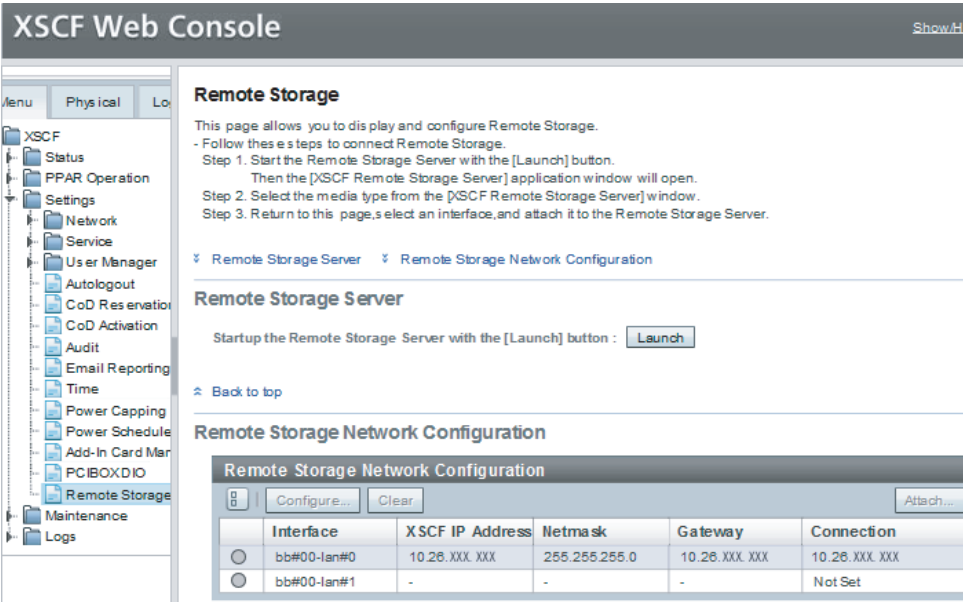
Figure 4-14 shows the [XSCF Remote Storage Server] screen. Use it to select/start media.

Figure 4-14   [XSCF Remote Storage Server] Screen
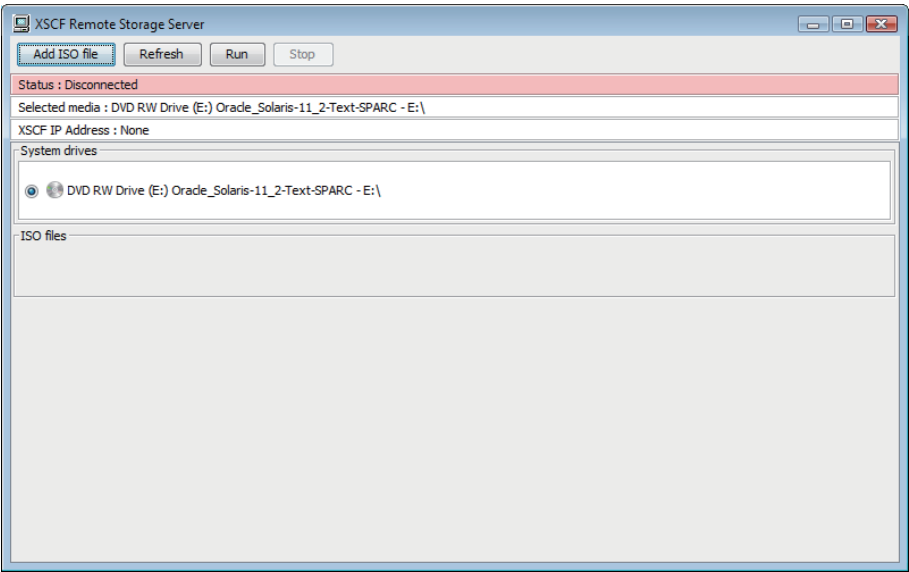
The two ways of opening the [XSCF Remote Storage Server] screen on a terminal (PC) are as follows:

■ Starting XSCF Remote Storage Server from XSCF Web

Click the [Launch] button on the [Remote Storage] page of XSCF Web (Figure 4-13) to start XSCF Remote Storage Server.

XSCF Remote Storage Server starts with the Java Runtime Environment software at the terminal, then the [XSCF Remote Storage Server] screen opens (Figure 4-14).

- Starting XSCF Remote Storage Server with the Java command from a terminal Execute the Java command from the command prompt on the terminal to start XSCF Remote Storage Server (see Figure 4-15). XSCF Remote Storage Server starts on the Java Runtime Environment software at the terminal, opening the [XSCF Remote Storage Server] screen (Figure 4-14).

Figure 4-15   Starting XSCF Remote Storage Server With the Java Command From a Terminal

```
C:\rdvd>"C:\Program Files (x86)\Java\jre1.8.0_201\bin\java.exe" -esa -cp rdvd_client.jar;lib\*
com.fujitsu.m10.rdvd.gui.GUIMain
```

Figure 4-15 shows an example of an environment where Oracle Java SE is installed. Specify the execution path of the Java command according to the environment used. For details on how to obtain and extract the file required for command execution, see "Before Using Remote Storage" in "4.6.9   Flow for Using Remote Storage."

The option and class path specified in the Java command are fixed. Specify "com.fujitsu.m10.rdvd.gui.GUIMain", even with the SPARC M12.

Media can be connected/stopped as many times as needed while XSCF Remote Storage Server is running.
While XSCF Remote Storage Server is running, you can connect media to the SPARC M12/M10 by performing the "Attach" operation from XSCF Web or with the setremotestorage command.

4.6.4   Operating Requirement of Terminals and Browsers

This section describes the necessary operating requirements and various settings for using remote storage.

Operating Requirement of Terminals and Browsers

Table 4-3 lists the operating requirement for the Windows OS on terminals, supporting remote storage.

Table 4-3　　Operating Requirement of Terminals

Type	Operating Requirement
Windows OS	Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (When Windows support ends, support for the remote storage function also ends.)

- Starting XSCF Remote Storage Server From XSCF Web
  The Java Runtime Environment installed on the terminal must be the version
  corresponding to the browser used with XSCF Web. Table 4-4 lists combinations
  of the Java Runtime Environment and browser.

Table 4-4　　Combinations of the Java Runtime Environment and Browser Used With XSCF Web

Browser	Java Runtime Environment (*1)
Microsoft Internet Explorer 8 or 9, 32-bit version	Java Runtime Environment 8, 32-bit version
Microsoft Internet Explorer 8 or 9, 64-bit version	Java Runtime Environment 8, 64-bit version
Microsoft Internet Explorer 10 or 11	Java Runtime Environment 8, 32-bit version
Mozilla Firefox 10.0 to ESR 52 32-bit version (*2)	Java Runtime Environment 8, 32-bit version

*1 Java applets can no longer be used when the April 2019 update or a later update
provided for Oracle Java SE 8 is applied. As a consequence, XSCF Remote Storage
Server cannot be started from XSCF Web. Start XSCF Remote Storage Server with
the Java command from a terminal.

*2 Java plug-in support ended with ESR 60. This means you cannot use remote
storage from ESR 60 or later. Use Internet Explorer.

Note - Download the Java Runtime Environment from the Oracle website.

- Starting XSCF Remote Storage Server with the Java command from a terminal
  Operation of XSCF Remote Storage Server has been confirmed on the Java
  Runtime Environments shown in Table 4-5.

Table 4-5　　Java Runtime Environment Versions Where Operation is Already Confirmed

Type	Version
Oracle Java SE	8u201, 8u202
Open Java Development Kit	11.0.2

For details of terminal operating systems, the latest supported versions of the Java

Runtime Environment, and supported browsers of XSCF Web, see the latest *Product Notes* for your server.

Directory Settings of the Windows OS Environment Variable TMP

When run, XSCF Remote Storage Server generates the following three files for maintenance and control. The files are generated in the folder that is set in the Windows OS environment variable TMP on the terminal. If these files cannot be generated in the set folder, XSCF Remote Storage Server fails to start, disabling remote storage.
- Trace file (Remote_Storage_Trace.txt, maximum 512 KB)
- Compressed trace file from the preceding generation (Remote_Storage_Trace_1.txt. zip, maximum size of 512 KB)
- Lock file for monitoring multiple startups (RemoteStorageLockFile 0B)

When using remote storage, be sure to confirm the following.
- A directory is set in the Windows OS environment variable TMP.
- The access privileges to the set directory are not administrator privileges.

In the Windows OS, the following folder is the default setting for the environment variable TMP.

```
%USERPROFILE%\AppData\Local\Temp
```

When remote storage is used with the default setting, the start of XSCF Remote Storage Server generates the files in the following folder. We recommend using the default setting.

```
C:\Users\UserName\AppData\Local\Temp\Remote_Storage\
```

Port Used and Permission on a Terminal

The terminal uses the tcp/3260 port for two-way communication between XSCF Remote Storage Server and the XSCF.

Therefore, make the following settings on the terminal.
- In the Windows OS, allow connection to port 3260.
- In the antivirus software used, allow connection to port 3260.
- When using the Windows firewall, allow the Java Runtime Environment program being used ("Java Platform SE binary" or "OpenJDK Platform binary").
  Starting XSCF Remote Storage Server while remote storage is used will output the warning message shown in Figure 4-16. In this case, perform the following step.

Figure 4-16　　　Warning Message if the Windows Firewall is Used

1. **Click the [Allow access] button.**
   This adds "Java Platform SE binary" or "OpenJDK Platform binary" to the allowed programs of the Windows firewall in the Control Panel.

Enabling Java and allowing add-ons

To start XSCF Remote Storage Server from XSCF Web, perform the following procedure to enable Java in the Web browser used with XSCF Web and to allow add-ons.

For Internet Explorer
1. **Select [Tools] - [Internet Options] - [Programs] tab - [Manage Add-ons].**
2. **Enable "Java Plug-in XX.XX.X".**
3. **In Internet Explorer 8.0, selecting the [Remote Storage] menu in XSCF Web when remote storage is used will open a page and trigger the output of a message. The message asks whether to allow a Java Runtime Environment add-on to run. Make the selection on this message screen to allow the add-on.**

For Firefox
1. **From the [Firefox] menu, select [Add-ons] - [Plugins].**
2. **Select "Java(TM) Platform" and then set [Ask to Activate] or [Always Activate].**
3. **Clicking the [Launch] button in XSCF Web during the use of remote storage will trigger the output of a message. The message asks whether to allow a plug-in to run. Select [Allow].**
4. **The message is output again to ask whether to allow the plug-in to run. Select [Allow Now] or [Allow and Remember], and click the [OK] button.**

Notes on terminals

When using XSCF Remote Storage Server on a PC connected to a remote desktop, you cannot access media inserted in a CD/DVD drive. Specify an ISO file.

4.6.5 Oracle Solaris Settings

To use remote storage, enable the removable media management services in Oracle Solaris. With the removable media management services enabled, Oracle Solaris automatically mounts removable media when connecting the media in the terminal.

- For Oracle Solaris 11 or later
  Removable media management services: svc:/system/hal:default

  svc:/system/filesystem/rmvolmgr:default

  svc:/system/dbus:default

- For Oracle Solaris 10
  volfs service: svc:/system/filesystem/volfs:default

For the procedure for enabling the removable media management services, see "2. How to connect/disconnect a USB-DVD drive" in the *External USB-DVD Drive User Manual*.

4.6.6 Remote Storage Software Versions

Table 4-6 lists the software versions that remote storage operates with. Remote storage does not operate with any version not included in Table 4-6. For detailed information on XCP, Oracle Solaris, and essential SRU/patches, see the latest *Product Notes* for your server.

Table 4-6   XCP, Oracle Solaris, and Essential SRU/Patches That Remote Storage Operates With

XCP	Oracle Solaris	Essential SRU (*1) Essential patch (*2)
2260 or later	Oracle Solaris 11.2 or later	None
	Oracle Solaris 11.1	SRU 2.5 or later (*3)
	Oracle Solaris 10 1/13	None

*1 For Oracle Solaris 11
*2 For Oracle Solaris 10
*3 If remote storage is assigned as a virtual disk to a guest domain, applying this to a service domain is required.

4.6.7 Remote Storage Device Paths and Aliases

For details on the device paths of SPARC M12/M10 models, see "Appendix A   Lists of SPARC M12/M10 System Device Paths." For details on DVD drive aliases, see "Appendix J   Lists of DVD Drive Aliases."

4.6.8 Notes on Remote Storage

Notes on Java Runtime Environments

Java applets can no longer be used when the April 2019 update or a later update provided for Oracle Java SE 8 is applied. As a consequence, XSCF Remote Storage Server cannot be started from XSCF Web.
To use remote storage in an environment where you cannot use Java applets, you need to start XSCF Remote Storage Server with the Java command from a terminal. In this case, obtain the archive file of XSCF Remote Storage Server from the XCP firmware download site, and extract it on the terminal in advance.

For details, see "4.6.9   Flow for Using Remote Storage" and "4.6.12   Connecting to Media When Using Remote Storage."

Notes on Using Remote Storage

Note the following points about using remote storage.
- Do not perform an operation to connect or stop remote storage until the power-on/off processing of a physical partition is completed.
- If no default gateway is set in the network settings, the Remote Storage Network Configuration table on the [Remote Storage] page of XSCF Web and the showremotestorage command will display "-" for the gateway.
- If you use remote storage to connect to an ISO image on the terminal, do not set read-only (R) as a property attribute of the ISO image and the folder containing that ISO image.
  If the read-only (R) property attribute is set, the media fails to start (Run).
- Ejecting or switching media through a terminal operation during use of remote storage is not supported. If that operation accesses the remote storage, an access error occurs.
  Ejecting media through a terminal operation means ejecting media without using the eject command from Oracle Solaris. The following operations are assumed:
  - Pressing the eject button on the CD/DVD drive of the terminal to eject media
  - Operating Windows on the terminal to eject media

  To eject media, perform the procedure in "4.6.14   Disconnecting From Media/ Ending Remote Storage" to end the remote storage, and then eject the media.

To switch media, perform the procedure in "Switching Media" in "4.6.13 Using Remote Storage From Oracle Solaris."

- If you click the [Stop] button on the [XSCF Remote Storage Server] screen and access remote storage during use of the remote storage, an access error occurs. If you clicked the [Stop] button during use of the remote storage, perform the procedure in "4.6.14 Disconnecting From Media/Ending Remote Storage" to end the remote storage. To use the remote storage again, perform the procedure in "4.6.12 Connecting to Media When Using Remote Storage."

- Do not use the deleteboard command to disconnect a SPARC M12/M10 with remote storage connected.

- To perform any operation (including firmware upgrade, etc.) that reboots the XSCF or switches between the master and standby XSCFs during use of remote storage, the remote storage has to be disconnected. Disconnect it while referring to "4.6.14 Disconnecting From Media/Ending Remote Storage."
  If not disconnected, it may cause the output of an error message or warning message to the domain console and the registration of an error log with the XSCF.

- An attempt to connect remote storage via a VPN or other network to which address translation is applied fails with an error message "iscsiadm: no records found!."
  Do not connect remote storage via a VPN or other network to which address translation is applied. If multiple network connections exist in a terminal, remote storage cannot be connected in some cases.

  In such cases, disable network devices on terminals other than the one used to connect the XSCF-LAN before connecting.

Note on using a CD (Compact Disc) as remote storage media

When using a CD (Compact Disc) as remote storage media, use a CD that was written with the Disc at once (DAO) method. If the media used is a CD that was not written with the Disc at once (DAO) method, an error may occur in the OpenBoot PROM or sd driver when the media is read.

4.6.9 Flow for Using Remote Storage

This section describes the flow for using remote storage. We recommend you perform operations from XSCF Web when using remote storage.

Before Using Remote Storage

To use remote storage, the following advance preparations are required.
- Referring to "4.6.2 Remote Storage Network Configuration" and "4.6.10 Configuring the XSCF-LAN Used with Remote Storage," make the XSCF network settings of the master/standby XSCF. The network settings of the master XSCF are a necessity for using XSCF Web.

- When you use XSCF Web, see "3.8   Configuring the HTTPS Service for Login to the XSCF," and enable the HTTPS service. Also, satisfy the requirements in "4.6.4 Operating Requirement of Terminals and Browsers."
- Referring to "4.6.5   Oracle Solaris Settings," make the required settings for Oracle Solaris.
- When you start XSCF Remote Storage Server with the Java command from a terminal, you need to obtain the archive file of the XSCF Remote Storage Server first and extract it on the terminal. You can obtain this archive file from the XCP firmware download site.
  Also, the archive file is compatible between the SPARC M12 and SPARC M10. In both the model series, you can use the file with all XCP firmware versions supporting the remote storage function.

Once you have completed the above preparations, perform basic operations.

Basic Operation Flow

To use remote storage, perform the basic operations shown in Figure 4-17.

Figure 4-17   Basic Remote Storage Operations
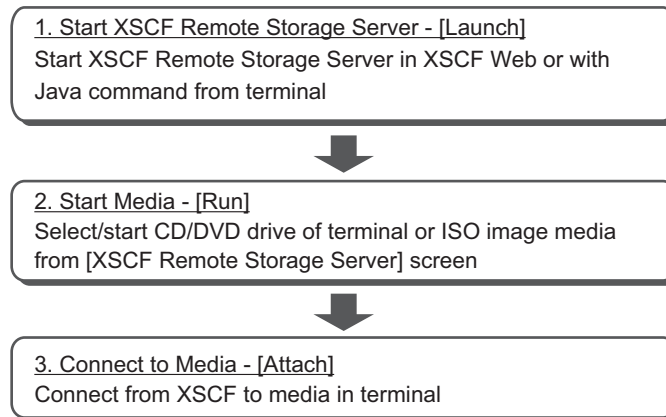
The following overview describes the basic operations.

1. **Starting XSCF Remote Storage Server - [Launch]**
    Start XSCF Remote Storage Server from the remote storage menu of XSCF Web or with the Java command from the terminal (Launch).
    Starting XSCF Remote Storage Server will open the [XSCF Remote Storage Server] screen for selecting/starting media on the terminal. From this screen, select/start media and display the status of media.

Note - XSCF Remote Storage Server starts with Java Runtime Environment.
Therefore, none of the XSCF shell commands starts XSCF Remote Storage Server.

---

2. **Starting media - [Run]**
    After displaying the [XSCF Remote Storage Server] screen, select the CD/DVD

drive or ISO image of the terminal to start the media. This operation allows the use of the network port used with the remote storage of this terminal and sets the wait state for connection from the XSCF.

3. **Connecting to media - [Attach]**
   Connect to the target media of a terminal from XSCF Web or the XSCF shell (Attach). At this time, specify the XSCF-LAN interface and the terminal IP address. These operations enable the use of the target media from OpenBoot PROM and Oracle Solaris.

   At this point, when accessing the media via a slave XSCF, you can make XSCF network settings from XSCF Web or the XSCF shell. An XSCF reboot is not required at this time.

   Use the setremotestorage and showremotestorage commands for the connections to media from the XSCF shell and for the network settings of the slave XSCF. Both commands are XSCF commands. For details of each command, see the man page of the command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

For details on each setting, see "4.6.12 Connecting to Media When Using Remote Storage."

4.6.10 Configuring the XSCF-LAN Used with Remote Storage

This section describes the XSCF-LAN settings used with remote storage.
To use remote storage, the XSCF-LAN interface network must be configured. After deciding to use either XSCF-LAN#0 or XSCF-LAN#1 of the master, standby, or slave XSCF, configure the XSCF network.

Configuring the master/standby XSCF to use XSCF Web

Before configuring remote storage with XSCF Web, you need to have completed the master/standby XSCF network settings. This enables the use of the XSCF Web, which needs the HTTPS service enabled. An XSCF reboot is required for these settings.

Make the XSCF network settings with the setnetwork command or the [Network] page of XSCF Web. These settings cannot be made with the setremotestorage command or the [Remote Storage] page of XSCF Web.

For details on the master/standby XSCF network settings and HTTPS service settings, see "3.9 Configuring the XSCF Network" and "3.8 Configuring the HTTPS Service for Login to the XSCF."

Using the master/standby XSCF

When using remote storage via the XSCF-LAN on all master/standby chassis, the XSCF network does not need to be configured if the settings in "Configuring the master/standby XSCF to use XSCF Web" have been completed.

Configure the XSCF network if not yet configured.
When not using XSCF Web, you do not need to configure the HTTPS service.

Note - If the master/standby XSCF is used, the physical IP address is used as the XSCF-LAN IP address when accessing media in a terminal with remote storage. The takeover IP address (virtual address) is not used.

Using a slave XSCF

Before using remote storage via a slave XSCF, you need to have already completed the master XSCF network settings. You can make the slave XSCF network settings before or while configuring remote storage.
Make the XSCF network settings with the setremotestorage command or the [Remote Storage] page of XSCF Web. These settings cannot be made with the setnetwork command or the [Network] page of XSCF Web.
Also, in a system connected to a crossbar box, remote storage is used via a slave XSCF that is a SPARC M12/M10. For this reason, the slave XSCF network must be configured.

The procedure for making slave XSCF network settings with XSCF Web is described below. For details of settings with the XSCF shell, see the setremotestorage command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

1. **Connect the XSCF LAN cable of the slave XSCF (XSCF-LAN#0 or XSCF-LAN#1).**

2. **Execute the sethttps command to enable the HTTPS service.**

3. **Log in to XSCF Web on the master XSCF.**

4. **Select [Menu] - [Settings] - [Remote Storage].**

5. **From Interface in the Remote Storage Network Configuration table, select either XSCF-LAN#0 or XSCF-LAN#1 of the slave XSCF. Then, click the [Configure] button.**

6. **Set IP Address, Netmask, and Gateway on the displayed screen, and click the [OK] button.**

7. **Referring to the Remote Storage Network Configuration table, confirm that all this set data is correct.**
   An XSCF reboot is not required for the slave XSCF network settings.

4.6.11 Status of XSCF Remote Storage Server

This section describes the Status display at the top of the [XSCF Remote Storage Server] screen.

Remote storage operations from the [XSCF Remote Storage Server] screen and XSCF Web will refresh the Status display at the top of the [XSCF Remote Storage Server] screen. You can use the Status data to check the status of connections between the XSCF and the media in terminals.

Table 4-7 lists the Status transitions on the [XSCF Remote Storage Server] screen from remote storage operations.

Table 4-7　Status Transitions on the [XSCF Remote Storage Server] Screen From Remote Storage Operations

Operation	Status
Connect	
Immediately after XSCF Remote Storage Server start - [Launch] button clicked on XSCF Web - XSCF Remote Storage Server started by Java command from terminal	Disconnected
Target media selected on [XSCF Remote Storage Server] screen	Disconnected
[Run] button clicked on [XSCF Remote Storage Server] screen	Waiting for connection from XSCF
[Attach] button clicked on XSCF Web	Connected
Disconnect	
Connected by clicking of [Attach] button	Connected
[Detach] button clicked on XSCF Web	Waiting for connection from XSCF
[Stop] button clicked on [XSCF Remote Storage Server] screen	Disconnected
Eject	
Connected by clicking on [Attach] button	Connected
Eject executed from Oracle Solaris	Ejected
[Run] button clicked on [XSCF Remote Storage Server] screen	Waiting for connection from XSCF
Several seconds elapsed after above [Run] button clicked	Connected

Table 4-8 lists the meanings of the Status display at the top of the [XSCF Remote Storage Server] screen.

Table 4-8　Meanings of Status of XSCF Remote Storage Server

Status	Meaning
Disconnected	Media in a terminal has been disconnected from the XSCF.
Waiting for connection from XSCF	Media in a terminal can be connected and is waiting for connection from the XSCF.
Connected	Media in a terminal is connected to the XSCF.
Ejected	The eject command was executed from Oracle Solaris.

4.6.12 Connecting to Media When Using Remote Storage

This section describes the operations for connecting to media in a terminal with the use of remote storage. Note that only reading of media is allowed. Writing is not allowed.

The descriptions are divided into the following three cases:
- Physical partition stopped
- Control domain at the ok prompt
- Oracle Solaris running on the control domain

In the above three cases, the basic operation for connecting to media is the same. However, the operations for the control domain after the media is connected are different. The basic operation for any of the above cases is the same as in the contents of "Physical Partition Stopped."

Note - To use remote storage in a guest domain, assign resources (ldm add-vdisk).

Note - When using remote storage, our recommendation is that no operation for connecting to media be performed during the startup or stop procedure of the physical partition or control domain. This prevents longer processing times in the startup and stop procedures of the physical partition and control domain. Depending on the timing, if media is connected during the startup procedure of the physical partition or control domain, OpenBoot PROM may not recognize the target media. Consequently, the control domain will need to be reset again.

The following procedure assumes that the operations in "Before Using Remote Storage" in "4.6.9 Flow for Using Remote Storage" were completed.

Physical Partition Stopped

1. **Start XSCF Remote Storage Server.**
   You can start it in either of the following ways: starting from XSCF Web, or starting with the Java command from a terminal.

- Starting from XSCF Web
  Select **[Menu] - [Settings] - [Remote Storage]** on XSCF Web, and click the [Launch] button.

  The Figure 4-18 screen appears. Click the [Run] button on the screen to display the [XSCF Remote Storage Server] screen.

Figure 4-18   Message When the [Launch] button is Clicked
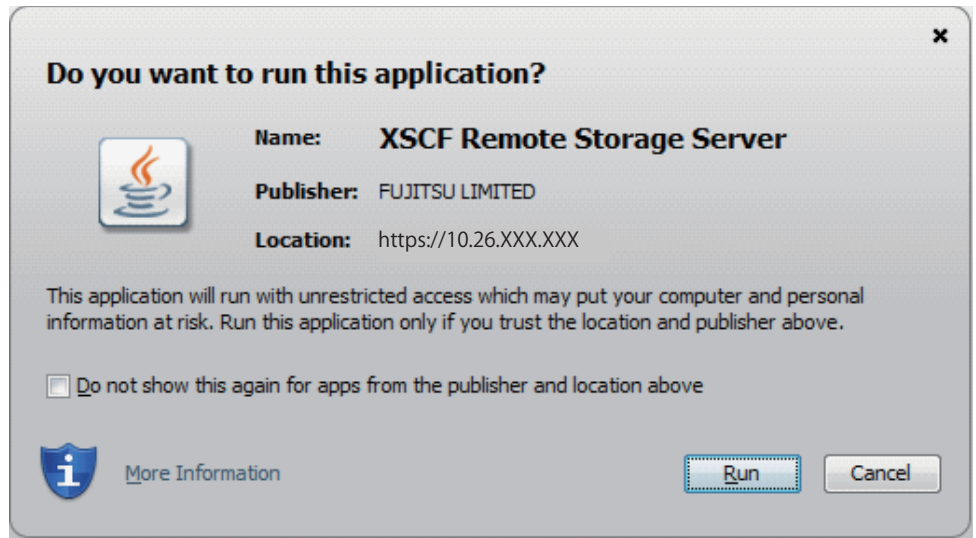
If the validity of the signed certificate for XSCF Remote Storage Server cannot be confirmed, a security warning like the one shown in Figure 4-19 is output. Check the [I accept the risk and want to run this application] check box, and then click the [Run] button.

Figure 4-19   Security Warning Message
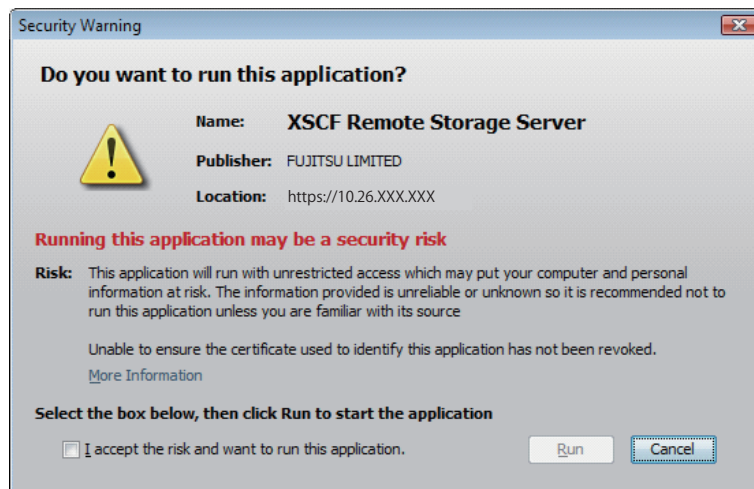
- Starting with the Java command from a terminal
  Execute the following command in the directory that has the extracted archive file of XSCF Remote Storage Server on the terminal. Specify the execution path of the Java command according to the environment used.

  The option and class path specified in the Java command are fixed. Specify "com.fujitsu.m10.rdvd.gui.GUIMain", even with the SPARC M12.

The following example shows that the XSCF Remote Storage Server is started by using Oracle Java SE at "C:\rdvd" where the archive file is extracted.

```
C:\>cd rdvd
C:\rdvd>dir /B
deployJava.js
lib
RdvdSpt32.dll
RdvdSpt64.dll
rdvd_client.jar
rdvd_client.jnlp
C:\rdvd>"C:\Program Files (x86)\Java\jre1.8.0_201\bin\java.exe" -esa -cp rdvd_
client.jar;lib\* com.fujitsu.m10.rdvd.gui.GUIMain
```

If the Windows firewall is used, the warning message shown in "Figure 4-16 Warning Message if the Windows Firewall is Used" is output. Follow the procedure in "Port Used and Permission on a Terminal" in "4.6.4   Operating Requirement of Terminals and Browsers."

2. **Select the media of the CD/DVD drive or ISO image displayed on the [XSCF Remote Storage Server] screen.**
   If no media appears on the screen, no media may have been inserted in the CD/DVD drive of the terminal, or no ISO image may have been added. If no media is inserted in the CD/DVD drive, insert media, and then click the [Refresh] button at the top of the screen. Alternatively, click the [Add ISO file] button to display the ISO image list. Select the target media from the displayed list.

   Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below. For the meanings of Status, see "4.6.11   Status of XSCF Remote Storage Server."

   Status   Disconnected
   Selected media   Selected media path
   XCP IP Address   None

3. **Click the [Run] button on the [XSCF Remote Storage Server] screen.**
   This operation allows the use of the network port of the terminal used with remote storage. The selected target media is waiting for a connection from the XSCF.

   Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below.

   Status   Waiting for connection from XSCF
   Selected media   Selected media path
   XCP IP Address   None

   When performed, this operation displays the [Information] screen shown in Figure 4-20. Click the [OK] button. This procedure describes the "Attach" operation performed in XSCF Web. Likewise, when performing the "Attach" operation in the XSCF shell, click the [OK] button.

Figure 4-20   [Information] Screen
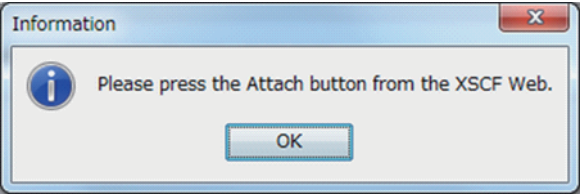
4. **Select an XSCF-LAN interface and connect media. [Attach]**
    - Operating with XSCF Web
      Select an XSCF-LAN interface from the Interface column in the Remote Storage
      Network Configuration table on XSCF Web, and click the [Attach] button.
      A screen for specifying the terminal IP address appears. After confirming that
      the IP address is correct, click the [OK] button. Connection in the Remote
      Storage Network Configuration table displays the terminal IP address.

    - Operating with the XSCF shell
      Specify the XSCF-LAN interface and the IP address of the terminal, and
      execute the setremotestorage -c attach command.

      If the network is not configured for the XSCF-LAN interface to connect to the
      target media, see "4.6.10   Configuring the XSCF-LAN Used with Remote
      Storage." Then, configure the network. In this way, the XSCF and target media
      are connected. Each line of Status, Selected media, and XSCF IP Address at the
      top of the [XSCF Remote Storage Server] screen is refreshed as shown below
      by the connection to the media.

         Status   Connected
         Selected media   Selected media path
         XCP IP Address   Physical IP address of connected XSCF-LAN

5. **Execute the poweron command to power on the physical partition.**

Note - To stop the control domain at the ok prompt, use the setenv command to change the
OpenBoot PROM environment variable auto-boot? to false.
[Example]
XSCF> **setpparparam -p 0 -s bootscript "setenv auto-boot? false"**

---

6. **Execute the cfgadm -al command from Oracle Solaris, and confirm that the
    remote storage device path has been added.**

```
# cfgadm -al
Ap_Id           Type            Receptacle        Occupant          Condition
 ...
usb1/3          usb-storage     connected         configured        ok
```

Note - If remote storage is not used in the control domain, step 10 is unnecessary. To use
remote storage in a guest domain, assign resources (ldm add-vdisk).

---

7. **If the target media has not been added, use the mount command of Oracle Solaris to mount it.**

    The following example shows a check of the mount state of the target media. Since the remote storage device has not been automatically mounted, the target media is going to be mounted.

    For details on the mount command, see the *Oracle Solaris Reference Manual* of the version used.

Note - For the procedure for enabling the removable media management services, see "4.6.5 Oracle Solaris Settings."

```
# df
/               (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices        (/devices          ):        0 blocks 0 files
...
# mount -F hsfs /dev/dsk/c4t0d0s2 /media/xxxxx
```

/dev/dsk/c4t0d0s2 specifies the device path name of remote storage.
For details on the mount command, see the *Oracle Solaris Reference Manual* of the version used.

You can now install software, read files, and perform other operations from the target media. Note that you cannot write to the target media.

Note - If the control domain is at the ok prompt, execute the show-disks command, and confirm that the remote storage device path has been added.

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

Control Domain at the ok Prompt

1. **Perform steps 1 to 4 in "Physical Partition Stopped."**

2. **Execute the console command from the XSCF shell to switch to the control domain console that is at the ok prompt.**

    The following example shows switching to the control domain console of physical partition#0.

```
XSCF> console -p 0
```

3. **Execute the reset-all command to reset the control domain that is at the ok**

prompt.

```
{0} ok reset-all
```

Note - To reset the control domain when stopping it again at the ok prompt, change the value of the OpenBoot PROM environment variable auto-boot? to false with the setenv command.

4. **At the ok prompt of the reset control domain, execute the show-disks command, and confirm that the remote storage device path has been added.**

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...

Enter Selection, q to quit:
```

You can set a remote storage device alias, install Oracle Solaris from the target media, and perform other operations.

Oracle Solaris Running on the Control Domain

1. **Perform steps 1 to 4 in "Physical Partition Stopped."**
2. **Execute the console command from the XSCF shell to switch to the control domain console where Oracle Solaris is running.**
   The following example shows switching to the control domain console of physical partition#0.

```
XSCF> console -p 0
```

3. **Execute the df command or cfgadm -al command from Oracle Solaris, and confirm that the remote storage device path has been added.**

Note - If the removable media management services are enabled (set to enable), the remote storage device is automatically mounted when the XSCF is connected to remote storage. For the procedure for enabling the removable media management services, see "4.6.5 Oracle Solaris Settings."

The following example executes the df command and shows that /media on the remote storage device has been automatically mounted.

```
# df
/               (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices        (/devices       ):       0 blocks 0 files
...
```

```
/media/DISC-LABEL(/dev/dsk/c4t0d0s2 ):      0 blocks 0 files
```

The following example executes the cfgadm command and shows that a remote storage device (usb1/3), whose type is usb-storage, has been added.

```
# cfgadm
Ap_Id          Type           Receptacle      Occupant        Condition
...
usb1/3         usb-storage    connected       configured      ok
```

> **Note -** If remote storage is not used in the control domain, step 4 is unnecessary. To use remote storage in a guest domain, assign resources (ldm add-vdisk).

4. **If the remote storage device is not mounted, use the mount command to mount it.**
   The following example shows that the remote storage device has not been automatically mounted, so it is going to be mounted.

```
# df
/                 (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices          (/devices         ):       0 blocks 0 files
...
# mount -F hsfs /dev/dsk/c4t0d0s2 /media/xxxxx
```

/dev/dsk/c4t0d0s2 specifies the device path name of remote storage.
For details on the mount command, see the *Oracle Solaris Reference Manual* of the version used.

You can now install software, read files, and perform other operations from the target media. Note that you cannot write to the target media.

4.6.13   Using Remote Storage From Oracle Solaris

This section describes examples of using remote storage.
The descriptions of the following two examples pertain to the SPARC M10-1:
- Installing Oracle Solaris
- Switching media

Installing Oracle Solaris

As described below, this example installs Oracle Solaris in the SPARC M10-1 control domain.

1. **Execute the console command from the XSCF shell to switch to the control domain console that is at the ok prompt.**
   The following example shows switching to the control domain console of physical partition#0.

```
XSCF> console -p 0
```

2. **Install Oracle Solaris from the target media in the CD/DVD drive.**
   The following example shows a check of the currently set device aliases and the
   specification of a checked device alias. If the alias number is omitted, the smaller
   LSB number is used from storage.

```
{0} ok devalias
{0} ok boot rcdrom
```

The following example shows a specified device path.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3/disk@0
```

> **Note -** For details on the device paths of SPARC M12/M10 models, see "Appendix A   Lists of
> SPARC M12/M10 System Device Paths." For details on device aliases, see "Appendix J   Lists
> of DVD Drive Aliases."

Switching Media

The procedure described here executes the eject command from Oracle Solaris to
switch the media of the CD/DVD drive or ISO image used with remote storage.

> **Note -** To switch media, execute the eject command from Oracle Solaris. Remote storage does
> not support media switching that uses the Eject button on the CD/DVD drive of a terminal. If
> media is switched using the Eject button, changes in data size may not be recognized, and a
> warning message may be output. In this case, execute the eject command first. Then, in XSCF
> Remote Storage Server, you need to click the [Run] button again.

1. **Execute the console command from the XSCF shell to switch to the control
   domain console where Oracle Solaris is operating.**
   The following example shows switching to the control domain console of
   physical partition#0.

```
XSCF> console -p 0
```

2. **Use the eject command to remove the target media.**
   With the eject command, you can display device names and a corresponding list
   of nicknames by specifying an option. The following example shows the -l
   option specified in the eject command, when using Oracle Solaris 11.

```
# eject -l
/dev/dsk/c4t0d0s2      cdrom,cdrom0,cd,cd0,DISC-LABEL,/media/DISC-LABEL
```

The following example shows the specified /media on the remote storage device.

```
# eject /media/DISC-LABEL
```

When performed, this operation displays the [Information] screen for XSCF Remote Storage Server as shown in Figure 4-21. Click the [OK] button to return to the [XSCF Remote Storage Server] screen.

Figure 4-21   [Information] Screen
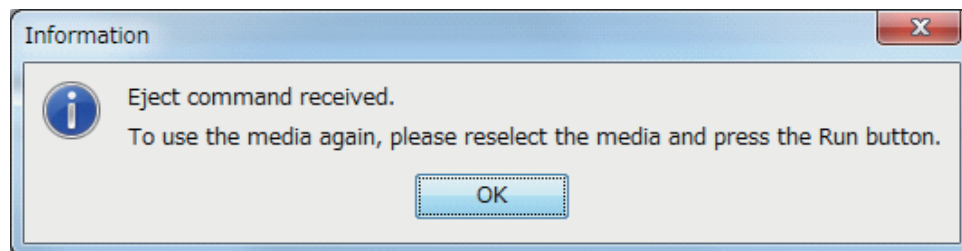
Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below. For the meanings of Status, see "4.6.11   Status of XSCF Remote Storage Server."

Status   Ejected
Selected media   None
XCP IP Address   None

Note - For details on the device paths and device aliases of each SPARC M12/M10 model, see "Appendix A   Lists of SPARC M12/M10 System Device Paths" and "Appendix J   Lists of DVD Drive Aliases," respectively.

---

3. **Switch the media in the CD/DVD drive, or reselect the ISO image.**

4. **Click the [Refresh] button on the [XSCF Remote Storage Server] screen, and select the CD/DVD drive.**
   Clicking the [Refresh] button will refresh the System drives information on the screen. The Selected media information on the screen is refreshed when a CD/DVD drive is selected again.

   Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below.

   Status   Ejected
   Selected media   Selected media path
   XCP IP Address   None

5. **Click the [Run] button on the [XSCF Remote Storage Server] screen.**
   This operation allows the use of the target media of the terminal used with remote storage.

   Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below.

```
Status             Connected
Selected media     Selected media path
XCP  IP Address    Physical IP address of specified XSCF-LAN
```

Note - To switch media at the ok prompt, perform the following procedure.
1. Perform steps 1 to 3 in "Physical partition stopped" in "4.6.14   Disconnecting From Media/Ending Remote Storage." Then, perform steps 2 to 4 in "Control Domain at the ok Prompt."
2. Switch the media in the CD/DVD drive, or reselect the ISO image.
3. Perform steps 2 to 4 in "Physical Partition Stopped" in "4.6.12   Connecting to Media When Using Remote Storage." Then, perform steps 2 to 4 in "Control Domain at the ok Prompt ."

4.6.14   Disconnecting From Media/Ending Remote Storage

This section describes the operations for disconnecting from media in the terminal used and ending remote storage.
The descriptions are divided into the following three cases:
- Physical partition stopped
- Control domain at the ok prompt
- Oracle Solaris running on the control domain

In the above three cases, the basic operation for disconnecting from media/ending remote storage is the same. However, the operations for the control domain before and after the media is disconnected/remote storage is ended are different. The basic operation for any of the above cases is the same as in the "Physical partition stopped" contents.

Physical partition stopped

1. **XSCF Remote Storage Server is running. Confirm that the status of each line of Status, Selected media, and XSCF IP Address at the top of the screen are as follows.**

   ```
   Status             Connected
   Selected media     Selected media path
   XCP  IP Address    Physical IP address of specified XSCF-LAN
   ```

2. **Disconnect XSCF Remote Storage Server and the XSCF. [Detach]**
   - Operating with XSCF Web

     -- From the Interface column in the Remote Storage Network Configuration table on the [Remote Storage] screen in XSCF Web, select the XSCF-LAN interface for disconnecting the target media of the terminal.

     -- Click the [Detach] button.

   Connection in the Remote Storage Network Configuration table displays "Available". This operation disconnects the XSCF from the target media. While XSCF Remote Storage Server is running, you can reconnect the media by clicking

the [Attach] button.

- Operating with the XSCF shell
  Specify the XSCF-LAN interface and the IP address of the terminal, and
  execute the setremotestorage -c detach command.
  This operation disconnects the XSCF from the target media. While XSCF
  Remote Storage Server is running, you can reconnect the media by executing
  the setremotestorage -c attach command.

Each Address line is refreshed as shown below.

```
Status           Waiting for connection from XSCF
Selected media   Selected media path
XCP  IP Address  None
```

3. **To disconnect the target media, click the [Stop] button on the [XSCF Remote Storage Server] screen.**
   A confirmation message appears. Click the [OK] button.

   This operation disconnects the target media. However, even after this operation is performed, the network port of the terminal used with remote storage can still be used. Clicking the [Run] button again will result in the target media waiting for connection from the XSCF.

   Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below.

```
Status           Disconnected
Selected media   Selected media path
XCP  IP Address  None
```

4. **To end remote storage, click [x] at the top right of the [XSCF Remote Storage Server] screen.**
   The screen closes and ends.

Control Domain at the ok Prompt

1. **Perform steps 1 to 4 in "Physical partition stopped."**

2. **Execute the console command from the XSCF shell to switch to the control domain console that is at the ok prompt.**
   The following example shows switching to the control domain console of physical partition#0.

```
XSCF> console -p 0
```

3. **Execute the reset-all command to reset the control domain that is at the ok prompt.**

```
{0} ok reset-all
```

Note - To reset the control domain when stopping it again at the ok prompt, change the value of the OpenBoot PROM environment variable auto-boot? to false with the setenv command.

4. **At the ok prompt of the reset control domain, execute the show-disks command, and confirm that the remote storage device path has been deleted.**

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...

Enter Selection, q to quit:
```

Oracle Solaris Running on the Control Domain

1. **Execute the console command from the XSCF shell to switch to the control domain console where Oracle Solaris is running.**
   The following example shows switching to the control domain console of physical partition#0.

```
XSCF> console -p 0
```

2. **Confirm that Oracle Solaris is not accessing the target media. If necessary, unmount the remote storage device.**
   The following example unmounts the remote storage device.

```
# cd /
# umount /media/xxxxx
```

3. **Stop the removable media management service.**
   The following example executes the svcadm command to stop the removable media management service.

   - For Oracle Solaris 11 or later

```
# svcadm disable hal
```

   - For Oracle Solaris 10

```
# svcadm disable volfs
```

Note - To use remote storage in a guest domain, stop the removable media management service of the guest domain.

---

4. **Execute the cfgadm -c unconfigure command from Oracle Solaris to stop the remote storage device on a particular path.**
   The following example executes the cfgadm command and shows that usb1/3 is a remote storage device.

```
# cfgadm
Ap_Id           Type            Receptacle      Occupant        Condition
...
usb1/3          usb-storage     connected       configured      ok
```

The following example executes the cfgadm -c unconfigure command and shows
that the remote storage device is stopped.

> **Note -** If the resource of remote storage (vdisk) has been assigned to a guest domain,
> disconnect the resource (ldm remove-vdisk) and then execute cfgadm -c unconfigure from
> the control domain.

```
# cfgadm -c unconfigure usb1/3
```

The following example executes the cfgadm command and checks that usb1/3 is
stopped.

```
# cfgadm
Ap_Id           Type            Receptacle      Occupant        Condition
...
usb1/3          usb-storage     connected       unconfigured    ok
```

5. **Perform steps 1 to 4 in "Physical partition stopped."**

6. **Execute the df command or cfgadm command from Oracle Solaris, and
   confirm that the remote storage device path has been deleted.**
   The following example executes the df command and shows that /media on the
   remote storage device has been deleted.

```
# df
/               (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices        (/devices        ):         0 blocks 0 files
...
```

The following example executes the cfgadm command and shows that the
remote storage device (usb1/3) is stopped.

```
# cfgadm
Ap_Id           Type            Receptacle      Occupant        Condition
...
usb1/3          unkown          empty           unconfigured    ok
```

4.6.15 Other Points to Note and Operations

This section describes points to note and methods of operation when remote storage is used.

Points to Note About Any Errors Occurring When Remote Storage is Used

An abnormal event, such as an XSCF reboot, master/standby XSCF switching, the XSCF-LAN disconnecting, and the terminal stopping, may occur with the use of remote storage from the ok prompt or Oracle Solaris. The results would be the output of an error or warning message on the domain console and the registration of an error log on the XSCF.
The following example shows the output of an error message after Oracle Solaris is installed from the ok prompt.

```
{0} ok boot rcdrom
Boot device: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@
3/disk@0,0:a File and args:
|
read failed
FCode aborted.
$boot failed
The file just loaded does not appear to be executable.
```

If an error occurs when remote storage is accessed on Oracle Solaris, the error is detected from the sd driver, and a warning message is output. The following example shows a warning message output by the sd driver.

```
WARNING: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0 (sd5):
        Error for Command: read(10)                    Error   Level: Retryable
        Requested Block: 39665                         Error   Block: 39665
        Vendor: Fujitsu                                Serial Number:
        Sense Key: Media_Error
        ASC: 0x11 (unrecovered read error), ASCQ: 0x0, FRU: 0x0
```

```
WARNING: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0 (sd5):
    SCSI transport failed: reason 'timeout': giving up
```

After recovery from an error that occurred, you can restore the remote storage connection by performing the respective operations of the XSCF and terminal. See "Restore operations for an error that occurred during use of remote storage."

Restore operations for an error that occurred during use of remote storage

This section describes the restore operation flow in the event of a failure occurring during use of remote storage. XSCF Web operations are used as examples.

1. **Log in to XSCF Web from the system management terminal.**

2. **Select [Menu] - [Settings] - [Remote Storage].**

3. **Check Connection in the Remote Storage Network Configuration table.**
   - If an IP address is displayed, perform the operations in step 4 and later.
   - If "Available" is displayed, perform the operations in step 6 and later.
   - If "Unavailable" is displayed, an XSCF reboot is in progress. After the "Available" state is entered, perform the operations in step 6 and later.
     To operate with the XSCF shell, confirm Connection with the showremotestorage command.

4. **From the Interface column in the Remote Storage Network Configuration table, select the XSCF-LAN interface to be connected to the target media.**
   To operate with the XSCF shell, perform steps 4 and 5 with the setremotestorage -c detach command.

5. **Click the [Detach] button.**

6. **Check Status on the [XSCF Remote Storage Server] screen.**
   If "Waiting for connection from XSCF" is displayed, perform the operations in step 8 and later.

   If "Connected" is displayed, click the [Stop] button. A confirmation message appears. Click the [OK] button.

Note - If the [XSCF Remote Storage Server] screen is already displayed, the Launch operation of the [XSCF Remote Storage Server] screen in XSCF Web is not necessary.

Note - If Connection in the Remote Storage Network Configuration table is "Available," "Connected" is displayed at Status on the [XSCF Remote Storage Server] screen. Therefore, click the [Stop] button to change Status to "Disconnected."
To operate with the XSCF shell, confirm Connection with the showremotestorage command.

---

7. **Click the [Run] button on the [XSCF Remote Storage Server] screen again.**
   The target media waits for connection from the XSCF.

8. **From the Interface column in the Remote Storage Network Configuration table of XSCF Web, select the XSCF-LAN interface to be connected to the target media.**
   To operate with the XSCF shell, perform steps 8 and 9 with the setremotestorage -c attach command.

9. **Click the [Attach] button.**
   At this time, a screen for specifying the terminal IP address appears. Confirm that the IP address is correct, and then click the [OK] button.

Connection in the Remote Storage Network Configuration table displays the terminal IP address. This operation connects the XSCF to the target media.

To operate with the XSCF shell, confirm Connection with the showremotestorage command.

Each line of Status, Selected media, and XSCF IP Address at the top of the [XSCF Remote Storage Server] screen is refreshed as shown below.

    Status   Connected
    Selected media   Selected media path
    XSCF IP Address   Physical IP address of connected XSCF-LAN

10. **While Oracle Solaris is running, log in to the domain using remote storage. Then, execute the cfgadm command and df command, and confirm that remote storage can be used. At the ok prompt, execute the show-disks command, and confirm that the remote storage device path has been added.**
The following example executes the cfgadm command on Oracle Solaris.

```
# cfgadm
Ap_Id           Type          Receptacle        Occupant         Condition
...
usb1/3          usb-storage   connected         configured       ok
```

The following example executes the show-disks command at the ok prompt.

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...

Enter Selection, q to quit:
```

Chapter 5

CPU Activation

CPU cores must be activated in order to use CPU core resources in the SPARC M12/M10. This chapter provides an overview of how to manage CPU cores. You can dynamically add or remove working CPU cores in your SPARC M12/M10 to better match workload requirements.

- Basic Concepts of CPU Activation
- CPU Activation Key
- Adding CPU Core Resources
- Deleting CPU Core Resources
- Moving CPU Core Resources
- Displaying CPU Activation Information
- Saving/Restoring CPU Activation Keys
- Troubleshooting CPU Activation Errors
- Important Notes about CPU Activation

5.1 Basic Concepts of CPU Activation

You can dynamically expand or reduce CPU core resources in the SPARC M12/M10 without interrupting system operation to meet your workload requirements. This functionality provides CPU core resource flexibility, so that you can increase as many CPU core resources as needed, when necessary, while lowering the initial server cost.

The cost of CPUs represented a major proportion of the investment in former servers because CPU core resources were purchased per chip unit. In addition, software costs were tied directly to the total number of cores in the server since the licenses of many software applications were based on the number of cores in the system.

In the SPARC M12/M10, the CPU Activation function allows you to purchase CPU cores at a finer granularity than one CPU chip.

Note - The SPARC M12/M10 requires a minimum number of activated CPU cores in order to

function. In addition, SPARC M12/M10 CPU Activation uncouples, in purchasing, CPU cores from memory and I/O (PCI Express slots, onboard devices and ports, and internal storages). Even when no core is activated in a given CPU chip, memory and I/O are available. You can use all DIMM slots, PCI Express slots, and onboard devices and ports independently of how many CPU cores are activated.

To enable CPU cores, you need to purchase a CPU Activation, a right to use the CPU cores. When you purchase a CPU Activation, you can get a CPU Activation key to make CPU core resources available. The purchase unit of CPU Activation for each server is as follows.

Table 5-1   Purchase Unit of CPU Activation

Server	Minimum Required Number of Cores	Purchase Unit
SPARC M12-1	1 core	1 core (1 set)
SPARC M12-2	2 cores	1 core (1 set)
SPARC M12-2S	2 cores	1 core (1 set)
SPARC M10-1	2 cores	2 cores (1 set)
SPARC M10-4	4 cores	2 cores (1 set)
SPARC M10-4S	4 cores	2 cores (1 set)

A CPU Activation key is factory registered to the XSCF before initial server installation. An additional CPU Activation key can be activated not just during initial server installation but even while the system in production is running. After registering a CPU Activation key to the XSCF, you need to assign CPU core resources to a physical partition. The license numbers and form of some types of software vary depending on the number of CPU cores used. Confirm the license terms of the software when adding CPU cores to be used.

Note - In the SPARC M12/SPARC M10, one CPU core has multiple threads. Oracle Solaris recognizes each hardware thread as one virtual CPU (vCPU).
In the SPARC M12, one set of CPU Activation is used to activate one CPU core, resulting in eight virtual CPUs becoming available to Oracle Solaris.
In the SPARC M10, one set of CPU Activation is used to activate two CPU cores, resulting in four virtual CPUs becoming available to Oracle Solaris.

A CPU Activation key can be moved between the units of the same model. A CPU Activation key registered on a server can be deleted and registered on a different server.
You can move a CPU Activation as follows:

- SPARC M12-1 ==> SPARC M12-1

- SPARC M12-2 ==> SPARC M12-2

- SPARC M12-2S ==> SPARC M12-2S

- SPARC M10-1 ==> SPARC M10-1

- SPARC M10-4 ==> SPARC M10-4

- SPARC M10-4S ==> SPARC M10-4S

You cannot move a CPU Activation between models other than the above:

5.2 CPU Activation Key

A CPU Activation key can be obtained with the purchase of a CPU Activation. The key is provided on CD-ROM media. Each CPU Activation key includes a character string representing encrypted CPU Activation information.

The CD-ROM contains the following:

/readme_ja.txt	:	Readme file in Japanese
/readme_en.txt	:	Readme file in English
/Activation_key/	:	Directory containing activation files
/Activation_key/$KEY_FILES (multiple files)		
	:	Each file contains one set of CPU Activation.
/Activation_key/$CONSOLIDATED_KEY_FILES		
	:	A single file contains information on all CPU Activation keys from every $KEY_FILES.
/Certificate/Certificate.pdf		
	:	Hardware activation certificate

$KEY_FILES and $CONSOLIDATED_KEY_FILES are plaintext files with file names in the following format:

$KEY_FILES	:	AK11111_01_001.txt
$CONSOLIDATED_KEY_FILES		
	:	AK11111_01.txt

The following example shows the contents of activation files on one set of CPU Activation keys (2 cores) in the SPARC M10.

```
Product: SPARC M10-1
SequenceNumber: 1234567890123456
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA……..
```

Information on each CPU Activation key consists of multiple lines. Each line has an item name and its value is concatenated with ":" as a delimiter. An example is shown below. In this example, the item name is "Cpu", and its value is "noExpiration 2". Note that one key contains two CPU Activations.

```
Cpu: noExpiration 2
```

Table 5-2   CPU Activation Key Items and Possible Values

Item	Value
Product	SPARC M12-2, SPARC M12-2S, SPARC M10-1, SPARC M10-4, or SPARC M10-4S
SequenceNumber	Numeric value consisting of 1 to 16 digits
Cpu	CPU capacity (unit: core) noExpiration + numeric value consisting of up to 4 digits
Text-Signature-xxxxxx-xxxxxx	Signature

CPU Activation key data is stored on the XSCF. The key information is also automatically backed up to the PSU backplane unit (PSUBP). If the XSCF fails and is replaced, the key information is restored on the new replacement XSCF from the PSUBP.

5.3   Adding CPU Core Resources

This section describes how to add CPU core resources to a physical partition and logical domain after purchasing a CPU Activation.

5.3.1   Workflow up to CPU Core Addition to a Physical Partition and Logical Domain

Figure 5-1 shows the steps from the purchase of a CPU Activation to the start of use of the CPU core resources added to a physical partition and logical domain.

Figure 5-1   Workflow up to CPU Core Addition to a Logical Domain
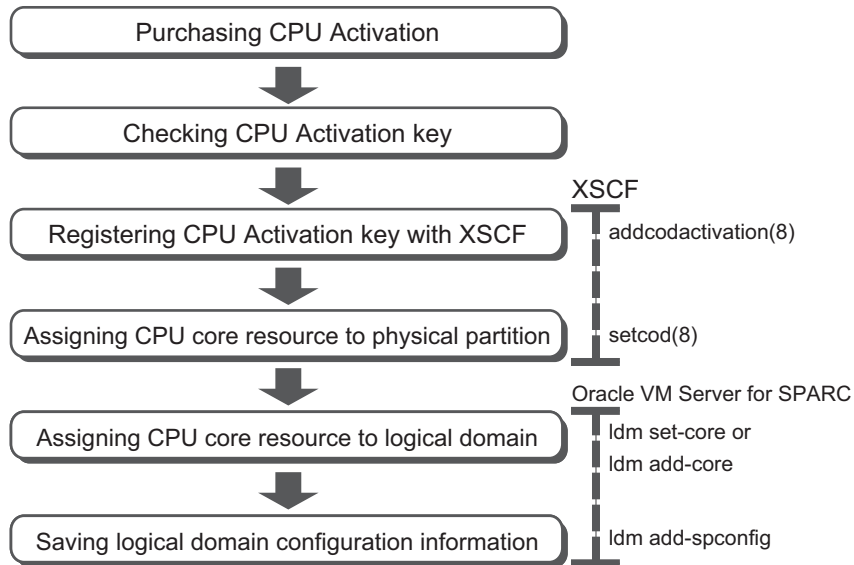
5.3.2　Purchase for Additional CPU Activation

When the load of SPARC M12/M10 increases, confirm if CPU core resources can be added. You can use the showcodusage command on the XSCF shell to check how many cores are being used in a physical partition, how many CPU cores are mounted, and how many CPU Activations are assigned to the physical partition. If the number of CPU Activations set for the physical partition is smaller than that of CPU cores mounted, CPU core resources can be added. For details, see "5.6.4 Displaying the Usage of Activated CPU Core Resources." To purchase additional CPU Activations, contact your local sales representative. To support the required load, you can use the CPU core temporarily until the CPU Activation is delivered. For details, see "Appendix K　CPU Activation Interim Permit."

5.3.3　Checking a CPU Activation Key

Upon obtaining ordered CPU Activations, confirm that the "Product" field in the file of each received CPU Activation key matches your model name. If not, the CPU Activation key cannot be registered.

5.3.4　Registering a CPU Activation Key

To register a received CPU Activation key with the XSCF, use the addcodactivation command on the XSCF shell or the XSCF Web. This section describes the procedures using the XSCF shell.

You need to have a user account that has the platadm privilege to execute this command.

```
XSCF> addcodactivation key-signature
```

Specify the received CPU Activation key as key-signature. To do so, either specify USB media with the -F option or copy and paste the contents of the CPU Activation key. The following command syntax shows how to specify USB media.

```
XSCF> addcodactivation -F file:///media/usb_msd/filename
```

To register all CPU Activation keys stored on the CD-ROM, specify $CONSOLIDATED_KEY_FILES for the file name.

Note - In versions earlier than XCP 2041, you cannot specify $CONSOLIDATED_KEY_FILES.

Operation Procedure

1. **Log in to the XSCF with a user account that has the platadm privilege.**
   For details, see "2.2 Logging In to the XSCF Shell."

2. **Execute the addcodactivation command to register a CPU Activation key with the XSCF.**
   To enter the CPU Activation key, specify the contents of the activation key when executing the addcodactivation command. Copy and paste all the contents of the Activation key, or read it from a file by specifying the -F option.

   Enter "y" for the confirmation message.

   The following example adds a CPU Activation key to the SPARC M10-1.

```
XSCF> addcodactivation "Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048: U1VOVyxTUEFSQy1FbnRlcnByaXNlAA........"
Above Key will be added, Continue?[y|n]: y
XSCF>
```

3. **Execute the showcodactivation command to confirm that the CPU Activation key was properly added to the XSCF.**
   With the -r option specified, the command displays the registered CPU Activation key.

   The following example shows output results from the showcodactivation command.

```
XSCF> showcodactivation -r
Product: SPARC M10-1
SequenceNumber: 1
```

```
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA........
```

At this point in time, CPU core resources are not ready for use on Oracle Solaris.

To make the CPU core resources ready for use, go to "5.3.5   Assigning a CPU Core Resource to a Physical Partition" to assign them to a physical partition.

4. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.

Note - If CPU Activation key information is corrupted because of an unexpected operation, the CPU Activation key may be required by the XSCF.   Ensure that CPU Activation keys are safely stored for recovery.

Note - Adding the same CPU Activation key to multiple SPARC M12/M10 units is not allowed.

5.3.5   Assigning a CPU Core Resource to a Physical Partition

To assign a CPU core resource to a physical partition, execute the setcod command with interactive operation from the XSCF shell. You need to have the platadm privilege to execute this command.

```
XSCF> setcod [-p ppar_id] -s cpu
PROC Permits installed: XX cores
PROC Permits assigned for PPAR 0 (X MAX)
 [Permanent Xcores]
Permanent [X]: permits
PROC Permits assigned for PPAR 1 (X MAX)
 [Permanent Xcores]
Permanent [X]: permits
 : Omitted
```

For -p ppar_id, specify the physical partition ID to which to assign the CPU core resource.   If the permits operand is not specified, the command starts an interactive session for assigning the CPU core resource.
If the applied XSCF firmware is XCP 2260 or later, you can also execute the following command.

The permits value specifies the number of CPU Activations for CPU cores whose use is allowed.
CPU Activations can be specified in units of one CPU core.

```
XSCF> setcod [[-q] -{y|n}] -p ppar_id -s cpu -c {set|add|del} permits
```

Note - We do not recommend using the setcod command specified in the following way.

XSCF> **setcod -p** *ppar_id* **-s cpu** *permits*

To execute the setcod command when the XCP firmware is XCP 2260 or later, specify the -c option or use interactive operation. Also, use interactive operation for XCP 2250 or earlier. The reasons are as follows.
- At command execution, no confirmation message ([y/n]) is output about implementing changes with the settings made.
- No warning message is output when the number of CPU Activation assignments for a running physical partition has been reduced. Any shortage in the number of CPU Activations, such as one due to permits being erroneously specified, may cause the system to stop.

You can specify with the setcod command up to the number of CPU Activations registered with the addcodactivation command.

Operation Procedure

1. **Log in to the XSCF with a user account that has the platadm privilege.**
   For details, see "2.2 Logging In to the XSCF Shell."

2. **Assign a CPU core resource to a physical partition with the setcod command.**

Note - To use -c set or not use the -c option, do not specify only the quantity to be added or deleted in the permits operand. Instead, specify the currently set quantity plus the number of added assignments, or specify the currently set quantity minus the number of deleted assignments. If you inadvertently specify only the quantity to be added/deleted, the number of CPU Activations may decrease, which may cause the system to stop.

The following example assigns four CPU core resources to physical partition 1.

```
XSCF> setcod -p 1 -s cpu -c set 4
PROC Permits assigned for PPAR 1 : 0 -> 4

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

The following example shows CPU core resources being assigned interactively to a physical partition.

```
XSCF> setcod -s cpu
PROC Permits installed: 5 cores
PROC Permits assigned for PPAR 0 (5 MAX) [Permanent 2cores]
 Permanent [2]:1
PROC Permits assigned for PPAR 1 (4 MAX) [Permanent 0cores]
 Permanent [0]:4
PROC Permits assigned for PPAR 2 (0 MAX) [Permanent 0cores]
```

```
 Permanent [0]:
PROC Permits assigned for PPAR 3 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 4 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 5 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 6 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 7 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 8 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 9 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 10 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 11 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 12 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 13 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 14 (0 MAX) [Permanent 0cores]
 Permanent [0]:
PROC Permits assigned for PPAR 15 (0 MAX) [Permanent 0cores]
 Permanent [0]:
```

The following example adds two CPU core resources to physical partition 0.

```
XSCF> showcod -p 0
PROC Permits assigned for PPAR 0: 10
XSCF> setcod -p 0 -s cpu -c add 2
PROC Permits assigned for PPAR 0 : 10 -> 12

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
XSCF> showcod -p 0
PROC Permits assigned for PPAR 0: 12
```

Note - With **setcod -p 0 -s cpu -c set 12** specified, the command yields the same results.

Note - The XSCF firmware of version XCP 2250 or earlier does not support the -c add, -c delete, and -c set options. Specify the setcod command options as follows to interactively add and delete assignments.
XSCF> **setcod -s cpu**

3. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.

5.3.6 Adding CPU Cores to a Logical Domain

To assign a CPU core to a logical domain, use add-core or set-core, each of which is an ldm subcommand of Oracle VM Server for SPARC.
For details, see "Chapter 3   Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

5.3.7 Saving Logical Domain Configuration Information

Execute the ldm command of Oracle VM Server for SPARC with the add-spconfig subcommand specified to save logical domain configuration information.

```
primary# ldm add-spconfig config_name
```

For config_name, specify the file name used to save logical domain configuration information to the XSCF.

Note - The add-spconfig subcommand cannot overwrite the configuration information in an existing file. Before specifying the name of an existing file for config_name, you need to delete the existing file by using the remove-spconfig subcommand.

5.4 Deleting CPU Core Resources

This section describes how to delete a CPU Activation from the SPARC M12/M10. In general, there is no need to delete a CPU Activation. When moving a CPU Activation to another server, you need to delete it from your SPARC M12/M10. For the moving procedures, see "5.5   Moving CPU Core Resources."

5.4.1 CPU Activation Deletion Workflow

Figure 5-2 shows the steps for deleting a CPU Activation.

Figure 5-2   CPU Activation Deletion Workflow

```
┌─────────────────────────────────────────────────────────────┐
│      Remove the CPU core resources from the logical domain   │
└─────────────────────────────────────────────────────────────┘
                              ▼
┌─────────────────────────────────────────────────────────────┐
│   Release the CPU core resources from the physical partition │
└─────────────────────────────────────────────────────────────┘
                              ▼
┌─────────────────────────────────────────────────────────────┐
│          Confirm the CPU Activation keys to be deleted       │
└─────────────────────────────────────────────────────────────┘
                              ▼
┌─────────────────────────────────────────────────────────────┐
│   Delete the CPU Activation keys from the SPARC M12/M10 server│
└─────────────────────────────────────────────────────────────┘
```
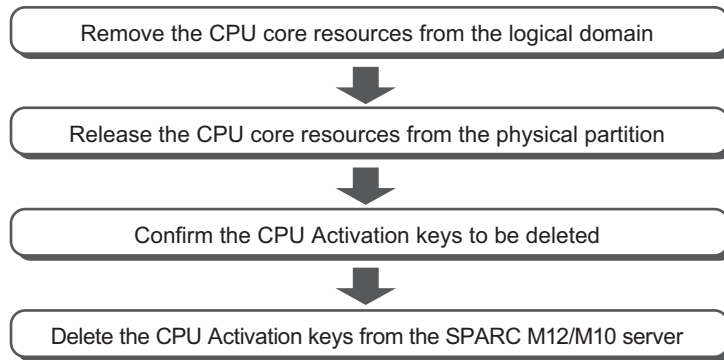
5.4.2   Removing CPU Cores From Logical Domains

To remove a CPU core from a logical domain, use remove-core or set-core, each of which is an ldm subcommand of Oracle VM Server for SPARC.
For details, see "Chapter 3   Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

5.4.3   Releasing CPU Core Resources From a Physical Partition

To release a CPU core resource from a physical partition, use the setcod command on the XSCF shell. You can release CPU core resources by specifying a smaller number of CPU Activations than the quantity currently set.

Execute the setcod command with interactive operation from the XSCF shell. You need to have the platadm privilege to execute this command.

```
XSCF> setcod [-p ppar_id] -s cpu
```

If the applied XSCF firmware is XCP 2260 or later, you can also execute the following command.
The permits value specifies the number of CPU Activations for CPU cores whose use is allowed.
CPU Activations can be specified in units of one CPU core.

```
XSCF> setcod [[-q] -{y|n}] -p ppar_id -s cpu -c {set|add|del} permits
```

For details, see "5.3.5   Assigning a CPU Core Resource to a Physical Partition."

5.4.4 Checking the CPU Activation Key to be Deleted

To identify the CPU Activation key to be deleted, use the showcodactivation command on the XSCF shell. You can select any CPU Activation key.
By entering the showcodactivation command, you can list the CPU Activation keys with an index.

```
XSCF> showcodactivation
Index   Description Count
------- ----------- ------
      1 PROC             2
      2 PROC             2
```

Next, find the index number of the CPU Activation key that you have decided to delete. Then, use the showcodactivation command to confirm the information on the CPU Activation key identified by the index.
For example, suppose that you are going to delete the CPU Activation key of index=1. Then, enter the following command to identify as follows the information on the CPU Activation key to be deleted.

```
XSCF> showcodactivation -r -i 1
*Index1
Product: SPARC M10-1
SequenceNumber: 116
Cpu noExpiration 2
Text-Signature-SHA256-RSA2048:
SBxYBSmB32E1ctOidgWV09nGFnWKNtCJ5N3WSlowbRUYlVVySvjncfOrDNteFLzo
   .
   .
1TSgrjnee9FyEYITT+ddJQ==
```

To record the information on the CPU Activation key to be deleted, you may need to copy and paste the entire contents of the key or write them down for your records.

5.4.5 Deleting CPU Activation Keys

To delete a CPU Activation key from the XSCF of the SPARC M12/M10, use the deletecodactivation command on the XSCF shell.
You need to have the platadm privilege to execute this command.

```
XSCF> deletecodactivation -i key-index
```

Specify the index number of the CPU Activation key to be deleted.
The deletecodactivation command does not allow you to delete CPU Activation keys in such a way that the quantity becomes less than the total number of CPU Activations set for the PPAR by the setcod command.
Reduce the number of CPU Activations set for the PPAR in advance.

5.5 Moving CPU Core Resources

When using multiple SPARC M12/M10 units, you can move a CPU Activation only between the same models.

5.5.1 CPU Activation Move Workflow

Figure 5-3 shows the steps for moving a CPU Activation.

Figure 5-3   CPU Activation Move Workflow

Remove the CPU core resources from logical domains	(Refer to 5.4.2)
Releasing CPU core resources from a physical partition	(Refer to 5.4.3)
Checking the CPU Activation key to be moved	(Refer to 5.5.2)
Deleting CPU Activation keys	(Refer to 5.4.5)
Register the deleted CPU Activation keys with another SPARC M12/M10	(Refer to 5.3.4 - 5.3.6)
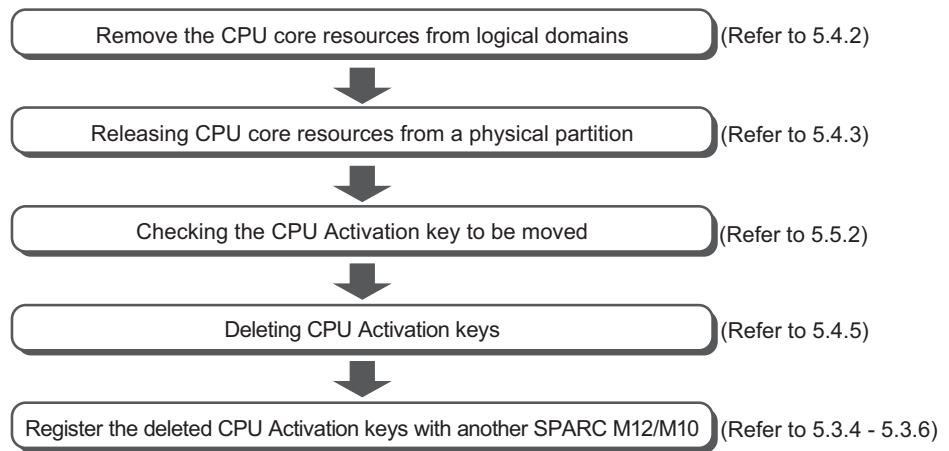
Note - If the SPARC M12/M10 system has failed, a CPU Activation key on the faulty SPARC M12/M10 system can be registered with another SPARC M12/M10 system. You do not need to delete the key from the faulty system.

5.5.2 Checking the CPU Activation Key to be Moved

To identify the CPU Activation key to be moved, use the showcodactivation command on the XSCF shell. You can select any CPU Activation key to check its information.

By entering the showcodactivation command, you can list the CPU Activation keys with an index.

```
XSCF> showcodactivation
Index    Description Count
-------  ----------- ------
```

```
        1 PROC           2
        2 PROC           2
```

Next, find the index number of the CPU Activation key that you have decided to move.

Then, use the showcodactivation command to confirm the information on the CPU Activation key identified by the index.
For example, suppose that you are going to move the CPU Activation key of index=1. Then, enter the following command to identify as follows the information on the CPU Activation key to be moved.

```
XSCF> showcodactivation -r -i 1
*Index1
Product: SPARC M10-1
SequenceNumber: 116
Cpu noExpiration 2
Text-Signature-SHA256-RSA2048:
SBxYBSmB32E1ctOidgWV09nGFnWKNtCJ5N3WSlowbRUYlVVySvjncfOrDNteFLzo
   .
   .
1TSgrjnee9FyEYITT+ddJQ==
```

Next, add exactly the same key to another M12/M10 of the same model by copying the entire contents of this key, starting from the Product line, and then pasting the content, or by writing the content.

5.6 Displaying CPU Activation Information

5.6.1 Displaying CPU Activation Registration and Setting Information

To display information on the CPU Activations registered and set in your SPARC M12/M10, use the showcod command on the XSCF shell. You need to have the platadm or platop privilege to execute this command. Alternatively, you can use a user account that has the pparadm, pparmgr, or pparop privilege for the target physical partition.

```
XSCF> showcod [-p ppar_id]
```

For the -p ppar_id option, specify the physical partition ID of the information to be displayed. If this option is not specified, the command displays information on all

accessible physical partitions.

The following information is displayed when the showcod command is executed.

- Number of CPU Activations registered in the system
- Number of CPU Activations set for a physical partition

Operation Procedure

1. **Log in to the XSCF with a user account that has the appropriate user privilege.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the showcod command to display CPU Activation information.**
   The following example displays detailed information on all CPU Activations.

```
XSCF> showcod -v -s cpu
PROC Permits installed : 8 cores
PROC Permits assigned for PPAR 0: 4 [Permanent 4cores]
  :
PROC Permits assigned for PPAR 15: 0 [Permanent 0cores]
```

3. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.

5.6.2   Checking the COD Log

To display a log of events such as adding/deleting a CPU Activation key, use the
showcodactivationhistory command on the XSCF shell.
You need to have the platadm, platop, or fieldeng privilege to execute this command.

```
XSCF> showcodactivationhistory [target_url]
```

Specify the file name for the resulting output file as target_url.

Operation Procedure

1. **Log in to the XSCF with a user account that has the platadm, platop, or
   fieldeng privilege.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the showcodactivationhistory command to display the CPU
   Activation key COD log.**

```
XSCF> showcodactivationhistory
11/30/2012 01:42:41PM PST: Report Generated SPARC M10-1 SN: 843a996d
10/02/2012 02:08:49PM PST: Activation history initialized: PROC 0
cores
```

```
10/15/2012 01:36:13PM PST: Capacity added: PROC 2 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 2 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 2 cores
11/07/2012 01:46:23PM PST: Capacity deleted: PROC 2 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 2 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 2 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 2 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 2 cores
11/30/2011 01:42:41PM PST: Summary: PROC 8 cores
Signature: 9138HVZQ0zFJh8EoRy7i1A
```

3. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.

5.6.3 Displaying CPU Activation Key Information

To display information on the CPU Activations keys registered in your system, use the showcodactivation command on the XSCF shell. You need to have the platadm or platop privilege to execute this command. By entering the showcodactivation command without specifying any options, you can list the CPU Activation keys with an index.

```
XSCF> showcodactivation [-r] [-v] [-y key-index] [-M]
```

Specify the index number of a CPU Activation key to display its information.

You can check the CPU Activation key of the specified index in raw data format by specifying the -i and -r options and executing the showcodactivation command. To display one screen at a time, specify the -M option.

Operation Procedure

1. **Log in to the XSCF with a user account that has the platadm or platop privilege.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the showcodactivation command without specifying any options to list the CPU Activation keys with an index.**

```
XSCF> showcodactivation
Index    Description Count
-------  ----------- ------
1        PROC             2
2        PROC             2
```

3. **Execute the showcodactivation command to display information on the CPU Activation keys in your system.**
   The following example displays information on the CPU Activation key of index

2 in raw data format.

```
XSCF> showcodactivation -r -i 2
*Index2
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA……..
```

4. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.

5.6.4 Displaying the Usage of Activated CPU Core Resources

The displayed CPU core resource usage includes the following items:

- CPU core resources in use

- Number of mounted CPU cores

- Number of CPU Activations set for a physical partition

- Any CPU Activation violations

To display the CPU core resource usage, use the showcodusage command on the XSCF shell.
You need to have the platadm, platop, or fieldeng privilege to execute this command.
Alternatively, you can use a user account that has the pparadm, pparmgr, or pparop privilege for the target physical partition.

```
XSCF> showcodusage [-v] [-M] [-p {resource|ppar|all}]
```

To display one screen at a time, specify the -M option.
To display the CPU core resource usage in all physical partitions, specify -p all.
To display the CPU core resource usage in each physical partition, specify -p ppar.
To display the CPU core resource usage for each CPU core resource, specify -p resource.

Operation Procedure

1. **Log in to the XSCF with a user account that has the appropriate user privilege.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the showcodusage command to display CPU Activation information.**
   The following example displays CPU Activation information.

   The example shows that the system has 16 installed CPU core resources and 4 registered CPU Activations, and that 4 of the CPU core resources are in use and the number of currently unused CPU Activations is 0.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC         4      16            4 OK: 0 cores available

Note:
  Please confirm the value of the "In Use" by the ldm command of
 Oracle VM Server for SPARC.

  The XSCF may take up to 20 minutes to reflect the "In Use" of
logical domains.
```

Note - The value of "In Use" that is displayed by the showcodusage command may not be the latest, depending on the timing of the XSCF update. It may take up to 20 minutes for the value of "In Use" to be updated to the latest one. If the value of "In Use" is different from what you expected, execute the showcodusage command again to check the value.

3. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.

5.7 Saving/Restoring CPU Activation Keys

In some cases, an operator may accidentally execute a command that deletes a CPU Activation key.
It may be a good idea to save CPU Activation keys for recovery in case of such an incident.
This section describes how to save and restore CPU Activation keys.

5.7.1 Saving CPU Activation Keys

To save the CPU Activation keys on your system, use the dumpcodactivation command on the XSCF shell.
You need to have a user account that has the platadm, platop, or fieldeng privilege to execute this command.

Specify the URL of the storage location for the CPU Activation key.
The following command syntax shows how to specify USB media.

```
XSCF> dumpcodactivation file:///media/usb_msd/filename
```

This command saves all the CPU Activation keys stored on the XSCF.
The CPU Activation keys are stored in plaintext by default.
With the -e option specified, the command encrypts and saves the CPU Activation keys.

5.7.2 Restoring CPU Activation Keys

To restore backed-up CPU Activation keys to your system, use the restorecodactivation command on the XSCF shell.
You need to have a user account that has the platadm, platop, or fieldeng privilege to execute this command.

Specify the URL of the location of the CPU Activation keys stored by the dumpcodactivation command.
The following command syntax shows how to specify USB media.

```
XSCF> restorecodactivation file:///media/usb_msd/filename
```

Before executing this command, you need to power off all the physical partitions.
The command restores all the CPU Activation keys stored at the URL.

5.8 Troubleshooting CPU Activation Errors

5.8.1 The Number of CPU Cores in Use Exceeds the Number of Activated CPU Cores

If the number of CPU cores in use exceeds the number of activated CPU cores, the following error is registered in the OVM service log (/var/svc/log/ldoms-ldmd:default.log).
Example:
CPU permits-violation detection. executing permits-violation clearance
If this service log registration occurs, action needs to be taken, such as stopping use of the CPU cores.
If the problem is not solved, CPU cores exceeding the number of activated CPU cores are automatically removed from logical domains. This removal of the CPU cores applies to all logical domains. If the CPU core removal fails to satisfy the condition for the number of activated CPU cores, the system stops the logical domains.

5.8.2 The Number of Working CPU Cores Drops Below the Number of CPU Activations Because of a Failure

If the number of working CPU cores drops below the number of CPU Activations because of a failure, any unassigned CPU core resources within the physical partition are dynamically added to the logical domain to meet the number of CPU cores that

were added to the logical domain.
The failed CPU cores are removed from the logical domain.
While this action is being taken, the total number of working CPU cores does not exceed the number of CPU Activations. Therefore, you do not have to prepare (purchase) any additional CPU Activations to allow this function to work.
This function is called automatic replacement of failed CPUs. The function is enabled by default.
For details, see "10.7   Setting Automatic Replacement of Failed CPU Cores" and the ldm command of Oracle VM Server for SPARC.

5.9   Important Notes about CPU Activation

This section provides the following notes about working with CPU Activation:

- Adding/Removing CPU Cores Dynamically
- Live Migration
- Adding/Removing the SPARC M12-2S/M10-4S in a Building Block Configuration
- Saving Logical Domain Configuration Information

Adding/Removing CPU Cores Dynamically

You can add or remove CPU cores dynamically by using the ldm command or through automatic replacement of failed CPUs.
This is achieved through a logical dynamic reconfiguration feature with the help of Oracle VM Server for SPARC.
However, in specific configurations, instead of the dynamic reconfiguration feature being used, logical domains need to be rebooted to add/remove CPU cores.
This situation occurs when CPU cores are assigned as physical resources.

For details, see "Assigning Physical Resources to Domains" in the *Oracle VM Server for SPARC Administration Guide* for the version used.

Note - The SPARC M12/M10 has the following two kinds of dynamic reconfiguration (DR):
- DR function that dynamically (re-)assigns CPU core/memory resources to and from your working logical domain. This is a function provided by the Oracle VM Server for SPARC software.
- DR function that dynamically (re-)assigns a building block (which means one SPARC M12-2S or SPARC M10-4S) to and from your working physical partition. This is a function provided by the Oracle VM Server for SPARC software and the XSCF firmware.

Live Migration

The physical partition that is the migration destination of a guest domain should have enough activated CPU core resources that are not assigned to physical domains. If the number of unused activated CPU Activations is insufficient, you may need to add CPU Activations. Even for live migration between SPARC M12/M10 of the same model, CPU Activations may need to be added to the destination. This is because it is

impossible to move CPU Activations between two systems (even if they are practically one system.)

For details of live migration, see "Chapter 7   Migrating a Guest Domain" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Adding/Removing the SPARC M12-2S/M10-4S in a Building Block Configuration

When adding a SPARC M12-2S/M10-4S in a building block configuration, check that the number of CPU Activations is sufficient and add the unit as necessary.

Saving Logical Domain Configuration Information

If you change the configuration of a logical domain, save the logical domain information by executing the ldm add-spconfig command.
For example, suppose that you moved a logical domain to another system through live migration and reduced the number of CPU Activations on the source system. In this case, save the logical domain configuration information by using the ldm add-spconfig command after the completion of live migration.
If you do not save the configuration information of the logical domain, the domain will start with the previous configuration information the next time the physical partition is started. In this case, the number of CPU Activations may be insufficient, and thus the start may fail.

Note - Even with a system that has only the control domain in its configuration, save the logical domain configuration information when you change the resource configuration with the ldm command of Oracle Solaris.

Chapter 6

Starting/Stopping the System

This chapter describes the start flow and stop flow of the SPARC M12/M10 systems and their operation procedures.

- Starting the System
- Stopping the System
- Rebooting the System
- Suppressing Starting Oracle Solaris at Power-on

6.1 Starting the System

This section describes the flow up to system start and the operation procedures.

6.1.1 Flow From Input Power-on to System Start

This section describes the flow from power-on to logical domain start.

Figure 6-1   Flow From Input Power-on to System Start
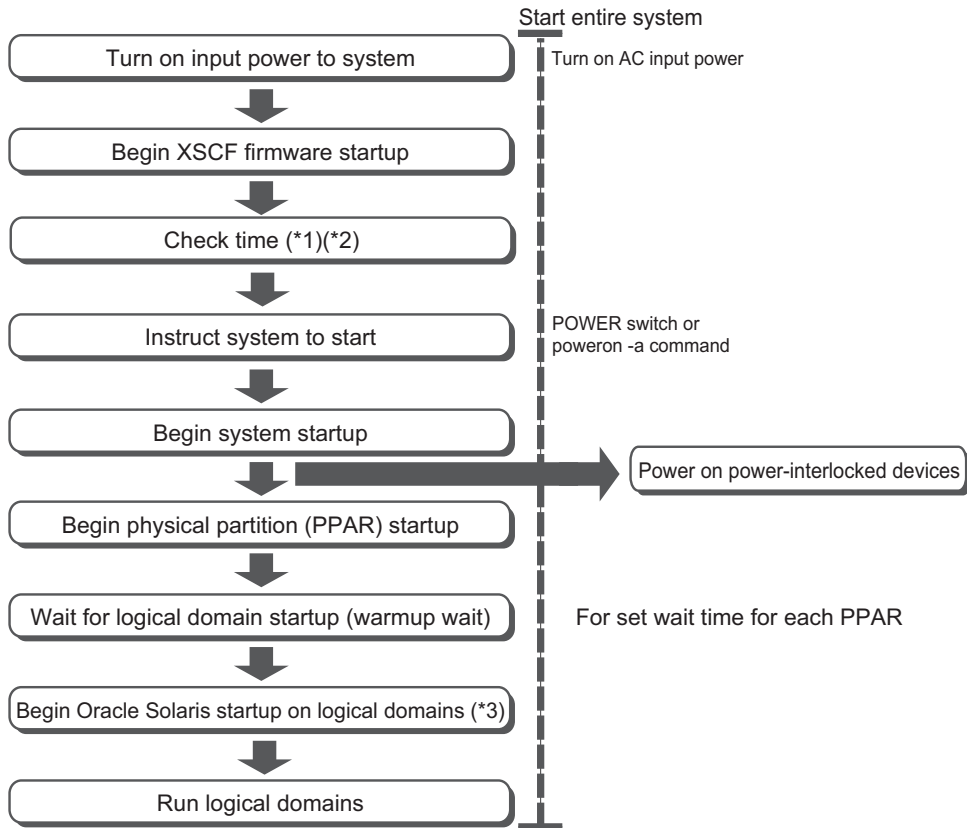
*1 For details on how to check the XSCF time, see "6.1.2   Setting the XSCF Time Before System Startup."

*2 For a logical domain configuration, if the logical domain configuration information was not saved in XSCF at the last time the physical partition stopped, the logical domain time may shift when the physical partition starts. (See "6.2   Stopping the System.")

With XCP 2350 or later, or XCP 3050 or later, you can check logical domains for a time deviation from the XSCF. To do so, execute the showdateinfo(8) command before starting the physical partition.

The logical domain information may not have been saved on the XSCF when the physical partition was stopped, or the logical domain time may have shifted. As required, set the logical domain time before beginning the work.

  *3 To suppress starting Oracle Solaris, see "6.4   Suppressing Starting Oracle Solaris at Power-on."

The two methods for specifying the system start instruction are listed below. With either method, perform their operations on the chassis that has the master XSCF.

■ Use the POWER switch on the operation panel (see "6.1.3   Using the POWER Switch").

- Use the poweron command of the XSCF firmware (see "6.1.4   Using the poweron Command").

6.1.2   Setting the XSCF Time Before System Startup

This section describes the procedure for setting the XSCF time before physical partition startup so that logical domains start with the correct time.

- Where the NTP client function is disabled
At initial system installation, use the setdate(8) command to set the XSCF time before starting the physical partition.

  After the initial installation, even if there is a time deviation from the XSCF before you start the physical partition, it will not affect the logical domain time.

  Therefore, you do not need to set the XSCF time when starting the physical partition.

- Where the NTP client function is enabled
There may be a time deviation from the XSCF because time synchronization failed between the NTP server and the XSCF when the XSCF started. (Note)

  If the physical partition starts in this state, the logical domain time may shift.

  Perform the following procedure to set the XSCF time, and then start the physical partition.

Note - For example, if the LAN between the NTP server and the XSCF was disconnected when the XSCF started, the XSCF time may shift even though the XSCF is now connected to the LAN.

---

1.   **Check the current XSCF time.**
    If the XSCF time is correct, step 2 and later are unnecessary.

```
XSCF> showdate
Sat May 19 14:53:00 JST 2018
```

2.   **Correct the XSCF time.**
a.   **Check the network environment and the NTP server status.**
b.   **Reboot the XSCF.**

```
XSCF> rebootxscf -a
```

c.   **After the XSCF reboot, check the current XSCF time.**

```
XSCF> showdate
Sat May 19 15:03:00 JST 2018
```

6.1.3 Using the POWER Switch

Press the POWER switch on the operation panel on the chassis that has the master XSCF. Pressing the POWER switch starts the supply of power in the proper order to all the physical partitions in the system. After that, all the logical domains in each physical partition are started in the proper order.

Note - Only the POWER switch on the chassis that has the master XSCF is functional. The POWER switches on the other chassis cannot power on the system.

Note - If the setpparparam command of the XSCF firmware has suppressed auto boot of a control domain, the suppressed control domain is not started. Furthermore, if the setpparmode command has suppressed auto boot of a physical partition and logical domains, the suppressed logical domains are not started. For details of the setpparparam and setpparmode commands, see the setpparparam(8) and setpparmode(8) command man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

The chassis that has the master XSCF varies depending on the model.

- SPARC M12-1
  POWER switch on the SPARC M12-1

- SPARC M12-2
  POWER switch on the SPARC M12-2

- SPARC M12-2S (no crossbar box)
  POWER switch on BB#00 or BB#01 (chassis whose MASTER LED is on) of the SPARC M12-2S

- SPARC M12-2S (with crossbar boxes)
  POWER switch on the crossbar box XBBOX#80 or XBBOX#81 (chassis whose MASTER LED is on)

- SPARC M10-1
  POWER switch on the SPARC M10-1

- SPARC M10-4
  POWER switch on the SPARC M10-4

- SPARC M10-4S (no crossbar box)
  POWER switch on BB#00 or BB#01 (chassis whose MASTER LED is on) of the SPARC M10-4S

- SPARC M10-4S (with crossbar boxes)
  POWER switch on the crossbar box XBBOX#80 or XBBOX#81 (chassis whose MASTER LED is on)

For details on the switches and LEDs on the operation panel, see the *Service Manual* for your server.

Figure 6-2   Operation Panel (SPARC M12-1/M10-1)

(1)

No.	Component
1	POWER switch

Figure 6-3   Operation Panel (SPARC M12-2/M10-4)

(1)
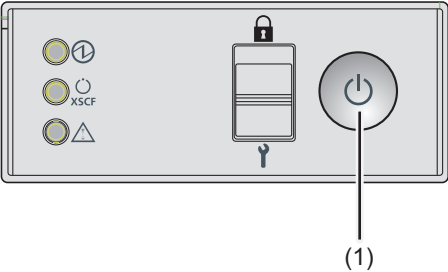
No.	Component
1	POWER switch

Figure 6-4   Operation Panel (SPARC M12-2S/M10-4S Crossbar Box)

(2)   (1)
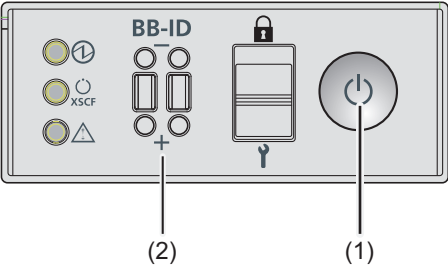
No.	Component
1	POWER switch
2	BB-ID switch

Operation Procedure

1. **Press the POWER switch on the operation panel of the chassis that has the master XSCF.**
   All the physical partitions in the system are started. After that, all the logical domains in each physical partition are started.

6.1.4 Using the poweron Command

Use the poweron command of the XSCF firmware to start the whole system. Execute the command with a user account that has the platadm or fieldeng privilege.

```
XSCF> poweron -a
```

To start the whole system, execute the poweron command with the -a option specified. Execution of the command outputs a confirmation message. Enter "y".

After the command is executed, all the physical partitions in the system are powered on in the proper order. After that, all the logical domains in each physical partition are started in the proper order.

Note - If the setpparparam command of the XSCF firmware has suppressed auto boot of a control domain, the suppressed control domain is not started. Furthermore, if the setpparmode command has suppressed auto boot of a physical partition and logical domains, the suppressed logical domains are not started. For details of the setpparparam and setpparmode commands, see the setpparparam(8) and setpparmode(8) command man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operation Procedure

1. **Execute the poweron -a command to power on the whole system. Enter "y" for the confirmation message.**

```
XSCF> poweron -a
PPAR-IDs to power on:00,01,02,03
Continue? [y|n] :y
00 :Powering on
01 :Powering on
02 :Powering on
03 :Powering on

*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

All the physical partitions in the system are powered on. After that, all the logical domains in each physical partition are started.

2. **Execute the showpparstatus command, and confirm that the power of all the physical partitions in the system is on.**

```
XSCF> showpparstatus -a
PPAR-ID        PPAR Status
00             Running
01             Running
02             Running
03             Running
```

6.2 Stopping the System

This section describes the flow up to system stop and the operation procedures.

6.2.1 Flow From System Stop to Input Power-off

This section describes the flow from stopping the system to turning off the input power.

Figure 6-5   Flow From System Stop Instruction to Input Power-off
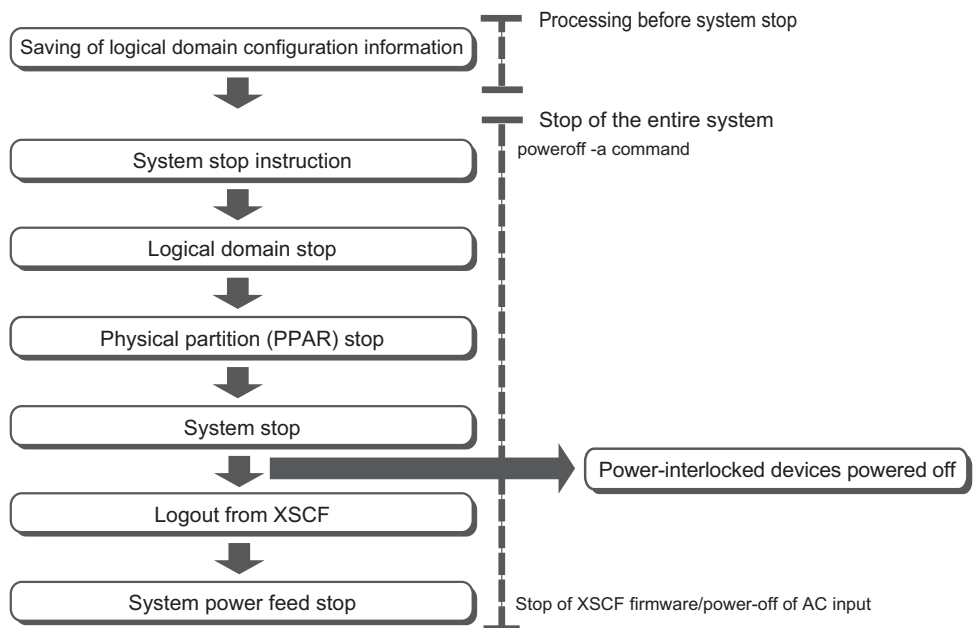
To stop the system, all the logical domains in the target physical partition must be shut down. The shutdown of the logical domains has a specific order: the domains

other than the control domain are shut down first, and then the control domain must be shut down.

The SPARC M12/M10 systems support a technique called ordered shutdown, which shuts down logical domains in an appropriate order and then stops the physical partition, so users do not need to pay attention to the shutdown of logical domains. For an ordered shutdown, numbers representing the order in the group to be shut down are defined for the logical domains in advance. The XSCF stores the defined order to enable shutdown in an appropriate order with this technique, even under XSCF management.
If a non-active guest domain is included in the group for which an ordered shutdown is defined, it takes about 10 minutes to shut down the group.

For details on an ordered shutdown, see "8.7   Ordered Shutdown of Logical Domains."

6.2.2 Saving the Logical Domain Configuration Information before System Stop

In the case of a logical domain configuration, execute the ldm add-spconfig command of Oracle VM Server for SPARC in the control domain to save the latest configuration information in the XSCF before stopping the physical partition.
For details, see "10.11.1   Saving/Displaying Logical Domain Configuration Information."

If the latest configuration information is not saved in the XSCF before stopping the physical partition, the following problems may occur.
- After changing the logical domain configuration, if the physical partition is stopped without the logical domain configuration information being saved, and then it is restarted, it starts with the logical domain configuration as it was before the change.
- Even if you save the latest configuration information in XSCF after changing the logical domain configuration, if it has been a long time since the logical domain configuration was last saved, the time of the logical domain may be deviated when the physical partition was stopped and then restarted.

6.2.3 Stopping the Whole System

Use the poweroff command of the XSCF firmware to stop the whole system.
Execute the command with a user account that has the platadm or fieldeng privilege.

Note - In Locked mode, power-off is not possible from the POWER switch on the operation panel on the chassis that has the master XSCF. For details on Locked mode, see "Chapter 13 Switching to Locked Mode/Service Mode."

```
XSCF> poweroff -a
```

To stop the whole system, execute the poweroff command with the -a option specified. Execution of the command outputs a confirmation message. Enter "y".

After the command is executed, the logical domains in each physical partition are shut down in accordance with the ordered shutdown rules. Then, the physical partition itself is powered off.

Operation Procedure

1. **Execute the poweroff -a command to power off the whole system. Enter "y" for the confirmation message.**

```
XSCF> poweroff -a
PPAR-IDs to power off:00,01,02,03
Continue? [y|n] :y
00 : Powering off
01 : Powering off
02 : Powering off
03 : Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

All the logical domains in each physical partition are shut down, and then all the physical partitions are powered off.

2. **Execute the showpparstatus command, and confirm that the power of all the physical partitions in the system is off.**

```
XSCF> showpparstatus -a
PPAR-ID        PPAR Status
00             Powered Off
01             Powered Off
02             Powered Off
03             Powered Off
```

6.3   Rebooting the System

This section describes how to reboot the system.

Use the rebootxscf command of the XSCF firmware to reboot the XSCF.
Execute the command with a user account that has the platadm or fieldeng privilege.

After the following XSCF items are configured, an XSCF reboot enables the settings:
- Applying the configured XSCF network to the XSCF (applynetwork)
- System altitude (setaltitude)
- NTP-related settings (setntp)

```
XSCF> rebootxscf -a | -b bb_id | -s
```

To reboot all the XSCFs in the system, specify -a. To reboot the XSCF of the specified SPARC M12-2S/M10-4S, specify -b bb_id. Only the master XSCF can execute the -a and -b options. To reboot the current working XSCF, specify -s.

Rebooting the XSCF disconnects the SSH, Telnet, and other connections to the XSCF. Establish the connections again.

Note - If an XSCF reboot by the setdate command of the XSCF firmware has been canceled, even an XSCF reboot by the rebootxscf command does not apply the settings. The setdate command must be executed again.

Operation Procedure

1. **Execute the rebootxscf command to reboot the XSCF. Enter "y" for the confirmation message.**
   The following example reboots all the XSCFs.

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] : y
```

6.4 Suppressing Starting Oracle Solaris at Power-on

This section describes how to suppress starting Oracle Solaris when powering on the SPARC M12/M10.

Note - In the SPARC M12/M10, even if you set the operation panel mode switch to "Service," you cannot suppress starting Oracle Solaris.

The method of suppressing starting Oracle Solaris at power-on in the SPARC M12/M10 is described below.

- Suppressing starting Oracle Solaris in the control domain
  Perform either of the following operations. After this operation, Oracle Solaris stops in OpenBoot PROM.
    - Set the value of the OpenBoot PROM environment variable auto-boot? to false with the setpparam command of the XSCF firmware.
      [Example] XSCF> **setpparam -p 0 -s bootscript** "setenv auto-boot? false"
    - Set the value of the OpenBoot PROM environment variable auto-boot? to false with the eeprom command of Oracle Solaris.

For details of the setpparam command, see the man page of the setpparam(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference*

Manual.

For details on changing the OpenBoot PROM environment variables with the XSCF firmware, see "8.9.1 OpenBoot PROM Environment Variables That Can be Set With the XSCF Firmware."

- Suppressing starting Oracle Solaris in the guest domain
  Set guestboot=off by the setpparmode command of the XSCF firmware.
  [Example] XSCF> **setpparmode -p 0 -m guestboot=off**

For details of the setpparmode command, see the man page of the setpparmode(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

Chapter 7

Controlling Physical Partitions

This chapter describes what is needed to control physical partitions.

- Configuring a Physical Partition
- Setting the Physical Partition Operation Mode
- Powering On a Physical Partition
- Powering Off a Physical Partition
- Changing the Configuration of a Physical Partition

7.1 Configuring a Physical Partition

This section provides an overview of physical partition configuration.

To configure a SPARC M12-2S or SPARC M10-4S system, configure a physical partition (PPAR) by combining one or more building blocks in a server of the same model. Configuring physical partitions is called partitioning, and the resulting configured object is called a physical partition (PPAR).
In the SPARC M12-2S/M10-4S, up to 16 physical partitions can be configured.
Note that since the SPARC M12-2/M10-1/M10-4 is a model consisting of a single chassis, it can be configured with only one physical partition.
In the XSCF firmware, when configuring a physical partition, one building block is treated as one system board (PSB).

Physical partitions are configured with the addboard command of the XSCF firmware. For details, see "Chapter 3   Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

7.2 Setting the Physical Partition Operation Mode

This section provides an overview of the physical partition operation mode.

In the SPARC M12/M10, the following operation modes can be set for each physical partition:
- Diagnosis level of the self-diagnosis test
- Detail level of self-diagnosis test console messages
- Alive Check (monitoring between the XSCF and Hypervisor)
- Operation when Host Watchdog (monitoring between Hypervisor and the control domain) times out
- Break signal suppression
- Auto boot of guest domains
- Power-saving operation
- I/O bus reconfiguration
- PPAR DR function
- CPU operational mode

Setting an operation mode enables control of a given physical partition such that it does not receive unnecessary signals and instructions while running or under maintenance.

The physical partition operation mode is set by the setpparmode command of the XSCF firmware. For details, see "Chapter 3 Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Note - The auto boot for the control domain is set by the setpparparam command. For details, see "8.9.1 OpenBoot PROM Environment Variables That Can be Set With the XSCF Firmware."

7.2.1 CPU Mounted on a Physical Partition and CPU Operational Mode

In the SPARC M10-4S, you can configure the system as a physical partition that has both SPARC M10-4S with SPARC64 X+ processor and a SPARC M10-4S with the SPARC64 X processor.
When the CPU operational mode of the setpparmode command of XSCF firmware is set and the type of CPU operation is specified by physical partition, at the next activation of Oracle Solaris, the system automatically judges if it should operate using the function of a SPARC64X+ processor or SPARC64X processor.

Types of CPU Operation

There are two types of CPU operation as follows:

- Operating using SPARC64 X+ function
  All CPUs on the physical partition operate using the enhanced function of the SPARC64 X+ processor.

  This applies only when CPU operational mode (cpumode) is set to "auto" with the setpparmode command, and all CPUs on the physical partition are configured with the SPARC64 X+ processor.

- Operating using SPARC64 X function
  All CPUs on the physical partition operate with the SPARC64 X processor function.

  When CPU operational mode (cpumode) is set to "compatible" with the setpparmode command, all CPUs of any type mounted on the physical partition operate with the SPARC64 X processor function.

  In addition, when CPU operational mode is set to "auto" with the setpparmode command, all CPUs operate with the SPARC64 X processor function if the SPARC64 X processor is mounted on the physical partition.

Note - For the XCP firmware to support the CPU operational mode setting and the Oracle Solaris version, see *Fujitsu M10/SPARC M10 Systems Product Notes* for the latest XCP version (XCP 2210 or later).

CPU Configuration and Operational Mode of Physical Partitions

As shown in PPAR#2 in Figure 7-1, you can configure one physical partition to have both the SPARC64 X+ processor and the SPARC64 X processor in a SPARC M10-4S system.

Figure 7-1 Example of Configuration of Processors and Physical Partitions Mounted on a SPARC M10-4S System
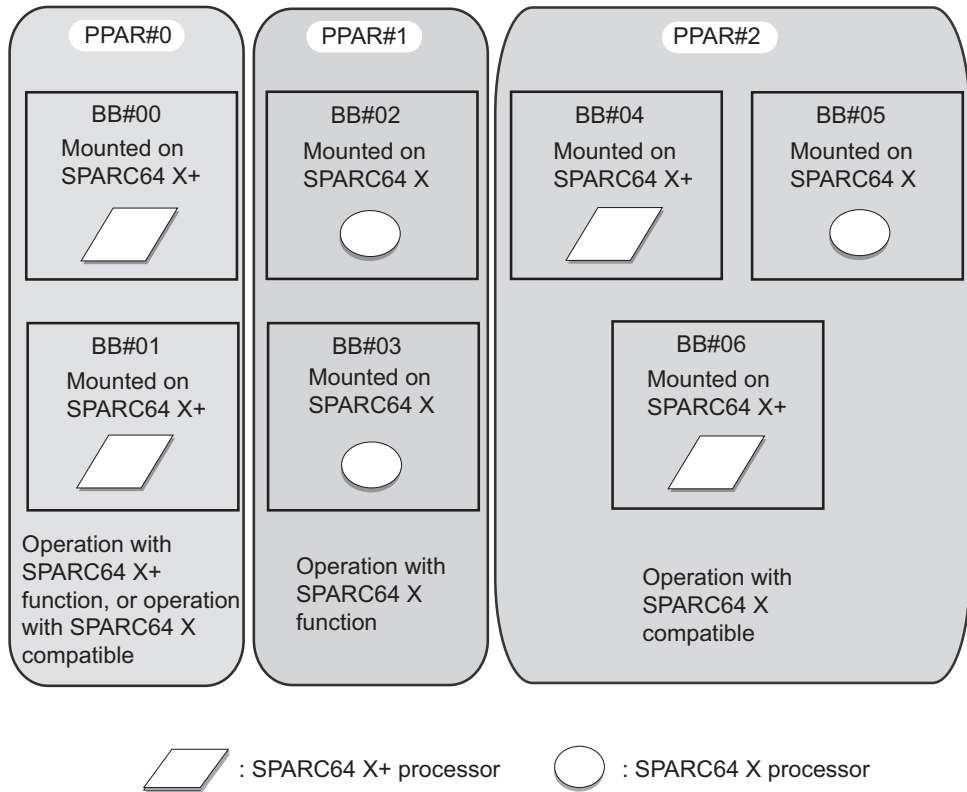
Table 7-1 lists the CPU configurations of physical partitions, CPU operational mode setting values, and CPU operating types on Oracle Solaris.

Table 7-1 CPU Configuration and Operational Mode of Physical Partitions

CPU Configuration of PPAR	CPU operational mode (CPU Mode) value of setpparmode command	CPU Operating Type of Oracle Solaris
SPARC64 X+	auto	Operation with SPARC64 X+ function
SPARC64 X+	compatible	Operation with SPARC64 X compatible
SPARC64 X+/X	"auto" or "compatible"	SPARC64 X+ operation with SPARC64 X compatible SPARC64 X operation with SPARC64 X function
SPARC64 X	"auto" or "compatible"	Operation with SPARC64 X function

For details of the CPU configuration of physical partitions at the PPAR DR operation time and the CPU operating types on Oracle Solaris, see "2.6 Considerations When

Using the SPARC64 X+ Processor" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Checking the Applied CPU Operating Type

To check the currently applied CPU operating type, execute the prtdiag or psrinfo command of Oracle Solaris. When the CPU of the physical partition is operating with the SPARC64 X+ function, "SPARC64-X+" is output on the System Processor Mode line. On the other hand, when it is operating with the SPARC64 X function, "SPARC64-X" is displayed on the System Processor Mode line.

1. **On the targeted physical partition, execute the prtdiag or psrinfo command of Oracle Solaris with the -pv option to check the currently applied CPU operating type.**
   In this case, the SPARC64 X+ function is used for operation.

The following example shows the prtdiag command execution results.

```
primary# prtdiag
System Configuration: Oracle Corporation sun4v SPARC M10-4S
Memory size: 391168 Megabytes

 ================================ Virtual CPUs ================================

CPU ID Frequency Implementation         Status
------ --------- ---------------------- -------
0      3700 MHz  SPARC64-X+             on-line
```

The following example shows the psrinfo -pv execution results.

```
primary# psrinfo -pv
The physical processor has 12 cores and 24 virtual processors (0-23)
  The core has 2 virtual processors (0 1)
  The core has 2 virtual processors (2 3)
  The core has 2 virtual processors (4 5)
  The core has 2 virtual processors (6 7)
  The core has 2 virtual processors (8 9)
  The core has 2 virtual processors (10 11)
  The core has 2 virtual processors (12 13)
  The core has 2 virtual processors (14 15)
  The core has 2 virtual processors (16 17)
  The core has 2 virtual processors (18 19)
  The core has 2 virtual processors (20 21)
  The core has 2 virtual processors (22 23)
    SPARC64-X+ (chipid 0, clock 3700 MHz)
```

Checking the Setting Status of CPU Operational Mode

Use the showpparmode command of the XSCF firmware to check the setting status of the CPU operational mode. Execute the command with a user account that has the platadm or fieldeng privilege. You can also execute it with a user account that has the pparadm privilege for the target physical partition.

Note - With the showpparmode command, the latest setting information set with the setpparmode command is displayed. There are cases that do not correspond to the currently applied CPU operating type. This is because the setting information set with the setpparmode command is reflected when the physical partition is restarted. For example, if the CPU operational mode is set to "auto" and the CPU operational mode is set to "compatible" for a physical partition that operates with the SPARC64 X+ function using the setpparmode command, "compatible" is output with the showpparmode command. However, it operates with the SPARC64 X+ function until the physical partition is restarted.

```
XSCF> showpparmode -p ppar_id
```

For ppar_id, specify the PPAR ID of the physical partition. You can specify a numeric value from 0 to 15.

1. **In the targeted physical partition, execute the showpparmode command of XSCF firmware, and check the CPU operational mode set with the setpparmode command.**
   In this case, it is checked against PPAR-ID 00.

```
XSCF> showpparmode -p 0
Host-ID                 :0f010f10
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
Elastic Mode            :off
IOreconfigure           :true
CPU Mode                :auto
PPAR DR(Current)        :off
PPAR DR(Next)           :off
```

Changing the CPU Operational Mode

The default CPU operational mode of the setpparmode command is set to "auto". When it is set to "auto", whenever a physical partition is started, the CPU operating type on Oracle Solaris is automatically selected depending on the type of CPU mounted on the physical partition.
When the CPU operational mode is changed from "auto" to "compatible" with the setpparmode command, regardless of the type of mounted CPU, at the next activation of the physical partition, the CPU operates with the SPARC64 X function.

Use the setpparmode command of the XSCF firmware to change the CPU operational mode. Execute the command with a user account that has the platadm privilege. You can also execute it with a user account that has the pparadm privilege for the target physical partition.

```
XSCF> setpparmode -p ppar_id -m cpumode=mode
```

For ppar_id, specify the PPAR ID of the physical partition. You can specify a numeric value from 0 to 15. For mode, specify the CPU operational mode. You can specify "auto" when the CPU is operated with the SPARC64 X+ function, and "compatible" when it is operated with the SPARC64 X function. The default is "auto".

Note - To change the CPU operational mode, it is necessary to power off the target physical partition.

1. **Execute the poweroff command to power off the targeted physical partition.**
   The following example powers off PPAR-ID 00.

```
XSCF> poweroff -p 0
PPAR-IDs to power off:00
Continue? [y|n] :y
00 : Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

2. **Execute the showpparmode command to confirm the current setting of the CPU operational mode (CPU mode).**
   In the following example, the CPU operational mode is set to "auto".

```
XSCF> showpparmode -p 0
Host-ID                   :0f010f10
Diagnostic Level          :min
Message Level             :normal
Alive Check               :on
Watchdog Reaction         :reset
Break Signal              :on
Autoboot(Guest Domain)    :on
Elastic Mode              :off
IOreconfigure             :true
CPU Mode                  :compatible
PPAR DR(Current)          :off
PPAR DR(Next)             :off
```

3. **Execute the setpparmode command to change the CPU operational mode.**
   In the following example, the CPU operational mode is changed from "auto" to "compatible".

```
XSCF> setpparmode -p 0 -m cpumode=compatible
Diagnostic Level          :max          -> -
Message Level             :normal       -> -
Alive Check               :on           -> -
Watchdog Reaction         :reset        -> -
Break Signal              :on           -> -
Autoboot(Guest Domain)    :on           -> -
```

```
Elastic Mode              :off       -> -
IOreconfigure             :true      -> -
CPU Mode                  :auto      -> compatible
PPAR DR                   :off       -> -
The specified modes will be changed.
Continue? [y|n] :y
configured.
Diagnostic Level          :max
Message Level             :normal
Alive Check               :on (alive check:available)
Watchdog Reaction         :reset (watchdog reaction:reset)
Break Signal              :on (break signal:non-send)
Autoboot(Guest Domain)    :on
Elastic Mode              :on
IOreconfigure             :false
CPU Mode                  :compatible
PPAR DR                   :off
```

4. **Execute the showpparmode command to confirm the current setting of the CPU operational mode (CPU mode).**
   In the following example, the CPU operational mode is set to "compatible".

```
XSCF> showpparmode -p 0
Host-ID                   :0f010f10
Diagnostic Level          :min
Message Level             :normal
Alive Check               :on
Watchdog Reaction         :reset
Break Signal              :on
Autoboot(Guest Domain)    :on
Elastic Mode              :off
IOreconfigure             :true
CPU Mode                  :compatible
PPAR DR(Current)          :off
PPAR DR(Next)             :off
```

5. **Execute the poweron command to power on the targeted physical partition.**
   The following example powers on PPAR-ID 00.

```
XSCF> poweron -p 0
PPAR-IDs to power on:00
Continue? [y|n] :y
00 :Powering on

*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

7.2.2 Checking Power Operation at Power Recovery/ Setting Automatic Power-on

This section describes how to check and set whether the following is done automatically at power recovery after a power outage: power-on of physical partitions and startup of Oracle Solaris on logical domains.

Checking power operations at power recovery

Use the showpowerschedule command to check whether a physical partition can be automatically powered on at power recovery. Use the showpparparam command or showpparmode command to check whether Oracle Solaris on a logical domain can be automatically started at power recovery. For any of these commands, an output result that is the default value means that the physical partition is powered on and Oracle Solaris starts on the logical domain at power recovery.

Operation Procedure

1. **Execute the showpowerschedule command, and check the power operations of physical partitions at power recovery.**

```
XSCF> showpowerschedule -a -m state
PPAR-ID schedule member recover mode
------- -------- ------ ------------
0       disable  -      on
1       enable   1      auto
```

   If [recover mode] is "on" (default), or if [schedule] is "enable" and [recover mode] is "auto," the physical partition is automatically powered on at power recovery.

   [schedule] has the following meanings.

   - disable: Scheduled power operations are disabled. (Default)

   - enable: Scheduled power operations are enabled.

   [recover mode] has the following meanings.

   - on: Restore power at power recovery to the same state as before the power outage.

      If the power was on before the power outage, the power will be turned on. (Default)

   - off: Do not turn on the power at power recovery.

   - auto: Turn on the power within the scheduled power operation period at power recovery.

2. **Execute the showpparparam command, and check the auto boot setting of the control domain.**
   The following example displays the set value of the OpenBoot PROM environment variable [auto-boot?] for the control domain of PPAR-ID 0.

The setting is "true" (default), so Oracle Solaris starts automatically at power recovery.

```
XSCF> showpparparam -p 0 -c auto-boot
auto-boot? :true
```

3. **Execute the showpparmode command, and check the auto boot setting of the guest domain.**
   The following example displays the value of the auto boot setting [Autoboot (Guest Domain)] of the set guest domain for PPAR-ID 0. The setting is "on" (default), so Oracle Solaris automatically starts at power recovery.

```
XSCF> showpparmode -p 0
Host-ID                 :9007002b
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
Elastic Mode            :off
IOreconfigure           :false
CPU Mode                :auto
PPAR DR(Current)        :-
PPAR DR(Next)           :off
```

Setting automatic power-on at power recovery

Use the setpowerschedule command to set the power operation of a physical partition at power recovery. Use the setpparparam or setpparmode command to set auto boot of a logical domain. Setting the power operation of a physical partition enables automatic power-on of the physical partition at power recovery. Enabling the auto boot function of a logical domain enables automatic Oracle Solaris startup at power recovery.

1. **Execute the setpowerschedule command to set the power operations of a physical partition at power recovery.**
   The two types of settings are as follows.

   - To restore power to the same state as before the power outage (Default)

```
XSCF> setpowerschedule -p ppar_id -c recover=on
```

   - To follow the scheduled power operations at power recovery

   Use this when the physical partition power schedule has been set by the addpowerschedule command. At a given time covered by the power schedule, the partition is powered on at power recovery, irrespective of the physical partition power status at the time of the power outage.

```
XSCF> setpowerschedule -p ppar_id -c control=enable
XSCF> setpowerschedule -p ppar_id -c recover=auto
```

2. **Execute the setpparparam command to set the OpenBoot PROM environment variable that prevents the control domain from stopping at the ok prompt.**

```
XSCF> setpparparam -p ppar_id -s bootscript "setenv auto-boot? true"
```

3. **To automatically start the guest domain of a physical partition, execute the setpparmode command.**

```
XSCF> setpparmode -y -p ppar_id -m guestboot=on
```

To automatically start a domain at power recovery, you need to use the ldm add-spconfig command on the control domain to save the logical domain configuration information after the domain enters the active state. For details, see the *Oracle VM Server for SPARC Administration Guide* of the version used.
Regardless of the above setting, power-on at power recovery is suppressed when the mode switch is set to "Service."

For details of the setpowerschedule, addpowerschedule, setpparparam, and setpparmode commands, see the man page of each command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

7.3　Powering On a Physical Partition

Use the poweron command of the XSCF firmware to power on physical partitions individually.
Execute the command with a user account that has the platadm or fieldeng privilege.
Alternatively, you can also execute it with a user account that has the pparadm or pparmgr privilege for the target physical partition.

```
XSCF> poweron -p ppar_id
```

To specify a physical partition, specify the -p ppar_id option. You can specify a numeric value from 0 to 15 for ppar_id, which is the PPAR-ID of the physical partition to be started.
Execution of the command outputs a confirmation message. Enter "y".

Note - The SPARC M12-2/M10-1/M10-4 has only one physical partition, so only 0 can be specified for its PPAR-ID.

After the command is executed, the specified physical partition is powered on. After that, all the logical domains in the physical partition are started. The control domain is started first, and then the other domains are started in no particular order.

Note - If the setpparparam command of the XSCF firmware has suppressed auto boot of a control domain, the suppressed control domain is not started. Furthermore, if the setpparmode command has suppressed auto boot of a physical partition and logical domains, the suppressed logical domains are not started. For details of the setpparparam and setpparmode commands, see the setpparparam(8) and setpparmode(8) command man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operation Procedure

1. **Execute the poweron command to power on the specified physical partition.**
   The following example powers on PPAR-ID 00.

```
XSCF> poweron -p 0
PPAR-IDs to power on:00
Continue? [y|n] :y
00 :Powering on

*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

The physical partition with PPAR-ID 00 is powered on. All the logical domains in the physical partition are started.

2. **Execute the showpparprogress command, and confirm that the power of the specified physical partition is on.**

```
XSCF> showpparprogress -p 0
PPAR Power On Preprocessing PPAR#0 [ 1/12]
PPAR Power On          PPAR#0 [ 2/12]
XBBOX Reset            PPAR#0 [ 3/12]
PSU On                PPAR#0 [ 4/12]
CMU Reset Start            PPAR#0 [ 5/12]
XB Reset 1            PPAR#0 [ 6/12]
XB Reset 2            PPAR#0 [ 7/12]
XB Reset 3            PPAR#0 [ 8/12]
CPU Reset 1            PPAR#0 [ 9/12]
CPU Reset 2            PPAR#0 [10/12]
Reset released            PPAR#0 [11/12]
CPU Start            PPAR#0 [12/12]
The sequence of power control is completed.
XSCF>
```

7.4 Powering Off a Physical Partition

In the case of a logical domain configuration, execute the ldm add-spconfig command of Oracle VM Server for SPARC in the control domain to save the latest configuration information in the XSCF before powering off the physical partition. For details, see "6.2.2　Saving the Logical Domain Configuration Information before System Stop" and "10.11.1　Saving/Displaying Logical Domain Configuration Information."

Use the poweroff command of the XSCF firmware to stop physical partitions individually.
Execute the command with a user account that has the platadm or fieldeng privilege. Alternatively, you can also execute it with a user account that has the pparadm or pparmgr privilege for the target physical partition.

```
XSCF> poweroff -p ppar_id
```

To specify a physical partition, specify -p ppar_id. You can specify a numeric value from 0 to 15 for ppar_id, which is the PPAR-ID of the physical partition to be powered off. The value depends on the system configuration.
Execution of the command outputs a confirmation message. Enter "y".

After the command is executed, the logical domains in each physical partition are shut down in accordance with the ordered shutdown rules. Then, the physical partition is powered off.

Operation Procedure

1. **Execute the poweroff command to power off the specified physical partition.**
   The following example powers off PPAR-ID 00.

```
XSCF> poweroff -p 0
PPAR-IDs to power off:00
Continue? [y|n] :y
00 : Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

All the logical domains in the physical partition with PPAR-ID 00 are shut down, and then the physical partition is powered off.

2. **Execute the showpparprogresss command, and confirm the power on/off status of the specified physical partition.**

```
XSCF> showpparprogress -p 0
PPAR Power Off          PPAR#0 [ 1/ 3]
CPU Stop                PPAR#0 [ 2/ 3]
PSU Off                 PPAR#0 [ 3/ 3]
The sequence of power control is completed.
XSCF>
```

7.5 Changing the Configuration of a Physical Partition

This section provides an overview of changing the configuration of a physical partition.

After configuring a physical partition in the SPARC M12/M10 system, you can change the configuration of the physical partition by adding or removing a physical system board (PSB).
Use the addboard or deleteboard command of the XSCF firmware to change the configuration of a physical partition. For details, see "Chapter 3   Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Chapter 8

Controlling Logical Domains

This chapter describes logical domain control and how to control logical domains.

- Configuring a Logical Domain
- Configuring the Oracle Solaris Kernel Zone
- Switching to the Control Domain Console From the XSCF Shell
- Returning to the XSCF Shell From the Control Domain Console
- Starting a Logical Domain
- Shutting Down a Logical Domain
- Ordered Shutdown of Logical Domains
- Checking CPU Activation Information
- Setting the OpenBoot PROM Environment Variables of the Control Domain
- Domain Console Logging Function
- Changing the Configuration of a Logical Domain
- Setting the Logical Domain Time
- Collecting a Hypervisor Dump File
- Managing Logical Domain Resources Associated with CPU Sockets
- Setting the Physical Partition Dynamic Reconfiguration Policy
- Setting the Maximum Page Size of a Logical Domain

8.1 Configuring a Logical Domain

A logical domain is a virtual hardware environment provided by Oracle VM Server for SPARC. You can divide one platform into multiple virtual hardware environments (logical domains), and Oracle Solaris on each logical domain can run independently. One SPARC M12/M10 can have a configuration of multiple logical domains, which thus integrates multiple servers and increases system availability. Furthermore, the CPUs, memory, I/O devices, and other mounted hardware resources on the platform can be flexibly distributed to the logical domains, which can thereby increase

resource utilization.

In the SPARC M12/M10 systems, after a physical partition is configured, logical domains are configured as independent system environments (virtual platforms) in the physical partitioning (PPAR).

For details on how to configure logical domains, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

8.2 Configuring the Oracle Solaris Kernel Zone

Oracle Solaris kernel zone is a function provided with Oracle Solaris 11.2 and later. A zone can run as an operating system (OS) independent from a global zone. Oracle Solaris kernel zone is different from a non-global zone and operates by individual kernels that do not rely on a global zone. This enhances the independence of the operating system and applications, and enhances security.
For details of the procedure for configuring Oracle Solaris kernel zone, see *Creating and Using Oracle Solaris Kernel Zones* of the version used. In addition, for known problems on kernel zones, see "Kernel Zone Issues" in *Oracle Solaris Release Notes* of the version used.

8.2.1 Hardware and Software Requirements of Oracle Solaris Kernel Zones

The following shows the XCP and Oracle Solaris versions and the SRU essential for executing Oracle Solaris kernel zones.
- SPARC M12 XCP 3021 or later, Oracle Solaris 11.2 SRU11.2.4.6.0 or later
- SPARC M10 XCP 2230 or later, Oracle Solaris 11.2 SRU11.2.4.6.0 or later

The following shows the XCP and Oracle Solaris versions and the SRU essential for performing a warm/live migration of an Oracle Solaris kernel zone.
- SPARC M12 XCP 3021 or later, Oracle Solaris 11.3 or later
- SPARC M10 XCP 2280 or later, Oracle Solaris 11.3 or later

Oracle Solaris kernel zone can run on a logical domain. However, there is a limit for the number of Oracle Solaris kernel zones that can run on one logical domain at the same time. The limit is 512 for SPARC M12 systems and 256 for SPARC M10 systems.

8.2.2 CPU Management on Oracle Solaris Kernel Zones

When Oracle Solaris kernel zones are configured on SPARC M10, we recommend executing the zonecfg command with the dedicated-cpu property to assign a

dedicated CPU to the Oracle Solaris kernel zone in units of core. This can maximize the CPU performance.

For details on the zonecfg command, see the *Oracle Solaris Reference Manuals*.

8.2.3 Notes on Oracle Solaris Kernel Zones

- If Oracle Solaris kernel zones are running on any domains in the physical partition, you cannot execute physical partition dynamic reconfiguration (PPAR DR). In that case, stop all the Oracle Solaris kernel zones, and then execute dynamic reconfiguration of the physical partition. In the case of the PPAR DR operation by the deleteboard command, restart the domains where the Oracle Solaris kernel zones are, before booting the zones.

- If Oracle Solaris kernel zones are running on a guest domain, you cannot perform a live migration of the domain. In that case, stop all the Oracle Solaris kernel zones on the domain, and then perform a live migration of the domain. After the live migration, restart the guest domain where the Oracle Solaris kernel zones are, before booting the zones.

- Before performing a warm/live migration of an Oracle Solaris kernel zone on which cpu-arch=sparc64-class1 is set between SPARC M12 and SPARC M10 systems, perform the following actions.

Note - If Oracle Solaris 11.4 or later has been installed in the Oracle Solaris kernel zone, you do not need to perform the procedure.

---

1. Add the following lines to /etc/system on the migration target kernel zone on which Oracle Solaris 11.3 is installed.

```
set enable_1ghz_stick = 1
set uhrt_enable=0x0
```

2. Restart the kernel zone to which the above lines were added.

- Before performing a warm/live migration of an Oracle Solaris kernel zone between a SPARC M10 system and a system other than the SPARC M10 or between SPARC M10 systems, perform the following actions.

    Logical domains/Oracle Solaris kernel zones requiring the actions are as follows.

    - All logical domains and Oracle Solaris kernel zones with Oracle Solaris 11.3 or later installed which are running on the SPARC M10 of the migration destination/source

    - Oracle Solaris kernel zones with Oracle Solaris 11.3 or later installed which are migrated from a system other than the SPARC M10

    1. Add the following line to the /etc/system file of logical domains/kernel zones that meet the above condition.

```
set uhrt_enable = 0x0
```

2. Restart the logical domains/kernel zones to which the above lines were added.

8.3 Switching to the Control Domain Console From the XSCF Shell

After logging in to the XSCF shell from the XSCF shell terminal and then executing the console command, you can use the control domain console.
A function called the XSCF console redirection function uses a command to switch from the XSCF shell to the control domain console. In the SPARC M12/M10 systems, the XSCF has a direct serial connection with the SPARC M12/M10 chassis. When the user executes the console command, the XSCF automatically selects the path to the valid control domain and switches to the control domain console.

8.3.1 How to Switch From the XSCF Shell to the Control Domain Console

On a PC with an XSCF-LAN or serial connection, you can operate the XSCF shell and control domain console exclusively in a single window. This section describes the switching procedure.

1. **Execute the console command on the XSCF shell terminal to switch to the control domain console.**
   The following example specifies physical partition 0.

```
XSCF> console -p 0
```

2. **Confirm that the window switches to the control domain console.**

```
#
```

Only one RW console can be connected per physical partition. If another RW console is forcibly connected by a user with either the platadm or pparadm user privilege for the physical partition, the currently connected RW console is disconnected.

8.3.2 Connecting to the Control Domain Console Under Appropriate Circumstances

Switching to the control domain console is not possible while the power of the target physical partition is off.
This section describes how to power on the physical partition and connect to the control domain console.

1. **On the XSCF shell terminal, specify a physical partition and execute the poweron command to power on the physical partition.**

2. **Referring to "2.2   Logging In to the XSCF Shell," set up and log in to another XSCF shell terminal to display the control domain console in another window.**

3. **Execute the console command.**

4. **Confirm the switch to the specified control domain console.**

8.4 Returning to the XSCF Shell From the Control Domain Console

After you finish using the control domain console, you can return to the XSCF shell by pressing the relevant keys.

8.4.1 How to Switch From the Control Domain Console to the XSCF Shell

This section describes how to switch from the control domain console back to the XSCF shell.

1. **To transition from the control domain console to the XSCF shell, press the [Enter] key, [#] key (default value for the escape character), and [.] (period) key in this order.**

   To set an escape character that is different from the default, specify the relevant option and execute the console command. Escape characters other than the default are valid only for the current session. The following example changes the escape character to [|].

   ```
   XSCF> console -p 0 -s "|"
   Console contents may be logged.
   Connect to DomainID 0?[y|n] :y
   ```

   For the types of escape characters, see the man page of the console(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

2. **Confirm that the XSCF shell prompt (XSCF>) is output to the terminal.**

8.4.2 Logging Out From the Control Domain Console

If you return to the XSCF shell from the domain console without logging out of the domain, you are automatically logged out of the domain. Likewise, if you exit the XSCF shell without logging out of the domain, you are automatically logged out of the domain. At that time, an end signal may be sent to background programs started from the domain console.

For details of the time setting for the session timeout when the domain console is left unused, see the ttymon explanation in the reference manual of Oracle Solaris.

8.5 Starting a Logical Domain

Use the ldm start-domain command of Oracle VM Server for SPARC to start logical domains individually.
Only a root user or a user with the ldomadm role can execute this command.

```
primary# ldm start-domain ldom
```

For ldom, specify the name of the logical domain to be started.
For details of the ldm command, see the *Oracle VM Server for SPARC Reference Manual* of the version used.

Operation Procedure

1. **Switch from the XSCF console to the control domain console to which the target logical domain belongs.**
   For details on how to switch to the control domain console, see "8.3   Switching to the Control Domain Console From the XSCF Shell."

   If you have already switched to the target control domain console, go to the next step.

2. **Execute the ldm list-domain command to check the start status of domains.**
   The following example checks the status of the primary, ldom1, ldom2, and ldom3 logical domains.

```
primary# ldm list-domain
NAME            STATE      FLAGS    CONS    VCPU   MEMORY    UTIL   UPTIME
primary         active     -n-cv-   SP      8      4G        3.1%   1d 36m
ldom1           active     -n----   5001    24     2G        34%    1m
ldom2           bound      ------   5002    16     1G
ldom3           active     -n----   5003    16     4G        17%    17h 48m
```

3. **Execute the ldm start-domain command to start the specified domain.**
The following example starts ldom2.

```
primary# ldm start-domain ldom2
```

4. **Execute the ldm list-domain command to check the start status of domains.**
The following example checks the status of the primary, ldom1, ldom2, and
ldom3 logical domains.

```
primary# ldm list-domain
NAME            STATE      FLAGS    CONS    VCPU   MEMORY    UTIL   UPTIME
primary         active     -n-cv-   SP      8      4G        3.1%   1d 36m
ldom1           active     -n----   5001    24     2G        34%    1m
ldom2           active     -n----   5002    16     1G        34%    17h 48m
ldom3           active     -n----   5003    16     4G        17%    17h 48m
```

You can see that the logical domain ldom2 has been successfully started.

8.6   Shutting Down a Logical Domain

Use the ldm stop-domain command of Oracle VM Server for SPARC to shut down
logical domains individually.
Only a root user or a user with the ldomadm role can execute this command.

```
primary# ldm stop-domain ldom
```

For ldom, specify the name of the logical domain to be shut down.
For details of the ldm command, see the *Oracle VM Server for SPARC Reference Manual*
of the version used.

Operation Procedure

1. **Switch from the XSCF console to the control domain console to which the
physical partition of the target logical domain belongs.**
For details on how to switch to the control domain console, see "8.3   Switching
to the Control Domain Console From the XSCF Shell."

If you have already switched to the target control domain console, go to the next
step.

2. **Execute the ldm list-domain command to check the start status of domains.**
The following example checks the status of the primary, ldom1, ldom2, and
ldom3 logical domains.

```
primary# ldm list-domain
NAME             STATE     FLAGS    CONS    VCPU   MEMORY    UTIL   UPTIME
primary          active    -n-cv-   SP      8      4G        3.1%   1d 36m
ldom1            active    -n----   5001    24     2G        34%    1m
ldom2            active    -n----   5002    16     1G        34%    17h 48m
ldom3            active    -n----   5003    16     4G 1      7%     17h 48m
```

3. **Execute the ldm stop-domain command to shut down the specified domain.**
   The following example shuts down ldom2.

```
primary# ldm stop-domain ldom2
```

4. **Execute the ldm list-domain command to check the start status of domains.**
   The following example checks the status of the primary, ldom1, ldom2, and
   ldom3 logical domains.

```
primary# ldm list-domain
NAME             STATE     FLAGS    CONS    VCPU   MEMORY    UTIL   UPTIME
primary          active    -n-cv-   SP      8      4G        3.1%   1d 36m
ldom1            active    -n----   5001    24     2G        34%    1m
ldom2            bound     ------   5002    16     1G
ldom3            active    -n----   5003    16     4G 1      7%     17h 48m
```

Once the domain is shut down, STATE changes to the resource bound state
(bound).

8.7 Ordered Shutdown of Logical Domains

In the SPARC M12/M10 systems, you can perform an ordered shutdown of all the
logical domains from the XSCF. For details on how to start an ordered shutdown, see
the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.
You can change priorities in the shutdown by setting shutdown group numbers for
the logical domains with the ldm command.
The logical domains are shut down in descending order of shutdown group number.
In other words, the domain with the highest number is shut down first. The domain
with the lowest number is shut down last. If multiple domains share a common
priority, they are shut down at the same time unless there is a master-and-slave
relationship. In that case, the slave domains are shut down before the master domain.

For details on how to set the master and slave, see the *Oracle VM Server for SPARC
Administration Guide*.

The effective values are 1 to 15. The shutdown group number of the control domain
is 0 and cannot be changed. The default value for other domains is 15.

```
# ldm set-domain shutdown-group=8 secondary
```

Suppose that all other guest domains have the default shutdown group number. Then, an ordered shutdown would shut down all these other guest domains first, the secondary domain after that, and the control domain last.

As an example, the set shutdown group number for a domain named "secondary" is not the default value.

Note - You can set the shutdown-group property when a logical domain is in any of the inactive, bound, and active states. Also, when creating a new logical domain, you can set its properties too. However, to enable an updated shutdown priority, the XSCF must recognize the new property values.
To have the XSCF recognize the set property values, set each domain to the bound or active state, and then use the ldm add-spconfig command to save the logical domain configuration information. After that, power on the server again so that the XSCF recognizes the values.

8.7.1 Domain Table (ldomTable)

The ldomShutdownGroup property has been added to ldomTable. ldomTable is used to represent the individual domains of the system, and its information can be obtained from Oracle VM Server for SPARC MIB.

Table 8-1   Domain Table (ldomTable)

Name	Data Type	Access	Description
ldomShutdownGroup	Integer	Read only	Shutdown group number of a guest domain. In the SPARC M12/M10 systems, when the XSCF starts an ordered shutdown, the domains are shut down in descending order of shutdown group number (in the order from 15 to 0). The default value is 15.

8.7.2 Domain Information (ldom_info) Resources

The shutdown-group property has been added to the option properties in the ldom_info resources.

```
<Envelope>
    <References/>
    <Content xsi:type="ovf:VirtualSystem_Type" id="primary">
      <Section xsi:type="ovf:ResourceAllocationSection_type">
        <Item>
          <rasd:OtherResourceType>ldom_info</rasd:OtherResourceType>
                :
                :
```

```
            <gprop:GenericProperty key="shutdown-group">0</gprop:GenericProperty>
                    :
                    :
        </Item>
      </Section>
    </Content>
</Envelope>
```

The <Content> section always contains the ldom_info resources. Use the tag with the following key in the ldom_info resources.
- shutdown-group
  This property indicates the shutdown priority used during an ordered shutdown. Shutdown requests are issued to the domains in descending order from shutdown group 15 to 0. The control domain is always shutdown group 0. The effective values for the shutdown groups of other domains are 1 to 15.

For details on other properties of the ldom_info resources, see the *Oracle VM Server for SPARC Administration Guide* of the version used.

8.8   Checking CPU Activation Information

You can display a list of CPU Activation information by using the ldm command. For details of CPU Activation, see "Chapter 5   CPU Activation."

1. **Execute the following subcommand to display a list of CPU Activation information.**

```
# ldm list-permits
```

The following information is displayed when the ldm list-permits command is executed.

Table 8-2   Content Displayed by the list-permits Command

Item	Description
PERMITS	Displays the number of CPU Activations assigned to the physical partition.
IN USE	Displays the number of CPU Activations used in the logical domains.
REST	Displays the number of CPU Activations not used in the logical domains.

In the following example, the PERMITS column shows that a total of 15 CPU Activations (number of permissions) have been assigned to the physical partition. The IN USE column shows that 14 CPU cores out of all those permitted are currently in use. The REST column shows that one additional CPU core can be used.

```
#ldm list-permits
CPU CORE
PERMITS(PERMANENT)   IN USE      REST
15     (15)          14          1
```

For details about displaying other lists of domain resources, see the *Oracle VM Server for SPARC Administration Guide* of the version used.

8.9 Setting the OpenBoot PROM Environment Variables of the Control Domain

This section describes what can be set with the XSCF firmware from among the OpenBoot PROM environment variables that can be set for the control domain.

For details on the OpenBoot PROM and OpenBoot PROM environment variables, see the eeprom explanation in the reference manual of Oracle Solaris and the *OpenBoot 4.x Command Reference Manual* of Oracle Corporation.
For details on the SPARC M12/M10 system-specific information for OpenBoot PROM commands and OpenBoot PROM environment variables, see "Appendix H OpenBoot PROM Environment Variables and Commands."

8.9.1 OpenBoot PROM Environment Variables That Can be Set With the XSCF Firmware

Of the OpenBoot PROM environment variables available for the control domain, the following environment variables are set with the XSCF firmware.

Table 8-3   OpenBoot PROM Environment Variables of the Control Domain as Set by the XSCF

OpenBoot PROM Environment Variable	Description	Setting Method
auto-boot?	Automatically starts the control domain at the power-on time (default is true). To configure the XSCF firmware to not automatically start the OS (stopping at {0}ok) before starting a physical partition, set this variable.	Boot script

Table 8-3   OpenBoot PROM Environment Variables of the Control Domain as Set by the XSCF *(continued)*

OpenBoot PROM Environment Variable	Description	Setting Method
input-device	Sets the input device of the control domain console (default is virtual-console). If OpenBoot PROM cannot start, set this variable so that the XSCF firmware can update the OpenBoot PROM environment variable and start OpenBoot PROM.	Boot script
output-device	Sets the output device of the control domain console (default is virtual-console). If OpenBoot PROM cannot start, set this variable so that the XSCF firmware can update the OpenBoot PROM environment variable and start OpenBoot PROM.	Boot script
use-nvramrc?	Sets whether to execute the nvramrc contents at control domain startup (default is false). If OpenBoot PROM cannot start, set this variable so that the XSCF firmware can update the OpenBoot PROM environment variable and start OpenBoot PROM.	use-nvramrc operand
security-mode	Sets the security mode of firmware (default is none). If OpenBoot PROM cannot start, set this variable so that the XSCF firmware can update the OpenBoot PROM environment variable and start OpenBoot PROM.	security-mode operand

The following are the setting methods with the setpparparam command for the above OpenBoot PROM environment variables, according to each type.

- Setting environment variables in the boot script
  The auto-boot?, input-device, and output-device OpenBoot PROM environment variables are set by the boot script for the setpparparam command. The boot script is a series of OpenBoot PROM commands executed when OpenBoot PROM starts. It can be set using the setpparparam command with the -s bootscript option specified. The boot script that is set by the setpparparam command is used only at control domain startup. The script contents are cleared after startup. You can write multiple OpenBoot PROM commands of up to 254 characters in the boot script. If the bootscript has been set incorrectly, or you want to delete a bootscript that has been set, specify the -r option along with -s bootscript.

- Setting environment variables as setpparparam command operands
  The OpenBoot PROM environment variables user-nvramrc? and security-mode are set using the operands of the setpparparam command. These environment variables cannot be set in the bootscript.

8.9.2 Setting OpenBoot PROM Environment Variables for the Control Domain

Use the setpparparam command of the XSCF firmware to set the OpenBoot PROM environment variables of the control domain.
Execute the command with a user account that has the platadm or fieldeng privilege. You can also execute it with a user account that has the pparadm privilege for the target physical partition.

Configuring the Boot Script

```
XSCF> setpparparam -p ppar_id -s bootscript value
```

For ppar_id, set the physical partition whose environment variables are to be stored in the boot script. You can specify an integer from 0 to 15, depending on the system configuration.
For value, set the OpenBoot PROM command to be stored in the boot script to change the OpenBoot PROM environment variables. Specify a value by enclosing it in double quotation marks ("").

Setting use-nvramrc? to false

```
XSCF> setpparparam -p ppar_id use-nvramrc
```

For ppar_id, set the physical partition whose environment variables are to be stored. You can specify an integer from 0 to 15, depending on the system configuration.

Setting security-mode to none

```
XSCF> setpparparam -p ppar_id security-mode
```

For ppar_id, set the physical partition whose environment variables are to be stored. You can specify an integer from 0 to 15, depending on the system configuration.

Operation Procedure

1. **Set OpenBoot PROM environment variables for the control domain.**
   The following example enables auto boot for the control domain of PPAR-ID 0.

```
XSCF> setpparparam -p 0 -s bootscript "setenv auto-boot? true"
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable bootscript will be changed.
Continue? [y|n]: y
```

The following example sets use-nvramrc?, an OpenBoot PROM environment

variable, for PPAR-ID 0 to false.

```
XSCF> setpparparam -p 0 use-nvramrc
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable use-nvramrc will be set to false.
Continue? [y|n]: y
```

The following example sets security-mode, an OpenBoot PROM environment variable, for PPAR-ID 0 to none.

```
XSCF> setpparparam -p 0 security-mode
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable security-mode will be set to none.
Continue? [y|n]: y
```

8.9.3 Displaying the Set OpenBoot PROM Environment Variables of the Control Domain

Use the showpparparam command of the XSCF firmware to display the OpenBoot PROM environment variables set for the control domain by the setpparparam command.
Execute the command with a user account that has the useradm, platadm, platop, or fieldeng privilege. You can also execute it with a user account that has the pparadm, pparmgr, or pparop privilege for the target physical partition.

```
XSCF> showpparparam -p ppar_id
```

For -ppar_id, set the physical partition whose environment variables are to be displayed. You can specify an integer from 0 to 15, depending on the system configuration.

Operation Procedure

1. **Display the set OpenBoot PROM environment variables and boot script of the control domain.**
   The following example displays the environment variables of the control domain of PPAR-ID 0.

```
XSCF> showpparparam -p 0
use-nvramrc        :false
security-mode      :none
bootscript         :
setenv auto-boot? true
```

The following example displays the current setting of auto-boot?, an OpenBoot PROM environment variable, for the control domain of PPAR-ID 0.

```
XSCF> showppparparam -p 0 -c auto-boot
auto-boot?          :true
```

8.9.4 Initializing the Set OpenBoot PROM Environment Variables of the Control Domain

Use the setppparam command of the XSCF firmware to clear the set OpenBoot PROM environment variables of the control domain and return them to their state at factory shipment.
Execute the command with a user account that has the platadm or fieldeng privilege. You can also execute it with a user account that has the pparadm privilege for the target physical partition.

```
XSCF> setppparam -p ppar_id set-defaults
```

For ppar_id, set the physical partition whose environment variables are to be initialized. You can specify an integer from 0 to 15, depending on the system configuration.

Operation Procedure

1. **Clear the set OpenBoot PROM environment variables of the control domain.**
   In the following example, the OpenBoot PROM environment variables set for the PPAR-ID 0 control domain are cleared, and the state at factory shipment is restored.

```
XSCF> setppparam -p 0 set-defaults
PPAR-ID of PPARs that will be affected:0
All OpenBoot PROM variables will be reset to original default
values.
Continue? [y|n]: y
```

8.10 Domain Console Logging Function

In a logical domain environment, the console output destination of the control domain is the XSCF. The console output destination of all the other logical domains is the service domain that started the virtual console terminal collection and distribution unit (vcc).
In Oracle Solaris 11.1 and later, service domains support the console logging function of logical domains other than control domains.
Log data is saved to a file named /var/log/vntsd/domain-name/console-log placed in the service domain that provides the virtual console terminal collection and

distribution unit. The console log file is rotated when the logadm command is executed. For details, see the man pages of the logadm command and logadm.conf file.

The Oracle VM Server for SPARC software allows you to enable and disable the console logging function for every logical domain except control domains. The console logging function is enabled by default.

8.10.1 Method of Disabling the Console Logging Function

1. **Display the current console settings of a domain.**

```
# ldm list -o console domain
```

2. **Disable the console logging function.**

```
# ldm set-vcons log=off domain
```

Note - To change the settings of the console logging function with the ldm set-vcons command, you need to set the guest domain to the unbind state, that is, the inactive state.

Note - You need to enable (on) or disable (off) the console logging function for each guest domain.

8.10.2 Method of Enabling the Console Logging Function

1. **Display the current console settings of a domain.**

```
# ldm list -o console domain
```

2. **Enable the console logging function.**

```
# ldm set-vcons log=on domain
```

8.10.3 Service Domain Requirement

To use the console logging function, the service domain must be started in Oracle Solaris 11.1 or later.

Note - You need to enable (on) or disable (off) the console logging function for each guest domain.

8.10.4 Virtual Console Group Table (ldomVconsTable)

The ldomVconsLog property has been added to ldomVconsTable as Oracle VM Server for SPARC MIB information. ldomVconsTable shows all the virtual console groups of virtual console services.

Table 8-4   Virtual Console Group Table (ldomVconsTable)

Name	Data Type	Access	Description
ldomVconsLog	Displayed character string	Read only	Console logging status. The property value is the character string of "on" or "off" specified by the ldm set-vcons command.

Note - If a group includes multiple domains, the ldomVconsLog property shows the console logging status changed by the last executed ldm set-vcons command.

8.10.5 Console Resources

The enable-log property has been added to the console resources as an XML interface.

```
<Envelope>
    <References/>
    <Content xsi:type="ovf:VirtualSystem_Type" id="ldg1">
      <Section xsi:type="ovf:VirtualHardwareSection_Type">
        <Item>
          <rasd:OtherResourceType>console</rasd:OtherResourceType>
                    :
                    :
          <gprop:GenericProperty key="enable-log">on</gprop:GenericProperty>
        </Item>
      </Section>
    </Content>
  </Envelope>
```

The <Content> section always contains the console resources. The tags with the following key can be used.

- enable-log
  This key enables or disables the virtual console logging of a target console.

For details on other properties of the console resources, see the *Oracle VM Server for SPARC Administration Guide* or the *Oracle VM Server for SPARC Management*

Information Base User Guide of the version used.

8.11 Changing the Configuration of a Logical Domain

For a logical domain, you can flexibly assign the mounted CPUs, memory, I/O devices, and other hardware resources in the physical partition. Moreover, the system can dynamically reconfigure CPUs and memory for the logical domain while it is running, so it can handle temporary load increases without stopping business. Since resources can be added and removed according to the domain operation status, the hardware resources in a single server can be utilized efficiently and have higher utilization.

Also, CPU core resources can be dynamically added to a logical domain through a combination of logical domain configuration changes and CPU Activations. Expansion of resources without removing resources from other domains to cope with demand is possible through the assignment of unused CPU core resources.

Oracle VM Server for SPARC is used for dynamic reconfiguration of CPUs and memory.

For the method of changing the configuration of logical domains, see "Chapter 3 Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

8.12 Setting the Logical Domain Time

This section describes the necessary knowledge and setting guidelines for setting the logical domain time.

The SPARC M12/M10 systems manage the following times.

- Time kept on the XSCF
  The XSCF manages the standard system time. Managed by the master XSCF, the same time is set on all the XSCFs. They keep the time even when the input power is off.

- Time kept on a physical partition
  Hypervisor manages the time for each physical partition.

- Time kept on a logical domain
  The time is managed for each logical domain. A different time can be kept for each logical domain.

For details on the relationship between the XSCF and logical domain time, see "3.6 Setting the XSCF Time/Date."

8.13 Collecting a Hypervisor Dump File

This section describes how to make settings for collecting a Hypervisor dump file.

8.13.1 Basics of Hypervisor Dump

Hypervisor may abort because of a hardware failure or software error. When Hypervisor aborts, after all the logical domains are reset, only the control domain starts in a special factory-default configuration to collect a Hypervisor dump, and Hypervisor information is saved as a dump file. This is called the Hypervisor dump function.
The collected dump file can be valuable information for diagnosing a problem that has occurred.

Note - If Hypervisor dump is enabled, a Hypervisor dump is also collected when the reset command of the XSCF firmware with xir specified is executed to reset a physical partition. For details on the physical partition reset, see "10.17   Resetting a Physical Partition."

Note - To return to the original configuration from the special factory-default configuration to collect a Hypervisor dump, you need to restart the physical partition.

A dump file with the following file name is collected in the control domain. Up to eight files can be collected.

- Storage directory:
  /var/opt/SUNWldm

- File name:
  hvdump.x.gz

  x: An integer from 0 to 7 is automatically assigned.

The next section describes the commands used with the Hypervisor dump function.

8.13.2 Commands Used With the Hypervisor Dump Function

Enabling/Disabling Hypervisor Dump

Use the ldm set-hvdump command of Oracle VM Server for SPARC to configure Hypervisor dump.

```
primary# ldm set-hvdump [hvdump=on|off] [hvdump-reboot=on|off]
```

For hvdump, specify whether to enable the Hypervisor dump function. To enable it,

specify on. To disable it, specify off. The default is enabled (on).

For hvdump-reboot, specify whether to automatically restart the physical partition after dump file collection. To restart the physical partition, specify on. To not restart it, specify off. The default value is off. If the value is set to off, even after a dump file is collected, the control domain remains in the special factory-default configuration to collect a Hypervisor dump.

If you change the hvdump and hvdump-reboot settings by the ldm set-hvdump command, use the ldm add-spconfig command to save the configuration information.

```
primary# ldm add-spconfig file
```

Note - Even if you restart the control domain started in a special factory-default configuration to collect a Hypervisor dump, the system does not return to the original configuration. To start the system in the original configuration, you need to restart the physical partition. After executing the poweroff command of the XSCF or the shutdown -i5 command of Oracle Solaris, execute the poweron command of the XSCF to restart the system.

Note - Even when the hvdump-reboot setting is on, if a dump file is not collected because eight dump files are already collected or the disk is running out of space, the physical partition cannot be restarted. In such cases, move or delete a collected dump file first. Then, use the ldm start-hvdump command to collect a dump file. After the dump file collection completed, restart the physical partition.

Displaying the Contents of the Hypervisor Dump Settings

Use the ldm list-hvdump command to display the contents of the Hypervisor dump settings.

```
primary# ldm list-hvdump
```

The following information is displayed when the ldm list-hvdump command is executed.

Table 8-5   Content Displayed by the ldm list-hvdump Command

Item	Description
hvdump	Whether the Hypervisor dump function is enabled. If enabled, on is displayed. If disabled, off is displayed.
hvdump-reboot	Whether to restart the system after dump file creation. If it will be restarted, on is displayed. If it will not be restarted, off is displayed.

Note - If dump file collection did not end normally, "Pending hvdump exists" message is displayed.

Operation Procedure

1. **Switch from the XSCF console to the target control domain console.**
   For details on how to switch to the control domain console, see "8.3   Switching to the Control Domain Console From the XSCF Shell."

   If you have already switched to the control domain console or to the XSCF, go to the next step.

2. **Configure the Hypervisor dump function.**
   The following example enables the Hypervisor dump function and sets the control domain to restart after dump file collection.

```
primary# ldm set-hvdump hvdump=on hvdump-reboot=on
```

3. **Display the settings made for the Hypervisor dump function.**
   The following example shows that the Hypervisor dump function is enabled and that restart after dump file collection is enabled.

```
primary# ldm list-hvdump
hvdump=on
hvdump-reboot=on
```

4. **Save the settings made for the Hypervisor dump function.**
   Designate and save a file name in *config_name* in the following example.

```
primary# ldm add-spconfig config_name
```

8.13.3   Points to Note on Using Hypervisor Dump

Note the following points on using the Hypervisor dump function.

- Even if an error occurs in Hypervisor, no dump file can be collected when the directory for saving dump files has:
  - Eight existing dump files, or
  - Insufficient disk space for the /var/opt/SUNWldm directory

  Routinely check the number of dump files and disk capacity of the directory for saving dump files to confirm that the requirements for dump file collection are met.

- If a dump file cannot be collected for a reason such as the above, processing stops. After solving the problem, execute the ldm start-hvdump command to collect a dump file. If you restart the control domain without executing the ldm start-hvdump command, no dump file is collected, and the logged Hypervisor information is lost. Even when the hvdump-reboot setting is on, if a dump file is not collected, the physical partition cannot be restarted. In such cases, move or delete a collected dump file first. Then, use the ldm start-hvdump command to

collect a dump file. After the dump file collection completed, restart the physical partition.

- Even when the hvdump-reboot setting is on, if the OpenBoot PROM environment variable auto-boot? is false, processing stops at the ok prompt without restarting Oracle Solaris.

- If the control domain is unintentionally started in the factory-default configuration, Hypervisor dump processing may not complete. This may be because the control domain is started in a special factory-default configuration to collect a Hypervisor dump. Execute the ldm list-hvdump command to check whether a dump file has been collected.
The following example shows that a dump file could not be collected.

```
primary# ldm list-hvdump
hvdump=on
hvdump-reboot=on
Pending hvdump exists
```

8.14 Managing Logical Domain Resources Associated with CPU Sockets

8.14.1 Overview of CPU Socket Constraints

CPU socket constraints enable you to create and configure a logical domain, which owns limited virtual CPUs, cores, or memory, with the specified CPU socket ID. Since the CPU socket ID is associated with the LSB number and CPU location number, you can fully control the hardware resources manually without using physical bindings, such as CID and PA.

The CPU socket ID is determined by the LSB number and CPU location number as follows.

```
CPU socket ID = LSB number x 4 + CPU location number
```

Figure 8-1 shows the physical resources in the physical partition configured with two SPARC M10-4S units (BB#0 and BB#1).

Figure 8-1　　Resources in a Physical Partition
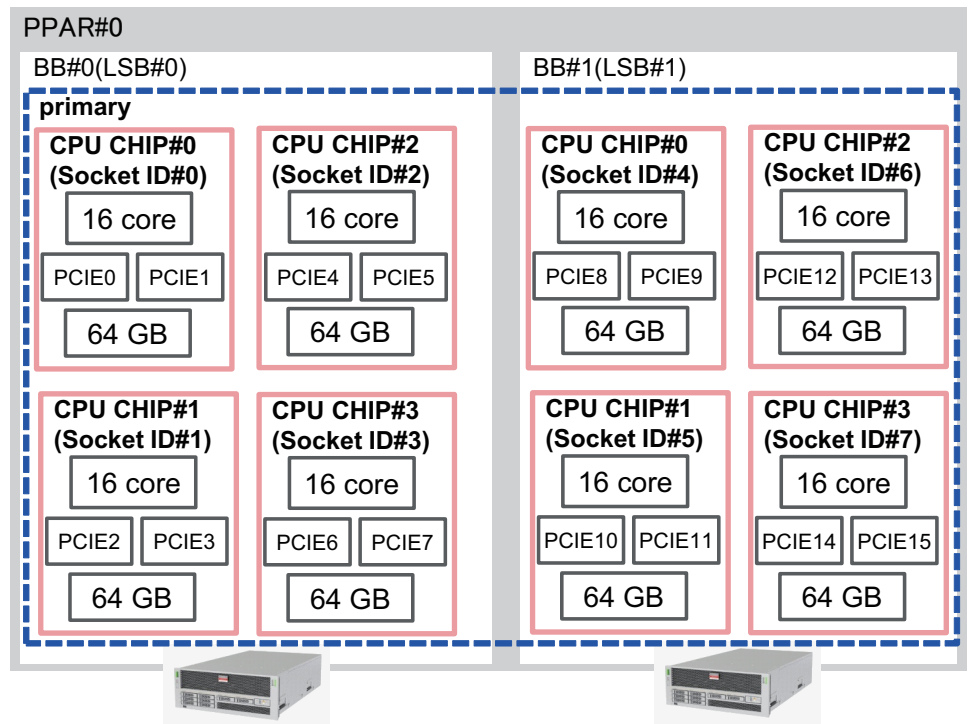
For details on the LSB number and CPU location number, see "2.4.1　Consideration of Logical Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

You can use the CPU socket constraints to perform tasks like the following.

- Create a highly reliable domain by using memory mirroring enabled on the specified CPU chip
- Before executing the dynamic reconfiguration (PPAR DR) of a physical partition, separate the SPARC M12-2S and SPARC M10-4S resources to be deleted in advance to minimize the time that a guest domain, on which PPAR DR is being executed, is stopped.
- Tune the performance by spreading the virtual CPUs to each CPU chip or by consolidating the virtual CPUs in one CPU chip.
- Configure a logical domain using only the SPARC64 X+ processor in a physical partition that also has the SPARC M10-4S with the SPARC64 X/SPARC64 X+ processor.

The following commands are provided as CPU socket constraint-related commands. For details on each command, see the *Oracle VM Server for SPARC Reference Manual* of the version used.

- ldm list-socket
- ldm set-socket
- ldm grow-socket
- ldm shrink-socket

8.14.2 CPU Socket Constraint Hardware and Software Requirements

This feature is supported on the SPARC M12/M10 platforms. However, since SPARC M12-1/M10-1 has a one-CPU configuration, it has no meaning in this feature.
To use the CPU socket constraints on the SPARC M12/M10, the system must meet the following requirements.

- Runs Oracle VM Server for SPARC 3.3 or later
- Runs XCP 2210 or later of the XCP firmware for SPARC M10
  To enable the --remap option of the CPU socket constraints, XCP 2260 or later of the XCP firmware is required.

  For SPARC M12, there are no XCP firmware requirements.

- Uses M12-2/M12-2S/M10-4/M10-4S(s)

8.14.3 CPU Socket Constraint Restrictions

CPU socket constraints have the following restrictions.

- If a domain is migrated, CPU socket constraints are also cleared in the same way as physically assigning a specified CID or PA.
- Execute the ldm set-socket command with the --restore-degraded option to restore the CPU socket constrains.
- Recovery mode ignores the CPU socket constraints of failed CPU chips.
- The ldm init-system -f command ignores the CPU socket constraints of the control domain.
- Automatic replacement of failed CPUs can only work in the specified socket resources. If there is no free CPU in the specified sockets, the failed CPUs are isolated but not replaced.

8.14.4 Creating a Highly Reliable Logical Domain by Using the CPU Socket Constraints

For a better understanding of the CPU socket constraints, this section describes how to create a highly reliable logical domain by using CPU socket constraints.

Figure 8-2 shows the flow of creating a highly reliable logical domain.

Figure 8-2   Flow of Creating a Highly Reliable Logical Domain

1. Configuring memory mirroring to the CPU chip
Use the setupfru command of the XSCF firmware to configure memory mirroring.
("8.14.5 Configuring memory mirroring to the CPU chip")

2. Removing the resources associated with the CPU socket from the control domain
Use the ldm shrink-socket command to remove resources from the control domain.
("8.14.6 Removing the resources associated with the CPU socket from the control domain")

3. Configuring the CPU socket constraints to the logical domain configuration
Use the ldm set-socket command to configure CPU socket constraints to logical domains.
("8.14.7 Configuring the CPU socket constraints to the logical domain configuration")

The subsequent sections 8.14.5 to 8.14.7 describe the procedure providing an example of creating logical domain ldom1 by assigning the resources of CPU chip #0 in BB#1 to a physical partition configured with two SPARC M10-4S units (BB#0 and BB#1).

8.14.5   Configuring Memory Mirroring to the CPU Chip

Use the setupfru command of the XSCF firmware to configure memory mirroring. For details on how to set memory mirror mode, see "14.1   Configuring Memory Mirroring." For details of the setupfru command, see the man page of the setupfru(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Use the ldm list-socket command to show the list of the resources of each CPU socket.
The following example shows that the size of the memory associated with CPU socket #4 decreases by half because memory mirror mode was set to CPU chip #0 in BB#1.

```
# ldm list-socket
CONSTRAINTS

SOCKET
    TENANT     VCPUS CORES SOCKET_ID    GROUP
    primary    32    16    0            /BB0
    primary    32    16    1            /BB0
    primary    32    16    2            /BB0
    primary    32    16    3            /BB0
    primary    32    16    4            /BB1
    primary    32    16    5            /BB1
    primary    32    16    6            /BB1
    primary    32    16    7            /BB1

MEMORY
```

```
     PA                  SIZE        SOCKET_ID       BOUND
     0x700000000000      64G         7               primary
     0x720000000000      64G         6               primary
     0x740000000000      64G         5               primary
     0x760050000000      31488M      4               primary
     0x780000000000      64G         3               primary
     0x7a0000000000      64G         2               primary
     0x7c0000000000      64G         1               primary
     0x7e0080000000      62G         0               primary

IO
     NAME        TYPE    BUS         SOCKET_ID       BOUND
     PCIE0       BUS     PCIE0       0               primary
     PCIE1       BUS     PCIE1       0               primary
     PCIE2       BUS     PCIE2       1               primary
     PCIE3       BUS     PCIE3       1               primary
     PCIE4       BUS     PCIE4       2               primary
     PCIE5       BUS     PCIE5       2               primary
     PCIE6       BUS     PCIE6       3               primary
     PCIE7       BUS     PCIE7       3               primary
     PCIE8       BUS     PCIE8       4               primary
     PCIE9       BUS     PCIE9       4               primary
     PCIE10      BUS     PCIE10      5               primary
     PCIE11      BUS     PCIE11      5               primary
     PCIE12      BUS     PCIE12      6               primary
     PCIE13      BUS     PCIE13      6               primary
     PCIE14      BUS     PCIE14      7               primary
     PCIE15      BUS     PCIE15      7               primary
```

Figure 8-3 shows a control domain in the physical partition that owns all the resources in the physical partition configured with two SPARC M10-4S units (BB#0 and BB#1).

Figure 8-3   CPU Cores and Memory in the Physical Partition
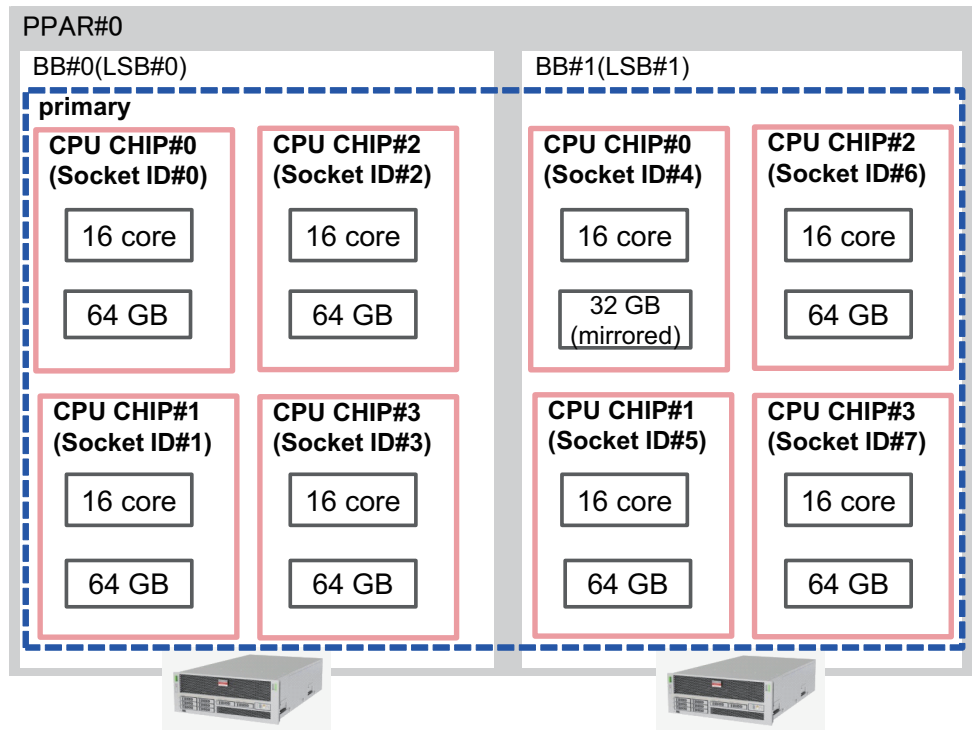
8.14.6   Removing the Resources Associated With the CPU Socket From the Control Domain

Use the ldm shrink-socket command to remove the resources in CPU socket #4 from a control domain.
The following example shows the removal of virtual CPUs and memory in CPU socket #4 from the control domain.

```
# ldm shrink-socket cores=16 socket_id=4 primary
# ldm shrink-socket memory=31488M socket_id=4 primary
```

Note - The ldm shrink-socket command may fail to remove the target resource if the resource is busy. If so, stop the logical domain, and retry the ldm shrink-socket command. If the domain is the control domain, use delayed reconfiguration and try again.

Use the ldm list-socket command to list the resources of each CPU socket. You can confirm that the memory in CPU socket#4 has been removed from the control domain.

```
# ldm list-socket
CONSTRAINTS

SOCKET
    TENANT      VCPUS CORES SOCKET_ID    GROUP
    primary     32    16    0            /BB0
    primary     32    16    1            /BB0
    primary     32    16    2            /BB0
    primary     32    16    3            /BB0
    primary     32    16    5            /BB1
    primary     32    16    6            /BB1
    primary     32    16    7            /BB1

    FREE        VCPUS CORES SOCKET_ID    GROUP
                32    16    4            /BB1

MEMORY
    PA                  SIZE        SOCKET_ID    BOUND
    0x700000000000      64G         7            primary
    0x720000000000      64G         6            primary
    0x740000000000      64G         5            primary
    0x760050000000      31488M      4
    0x780000000000      64G         3            primary
    0x7a0000000000      64G         2            primary
    0x7c0000000000      64G         1            primary
    0x7e0080000000      62G         0            primary
--- Omitted ---
```

Figure 8-4 shows the physical partition configuration after the ldm shrink-socket command is executed in the physical partition configured with two SPARC M10-4S units (BB#0 and BB#1).

Figure 8-4   Resources After Execution of the ldm shrink-socket Command
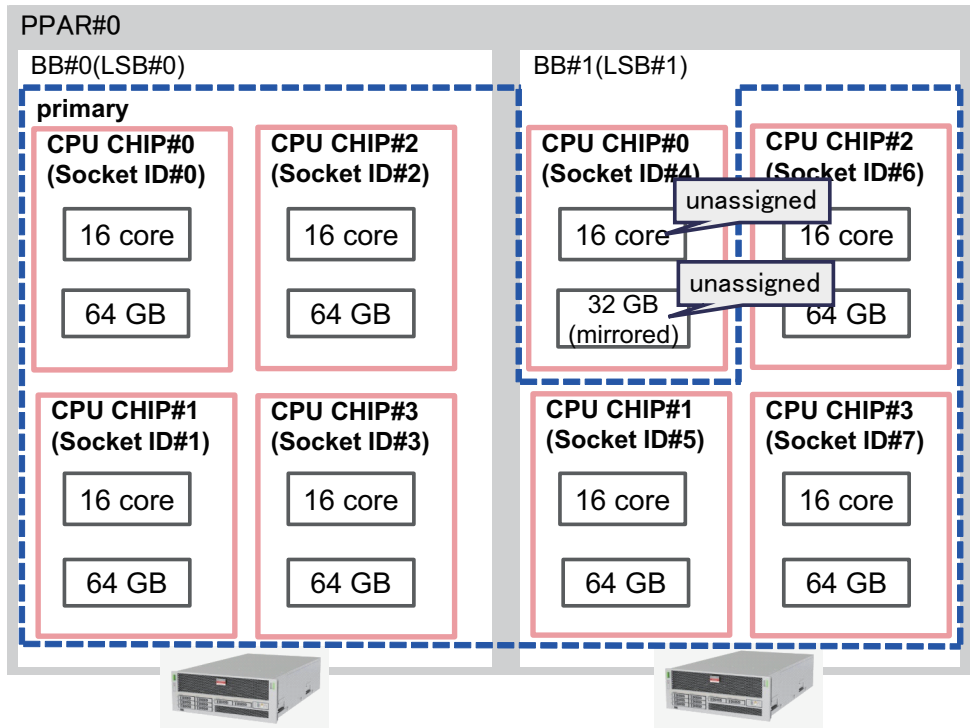
8.14.7   Configuring the CPU Socket Constraints to the Logical Domain Configuration

The following example describes how to create the logical domain ldom1 which owns 16 GB mirrored memory and 8 CPU cores that are associated with CPU socket #4.

Use the ldm add-domain command to create the logical domain ldom1.

```
primary# ldm add-domain ldom1
```

Use the ldm set-socket command to constrain ldom1 to use the resources that are associated with CPU socket#4.

```
primary# ldm set-socket socket_id=4 ldom1
```

Allocate 8 CPU cores and 16-GB memory to ldom1.

```
primary# ldm set-core 8 ldom1
primary# ldm set-memory 16G ldom1
```

Bind the resources to ldom1 and start ldom1.

```
primary# ldm bind-domain ldom1
primary# ldm start-domain ldom1
```

Note - To bind and start the logical domain, you should prepare a virtual console concentrator, a virtual network switch, and a virtual disk service. For details on each item, see the *Oracle VM Server for SPARC Administration Guide* of the version used.

Use the ldm list-socket command to show the list of the resources of each CPU socket.
You can confirm only the resources that are associated with CPU socket #4 are assigned to ldom1.

```
# ldm list-socket ldom1
CONSTRAINTS
    DOMAIN             SOCKET_ID     STATE
    ldom1              4             active

SOCKET
    TENANT             VCPUS CORES SOCKET_ID     GROUP
    ldom1              16    8     4             /BB1

MEMORY
    PA                 SIZE          SOCKET_ID   BOUND
    0x760050000000     16G           4           ldom1

IO
```

Figure 8-5 shows the physical partition configuration after the ldm set-socket command is executed in the physical partition configured with two SPARC M10-4S units (BB#0 and BB#1).

Figure 8-5   Resources After the Execution of the ldm set-socket Command
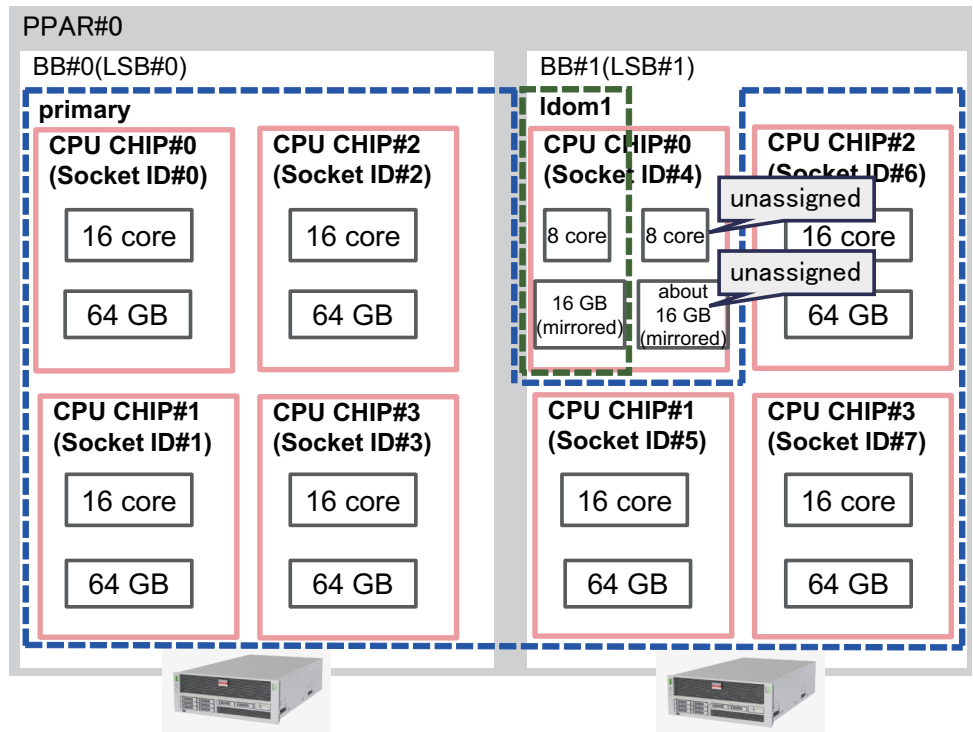
8.15   Setting the Physical Partition Dynamic Reconfiguration Policy

This section describes how to set the dynamic reconfiguration policy of a physical partition.

8.15.1   Physical Partition Dynamic Reconfiguration Policy

The physical partition dynamic reconfiguration (PPAR DR) policy function is supported for Oracle VM Server for SPARC 3.4 or later. With the PPAR DR policy, you can change the resource reduction policy that Oracle VM Server for SPARC uses when the PPAR DR operation is executed by the deleteboard command.
The resource reduction policy is set to the ldmd/fj_ppar_dr_policy property of the ldmd service. The resource reduction policy that can be set up is "auto," "ratio," or "targeted."
For details on each resource reduction policy, see "8.15.2   Details on Resource Reduction Policies."

8.15.2 Details on Resource Reduction Policies

This section describes the details on each resource reduction policy.

fj_ppar_dr_policy = auto
This PPAR DR policy setting is one for automatically using the latest policy. When "auto" is set for the system with Oracle VM Server for SPARC 3.4, the system operates in the same way as when "ratio" is set. The "auto" setting is the default policy.

fj_ppar_dr_policy = ratio
This policy is functional on systems with Oracle VM Server for SPARC 3.4 or later, when all the logical domains in the physical partition are running Oracle Solaris 11.3 or later, and when XCP 2271 or later has been applied to the system. Otherwise, the system operates in the same way as when "targeted" is set.
Suppose you set the resource reduction policy to "ratio" and perform the deleteboard operation when the free resources on the remaining building blocks are not sufficient to move resources from the building block (system board) to be deleted, and resources are reduced by the automatic release of resources from all the existing domains.
In this situation, resources are automatically freed according to the proportion of resources assigned to the existing domains. Because resources are busy or due to other reasons, exact proportional reduction does not always work. The proportional reduction is on a best effort basis.
This policy also supports a memory block splitting feature which automatically divides a large memory block into smaller memory blocks. Memory block splitting eliminates the requirement to have sufficient free contiguous memory regions on the destination building block for each relocated memory block from the building block being removed with PPAR DR. The deleteboard operation splits up memory blocks in the domain to fit into available free regions on the remaining building blocks.
If unable to secure enough free resources from the move-destination building block because resources are in use or for other reasons, the deleteboard command fails with an error message displayed. In this case, identify the cause of the error from the error message output by the deleteboard command and the Oracle Solaris message, and take appropriate action. For details on error messages output by the deleteboard command, see "C.1.2　deleteboard" in the *Fujitsu SPARC M12 and Fujitsu M10/ SPARC M10 Domain Configuration Guide*. That being said, you may need to power off or restart the physical partition, depending on the details of the error that occurred.

The concept of memory deletion when "ratio" is set is described in Figure 8-6.

Figure 8-6   Concept of Memory Deletion (When Using fj_ppar_dr_policy = ratio)

Delete BB#1 by PPAR DR.

BB#0
primary 64G
guest1 64G

BB#1
guest2 64G
free 64G

1. The memory of each domain is deleted proportionally.

BB#0
primary 42.5GB
free 21.5GB
guest1 42.5GB
free 21.5GB

BB#1
guest2 43GB
free 21GB
free 64GB

2. The memory of guest2 is devided to be reallocated to the free blocks of BB#0.

BB#0
primary 42.5GB
guest2 21.5GB
guest1 42.5GB
guest2 21.5GB

BB#1
guest2 43GB
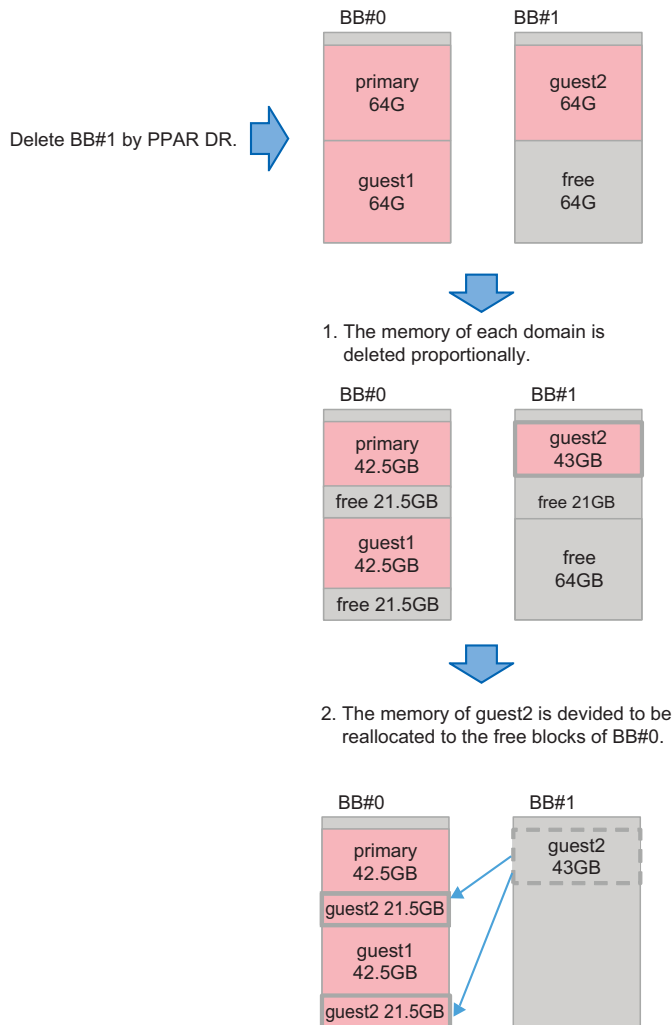
fj_ppar_dr_policy = targeted

"Targeted" policy will be used for all versions earlier than Oracle VM Server for SPARC 3.4. If free resources are not available with this policy, resources are released from each logical domain that has the CPU/memory on the building block to be deleted first.

If free resources are not sufficient even after this deletion operation, resources are released from each logical domain that has the CPU/memory on a remaining building block. The order of logical domains from which resources are released is determined by "failure-policy." This order in this policy is the default logical domain (no specification), logical domain specified as master, I/O domain, root domain, and control domain. The order among domains with the same role is alphabetical order. For details of the "failure-policy" and "master" domains, see "Configuring Domain Dependencies" in the *Oracle VM Server for SPARC Administration Guide*.

If unable to secure free resources in the move-destination system board, the

deleteboard command fails with an error message displayed. In this case, identify the cause of the error from the error message output by the deleteboard command and the Oracle Solaris message, and take appropriate action. However, you may need to power off or restart the physical partition, depending on the details of the error that occurred.

Figure 8-7   Concept of Memory Deletion (When Using fj_ppar_dr_policy = targeted)
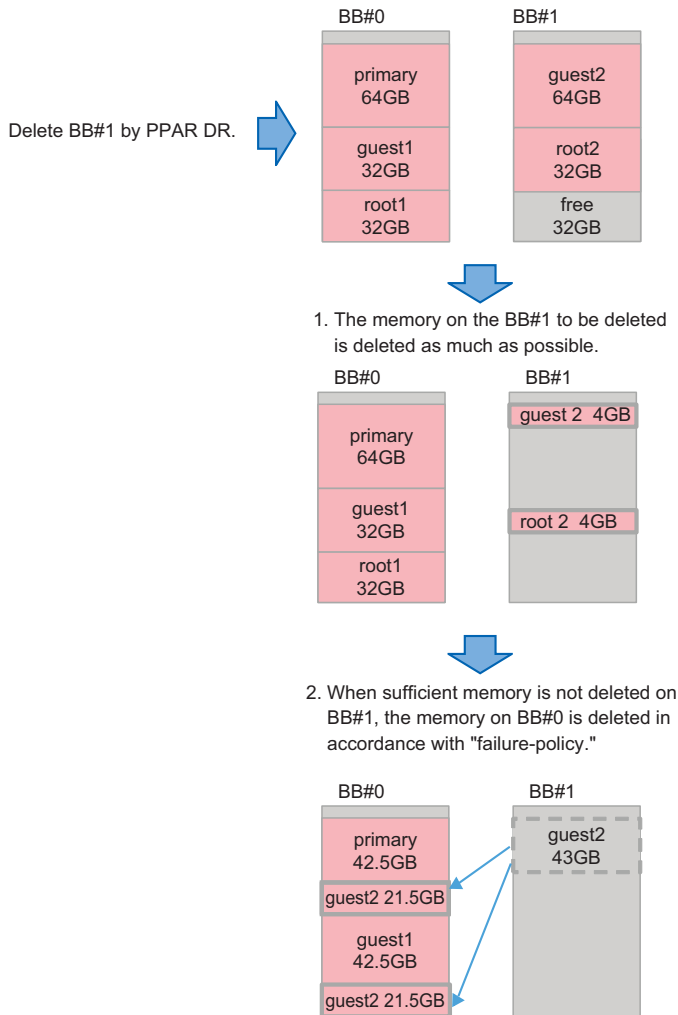
8.15.3   How to Change the PPAR DR Policy

In Oracle VM Server for SPARC 3.4 or later, the policy is changed by setting the PPAR DR policy to the fj_ppar_dr_policy property of the ldmd service by using the svccfg command.

For details on PPAR DR policies that can be set, "8.15.2   Details on Resource Reduction Policies."

The setting procedure is described below.

1. **Log in to the control domain.**

2. **Become the administrator.**
    For details, see *Securing Users and Processes in Oracle Solaris*.

3. **Display the fj_ppar_dr_policy property value.**

```
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
```

4. **Stop the ldmd service.**

```
# svcadm disable ldmd
```

5. **Change the fj_ppar_dr_policy property value.**

```
# svccfg -s ldmd setprop ldmd/fj_ppar_dr_policy=value
```

6. **Refresh and restart the ldmd service.**

```
# svcadm refresh ldmd
# svcadm enable ldmd
```

The following example shows how to display the fj_ppar_dr_policy property value and how to change it from "auto" to "targeted".

```
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
ldmd/fj_ppar_dr_policy astring auto
# svcadm disable ldmd
# svccfg -s ldmd setprop ldmd/fj_ppar_dr_policy=targeted
# svcadm refresh ldmd
# svcadm enable ldmd
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
ldmd/fj_ppar_dr_policy astring targeted
```

8.16   Setting the Maximum Page Size of a Logical Domain

This section describes how to set the maximum page size of a logical domain and the effect of doing so.

This setting is applicable to Oracle VM Server for SPARC 3.5 or later.

8.16.1　Maximum Page Size of a Logical Domain

Three maximum page size settings (256 MB, 2 GB, and 16 GB) are supported by the SPARC M12. For details on how to check the maximum page size, see "8.16.5 Checking the Maximum Page Size of a Logical Domain."
The SPARC M10 supports only 256 MB for the maximum page size, and the setting cannot be changed.

8.16.2　Advantages of a Larger Maximum Page Size

When a large value is set for the maximum page size, large pages can be used by the logical domain. In general, applications that use a large amount of memory will typically run faster when the maximum page size is set to 2 GB or 16 GB, as opposed to 256 MB.

8.16.3　Disadvantages of a Larger Maximum Page Size

A larger than standard value for the maximum page size can adversely affect the success rate of live migration of a logical domain, live migration of an Oracle Solaris kernel zone on a logical domain, and the PPAR DR operation by the deleteboard command.
We recommend setting the maximum page size to 256 MB to ensure the highest success rate for live migration of logical domains and Oracle Solaris kernel zones and in the PPAR DR operation by the deleteboard command. For details, see the descriptions below.

Success Rate of Live Migration and the PPAR DR Operation by the deleteboard Command

The success rate of live migration and the PPAR DR operation done by the deleteboard command depends on the memory usage at the destination.
Memory alignment for logical domains is constrained to multiples of the maximum page size. If the boundaries of the free contiguous memory region at the destination are not multiples of the maximum page size, the memory move fails.

Examples of Memory Usage at the Destination and the Effect of Large Maximum Page Sizes

Figure 8-8 shows an example of moving memory when the maximum page size of the logical domain is set to 2 GB. Even though there is a free contiguous memory region of 2 GB at the destination, the memory move fails because the boundaries of the free contiguous memory region are not multiples of the maximum page size.

Figure 8-8   When the Maximum Page Size of a Logical Domain Is Set to 2 GB
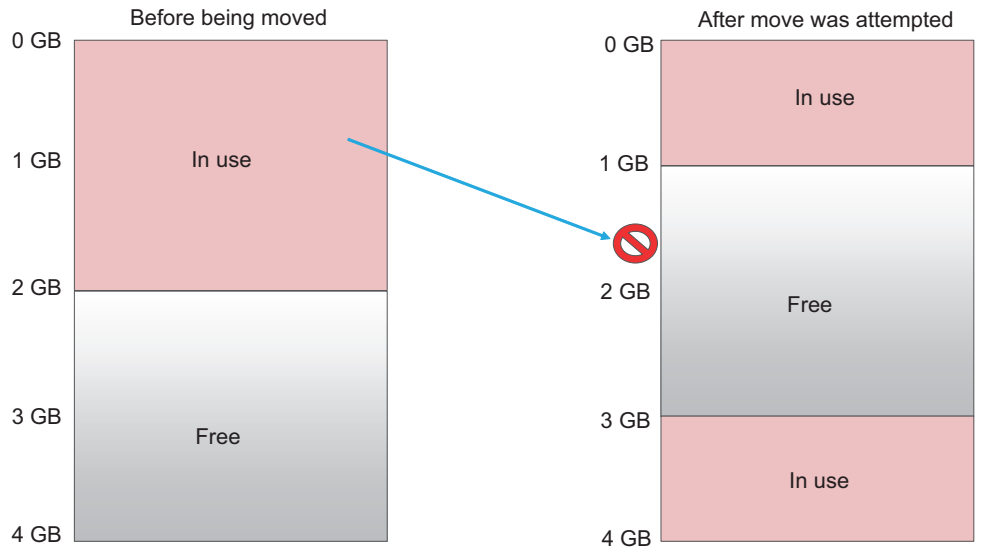
Figure 8-9 shows an example of moving memory when the maximum page size of the logical domain is set to 256 MB. The memory move succeeds because the boundaries of the free memory region at the destination can be set to multiples of 256 MB.

Figure 8-9   When the Maximum Page Size of a Logical Domain Is Set to 256 MB
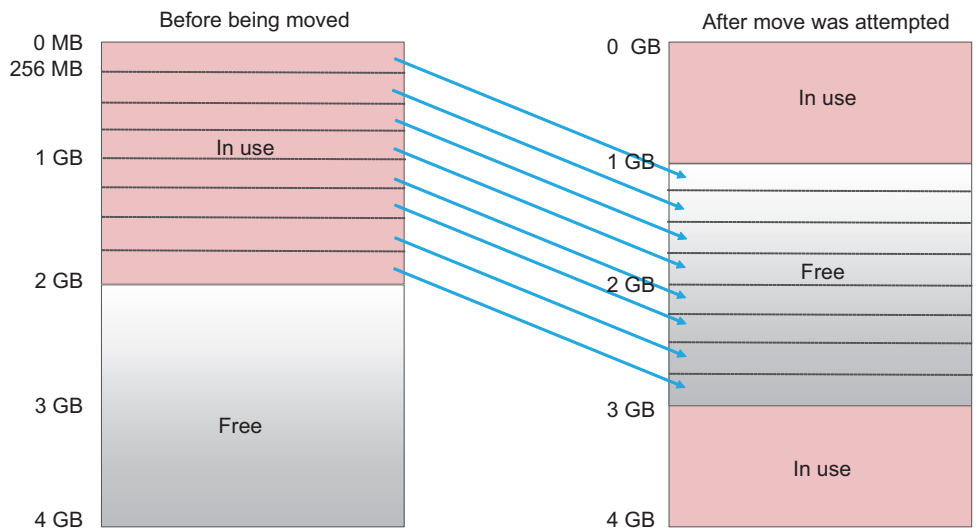
8.16.4 Setting and Changing the Maximum Page Size of a Logical Domain

The following methods are available for setting the maximum page size of a logical domain.

- Setting the fj_dr_sw_limit_pagesize property of the ldmd service
- Setting and Changing fj-software-limit-pagesize With the ldm add-domain/ldm set-domain Command

Setting the fj_dr_sw_limit_pagesize property of the ldmd service

You can set the fj_dr_sw_limit_pagesize property value to "true" or "false".

- **fj_dr_sw_limit_pagesize=false [default]**
  The maximum page size of a logical domain is automatically set based on the size of memory allocated to the logical domain and the maximum page size supported in the system.
  You can set the maximum page size (fj-software-limit-pagesize) with the ldm add-domain or ldm set-domain command.

- **fj_dr_sw_limit_pagesize=true**
  The maximum page size is set to 256 MB for newly created logical domains. Even when set to "true," this property does not change the current maximum page size of the control domain and existing logical domains.

The procedure to set the fj_dr_sw_limit_pagesize property for the ldmd service is described below.

1. **Log in to the control domain.**

2. **Switch to administrator privileges.**
   For details, see *Securing Users and Processes in Oracle Solaris*.

3. **Display the fj_dr_sw_limit_pagesize property value.**

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
```

4. **Stop the ldmd service.**

```
primary# svcadm disable ldmd
```

5. **Change the fj_dr_sw_limit_pagesize property value.**

```
primary# svccfg -s ldmd setprop ldmd/fj_dr_sw_limit_pagesize=value
```

6. **Refresh and restart the ldmd service.**

```
primary# svcadm refresh ldmd
primary# svcadm enable ldmd
```

In the following example, the fj_dr_sw_limit_pagesize property value is checked and then changed from "false" to "true."

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
ldmd/fj_dr_sw_limit_pagesize boolean false
primary# svcadm disable ldmd
primary# svccfg -s ldmd setprop ldmd/fj_dr_sw_limit_pagesize=true
primary# svcadm refresh ldmd
primary# svcadm enable ldmd
```

In the following example, the fj_dr_sw_limit_pagesize property value is confirmed as "true."

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
ldmd/fj_dr_sw_limit_pagesize boolean true
```

Setting and Changing fj-software-limit-pagesize With the ldm add-domain/ ldm set-domain Command

- **To set fj-software-limit-pagesize with the ldm add-domain command**
  The maximum page size of a logical domain can be set with the ldm add-domain command.
  If the fj_dr_sw_limit_pagesize property is set to "true," the maximum page size is set to 256 MB, and it cannot be changed.
  For details on the ldm commands, see the *Oracle VM Server for SPARC 3.5 Reference Manual*.
  The following example sets 256 MB as the maximum page size of domainA, a newly created logical domain.

```
primary# ldm add-domain fj-software-limit-pagesize=256MB domainA
```

- **To set and change fj-software-limit-pagesize with the ldm set-domain command**
  The maximum page size of a logical domain can be set and changed with the ldm set-domain command. The maximum page size cfan be set and changed only when the logical domain is in the delayed reconfiguration or inactive state. However, if the fj_dr_sw_limit_pagesize property is set to "true," the maximum page size is set to 256 MB, and it cannot be changed.
  For details on the ldm commands, see the *Oracle VM Server for SPARC 3.5 Reference Manual*.
  The following example sets 256 MB for the maximum page size of the control domain.

```
primary# ldm start-reconf primary
primary# ldm set-domain fj-software-limit-pagesize=256MB primary
primary# shutdown -y -i6 -g0
```

The following example sets 2 GB for the maximum page size of domainB, a
logical domain.

```
primary# ldm stop-domain domainB
primary# ldm unbind-domain domainB
primary# ldm set-domain fj-software-limit-pagesize=2GB domainB
primary# ldm bind-domain domainB
primary# ldm start-domain domainB
```

8.16.5   Checking the Maximum Page Size of a Logical Domain

The maximum page size (fj-software-limit-pagesize) of each logical domain can be
checked with the ldm list-domain command.
The following example shows that the maximum page size of domainC is 2 GB.

```
primary# ldm list-domain -l domainC
NAME             STATE       FLAGS    CONS    VCPU  MEMORY    UTIL  NORM  UPTIME
domainC          active      -n----   5003    8     6G        0.1%  0.0%  58m
SOFTSTATE
Solaris running
UUID
    xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
MAC
    xx:xx:xx:xx:xx:xx
HOSTID
    0xxxxxxxxx
CONTROL
    failure-policy=ignore
    extended-mapin-space=on
    cpu-arch=native
    rc-add-policy=
    shutdown-group=15
    perf-counters=
    boot-policy=warning
    effective-max-pagesize=256MB
    hardware-max-pagesize=16GB
    fj-software-limit-pagesize=2GB
```

Chapter 9

Managing the Systems Daily

This chapter describes the daily work required in SPARC M12/M10 system management.

Backing Up XSCF Settings Information

Regularly back up the XSCF settings information stored on the master XSCF. After replacement of a field replaceable unit (FRU) due to the failure of the FRU including the master XSCF, restoring the XSCF settings information stored as a backup enables system operation to continue without change, as it was before the failure.

For details, see "10.10   Saving/Restoring XSCF Settings Information."

Backing Up Logical Domain Configuration Information

Regularly back up the logical domain configuration information configured by Oracle VM Server for SPARC. Make a backup for each logical domain from the control domain. The configuration information of the logical domain can be stored using the following two methods:
- Saving in XSCF
- Saving as XML file
After changing the domain configuration, be sure to back up the latest configuration information. We recommend saving duplicates of backup files onto other media in case of disk failure.

For details, see "10.11   Saving/Restoring Logical Domain Configuration Information in the XSCF" and "10.12   Saving/Restoring Logical Domain Configuration Information in an XML File."

Backing Up the OpenBoot PROM Environment Variables

Record and back up the OpenBoot PROM environment variables set in the control domain periodically.

If you want to change the logical domains to the factory-default configuration to restore logical domain configuration information from an XML file, the OpenBoot PROM environment variables in the control domain are initialized, and Oracle Solaris boot cannot be performed.

To prevent this from happening, record and save the OpenBoot PROM environment variables in the control domain before changing to the factory-default configuration. After changing the logical domains to the factory-default configuration, restore the OpenBoot PROM environment variables in the control domain using the saved information.

For details, see "10.13   Saving/Restoring the OpenBoot PROM Environment Variables."

Backing Up Internal Disk Drives

Regularly back up the data on internal disk drives. The backup method varies depending on the configuration of the installed drives. Execute backup according to the drive configuration.

Updating to the Latest Firmware

The XSCF firmware for SPARC M12/M10 system management is provided as the XCP package together with OpenBoot PROM, Hypervisor, and POST. The latest version of the XCP package is regularly released with new added functions, bug fixes, etc. Always update to the latest version of the XCP package immediately after it is published.

For details about updating to the latest firmware, see "Chapter 16   Updating the XCP Firmware."

New functions and changes in the XCP package are mentioned in the *Product Notes* of the corresponding XCP version for your server. Be sure to read it.

Monitoring the System Status

The XSCF constantly monitors system operation.
You can get a grasp of the server status by accessing the XSCF from the XSCF shell or XSCF Web.
Use the XSCF SNMP agent function, failure information notification function, and various messages and logs to monitor system failures and events.
For details, see "10.2 Receiving Notification by E-mail When a Failure Occurs," "10.3 Monitoring/Managing the System Status with the SNMP Agent," and "Chapter 12 Checking Logs and Messages."

Chapter 10

Preparing/Taking Action for Failures

This chapter describes the functions that are configured in advance to prepare for possible failure occurrences in the SPARC M12/M10 systems. These systems provide various functions for preparing for possible failure occurrences. For the purpose of finding and taking action for failures earlier, users need to make some preparations such as configuring system monitoring, making hardware redundant, and saving data.

This chapter describes these management methods.

- Learning about Troubleshooting and Related Functions
- Receiving Notification by E-mail When a Failure Occurs
- Monitoring/Managing the System Status With the SNMP Agent
- Monitoring the System
- Understanding the Failure Degradation Mechanism
- Checking Failed Hardware Resources
- Setting Automatic Replacement of Failed CPU Cores
- Setting Recovery Mode
- Setting Up a Redundant Component Configuration
- Saving/Restoring XSCF Settings Information
- Saving/Restoring Logical Domain Configuration Information in the XSCF
- Saving/Restoring Logical Domain Configuration Information in an XML File
- Saving/Restoring the OpenBoot PROM Environment Variables
- Saving/Restoring the Contents of a Hard Disk
- Resetting a Logical Domain
- Causing a Panic in a Logical Domain
- Resetting a Physical Partition
- Returning the Server to the State at Factory Shipment
- Collecting a Crash Dump File Using Deferred Dump

10.1 Learning about Troubleshooting and Related Functions

Table 10-1 lists the actions and functions used to prepare for possible failure occurrences. For details of individual items, see the subsequent sections.

Table 10-1   Troubleshooting and Functions

Action	Function	Related Command
Send failure information early to users	- E-mail notification	setsmtp(8), showsmtp(8), setemailreport(8), showemailreport(8)
	- Remote maintenance service	See the latest *Product Notes* for your server.
Monitor/Manage failures and events	- System monitoring with the SNMP agent function	setsnmp(8), showsnmp(8), setsnmpusm(8), showsnmpusm(8), setsnmpvacm(8), showsnmpvacm(8)
Find failures early to determine server operations	- System monitoring, heartbeat, Alive check - Server operation control	setpparmode(8), showpparmode(8), setpparparam(8), showpparparam(8)
Prevent failures from affecting other parts, or take measures with a redundant configuration	- Failure degradation - Redundant component configuration	showstatus(8), showhardconf(8)
Protect the current setting data so as to return it to its original state	- Saving/Restoring XSCF settings information - Saving/Restoring logical domain information - Saving/Restoring hard disks	dumpconfig(8), restoreconfig(8), Commands of Oracle VM Server for SPARC

Note - If the XSCF fails, no notification is issued using the XSCF e-mail notification function, SNMP traps, or the remote maintenance service (ASR function, REMCS, etc.). To monitor XSCF failures, use server monitoring software. For details, see the software manuals related to management of the server used.

10.2 Receiving Notification by E-mail When a Failure Occurs

In preparation for the failures and events that may occur in these systems, the XSCF can be configured to notify users of the status by e-mail.

We strongly recommend setting e-mail notification. Once e-mail notification by the XSCF is set, a given user (such as a system administrator who has the platadm user privilege) can immediately receive notification of server and physical partition failures.

10.2.1 Features of the E-mail Notification Function

The e-mail notification function has the following features.

- Notification by e-mail of failing parts in the system monitored by the XSCF
  The e-mail can be sent without fail even when the system goes down or a serious error that disables reboots has occurred.

- Enabling the POP authentication function and SMTP authentication function at the e-mail transmission time
  To prevent unauthorized e-mail transmission, POP authentication (POP before SMTP) or SMTP authentication (SMTP-AUTH) can be performed before e-mail transmission is accepted using the SMTP server.

Figure 10-1 outlines a case where the XSCF sends an e-mail via each of the servers.

Figure 10-1   Outline of the XSCF E-mail Function
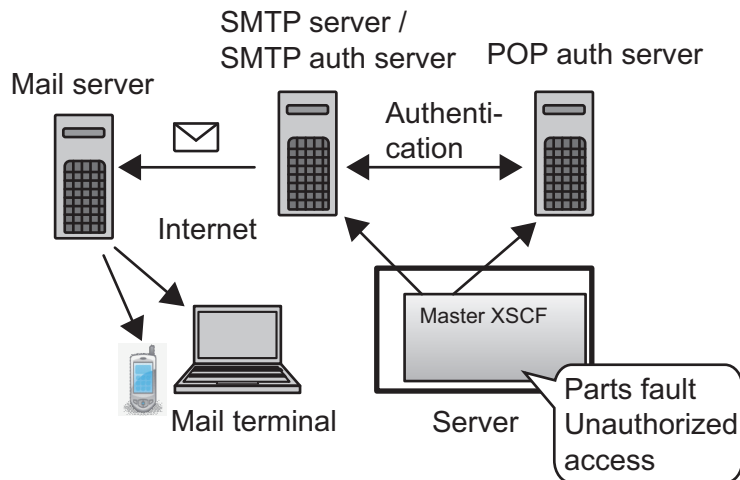
10.2.2 Failure Notification Details

Figure 10-2 shows an example of a notification e-mail.

Figure 10-2   Example of an E-mail When a Part Fails

```
Date: Mon, 02 Aug 2012 16:03:16 +0900
From: XSCF <root@host-name.example.com>      ——— 1
To: mail-address@smtp.example.com       ——— 2
Subject: Error: xxxxxxxxxx      ——— 3


TYPE: Error, VER: XCP-32303030
MODE-SWITCH: -
SEVERITY: Alarm
EVENT-TIME: 08-02-2012 15:55:04 JST
CSN: CNL1126007
SERVER-ID: EM1U1S002
FRU: -
DIAGCODE: Code:0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
Msg: FAN shortage
```

1   "Reply e-mail address" that is set in e-mail settings

2   "Destination e-mail address" that is set in e-mail settings

3   E-mail title

The following items appear in the e-mail example.

Table 10-2   Content of a Notification E-mail at the Time of Failure

Item	Description
TYPE	Notification type
VER	Version
MODE	Mode switch status
SEVERITY	Error level
EVENT-TIME	Failure occurrence time (shown in local time)
CSN	Chassis serial number
SERVER-ID	ID of this system
FRU	Part that is likely faulty

Table 10-2   Content of a Notification E-mail at the Time of Failure *(continued)*

Item	Description
DIAGCODE	Used for troubleshooting by field engineers and service engineers. Users are requested to report this code to a field engineer or service engineer. The code helps find an early solution to the problem.
Msg	Message outlining the problem

10.2.3   Checking the Setting Items and Commands Related to E-mail Notification

Table 10-3 lists the setting items related to XSCF e-mail notification and the corresponding XSCF shell commands.

Table 10-3   Setting Items Related to E-mail Notification

Setting Item	Required or Optional Setting	Related Command
SMTP server - Host name - Port number - Reply e-mail address	Optional	setsmtp(8), showsmtp(8)
Enabling/Disabling the e-mail notification function	Optional	setemailreport(8), showemailreport(8)
Destination e-mail address	Optional	setemailreport(8), showemailreport(8)
Authentication server - POP authentication/SMTP authentication - Host name - User ID/password	Optional	setsmtp(8), showsmtp(8)

Only one SMTP server is specified. To specify an SMTP server by its host name, DNS servers must be able to resolve the server name.

The default port number of the SMTP server is 25.

The reply e-mail address is the e-mail address used to transmit an error e-mail when there is a problem on the path to the destination e-mail address. The e-mail is transmitted by an e-mail server on that path.

10.2.4   E-mail Notification Setting Flow

This section describes the XSCF e-mail notification setting flow.

1. **Log in to the XSCF.**
2. **Specify the host name or IP address of the SMTP server (see setsmtp(8)).**
3. **Select POP or SMTP authentication (see setsmtp(8)).**
4. **Specify the reply e-mail address (From specification) (see setsmtp(8)).**
5. **Specify the destination e-mail address for the system administrator (see setemailreport(8)).**
6. **Enable XSCF e-mail notification (see setemailreport(8)).**
7. **Issue a test e-mail.**
   After the e-mail settings are completed, the test e-mail is automatically issued. When the issued test e-mail arrives in the e-mails for the system administrator, the settings are complete. If the e-mail does not arrive, an error e-mail is sent to the reply e-mail address (From specification), or this event is recorded in an error log. In this case, after identifying the cause and solving the problem, repeat the procedure from step 1. The e-mail notification function is enabled when the test completes normally.

10.2.5 Setting the SMTP Server Host Name, Port Number, Reply E-mail Address, and Authentication Method

1. **Execute the showsmtp command to display SMTP server setting information.**

```
XSCF> showsmtp
Mail Server:
Port : 25
Authentication Mechanism: none
Reply address:
```

2. **Execute the setsmtp command to set SMTP server information.**
   The following example specifies a host name, a port number, a reply e-mail address, and SMTP authentication.

```
XSCF> setsmtp -s mailserver=192.1.4.5 -s port=25 -s
replyaddress=yyyy@example.com -s auth=smtp-auth -s user=usr001 -s
password=xxxxxxxx
```

The following example specifies, in interactive mode, a host name, a port number, a reply e-mail address, and POP authentication.

```
XSCF> setsmtp
Mail Server [192.1.4.2]: 192.1.4.5
Port[25]:
Authentication Mechanism [none]:pop
POP Server [192.1.4.2]:
```

```
User Name []: usr001
Password []: xxxxxxxx
Reply Address [yyyy@example.com]:
```

3. **Execute the showsmtp command, and confirm the SMTP server setting information.**

```
XSCF> showsmtp
Mail Server: 192.1.4.5
Port: 25
Authentication Mechanism : pop
User Name: usr001
Password: ********
Reply Address: yyyy@example.com
```

10.2.6 Setting the Destination E-mail Address for Notification and Enabling/Disabling the E-mail Notification Function

Configure the SMTP server in advance, as described in "10.2.5　Setting the SMTP Server Host Name, Port Number, Reply E-mail Address, and Authentication Method."

After configuring the XSCF e-mail function, you can issue a test e-mail to confirm the settings. The issuing time (shown in local time) of the test e-mail and information on the e-mail source are displayed. Also, the test e-mail title contains the characters "Test Mail:".

1. **Execute the showemailreport command to display e-mail notification setting information.**

```
XSCF> showemailreport
E-Mail Reporting: disabled
```

2. **Execute the setemailreport command to set e-mail notification information.**
   The following example specifies, in interactive mode, enabling of e-mail notification and the destination e-mail address.

```
XSCF> setemailreport
Enable E-Mail Reporting? [no]: yes
E-mail Recipient Address []: xxxxx@example.com
Do you want to send a test mail now [no]?: yes
... Sending test mail to 'xxxxx@example.com'
```

3. **Execute the showemailreport command, and confirm the e-mail notification setting information.**

```
XSCF> showemailreport
E-Mail Reporting: enabled
E-Mail Recipient Address: xxxxx@example.com'
```

4. **Confirm that the test e-mail with the title "Test Mail" can be received.**

10.3   Monitoring/Managing the System Status With the SNMP Agent

This section describes how to monitor system failures and events.

With the SNMP agent configured on the XSCF, the server manager can monitor/manage failures and events.

10.3.1   Basics of SNMP

The Simple Network Management Protocol (SNMP) is a network management protocol.

SNMP is referred to as a query, command, or response protocol for testing and changing the configuration parameters of a LAN or WAN to which bridges, routers, switches, and other devices are connected.

The following versions are currently offered: SNMPv1, SNMPv2c, and SNMPv3. In contrast to SNMPv1 and SNMPv2c, SNMPv3 has added encryption and authentication functions.

The SNMP manager centrally manages the operation status and problem status of the terminals on a network. The SNMP agent returns management information called Management Information Base (MIB), in response to a manager request. The agent can also asynchronously notify the manager of given information, by using the function called Trap.

Figure 10-3 shows an example of a network management environment using SNMP.

Figure 10-3　　Example of a Network Management Environment
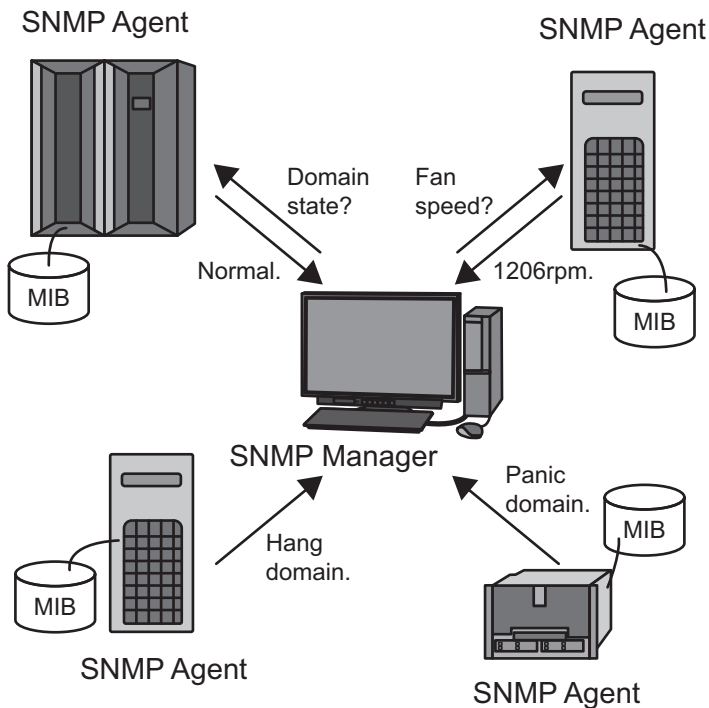
Default Port Numbers Used by SNMP

The default port numbers used by SNMP are as follows.

- For the SNMP agent: Port 161
- For trap: Port 162

10.3.2　SNMP-related Terms

Table 10-4 lists SNMP-related terms.

Table 10-4　　SNMP-related Terms

Term	Description
USM	Abbreviation for User-based Security Model. This security model is based on the users defined in SNMPv3.
VACM	Abbreviation for View-based Access Control Model. This access control model is based on the views defined in SNMPv3.
Group	Aggregation of users belonging to the VACM model. A group is defined with the access privileges of all the users belonging to the group.

Term	Description
OID	Abbreviation for Object Identifier. An OID is an object identification number. Regarding objects in a MIB definition file, the numeric address of the MIB is denoted by the concatenation of integers with dots.
View (MIB view)	A view is a method of referencing a MIB definition file. The view is a subtree of the MIB defined with an OID and OID mask. A MIB access control view can be assigned to a group.

Table 10-4   SNMP-related Terms *(continued)*

10.3.3   Basics of a MIB Definition File

The SNMP agent function has management information called MIB. The function returns this MIB information in response to a request from the manager.

Standard MIB

The XSCF supports MIB-II (supporting SNMPv2 and v3) and MIB-I (supporting SNMPv1), which are defined as Internet standards, to mainly manage the following information:

- Basic XSCF-LAN-related information (e.g., administrator name)
- XSCF-LAN communication processing-related information
- XSCF SNMP agent operation-related information

For details on the standard MIBs supported by the XSCF, see "Appendix D   XSCF MIB Information."

Extended MIB

In addition to the standard MIBs, these systems support the following extended MIB:

- XSCF extended MIB: Extended MIB for the XSCF SNMP agent

This MIB mainly manages the following information:

  - Basic system-related information (e.g., serial number)
  - Various system-related status information (e.g., high-level Oracle Solaris operation status)
  - Information on physical partitions in the system
  - Information on parts failures in the system
  - Information related to power values in the system

The following example shows the data in management information for the XSCF extended MIB.

```
scfMachineType OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION "System model name and model type name."
```

```
::= { scfInfo 1 }
scfNumberOfCpu OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION "Number of CPUs"
::= { scfInfo 2 }
scfSysSerial OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION "System serial number"
::= { scfInfo 3 }
```

For details on the XSCF extended MIB supported by the XSCF, see "Appendix D XSCF MIB Information."

Installing an Extended MIB Definition File

A MIB definition file is defined according to the ASN1 standard notation.
The XSCF extended MIB definition file defines management information so that these systems are monitored by the SNMP manager. To monitor the server, install the XSCF extended SNMP definition file for the SNMP manager.

For details on how to install it, see the manual of the SNMP manager used. For the place to obtain the extended MIB definition file, see the latest *Product Notes* for your server or the MIB definition file-related information at the firmware download site.

10.3.4 Traps

If you enable the SNMP agent function, a notification called Trap is issued to the SNMP manager. XSCF traps cover the following events:

- Heartbeat notification (XCP 2050 or later)
- XSCF failover occurrence
- Configuration changes due to the addition, removal, replacement, etc. of PSBs and components
- Failure occurrence of a part in the system, or replacement of the failed part in the system followed by recovery in such cases
- Change of a physical partition to the start, panic, power-off, or other state
- Incorporation or release of a BB (PSB) in a physical partition
- Hypervisor abort
- Configuration changes such as the addition and deletion of parts in the PCI expansion unit
- Change of the LED status of a part in the PCI expansion unit
- Abnormal temperature of the PCI expansion unit
- Mode switch change

- When a panic or other change in status of the logical domain occurs
- Start of the XSCF SNMP agent function (standard trap)
- Unauthorized access to the XSCF SNMP agent (standard trap)
- Issuing of a cold start trap (standard trap) generated when a change in management object configuration occurred at the SNMP agent start time

Among the parts monitored by the XSCF in the system, the target part of a trap can be identified from the failure location and part number. A trap is generated when an XSCF event notification is issued, even if the part cannot be identified.

The following example shows the SNMP-Trap for the failure occurrence of a part in the system.

```
Aug 12 06:07:16 paplsv2 snmptrapd[11958]: 2012-08-12 06:07:16
A4U4S141 [10.26.147.50] (via UDP: [10.26.147.50]:38221) TRAP,
SNMP v1, community abccommunity   XSCF-SP-MIB::scfMIBTraps
Enterprise Specific Trap (XSCF-SP-MIB::scfComponentStatusEvent)
Uptime: 6:27:33.28    XSCF-SP-MIB::scfComponentErrorStatus.bb.
0.cmuu.0.notApplicable.0 = INTEGER: deconfigured(4)      XSCF-
SP-MIB::scfTrapStatusEventType.0 = INTEGER: alarm(1)
```

This example contains the following information:
- IP address of the XSCF that issued the trap (e.g., 10.26.147.50)
- Community string under SNMPv1 (e.g., adcommunity)
- Trap type (e.g., EnterpriseSpecific, model-specific trap)
- Trap issuing time (e.g., Uptime: 6:27:33:28)
- Additional trap information
  The information may include a possibly faulty part, event type, or error level.

For the firmware version XCP 2050 or later, if you enable the XSCF SNMP agent function, the XSCF heartbeat notification (existence information) traps are sent to the system.

The heartbeat notifications are sent at the occurrence of the following events.
- When the XSCF SNMP agent function is started or resumed.
- Every 12 hours since the start of the XSCF SNMP agent function
- When the rastest -c hb command is executed

The following example shows an SNMP trap concerning the XSCF heartbeat notification.
You can confirm the XSCF heartbeat notification when the trap code is "FF010001" and MessageId of the trap is "M10-Heartbeat."

```
(solaris.4.1.1.12.2.1.13.100.0.254.0.254.0 [1 1 0] 1)
(solaris.4.1.2.1.2.0 [1 1 0] 4)
(solaris.4.1.1.4.3.0 [2 10 0] PZ31426015)
(solaris.4.1.1.4.2.0 [2 11 0] SPARC M10-1)
(solaris.4.1.1.4.1.0 [2 10 0] x-integ-ts)
(solaris.4.1.2.1.14.0 [2 8 0] FF010001)
(solaris.4.1.2.1.15.0 [2 28 0] Oct 23 03:06:04.367 JST 2014)
```

```
(solaris.4.1.2.1.16.0 [2 0 0] )
(solaris.4.1.2.1.17.0 [2 0 0] )

(solaris.4.1.2.1.18.0 [2 0 0] )
(solaris.4.1.2.1.19.0 [2 0 0] )
(solaris.4.1.2.1.20.0 [2 0 0] )
(solaris.4.1.2.1.21.0 [2 0 0] )
(solaris.4.1.2.1.22.0 [2 0 0] )
(solaris.4.1.2.1.23.0 [2 0 0] )
(solaris.4.1.2.1.24.0 [2 13 0] Fujitsu M10-1)
(solaris.4.1.2.1.25.0 [1 1 0] 1)
(solaris.4.1.2.1.26.0 [2 13 0] M10-Heartbeat)
```

For details of the OID information about the XSCF heartbeat notification, see "Chapter 5 XSCF Trap Type List" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists*.

XSCF Trap Information

XSCF traps consist of traps that report failures and traps that report changes in the system status. To send the appropriate traps to the systems used, make the necessary trap reception settings with the SNMP manager.
For information on the lists of XSCF SNMP MIB traps, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists*.

10.3.5 Checking the Setting Items and Commands Related to the SNMP Agent

Table 10-5 lists the setting items related to the XSCF SNMP agent and the corresponding XSCF shell commands.

Table 10-5   Setting Items Related to the SNMP Agent

Setting Item	Required or Optional Setting	Related Command
System management information - Agent system installation location - Administrator e-mail address - Agent system description - Agent port number (listening port number)	Optional	setsnmp(8), showsnmp(8)
Enabling/Disabling the agent	Optional Default: Disabled	setsnmp(8), showsnmp(8)

Table 10-5   Setting Items Related to the SNMP Agent *(continued)*

Setting Item	Required or Optional Setting	Related Command
SNMPv3 trap - User name - Authentication password - Encryption password - Local agent engine ID, or request for acknowledgment from the receiving host - Authentication algorithm - Encryption protocol - Trap destination port number - Trap destination host name	Optional	setsnmp(8), showsnmp(8)
Disabling SNMPv3 traps	Optional	setsnmp(8), showsnmp(8)
Enabling/Disabling SNMPv1 and SNMPv2c communication	Optional	setsnmp(8), showsnmp(8)
SNMPv1/SNMPv2c trap - Trap type specification - Community string - Trap destination port number - Trap destination host name	Optional	setsnmp(8), showsnmp(8)
Disabling SNMPv1/SNMPv2c traps	Optional	setsnmp(8), showsnmp(8)
Initializing SNMP settings	Optional	setsnmp(8), showsnmp(8)
USM management information (settings for SNMPv3) - Registering an authentication/ encryption password for a user - Changing the authentication/ encryption password of a user - Specifying an authentication algorithm - Specifying an encryption protocol - Copying a user - Deleting a user	Optional	setsnmpusm(8), showsnmpusm(8)
VACM management information (settings for SNMPv3) - Registering an access control group for a user - Deleting the access control group of a user - Creating a MIB access control view - Deleting a MIB access control view - Assigning a MIB access control view to a group - Deleting a group from all MIB access control views	Optional	setsnmpvacm(8), showsnmpvacm(8)

10.3.6   SNMP Agent Setting Flow

This section describes the XSCF SNMP agent setting flow.

For details on each step, see "10.3.7   Setting System Management Information on the SNMP Agent and Enabling/Disabling the SNMP Agent" and the subsequent sections.

SNMPv1 and SNMPv2c cannot be said to be secure since they do not provide communication data encryption. Data can be sent and received more securely with SNMPv3, using the authentication/encryption settings made on both the agent and manager sides. These systems provide SNMPv3 as the default SNMP agent.

Starting Sending and Receiving

1. **Log in to the XSCF.**
2. **Set the following management information common to the SNMPv1, SNMPv2c, and SNMPv3 agent protocols (see setsnmp(8)).**
   - Agent system installation location
   - Administrator e-mail address
   - Agent system description
   - Agent port number (listening port number)
3. **Set the following management information for SNMPv3 or that for SNMPv1 and SNMPv2c (see setsnmp(8)).**
   -- Setting SNMPv3 management information
   - User name
   - Authentication password
   - Encryption password
   - Authentication algorithm
   - Encryption protocol
   - Trap destination port number
   - Trap destination host name

   -- Setting SNMPv1 and SNMPv2c management information
   - Trap type specification (selection of v1, v2c, or inform <v2c and response>)
   - Community name
   - Trap destination port number
   - Trap destination host name
4. **Enable the XSCF SNMP agent function. Enable the function in one or both of the following ways, according to the user environment (see setsnmp(8)).**
   - Enabling SNMPv1 and SNMPv2c
   - Enabling SNMPv3

Note - If the XSCF SNMP agent has been enabled, all MIB information except the setting items of step 3 is initialized.

Stopping or Disabling Sending and Receiving

- Disabling the XSCF SNMP agent function
  Disable the function in one or both of the following ways, according to the user environment:

    - SNMPv1 and SNMPv2c nullification
    - SNMPv3 nullification

- Disabling transmission to the intended trap destination host for SNMPv3
  Specify the following items to disable transmission:

    - User name
    - Trap destination host

- Disabling transmission to the intended trap destination host for SNMPv1 or SNMPv2c
  Specify the following items to disable transmission:

    - Protocol type (v1/v2c) specification
    - Trap destination host

Managing Users (USM Management) and Managing the Access Control Views of MIB Definition Files (VACM Management)

Manage USM and VACM for SNMPv3.

When using an SNMPv3 agent, use the setsnmp command to set the authentication protocol and the encryption protocol. Next, be sure to use the setsnmpusm command to set the management information for the User-based Security Model (USM), and use the setsnmpvacm command to set the management information for the View-based Access Control Model (VACM). When making settings for SNMPv3, the specification of an authentication protocol and an encryption protocol is required. Moreover, password entry is required when using the setsnmp and setsnmpusm commands.

1. **Log in to the XSCF.**

2. **Register, change, or delete the following user management information (see setsnmpusm(8) and setsnmpvacm(8)).**
   - Specifying a user authentication algorithm

   - Specifying a user encryption protocol

   - Registering an authentication/encryption password for a user

   - Changing the authentication/encryption password of a user

   - Copying a user

   - Deleting a user

3. **Register, assign, or delete the access control group and access control view (MIB view) for a user as follows:**
   - Registering an access control group for a user
   - Deleting the access control group of a user
   - Creating a MIB access control view
   - Deleting a MIB access control view
   - Assigning a MIB access control view to a group
   - Deleting a group from all MIB access control views

10.3.7 Setting System Management Information on the SNMP Agent and Enabling/Disabling the SNMP Agent

The SNMP agent is disabled by default. The default port number for the agent is 161. Specify an e-mail address up with 128 characters. When placing a limit on the receiving e-mail address, confirm the setting.

1. **Execute the showsnmp command to display the SNMP settings.**
   The following example displays the status where no management information is set.

```
XSCF> showsnmp
Agent Status:       Disabled
Agent port:         161
System Location:    Unknown
System Contact:     Unknown
System Description: Unknown
:
```

2. **Execute the setsnmp command to configure SNMP.**
   The following example specifies the system installation location, description, and administrator e-mail address.

```
XSCF> setsnmp -l MainTower21F -c foo@example.com -d DataBaseServer
```

3. **Execute the setsnmp command to enable the SNMP agent.**
   The following example enables the agent.

```
XSCF> setsnmp enable
```

   The following example disables the agent.

```
XSCF> setsnmp disable
```

4. **Execute the showsnmp command, and confirm the SNMP settings.**
   In the following example, the SNMP agent is enabled.

```
XSCF> showsnmp
Agent Status:      Enabled
Agent port:        161
System Location:   MainTower21F
System Contact:    foo@example.com
System Description: DataBaseServer
 :
```

10.3.8 Configuring SNMPv3 Traps

Set an SNMPv3 user name and authentication/encryption password common to the sending and receiving sides. The engine ID must start with "0x" and be an even hexadecimal number.

The authentication algorithm is Secure Hash Algorithm 256 (SHA256) or MD5.

The encryption protocols are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

No default has been set for the trap destination host. The default port number for the trap destination is 162.

1. **Execute the showsnmp command to display the SNMP settings.**
   The following example displays the status where SNMPv1 and SNMPv2c are configured.

```
XSCF> showsnmp
Agent Status:      Enabled
Agent port:        161
System Location:   MainTower21F
System Contact:    foo@example.com
System Description: DataBaseServer
Trap Hosts:None
Hostname Port Type Community String Username Auth Encrypt
-------- ---- ---- ---------------- -------- ---- ---------
host1      62  v1  public                    n/a  n/a  n/a
host2    1162  v2  public                    n/a  n/a  n/a
SNMP V1/V2c:
Status:            Enabled
Community String:  public
```

2. **Execute the setsnmp command to configure SNMPv3 traps.**
   The following example specifies, along with the addv3traphost operand, a user name, engine ID, authentication algorithm, authentication password, encryption

password, and trap destination host name or IP address.

```
XSCF> setsnmp addv3traphost -u yyyyy -n 0x### -r SHA host3
Enter the trap authentication passphrase: xxxxxxxx
Enter the trap encryption passphrase: xxxxxxxx
```

3. **Execute the showsnmp command, and confirm the SNMPv3 trap settings.**

```
XSCF> showsnmp
Agent Status:       Enabled
Agent port:         161
System Location:    MainTower21F
System Contact:     foo@example.com
System Description: DataBaseServer

Trap Hosts:

Hostname Port Type Community String Username Auth Encrypt
-------- ---- ---- ---------------- -------- ---- ---------
host3    162  v3   n/a              yyyyy SHA DES
host1     62  v1   public           n/a   n/a n/a
host2   1162  v2   public           n/a   n/a n/a
SNMP V1/V2c:
Status:           Enabled
Community String: public

Enabled MIB Modules:
SP MIB
```

10.3.9 Disabling Traps to the Intended Host for SNMPv3

1. **Execute the showsnmp command to display the SNMP settings.**

```
XSCF> showsnmp
```

2. **Execute the setsnmp command to disable the intended trap destination host for SNMPv3.**
   The following example specifies, along with the remv3traphost operand, a user name and a host name.

```
XSCF> setsnmp remv3traphost -u yyyyy host3
```

3. **Execute the showsnmp command, and confirm that the intended trap destination host is disabled.**

```
XSCF> showsnmp
```

10.3.10 Enabling/Disabling SNMPv1 and SNMPv2c Communication

The community string for enabling SNMPv1 and SNMPv2c is Read-Only.

1. **Execute the showsnmp command to display the SNMP settings.**

```
XSCF> showsnmp
```

2. **Execute the setsnmp command to enable SNMPv1 and SNMPv2c communication.**
   The following example specifies the enablev1v2c operand to enable SNMPv1 and SNMPv2c.

```
XSCF> setsnmp enablev1v2c public
```

   The following example specifies the disablev1v2c operand to disable SNMPv1 and SNMPv2c.

```
XSCF> setsnmp disablev1v2c
```

3. **Execute the setsnmp command to enable the SNMP agent.**

```
XSCF> setsnmp enable
```

4. **Execute the showsnmp command, and confirm that the agent is enabled/ disabled.**

```
XSCF> showsnmp
```

10.3.11 Configuring SNMPv1 and SNMPv2c Traps

Select a trap type from the following three:
   - v1
   - v2
   - inform

If inform is specified, InformRequest is transmitted using the SNMPv2c agent.

The default port number for the trap destination is 162.

1. **Execute the showsnmp command to display the SNMP settings.**

```
XSCF> showsnmp
```

2. **Execute the setsnmp command to configure SNMPv1 or SNMPv2c traps.**
   The following example specifies, along with the addtraphost operand, the SNMPv2c type.

```
XSCF> setsnmp addtraphost -t v2 -s public host2
```

The following example specifies the SNMPv1 type.

```
XSCF> setsnmp addtraphost -t v1 -s public host1
```

3. **Execute the showsnmp command, and confirm the SNMPv1 and SNMPv2c trap settings.**

```
XSCF> showsnmp
```

10.3.12 Disabling Traps to the Intended Host for SNMPv1 and SNMPv2c

1. **Execute the showsnmp command to display the SNMP settings.**

```
XSCF> showsnmp
```

2. **Execute the setsnmp command to disable the intended trap destination host for SNMPv1 or SNMPv2c.**
   The following example specifies the remtraphost operand to disable a host of the SNMPv2c type.

```
XSCF> setsnmp remtraphost -t v2 host2
```

3. **Execute the showsnmp command, and confirm that the trap destination host is disabled.**

```
XSCF> showsnmp
```

10.3.13 Returning the SNMP Settings to the Default Values

You can return the set data to the default values by disabling the SNMP agent.

1. **Execute the showsnmp command to display the SNMP settings.**

```
XSCF> showsnmp
```

2. **Execute the setsnmp command to return the SNMP settings to their defaults.**
   The SNMP agent is disabled at this time.

```
XSCF> setsnmp default
```

3. **Execute the showsnmp command, and confirm the return of the SNMP settings to their defaults.**

```
XSCF> showsnmp
```

4. **Execute the setsnmp command, and configure SNMP again. Then, enable the SNMP agent.**

```
XSCF> setsnmp enable
```

5. **Execute the showsnmp command, and confirm the SNMP settings.**

```
XSCF> showsnmp
```

10.3.14 Setting USM Management Information

USM management information consists of settings for SNMPv3. Set the following:

- User authentication algorithm
- User encryption protocol
- Authentication/Encryption password
- Copying/Deleting a user

1. **Execute the showsnmpusm command to display USM management information.**

```
XSCF> showsnmpusm

Username   Auth  Encrypt
--------   ----  -------------
yyyyy      SHA   DES
```

```
user2     SHA  DES
```

2. **Execute the setsnmpusm command to set USM management information.**
   The following example registers an authentication algorithm, authentication password, and encryption password for a new user. Specify eight or more characters for the password.

```
XSCF> setsnmpusm create -a SHA yyyyy
Enter the user authentication passphrase: xxxxxxxx
Enter the user encryption passphrase: xxxxxxxx
```

The following example changes only the authentication password.

(If no password is entered, the user is asked to enter one.)

```
XSCF> setsnmpusm passwd -c auth -o xxxxxxxx -n xxxxxxxx yyyyy
```

The following example copies an existing user to add a user as a clone.

```
XSCF> setsnmpusm clone -u yyyyy newuser
```

The following example deletes a user.

```
XSCF> setsnmpusm delete yyyyy
```

3. **Execute the showsnmpusm command to display USM management information.**

```
XSCF> showsnmpusm

Username  Auth Encrypt
--------  ---- -------------
yyyyy     SHA  DES
user2     SHA  DES
```

10.3.15   Setting VACM Management Information

VACM management information consists of settings for SNMPv3. Set the following:
   - Registering/Deleting a user in an access control group
   - Creating/Deleting a MIB access control view
   - Assigning a MIB access control view to a group
   - Deleting a group from all MIB access control views

The Read-Only view is assigned when an access control view is assigned to a group.

1. **Execute the showsnmpvacm command to display VACM management**

information.

```
XSCF> showsnmpvacm
Groups:
Groupname    Username
---------    ----------------
xxxxx        user1, user2
Views
View         Subtree          Mask         Type
---------    ----------------  ------------  -------------------
all_view     .1                ff           include
Access
View Group
---------    ----------------
all_view     xxxxx
```

2. **Execute the setsnmpvacm command to set VACM management information.**
   The following example adds the access control group xxxxx to user yyyyy.

```
XSCF> setsnmpvacm creategroup -u yyyyy xxxxx
```

   The following example deletes user yyyyy from the access control group xxxxx.

```
XSCF> setsnmpvacm deletegroup -u yyyyy xxxxx
```

   The following example unconditionally creates a MIB access control view.

```
XSCF> setsnmpvacm createview -s .1 all_view
```

   The following example creates a MIB access control view by using an OID mask.

```
XSCF> setsnmpvacm createview -s .1.3.6.1.2.1 -m fe excl_view
```

   The following example deletes a MIB access control view.

```
XSCF> setsnmpvacm deleteview -s .1.3.6.1.2.1 excl_view
```

   The following example assigns a MIB access control view to the group xxxxx.

```
XSCF> setsnmpvacm createaccess -r all_view xxxxx
```

   The following example deletes group1 from all MIB access control views.

```
XSCF> setsnmpvacm deleteaccess group1
```

3. **Execute the showsnmpvacm command, and confirm the set VACM management information.**

```
XSCF> showsnmpvacm
```

10.4 Monitoring the System

This section describes the monitoring of Oracle Solaris and each piece of firmware on these systems.

10.4.1 Understanding the Mechanism of the Host Watchdog Function/Alive Check

An Oracle Solaris logical domain, OpenBoot PROM, Hypervisor, POST, and the XSCF communicate with one another and mutually monitor the alive status. Upon detection of any failure, a panic is generated or they are individually stopped to prevent the effect of the failure from spreading.

In these systems, Hypervisor monitors the logical domain/OpenBoot PROM, and the XSCF monitors POST.

The mechanism of monitoring between Hypervisor and the logical domain and between Hypervisor and OpenBoot PROM is called the Host watchdog function. Also the mechanism of monitoring between XSCF and POST is called the Alive check function.

Figure 10-4 shows the respective resources monitoring one another.

Figure 10-4   System Monitoring Feature
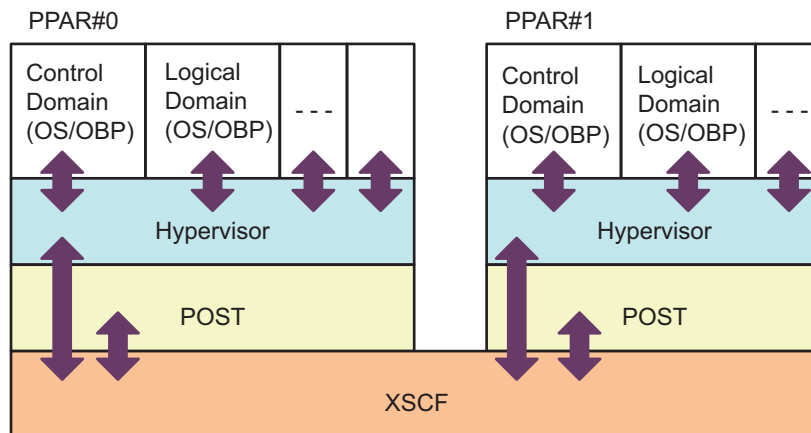
Note - OBP in Figure 10-4 stands for OpenBoot PROM.

XSCF monitors POST and judges as a failure when there is no response after a specific elapsed time, and then resets the physical partition or turns off the power.

Hypervisor regularly monitors the operation status of logical domains (Oracle Solaris/OpenBoot PROM) to detect any Oracle Solaris hang-up. Upon detecting an Oracle Solaris hang-up, Hypervisor generates an Oracle Solaris panic in the relevant domain.

Note - For support information on the Alive check function between the XSCF and Hypervisor, which is set up by the setpparmode command, see the latest *Product Notes* for your server.

10.4.2 Controlling Monitoring and Server Operation

While the system is running or under maintenance, you may want to suppress some functions for individual physical partitions or logical domains. For example, suppose that your preferences for system maintenance include no automatic boot (auto boot suppression enabled) and no receiving of Break signals from the console (Break signal suppression enabled).

In these systems, the operation mode specified for each physical partition include the monitoring method and diagnostic level. This provides control over the operation of the logical domains and physical partition.

You can set the following for each specified physical partition by using the setpparmode command: initial diagnostic level of hardware, message level, Alive check function, reaction when Host watchdog times out, enabling/disabling break signal transmission suppression, enabling/disabling auto boot of guest domains, enabling/disabling the power saving function, and enabling/disabling the IO bus reconfiguration function.
You can also enable/disable auto boot for the control domain for each specified physical partition by using the setpparparam command.

For details of server operation control with the setpparmode command, see "Chapter 3   Operations for Domain Configuration" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Note - For details of the setpparmode command and support information on each function of this command, see the latest *Product Notes* for your server.

10.5 Understanding the Failure Degradation Mechanism

Releasing a component from the system when hardware fails is called degradation. Degradation cuts off access to that component, thereby preventing the problem in the system from being exacerbated.

The degradation scenarios are described below.

- Reserved degradation
  If degradation is not possible immediately at reboot or when a fatal error occurs, the degradation is reserved in the system to perform the degradation at the restart time. This scenario can be realized with the XSCF retaining the degradation location in memory.

- Degradation while Oracle Solaris is running
  CPUs, memory, etc. are degraded when they can be released while Oracle Solaris is running. Only the components allowed to be released while Oracle Solaris is running are subject to degradation.

- Degradation while POST is running
  A physical partition is degraded without being reset.

- Reserved degradation while OpenBoot PROM is running
  Degradation is reserved while OpenBoot PROM is running, and the degradation is performed after a reset. PCI adapter errors, memory errors, etc. are targets for degradation.

- Dynamic degradation of the internal paths in the hardware
  A lane is dynamically degraded in the paths between chassis, such as the SPARC M12/M10 chassis, crossbar units, and crossbar units in a crossbar box, and between components without resetting the system.

Use the showstatus command to display component degradation information. For details about managing failure degradation information, see "11.1.4   Checking Failed/Degraded Components."

10.6 Checking Failed Hardware Resources

The SPARC M12/M10 systems automatically detect and degrade failed memory and CPU resources.
You can display whether there has been memory or CPU resource failures by specifying the -S option in the ldm list-domain and ldm list-devices commands.
For details of the ldm list-domain and ldm list-device commands, see the *Oracle VM Server for SPARC Reference Manual* of the version used. Also see "10.7   Setting Automatic Replacement of Failed CPU Cores." The section describes the setting methods to automatically replace a failed CPU core.

10.6.1 Checking Failed Memory or CPUs With the list-domain Command

1. **Display the detailed information of a logical domain in a physical partition along with the information on whether or not there has been a memory or CPU failure.**

```
primary# ldm list-domain -l -S
```

10.6.2 Checking Failed Memory or CPUs With the list-device Command

1. **Display the resource information of available memory or available CPUs in a physical partition along with the information on whether or not there has been a memory or CPU failure.**

```
primary# ldm list-devices -S mem cpu
```

10.7 Setting Automatic Replacement of Failed CPU Cores

The SPARC M12/M10 can operate systems continuously without reducing CPU resources by using the CPU automatic replacement function to automatically assign another CPU core even if some CPU core fails.

The CPU automatic replacement function is enabled/disabled based on the automatic replacement policy of the ldmd service specified by the svccfg command of Oracle Solaris. The default is enabled.
If the automatic replacement policy is enabled, the failed CPU core that was automatically replaced is controlled so as not to be assigned to a logical domain after that. If the failed CPU core was not automatically replaced, the CPU core remains to be assigned to a logical domain.
If the automatic replacement policy is disabled, then the failed CPU core is not replaced.
For the procedures to change the automatic replacement policy, see "10.7.2   Method of Changing the Automatic Replacement Policy."

10.7.1 Conditions for Automatically Replacing a CPU Core

To perform the automatic replacement of CPU cores, the following conditions must be met.

- Of all the CPU cores mounted on a physical partition, at least one core is ensured not to be assigned to the PPAR.
  If you allocate all the CPU cores mounted on the PPAR to the PPAR with the setcod(8) command of the XSCF firmware, automatic replacement is unavailable.

  For the SPARC M10-4 (4-CPU x 16-core configuration), for example, 64 CPU cores are mounted on the PPAR. To use the automatic replacement function in this configuration, it is necessary to set the number of CPU cores allocated on the PPAR to 63 or less by using the setcod command.

  When 56 CPU cores are allocated to PPAR-ID 0 as follows, 64 CPU cores are mounted on the PPAR and so cores can be automatically switched.

```
XSCF> setcod -p 0 -s cpu -c set 56
PROC Permits assigned for PPAR 0 : 0 -> 56

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

Note - The XSCF firmware of version XCP 2250 or earlier does not support the -c add, -c delete, and -c set options. Specify the setcod command options as follows to interactively add and delete assignments.
XSCF> **setcod -s cpu**

The number of CPU cores available for automatic replacement has no relationship to the number of CPU cores registered with the CPU Activation keys. For example, if 56 CPU Activations are registered in the above example of SPARC M10-4, then up to 8 available CPU cores can be switched with the automatic replacement function, even when 56 CPU cores are allocated with the setcod(8) command. In this case, the 8 CPU cores available for switching do not require CPU Activation keys.

- CPU cores can be dynamically deleted.

Automatic replacement of CPU cores is unavailable under the following cases.

- Physical core IDs (cid option) are specified when CPU cores are assigned to the logical domain.
  Automatic replacement of CPU cores is unavailable if the CPU cores are assigned to the logical domain with the cid option specified as follows.

```
# ldm set-core cid=20 ldom
# ldm add-core cid=20 ldom
```

If you have assigned CPU cores with cid specified, remove the cid specification. For the method of removing the cid specification, see "How to Remove the physical-bindings Constraint" in the *Oracle VM Server for SPARC Administration Guide* of the version used.

Note - To use the CPU automatic replacement function, do not use the Oracle Solaris kernel zones.
When Oracle Solaris kernel zones are in use, CPU cores assigned to Oracle Solaris kernel zones are not automatically replaced in a correct way.

The six subsequent restrictions are abolished in Oracle VM Server for SPARC 3.3 and later.

- When only one CPU core is assigned to a logical domain
  Use the ldm set-core or ldm add-core command to assign two or more CPU cores to a domain. You can confirm CPU core resources used by the logical domain with the ldm list-domain -o core command.

- When the processor set of the resource pool does not meet the following conditions [SPARC M12]

  The pset.min property is set to 9 or more, and the pset.max property is set to pset.min + 8 or more.

  [SPARC M10]

  The pset.min property is set to 3 or more, and the pset.max property is set to pset.min + 2 or more.

  For the method for configuring the processor set of the resource pool, see the *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

- When specifying any specific number of CPUs for the dedicated-cpu resource of an Oracle Solaris zone
  Specifying a specific number of CPUs when using the dedicated-cpu resource of an Oracle Solaris zone is incompatible with automatic CPU core replacement. (e.g., ncpu=5)

- When the range of CPUs specified for the dedicated-cpu resource of an Oracle Solaris zone does not meet the following conditions
  [SPARC M12]

  Nine or more CPUs (two cores) for the minimum value, and the minimum value + eight or more CPUs for the maximum value

  (e.g., ncpus=9-17)

  [SPARC M10]

  Three or more CPUs (two cores) for the minimum value, and the minimum value + two or more CPUs for the maximum value

  (e.g., ncpus=3-5)

- When any processes are bound to the CPU core with the pbind command

You must check/release any processes bound to the CPU core with the pbind command to use the CPU core with the automatic CPU core replacement function.

- When processes are bound to only one CPU core with the psrset command Assign two or more CPU cores to the processor set, or remove the processor set, releasing the CPU core that you want to use with the automatic CPU core replacement function.

10.7.2 Method of Changing the Automatic Replacement Policy

The automatic replacement policy can be changed using the svccfg command of the Oracle VM Server for SPARC.
The automatic replacement can be enabled/disabled by the autoreplacement_policy_cpu property of the ldmd service. You can use the following values for the autoreplacement_policy_cpu property.

- autoreplacement_policy_cpu=1
  A failed CPU resource is automatically replaced. This is the default policy.
- autoreplacement_policy_cpu=0
  If a failure occurs in a CPU, it is not automatically replaced.

The setting procedure is described below.

1. **Log in to the control domain.**

2. **Become the administrator.**

3. **Display the autoreplacement_policy_cpu property value.**

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu
```

4. **Stop the ldmd service.**

```
# svcadm disable ldmd
```

5. **Change the autoreplacement_policy_cpu property value.**

```
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=value
```

6. **Refresh and restart the ldmd service.**

```
# svcadm refresh ldmd
# svcadm enable ldmd
```

The following example shows how to display the current value of the autoreplacement_policy_cpu property and how to change it to a new value. The original value of this property is 0. In that case, the CPU automatic replacement

process is disabled. To stop or restart the ldmd service, use the svcadm command. To display or set property values, use the svccfg command.

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu
ldmd/autoreplacement_policy_cpu integer 0
# svcadm disable ldmd
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=1
# svcadm refresh ldmd
# svcadm enable ldmd
```

10.7.3 Methods of Changing the Maximum Retry Count and Retry Interval

In addition to changing the automatic replacement policy, you can set the maximum retry count and retry interval for the CPU automatic replacement process.
- To specify the maximum retry count, set the autoreplacement_retry_counter property of the ldmd service. If 0 is specified, there is no limit on the retry count. The default value is 5.
- To specify the retry interval, set the autoreplacement_retry_interval property of the ldmd service. The minimum interval is 1 second. The default value is 300 seconds.

The procedures for changing these properties are the same as that for changing the autoreplacement_policy_cpu property value. See "10.7.2 Method of Changing the Automatic Replacement Policy."

10.8 Setting Recovery Mode

Domain configuration that cannot be started due to resource problems, missing resources, etc., can be recovered automatically by setting recovery mode, which is offered by Oracle VM Server for SPARC 3.1 and later.
This function is enabled by default in Oracle VM Server for SPARC 3.3 or later.
For details on recovery mode, see "Handling Hardware Errors" in the *Oracle VM Server for SPARC Administration Guide* of the version used. In addition, for fixes required for recovery mode, see the *Oracle VM Server for SPARC Release Notes* of the version used.

10.9 Setting Up a Redundant Component Configuration

With components in a redundant configuration, if one of the components fails, the

system can continue operating with the remaining components.

For details of redundant component configurations, see the *Service Manual* for your server.

Use the showhardconf command to display the component configuration. For details on how to check components, see "11.1.2 Checking Mounted Components in the System."

10.10 Saving/Restoring XSCF Settings Information

To save/restore XSCF settings information, execute the dumpconfig or restoreconfig command of the XSCF firmware. Execution of the command with specified options saves or restores all of the XSCF settings information at the specified location.

10.10.1 Understanding How to Save/Restore XSCF Settings Information

This section describes the following two methods of saving/restoring XSCF settings information.

- Save/Restore the setting information locally by connecting a USB device to one of the USB ports mounted on the XSCF unit panel (rear panel) of the master XSCF.

- Transfer data to the network host via the network. The data transfer at this time uses an encryption protocol.

Note - When replacing the XSCF unit of the SPARC M12-2/M12-2S, the XSCF settings information can be taken over by also swapping the SD card. When replacing the crossbar box (XBBOX) or CPU memory unit (lower) (CMUL) of the SPARC M10-4/M10-4S, the XSCF settings information can be taken over by also swapping the microSD card.
For details, see the section "Replacing the SD card" or "Replacing microSD card" in the *Service Manual* for your server. When replacing the XSCF unit of a crossbar box, see "8.5 Switching the microSD Card" in the *Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

Purposes of Saving

The purposes of saving XSCF settings information with the dumpconfig command are as follows.

- Backing up the setting information enables the data to be restored after a failure.

- Copying the master XSCF settings information allows the same setting information to be used by the XSCFs of other servers.

Notes on Saving and Restoration

■ USB devices need to be formatted with the FAT32 file system. For the capacity of the USB device used to save/restore the setting information locally and for points to note about handling, ask a service engineer.

■ This setting information can be restored on only the same model where the setting information was saved. For example, the setting information saved on a SPARC M10-1 system can be restored on only a SPARC M10-1 system. To restore data, consistency between the configuration file of the current system and the configuration file being restored is checked. The file is restored only when the configuration file versions, system names, and other information can be confirmed to be consistent. Note that the configuration file version does not depend on the XCP version. The configuration files may be different versions even when the XCP versions are the same at the save/restore time.

■ The systems with multiple XSCFs save/restore the data on the master XSCF side.

■ The dumpconfig command can be used with specified options to encrypt saved data. You can safely restore the encrypted data by entering the key specified at the save time and executing the restoreconfig command.

■ The following identification information is added to the beginning of a saved configuration file. You can refer to the identification information in the text.
- User comment
- Data version
- Whether encryption is enabled or disabled
- Save time
- System name
- Serial number
- XCP version

■ The XSCF network settings specify options to restore data.

■ To restore the setting information, power off all physical partitions. Additionally, when the restore command is executed, the XSCF settings information is loaded, so the correctness of its content can be checked. Once the confirmation is complete, the XSCF is rebooted and the data is restored.

10.10.2 Saving XSCF Settings Information

This section describes the procedure for saving the XSCF configuration file.

Note - With the dumpconfig command, the XSCF settings information can be encrypted and saved. For details, see the dumpconfig(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Saving the Setting Information to a USB Device on the Master XSCF

1. **Connect a USB device to a USB port on the XSCF unit panel (rear panel) of the master XSCF.**
2. **Specify the name of the output file for the local USB device on the XSCF, and execute the dumpconfig command.**

```
XSCF> dumpconfig file:///media/usb_msd/backup-file.txt
```

3. **Remove the USB device from the USB port when the data transfer has completed.**
4. **Confirm the identification information at the beginning of the configuration file that was saved.**

Specifying the Target Directory and Saving the Setting Information via a Network

1. **Specify the target directory and the output file name, and execute the dumpconfig command.**

```
XSCF> dumpconfig ftp://server/backup/backup-sca-ff2-16.txt
 :
```

2. **Confirm the identification information at the beginning of the saved configuration file when the data transfer has completed.**

Configuration File Format

The saved configuration file has the following format:
- File name: User-specified name
- File format: base64 encoded text

10.10.3 Restoring XSCF Settings Information

This section describes the procedure for restoring a configuration file.

Note - The restoreconfig command is capable of decrypting files that were encrypted using the dumpconfig command. For details, see the restoreconfig(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Note - When you save logical domain configuration information by using the ldm add-spconfig command on the control domain after executing the dumpconfig command, restoring the logical domain configuration information with the restoreconfig command may not work correctly. Therefore, before restoring the XSCF settings information with the restoreconfig command, use the ldm remove-spconfig command on all of the control

domains to remove all the logical domain configuration information except factory-default. To check the dates of the configuration information files that have been saved by using the ldm add-spconfig command, execute the showdomainconfig command for all of the physical partitions.

For details of logical domain configuration information, see "Managing Domain Configurations" in the *Oracle VM Server for SPARC Administration Guide* of the version used.

Restoring the Setting Information From the USB Device on the Master XSCF

1. **Power off all physical partitions.**

2. **Connect the USB device containing the configuration file to a USB port on the XSCF unit panel (rear panel) of the master XSCF.**

3. **Specify the local USB device on the XSCF unit as the input file, and execute the restoreconfig command.**

```
XSCF> restoreconfig file:///media/usb_msd/backup-file.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
:
*** You will need to power-cycle the entire system after this operation
is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

The message displays the identification information in the configuration file to be restored.

4. **If the information is correct, enter "y" to restore the file.**
   The XSCF is rebooted.

5. **The session is disconnected once. Reconnect.**

6. **Remove the USB device from the USB port when the restoration has completed.**

Specifying the Target Directory and Restoring the Setting Information via a Network

1. **Power off all domains.**

2. **Specify the target directory, and execute the restoreconfig command.**

```
XSCF> restoreconfig ftp://server/backup/backup-sca-ff2-16.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
:
*** You will need to power-cycle the entire system after this operation
is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

The message displays the identification information in the configuration file to be restored.

3. **If the information is correct, enter "y" to restore the file.**

The XSCF is rebooted.

4. **The session is disconnected once. Reconnect.**

10.11 Saving/Restoring Logical Domain Configuration Information in the XSCF

This section describes how to save logical domain configuration information in XSCF and how to restore the saved configuration information.
For the method of saving/restoring logical domain configuration information in an XML file, see "10.12   Saving/Restoring Logical Domain Configuration Information in an XML File."

10.11.1 Saving/Displaying Logical Domain Configuration Information

You can save logical domain configuration information for individual physical partitions. To save configuration information, log in to the control domain of the target physical partition. The save destination for the saved configuration information is the service processor in the physical partition.

You can save up to eight sets of logical domain configuration information per physical partition. One of the saved sets reflects the state at factory shipment, and its name is factory-default. Since factory-default is already saved, you can save up to seven remaining sets of configuration information. By saving a variety of configuration patterns in advance, you can specify the appropriate logical domain configuration for business when restarting the physical partition. For details of logical domain configuration information, see "Managing Domain Configurations" in the *Oracle VM Server for SPARC Administration Guide* of the version used.

Saving Logical Domain Configuration Information

Execute the ldm command of Oracle VM Server for SPARC with the add-spconfig subcommand specified to save logical domain configuration information.

```
primary# ldm add-spconfig config_name
```

For config_name, specify the file name used to save logical domain configuration information to the XSCF.

Note - Make sure that each logical domain is in the "active" or "bound" state, and then save the logical domain configuration information.

Note - The add-spconfig subcommand cannot overwrite the configuration information in an

existing file. Before specifying the name of an existing file for config_name, you need to delete the existing file by using the remove-spconfig subcommand.

Displaying Logical Domain Configuration Information

You can display the logical domain configuration information on either the control domain of a physical partition or the master XSCF.

- Displaying information on the control domain of a physical partition
  Execute the ldm command of Oracle VM Server for SPARC with the list-spconfig subcommand specified to display the saved logical domain configuration information on the control domain.

```
primary# ldm list-spconfig
```

- Displaying information on the XSCF shell
  Use the showdomainconfig command of the XSCF firmware to display the saved logical domain configuration information on the XSCF shell.

```
XSCF> showdomainconfig -p ppar_id
```

For ppar_id, specify the PPAR-ID of the physical partition for the saved logical domain configuration information you wish to display. You can specify only a single integer from 0 to 15, depending on the system configuration.

Operation Procedure

1. **Switch from the XSCF shell to the control domain console of the target physical partition.**
   For details on how to switch to the control domain console, see "8.3   Switching to the Control Domain Console From the XSCF Shell."

2. **Execute the ldm list-spconfig command to display the currently saved logical domain configuration information.**

```
primary# ldm list-spconfig
```

3. **Execute the ldm add-spconfig command to save the logical domain status as configuration information.**
   The following example shows that the file named ldm_set1 is the save destination.

```
primary# ldm add-spconfig ldm_set1
```

4. **Execute the ldm list-spconfig command, and confirm that the configuration information was saved correctly.**

```
primary# ldm list-spconfig
```

10.11.2 Restoring Logical Domain Configuration Information

When restarting a physical partition, you can specify logical domain configuration information from a list of configurations saved for the physical partition. This can be useful when you want to restart it with a different logical domain configuration than the current configuration.

Note - To restore logical domain configuration information, the logical domain configuration information must have been saved in advance. For details, see "10.11.1 Saving/Displaying Logical Domain Configuration Information."

Restoring Saved Logical Domain Configuration Information

Execute the setdomainconfig command of the XSCF firmware as shown below to restore the logical domain configuration information saved on the control domain.

```
XSCF> setdomainconfig -p ppar_id [-i index]
```

For ppar_id, specify the PPAR-ID of the physical partition. You can specify only a single integer from 0 to 15, depending on the system configuration. For index, specify the index number of the configuration information. If omitted, you can specify an index number interactively while checking a list of saved configuration information.

Operation Procedure

1. **Execute the setdomainconfig command, and specify the logical domain configuration to be used when the physical partition is started next time.**
   The following example shows the logical domain configuration of PPAR-ID 0 being specified interactively during a check of a list of saved configuration information.

```
XSCF> setdomainconfig -p 0
PPAR-ID    :0
Booting config
(Current)  :ldm-set2
(Next)     :ldm-set2
-------------------------------------------------------------------------
Index      :1
config_name :factory-default
domains    :1
date_created:-
-------------------------------------------------------------------------
Index      :2
config_name :ldm-set1
domains    :8
date_created:'2012-08-08 11:34:56'
-------------------------------------------------------------------------
```

```
Index       :3
config_name :ldm-set2
domains     :20
date_created:'2012-08-09 12:43:56'
------------------------------------------------------------------------------
Select Index of Using config_name:2
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "ldm-set1".
Continue? [y|n] :y
XSCF>
```

The following example shows index number 1 being specified for PPAR-ID 0 to specify configuration information.

```
XSCF> setdomainconfig -p 0 -i 1
Index       :1
config_name :factory-default
domains     :1
date_created:-
------------------------------------------------------------------------------
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "factory-default".
Continue? [y|n] : y
XSCF>
```

Restoring Logical Domains to Their State at Factory Shipment

Execute the setdomainconfig command of the XSCF firmware as shown below to restore the logical domain configuration information to the state at factory shipment.

```
XSCF> setdomainconfig -p ppar_id -c default
```

For ppar_id, specify the PPAR-ID of the physical partition. You can specify only a single integer from 0 to 15, depending on the system configuration. To restore the state at factory shipment, specify -c default.

Operation Procedure

1. **Execute the setdomainconfig command, and specify the configuration information to be used at the logical domain restart time.**
   The following example shows the logical domain configuration of PPAR-ID 0 being restored to its state at factory shipment.

```
XSCF> setdomainconfig -p 0 -c default
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "factory-default".
Continue? [y|n] : y
XSCF>
```

10.12 Saving/Restoring Logical Domain Configuration Information in an XML File

This section describes how to save all logical domain configuration information in an XML file and how to restore the configuration information saved in an XML file. When information saved to the XSCF is lost, use an XML file to restore the system.

10.12.1 Saving/Confirming Logical Domain Configuration Information

You can save logical domain configuration information per physical partition in an XML file. To save logical domain configuration information in an XML file, log in to the control domain of the target physical partition.
For details, see "Managing Domain Configurations" in the *Oracle VM Server for SPARC Administration Guide* of the version used.

Saving Logical Domain Configuration Information

Execute the ldm list-constraints -x command of Oracle VM Server for SPARC to save logical domain configuration information.

```
primary# ldm list-constraints -x > file_name.xml
```

Designate a file name to save configuration information in file_name.xml.

Operation Procedure

1. **Switch from the XSCF shell to the control domain console of the target physical partition.**
   For details on how to switch to the control domain console, see "8.3   Switching to the Control Domain Console From the XSCF Shell."

2. **Execute the ldm list-spconfig command to confirm that the current logical domain configuration information is saved to the XSCF.**

Note - The ldm list-spconfig command lists the names of the saved domain configuration information. It does not show creation times, number of domains, or whether any saved configuration information matches the current domain configuration. An administrator needs to keep track of the saved configuration file names, what configurations they map to, and whether they match the current logical domain configuration. You can also use the showdomainconfig command to see the date/time of creation and number of logical domains in each saved configuration.

In the following example, the current configuration information is set to test1.

When the current configuration information is not stored on the XSCF, save the information using the ldm add-spconfig command.

```
primary# ldm list-spconfig
factory-default
test1 [current]
test2
test3
```

3. **Execute ldm list-constraints –x and save the logical domain configuration information in an XML file.**
   The example shows how to save the information in /ldm-set1.xml.

```
primary# ldm list-constraints -x > /ldm-set1.xml
```

4. **Execute commands such as the more command and confirm that the configuration information is stored in the XML file.**

```
primary# more /ldm-set1.xml
<?xml version="1.0"?>
<LDM_interfaceversion="1.3" xmlns:xsi=http://www.w3.org/2001/XMLSchema-instancce
```

To be prepared in case a saved XML file is lost, back up the file to other media.

Note - If a virtual function (VF) is assigned to a logical domain using the SR-IOV function, execute the ldm command to save the information set for each VF in advance.

10.12.2 Restoring Logical Domain Configuration Information

Execute the ldm init-system command to reflect the setting of the XML file that was saved, and execute the shutdown command to restart the control domain.

Restoring Saved Logical Domain Configuration Information

To restore the configuration information saved in the XML file, execute the ldm init-system command on the control domain as shown below.

```
primary# ldm init-system -i file_name.xml
```

Operation Procedure

1. **Confirm that the current logical domain configuration is factory-default.**

```
primary# ldm list-config | grep "factory-default"
factory-default [current]
```

If [current] is not displayed next to factory-default, the current logical domain configuration is not factory-default. In such case, follow the procedures below to change the current logical domain configuration to factory-default.

Specify factory-default and execute the ldm set-spconfig command.

```
primary# ldm set-spconfig factory-default
```

Execute the poweroff command of the XSCF firmware to power off the physical partition.

```
XSCF> poweroff -p ppar_id
```

2. **Execute the ldm init-system command to reflect the setting of the saved XML file.**
    This example displays how to restore the configuration information saved in /ldm-set1.xml.

```
primary# ldm init-system -i /ldm-set1.xml
Initiating a delayed reconfiguration operation on the primary
domain.
All configuration changes for other domains are disabled until
the primary
domain reboots, at which time the new configuration for the
primary domain
will also take effect.
```

3. **Execute the shutdown command to restart the control domain.**

```
primary# shutdown -y -g0 -i6
```

4. **Bind the resource to a logical domain other than the control domain to start the domain.**
    In the following example, the resource is bound to ldom1 to start the domain.

```
primary# ldm bind ldom1
primary# ldm start ldom1
```

10.13 Saving/Restoring the OpenBoot PROM Environment Variables

To restore logical domain configuration information from an XML file, record and save the OpenBoot PROM environment variables in the control domain before you change the logical domains to the factory-default configuration.
After changing to the factory-default configuration, restore the OpenBoot PROM environment variables using the saved information.

When saving/restoring the OpenBoot PROM environment variables, check the OpenBoot PROM environment variables by executing the printenv command of OpenBoot PROM and save the contents. Then, use the setenv command to restore.

10.13.1 Saving the OpenBoot PROM Environment Variables

This section describes the procedure for saving the OpenBoot PROM environment variables.

1. **Execute the printenv command to check the OpenBoot PROM environment variables.**

```
{0} ok printenv
Variable Name           Value                         Default Value
ttya-rts-dtr-off        false                         false
ttya-ignore-cd          true                          true
keyboard-layout
reboot-command
security-mode           none                          No default
security-password                                     No default
security-#badlogins     1                             No default
diag-switch?            false                         false
local-mac-address?      false                         true
fcode-debug?            false                         false
scsi-initiator-id       7                             7
oem-logo                                              No default
oem-logo?               false                         false
oem-banner                                            No default
oem-banner?             false                         false
ansi-terminal?          true                          true
screen-#columns         80                            80
screen-#rows            34                            34
ttya-mode               9600,8,n,1,-                  9600,8,n,1,-
output-device           virtual-console               virtual-console
input-device            virtual-console               virtual-console
auto-boot-on-error?     false                         false
load-base               16384                         16384
auto-boot?              false                         true
```

```
   os-root-device
   network-boot-arguments   host-ip=192.168.123.100, ...
   boot-command             boot                         boot
   boot-file
   boot-device              mydisk1 mydisk2 mydisk3  ...    disk net
   multipath-boot?          false                        false
   boot-device-index        0                            0
   use-nvramrc?             true                         false
   nvramrc                  devalias mydisk1 /pci@80 ...
   error-reset-recovery     boot                         boot
   {0} ok
```

2. **Save the output result to a text file.**

3. **If there is a variable with a value replaced with "..." in step 1, execute the
   printenv command with the corresponding variable specified.**
   The following example checks the boot-device variable.

```
{0} ok printenv boot-device
boot-device =             mydisk1 mydisk2 mydisk3 mynet
```

The following example checks the nvramrc settings.

```
   {0} ok printenv nvramrc
   nvramrc =               devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@
0/disk@p3,0:a
                           devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p0,0:a
                           devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p1,0:a
                           devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
                           h# 8 value video-mode
```

The following example checks the network-boot-arguments settings.

```
   {0} ok printenv network-boot-arguments
   network-boot-arguments =  host-ip=192.168.123.100,subnet-mask=255.255.255.
0,iscsi-target-ip=192.168.100.10,iscsi-target-name=iqn.2016-12.com.fujitsu:02:
iscsiboot,iscsi-lun=0
```

4. **Save the output result in step 3 to a text file.**

10.13.2   Restoring the OpenBoot PROM Environment Variables

This section describes the procedure for restoring the OpenBoot PROM environment
variables.

- When restoring other than nvramrc

1. **Check the OpenBoot PROM environment variables saved in a text file.**
2. **Execute the setenv command to restore the values and the printenv command to check the contents.**
   If you are planning to restore logical domain information using a saved XML file, set auto-boot? to "false" and security-mode to "none" prior to issuing the next reboot.

   The following example restores local-mac-address? to "false."

   ```
   {0} ok setenv local-mac-address? false
   local-mac-address? =    false
   {0} ok printenv local-mac-address?
   local-mac-address? =    false
   ```

   The following example restores boot-device to "mydisk1 mydisk2 mydisk3 mynet."

   ```
   {0} ok setenv boot-device mydisk1 mydisk2 mydisk3 mynet
   boot-device =           mydisk1 mydisk2 mydisk3 mynet
   {0} ok printenv boot-device
   boot-device =           mydisk1 mydisk2 mydisk3 mynet
   ```

   The following example restores use-nvramrc? to "true."

   ```
   {0} ok setenv use-nvramrc? true
   use-nvramrc? =          true
   {0} ok printenv use-nvramrc?
   use-nvramrc? =          true
   ```

- When restoring nvramrc

1. **Check the OpenBoot PROM environment variables saved in a text file.**
2. **Execute the nvedit command to set a value to nvramrc.**
   The following example writes the contents checked in step 1 to nvramrc.

```
{0} ok nvedit
   0: devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3,0:a
   1: devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0,0:a
   2: devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1,0:a
   3: devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
   4: h# 8 value video-mode
   5:
```

3. **Press the [Ctrl] and [C] keys to exit from nvedit and return to the ok prompt.**
4. **Execute the nvstore command to save the edit.**

```
{0} ok nvstore
```

5. **Execute the printenv command to check if nvramrc has been correctly written.**

```
   {0} ok printenv nvramrc
  nvramrc =              devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@
0/disk@p3,0:a
                         devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p0,0:a
                         devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p1,0:a
                         devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
                         h# 8 value video-mode
```

6. **If the OpenBoot PROM environment variable auto-boot? is "true," execute the setenv command to set it to "false."**

```
   {0} ok setenv auto-boot? false
```

7. **Execute the reset-all command to restart OpenBoot PROM.**

```
   {0} ok reset-all
```

8. **Then, boot Oracle Solaris and restore logical domain information using an XML file.**
   This allows the restoration of the OpenBoot PROM environment variables in all logical domains, except for security-password, in the physical partition including the control domain.

For details on restoring logical domain configuration information using an XML file, see "10.12   Saving/Restoring Logical Domain Configuration Information in an XML File."

For logical domains with security-mode set to command or full, ask the system administrator to set security-password.

10.14   Saving/Restoring the Contents of a Hard Disk

Regular backup of the contents of a hard disk is important for preventing a critical loss of data, such as from a hard disk failure.

The SPARC M12/M10 systems support redundant disk configurations using the hardware RAID function. The redundant disk configurations make system operation

highly reliable.

In preparation for possible data loss due to multiple disk failures, regular backup of the contents of the hard disks is necessary.

Examine the backup methods appropriate to the system in operation, and implement one. The methods of saving and restoring the contents of hard disks vary depending on the implemented backup method. Use a method that is appropriate with the implemented backup method.

10.15 Resetting a Logical Domain

Use the reset command of the XSCF firmware to reset the specified logical domain. Execute the command with a user account that has the platadm or fieldeng privilege. Alternatively, you can execute it with a user account that has the pparadm or pparmgr privilege for the physical partition to which the target logical domain belongs.

Note - The reset command forcibly resets the specified physical partition, so it may cause the failure of a disk, etc. Use the command only for emergency purposes, such as recovery of Oracle Solaris when it hangs up.

```
XSCF> reset -p ppar_id -g domainname sir | panic
```

For ppar_id, specify the PPAR-ID of the physical partition to which the logical domain to be reset belongs. You can specify only a single integer from 0 to 15, depending on the system configuration.
For domainname, specify the name of the logical domain to be reset.
To reset the logical domain itself, specify sir. To cause a panic in Oracle Solaris on the logical domain, specify panic.

Operation Procedure

1. **Execute the reset command to reset the specified logical domain. Enter "y" for the confirmation message.**
   The following example resets the guest domain ldom1 of PPAR-ID 00.

```
XSCF> reset -p 0 -g ldom1 sir
PPAR-ID:00 GuestDomain to sir:ldom1
Continue? [y|n] : y
00 ldom1 :Resetting

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the
 "showdomainstatus".
```

```
XSCF>
```

2. **Execute the showdomainstatus command, and confirm that the specified logical domain was reset.**
   The following example checks the status of the logical domains of PPAR-ID 0. OpenBoot initializing or OpenBoot Running appears at Status, which then eventually displays Solaris running.

```
XSCF> showdomainstatus -p 0
```

10.16 Causing a Panic in a Logical Domain

This section describes how to cause a panic in the specified logical domain.

After a panic in the target logical domain when the logical domain has an abnormal load increase, or the logical domain hangs up, a dump file is collected.

10.16.1 Causing a Panic in a Guest Domain

Execute the ldm panic-domain command of Oracle VM Server for SPARC from the control domain to cause a panic in the specified guest domain.
For details of the ldm command, see the *Oracle VM Server for SPARC Reference Manual* of the version used.

Note - The ldm panic-domain command forcibly causes a panic in the specified guest domain, so it may cause the failure of a disk, etc. Limit use of the command to emergencies, etc.

```
primary# ldm panic-domain ldom
```

For ldom, specify the name of the guest domain where the panic will occur.

Note - You can also cause a panic in a guest domain by using the reset command of the XSCF firmware. For details, see the reset(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

10.16.2 Causing a Panic in a Control Domain

Use the reset command of the XSCF firmware to cause a panic in the specified control

domain.
Execute the command with a user account that has the platadm or fieldeng privilege.
You can also execute it with a user account that has the pparadm or pparmgr
privilege for the target physical partition.

Note - The reset command forcibly causes a panic in the specified control domain, so it may
cause the failure of a disk, etc. Limit use of the command to emergencies, etc.

```
XSCF> reset -p ppar_id -g primary panic
```

For ppar_id, specify the physical partition ID associated with the control domain (the
domain belongs to the partition) where the panic will occur. You can specify an
integer from 0 to 15, depending on the system configuration.

The reset command is ignored while the input power is off and while the control
domain is shut down.

Operation Procedure

1. **Execute the reset command to cause a panic in the specified control domain.**
    The following example causes a panic in the control domain of physical partition
    ID 0.

```
XSCF> reset -p 0 -g primary panic
PPAR-ID:00
GuestDomain to panic:primary
Continue? [y|n] : y
00 primary :Resetting

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the
 "showdomainstatus".
XSCF>
```

2. **Execute the showdomainstatus command and confirm that a panic occurred
    in the specified control domain.**

```
XSCF> showdomainstatus -p 0
```

10.17   Resetting a Physical Partition

Use the reset command of the XSCF firmware to reset the specified physical partition.
Execute the command with a user account that has the platadm or fieldeng privilege.

Alternatively, you can also execute it with a user account that has the pparadm or pparmgr privilege for the target physical partition.

Note - The reset command forcibly resets the specified physical partition, so it may cause the failure of a disk, etc. Use the command only for emergency purposes, such as recovery of Oracle Solaris when it hangs up.

```
XSCF> reset -p ppar_id por | xir
```

For ppar_id, specify the PPAR-ID of the physical partition to be reset. You can specify only a single integer from 0 to 15, depending on the system configuration. To reset the physical partition itself, specify por. To reset all the CPUs in the physical partition, specify xir.

Note - If the physical partition is reset with xir specified and Hypervisor dump enabled, a Hypervisor dump is collected, and then logical domains start in the factory-default configuration after the reset. To return to the logical domain configuration from before the physical partition reset, power off the physical partition once, and then power it on again. For details of the Hypervisor dump function, see "8.13 Collecting a Hypervisor Dump File."

If the auto boot function for the control domain as set by the setpparparam command is disabled when the reset command is executed, the processing stops before Oracle Solaris starts.

Operation Procedure

1. **Execute the reset command to reset the specified physical partition. Enter "y" for the confirmation message.**
   The following example resets PPAR-ID 00.

```
XSCF> reset -p 0 por
PPAR-ID to reset:00 Continue? [y|n] : y
00 :Resetting

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

2. **Execute the showpparprogress command, and confirm that the specified physical partition was reset.**

```
XSCF> showpparprogress -p 0
PPAR Power On Preprocessing PPAR#0 [ 1/12]
PPAR Power On              PPAR#0 [ 2/12]
XBBOX Reset                PPAR#0 [ 3/12]
PSU On                     PPAR#0 [ 4/12]
CMU Reset Start                PPAR#0 [ 5/12]
XB Reset 1                 PPAR#0 [ 6/12]
```

```
XB Reset 2                PPAR#0 [ 7/12]
XB Reset 3                PPAR#0 [ 8/12]
CPU Reset 1               PPAR#0 [ 9/12]
CPU Reset 2               PPAR#0 [10/12]
Reset released            PPAR#0 [11/12]
CPU Start                 PPAR#0 [12/12]
The sequence of power control is completed.
XSCF>
```

10.18 Returning the Server to the State at Factory Shipment

This section describes how to return the SPARC M12/M10 to the state at factory shipment.
To restore the backup data of the XSCF settings information in the SPARC M12/M10 chassis, or to return the XSCF settings information in the XSCF unit to its state at factory shipment, execute the initbb command or restoredefaults command of the XSCF firmware.

Caution - Execution of the command deletes the user-defined XSCF unit setting information and error information, or it deletes the XSCF backup information on each chassis.

10.18.1 Understanding Initialization Commands

The initbb and restoredefaults commands have the following roles.

- **restoredefaults command**
  This command initializes the master XSCF chassis. The command initializes both the XSCF unit setting information and its backup information, or it initializes only the XSCF unit setting information.

- **initbb command**
  This command initializes, from the master XSCF, information for a chassis other than the master chassis. The command cannot be used on systems that have one XSCF.

Note - The restoredefaults command restores the XSCF settings information and backup information to the state at factory shipment.

Note - If a CPU Activation key has not been saved and the restoredefaults command is executed, the CPU Activation key will need to be registered again.

10.18.2 Initializing the Server

In the Systems With One XSCF

Use the restoredefaults command to initialize the server.

Operation Procedure

1. **Establish a serial connection with the XSCF.**
2. **Log in to the XSCF.**
3. **Execute the poweroff -a command to stop the system.**
4. **Execute the restoredefaults command to initialize the chassis (the XSCF unit setting information and its backup information) or XSCF unit setting information.**

Note - For details on how to specify options of the restoredefaults command and the related notes, see the restoredefaults(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

In the Systems With Multiple XSCFs

Initialization has the following prerequisites.
- Each chassis is connected to the XSCF network.
- If the PPAR-ID of a physical partition in operation is the same as the BB-ID of the chassis to be initialized, that physical partition must be powered off.
- The PSB of the chassis to be initialized is in the system board pool state.
- The PSB of the chassis to be initialized does not belong to any PPAR.
- If a crossbar box other than the master XSCF is to be initialized, the poweroff -a command must be executed to stop the system.

Operation Procedure

1. **To initialize the master XSCF, execute the poweroff command with the -a option specified to stop the system.**
2. **Establish a serial connection with the master XSCF.**
3. **Log in to the master XSCF.**
4. **Initialize the target chassis by specifying its BB-ID and executing the initbb command.**
   Perform this step for a target other than the master.

   Next, to initialize the master chassis, perform the following steps.
5. **Execute the restoredefaults command to initialize the chassis (the XSCF unit setting information and its backup information) or XSCF unit setting information.**

Note - For details on how to specify options of the initbb(8) and restoredefaults(8) commands and the related notes, see the man page of each command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Note - For details on how to connect cables, see "Chapter 4   Setting the SPARC M12-2S in a Building Block Configuration" in the *Fujitsu SPARC M12-2S Installation Guide* or "Chapter 4 Configuring Building Block Connections" in the *Fujitsu M10-4S/SPARC M10-4S Installation Guide*.

Note - For details of support information on this command, see the latest *Product Notes* for your server.

10.19   Collecting a Crash Dump File Using Deferred Dump

In XCP 2290 or later and Oracle Solaris 11.2 SRU11.2.8.4.0 or later, the crash dump file may be saved in memory until the system is rebooted after the system crashes. During the rebooting of the system, the crash dump file is extracted from memory to the file system defined by the dump configuration.
After these files are written, the system is automatically rebooted to the normal multi-user configuration.
This process is called deferred dump. When this deferred dump is used, the system can return to the operational status in a short period after the kernel panic.
For details on deferred dump functions, see the *Managing Devices in Oracle Solaris* for your Solaris version.

Chapter 11

Checking the System Status

This chapter describes how to check the system hardware configuration/status and physical partition configuration/status when configuring or operating the system.

- Checking the System Configuration/Status
- Checking a Physical Partition

11.1 Checking the System Configuration/Status

11.1.1 Checking the Items and Commands Related to the System Configuration/Status

Table 11-1 lists the items and XSCF shell commands for checking the system configuration/status.

For details of individual items, see the subsequent sections.

Table 11-1   Commands for Checking the Configuration and Status

Check Item	Related Command
Checking mounted components - All mounted parts in the system - Mode switch state	showhardconf(8)
Checking failed/degraded components	showstatus(8)

Table 11-1   Commands for Checking the Configuration and Status *(continued)*

Check Item	Related Command
Checking system environment information - Ambient temperature - Voltage - Fan speed level - Power consumption - Exhaust airflow	showenvironment(8)
Checking PCI expansion unit setting information	ioxadm(8)

11.1.2   Checking Mounted Components in the System

You can check all the mounted components in the system and their status by using the showhardconf command. The command displays an asterisk (*) to mark a part that has a problem. The system administrator can get a grasp of the component configuration, number of mounted units, Mode switch state, and field replaceable units (FRUs).

Component Information

Table 11-2 lists information of each component of the SPARC M12. You can check the component details in a hierarchical structure by executing the showhardconf command.

Table 11-2   Information of Each Component of the SPARC M12

Component	Description
System information	Serial number, mode switch status, system power status, system power phase, physical partition status
SPARC M12-2/M12-2S information	Unit number, status, role, version, serial number, FRU number, input power type, memory capacity The role appears as Master, Standby, or Slave.
CPU memory unit (lower) (CMUL) information (SPARC M12-2/M12-2S)	Status, version, serial number, FRU number, memory capacity, type
CPU memory unit (upper) (CMUU) information (SPARC M12-2/M12-2S)	Status, version, serial number, FRU number, memory capacity, type
Motherboard unit (MBU) information (SPARC M12-1)	Status, version, serial number, FRU number, memory capacity, type
CPU information	Unit number, status, version, serial number, CPU operating frequency, CPU type, number of CPU cores, number of CPU strands
Memory (MEM) information	Unit number, status, code, type (unique ID), capacity

Table 11-2   Information of Each Component of the SPARC M12 *(continued)*

Component	Description
PCI information	Unit number, status, name property, vendor ID, device ID, subsystem vendor ID, subsystem ID, VPD number, connection, PCI expansion unit information
PCI expansion unit (PCIBOX) information	Unit number, status, version, serial number, FRU number IO board (IOB) information: Status, serial number, type, FRU number Link board information: Status, version, serial number, FRU number PCI information: Unit number, name property, vendor ID, device ID, subsystem vendor ID, subsystem ID, VPD number Fan backplane (FANBP) information: Unit number, status, serial number, FRU number PSU backplane (PSUBP) information: Unit number, status, serial number, FRU number Power supply unit (PSU) information: Unit number, status, serial number, FRU number Fan unit (FAN) information: Unit number, status
Crossbar unit (XBU) information (SPARC M12-2/M12-2S)	Unit number, status, version, serial number, FRU number, type
Crossbar cable (CBL) information	Unit number, status, vendor ID, version, cable type, length
XSCF unit (XSCFU) information	Status, version, serial number, FRU number, type
Operation panel (OPNL) information	Status, version, serial number, FRU number, type
PSU backplane (PSUBP) information	Status, version, serial number, FRU number, type
Power supply unit (PSU) information	Unit number, status, serial number, FRU number, power state, power supply type, voltage, type The power supply type is AC (alternating current).
Fan unit (FANU) information	Unit number, status, type
HDD backplane (HDDBP) information	Unit number, status, type
Crossbar box (XBBOX) information (SPARC M12-2S)	Unit number, status, role, version, serial number, FRU number, input power type Crossbar unit (XBU) information: Unit number, status, version, serial number, FRU number, type Crossbar cable (CBL) information: Unit number, status, FRU number, version, cable type, length XSCF unit (XSCFU) information: Status, version, serial number, FRU number Operation panel (OPNL) information: Status, version, serial number, FRU number Crossbar backplane (XBBPU) information: Status, version, serial number, FRU number, type XSCF interface unit (XSCFIFU) information: Status, version, serial number, FRU number, type

Table 11-3 lists information of each component of the SPARC M10. You can check the component details in a hierarchical structure by executing the showhardconf command.

Table 11-3   Information of Each Component of the SPARC M10

Component	Description
System information	Serial number, mode switch status, system power status, system power phase, physical partition status
SPARC M10-4/M10-4S information	Unit number, status, role, version, serial number, FRU number, input power type, memory capacity The role appears as Master, Standby, or Slave.
CPU memory unit (lower) (CMUL) information (SPARC M10-4/M10-4S)	Status, version, serial number, FRU number, memory capacity, type
CPU memory unit (upper) (CMUU) information (SPARC M10-4/M10-4S)	Status, version, serial number, FRU number, memory capacity, type
Motherboard unit (MBU) information (SPARC M10-1)	Status, version, serial number, FRU number, memory capacity, type
CPU information	Unit number, status, version, serial number, CPU operating frequency, CPU type, number of CPU cores, number of CPU strands
Memory (MEM) information	Unit number, status, code, type (unique ID), capacity
PCI information	Unit number, status, name property, vendor ID, device ID, subsystem vendor ID, subsystem ID, VPD number, connection, PCI expansion unit information
PCI expansion unit (PCIBOX) information	Unit number, status, version, serial number, FRU number IO board (IOB) information: Status, serial number, type, FRU number Link board information: Version, serial number, FRU number PCI information: Unit number, name property, vendor ID, device ID, subsystem vendor ID, subsystem ID, VPD number Fan backplane (FANBP) information: Unit number, status, serial number, FRU number PSU backplane (PSUBP) information: Unit number, status, serial number, FRU number Power supply unit (PSU) information: Unit number, status, serial number, FRU number Fan unit (FAN) information: Unit number, status
Crossbar unit (XBU) information (SPARC M10-4/M10-4S)	Unit number, status, version, serial number, FRU number, type
Crossbar cable (CBL) information	Unit number, status, FRU number, version, cable type, length
Operation panel (OPNL) information	Status, version, serial number, FRU number

Table 11-3 Information of Each Component of the SPARC M10 *(continued)*

Component	Description
XSCF unit (XSCFU) information	Status, version, serial number, FRU number
PSU backplane (PSUBP) information	Status, version, serial number, FRU number, type
Power supply unit (PSU) information	Unit number, status, serial number, FRU number, power state, power supply type, voltage, type The displayed power supply type is AC (alternating current) or DC (direct current).
Fan unit (FANU) information	Unit number, status, type
Crossbar box (XBBOX) information (SPARC M10-4S)	Unit number, status, role, version, serial number, FRU number, input power type Crossbar unit (XBU) information: Unit number, status, version, serial number, FRU number, type Crossbar cable (CBL) information: Unit number, status, FRU number, version, cable type, length XSCF unit (XSCFU) information: Status, version, serial number, FRU number Operation panel (OPNL) information: Status, version, serial number, FRU number Crossbar backplane (XBBPU) information: Status, version, serial number, FRU number, type XSCF interface unit (XSCFIFU) information: Status, version, serial number, FRU number, type

Operation Procedure

1. **Execute the showhardconf command to check the component configuration and Mode switch state.**
   The following example displays the SPARC M10-1 system.

```
XSCF> showhardconf
SPARC M10-1;
    + Serial:2101151008A; Operator_Panel_Switch:Locked;
    + System_Power:On; System_Phase:Cabinet Power On;
      Partition#0 PPAR_Status:Powered Off;
    MBU Status:Normal; Ver:0101h; Serial:7867000297;
        + FRU-Part-Number:CA20393-B50X A2 ;
        + Power_Supply_System:Single;
        + Memory_Size:16 GB;
        CPU#0 Status:Normal; Ver:0201h; Serial:PP0629L068
            + Freq:2.800 GHz; Type:32;
            + Core:16; Strand:2;
        MEM#00A Status:Normal;
 :
```

2. **Execute the showhardconf command to check the number of mounted FRUs.**
   In the following example, the -u option is specified to display the number of
   FRUs mounted in the SPARC M10-1 system.

```
XSCF> showhardconf -u
SPARC M10-1; Memory_Size:16 GB;
+----------------------------------+------------+
| FRU                              | Quantity   |
+----------------------------------+------------+
| MBU                              |     1      |
|     CPU                          |     1      |
|         Freq:2.800 GHz;          |    ( 1)    |
|     MEM                          |    16      |
|         Type:01; Size:4 GB;      |    ( 16)   |
| PCIBOX                           |     1      |
|     IOB                          |     1      |
|     PSU                          |     2      |
|     FAN                          |     2      |
| OPNL                             |     1      |
| PSUBP                            |     1      |
|     PSU                          |     2      |
|     FAN_A                        |     2      |
+----------------------------------+------------+
```

11.1.3   Checking the System Environment

The showenvironment command displays all of the system sensor values. With
knowledge of the system intake temperature, voltage, and fan speed, the system
administrator can check for any abnormalities in the system operating environment.
Also, with knowledge of the power consumption and exhaust airflow of the system,
the facility manager can identify potential energy reductions at parts of the system
installation site.

Operation Procedure

1. **Execute the showenvironment command to check the system environment
   information and voltages.**
   The following example displays the intake temperatures.

```
XSCF> showenvironment
BB#00
    Temperature:30.71C
BB#01
    Temperature:29.97C
```

The following example specifies the temp operand to display the temperatures
of components.

```
XSCF> showenvironment temp
BB#00
    Temperature:30.71C
    CMUU
        CPU#0
        CPU#0:45.21C
        CPU#0:45.42C
        CPU#0:43.24C
        CPU#0:47.11C
    CPU#1
        CPU#1:45.21C
        CPU#1:45.42C
        CPU#1:43.24C
        CPU#1:47.11C
...
```

The following example specifies the volt operand to display the voltages of components.

```
XSCF> showenvironment volt
MBU
    0.89V Power Supply Group:0.891V
    0.90V#0 Power Supply Group:0.898V
    0.90V#1 Power Supply Group:0.894V
    0.90V#2 Power Supply Group:1.023V
    0.90V#3 Power Supply Group:1.024V
    1.0V#0 Power Supply Group:1.038V
    1.0V#1 Power Supply Group:1.041V
    1.35V#0 Power Supply Group:1.346V
    1.35V#1 Power Supply Group:1.348V
    1.5V#0 Power Supply Group:1.539V
    1.5V#1 Power Supply Group:1.506V
    1.8V#0 Power Supply Group:1.804V
PSUBP
    3.3V Power Supply Group:3.300V
    5.0V Power Supply Group:5.000V
XSCF>
```

Ambient Temperature and Fan Speed Level

As a result of setting the altitude of the installation location, the fan speed level varies according to the ambient temperature. The higher the level number for the fan speed level, the faster the fan speed.

Table 11-4 lists the fan speed levels displayed by the showenvironment command, for the corresponding set altitudes and ambient temperatures.

Table 11-4   Fan Speed Levels Corresponding to Altitude and Ambient Temperature
             (Common to the SPARC M12/M10)

Fan Speed Level	Ambient Temperature by Altitude			
	500 m or Lower	501 to 1000 m	1001 to 1500 m	1501 to 3000 m
High speed (level-3 ->level-4)	31°C or higher	29℃ or higher	27℃ or higher	25℃ or higher
Middle speed (level-4 ->level-3)	29°C or lower	27℃ or lower	25℃ or lower	23℃ or lower
Middle speed (level-2 ->level-3)	26℃ or higher	24℃ or higher	22℃ or higher	20℃ or higher
Low speed (level-3 ->level-2)	24℃ or lower	22℃ or lower	20℃ or lower	18℃ or lower
Low speed (level-1 ->level-2)	22℃ or higher	20℃ or higher	18℃ or higher	16℃ or higher
Low speed (level-2 ->level-1)	20℃ or lower	18℃ or lower	16℃ or lower	14℃ or lower

Operation Procedure

1. **Execute the showenvironment command to check the fan speed level.**
   The following example specifies the Fan operand to display the fan speed level
   of the fan units.

```
XSCF> showenvironment Fan
BB#00
    FANU#0: Middle speed (Level-3)
        FAN#0: 14323rpm
        FAN#1: 14285rpm
    FANU#1: Middle speed (Level-3)
        FAN#0: 14173rpm
        FAN#1: 14285rpm
    FANU#2: Middle speed (Level-3)
        FAN#0: 14248rpm
        FAN#1: 14136rpm
    FANU#3: Middle speed (Level-3)
        FAN#0: 14099rpm
        FAN#1: 14062rpm
    FANU#4: Middle speed (Level-3)
        FAN#0: 14323rpm
        FAN#1: 14099rpm
```

Power Consumption and Exhaust Airflow

Use the power monitor function and airflow indicator to display the power
consumption and exhaust airflow of the system. The power monitor function and
airflow indicator enable routine checks of the amount of actual power consumption
by the system in operation, as well as the exhaust airflow volume.

Use the showenvironment power command to display the power consumption. The command displays the power consumption value of the system, the maximum power consumption value (Permitted AC power consumption) and actual power consumption value (Actual AC power consumption) in the chassis, etc. If the power supply type is DC, "...DC power..." is displayed instead.

Note - In SPARC M12 systems, the rated power consumption in the chassis is displayed as "Available AC power consumption."

Use the showenvironment air command to display the exhaust airflow. The SNMP agent function can also be used to acquire power consumption and exhaust airflow information.
To acquire power consumption and exhaust airflow information through the SNMP agent function, install the latest XSCF extended MIB definition file for the SNMP manager. For the place to obtain the XSCF extended MIB definition file, see the latest *Product Notes* for your server or the MIB definition file-related information at the firmware download site.

Note - In the following cases, the power consumption and exhaust airflow values may not be correctly displayed by MIB information, the showenvironment power command, the showenvironment air command, and XSCF Web. Check the values again after one minute.

- During system power-on/off or during a short period after the power-on/off is completed
- During active replacement of a power supply unit or during a short period after the active replacement is completed

Note - The PCI expansion unit and peripheral I/O devices are not included in power consumption and exhaust airflow information.

Operation Procedure

1. **Execute the showenvironment command to check the exhaust airflow of the system.**
    The following example specifies the air operand to display the exhaust airflow of the system.

```
XSCF> showenvironment air
BB#00
    Air Flow:306CMH
```

Note - The unit of exhaust airflow (CMH = m^3/h) indicates how many cubic meters of airflow are generated per hour.

2. **Execute the showenvironment command to check the power consumption of the system.**
    The following example specifies the power operand to display power

consumption information. The display content shows, from the top, the
maximum power supply value of the power supply unit (PSU) for the entire
system, the minimum power consumption value and maximum power
consumption value of the system, followed by the maximum power consumption
value and actual power consumption value of the chassis.

```
XSCF> showenvironment power
Power Supply Maximum :5000W
Installed Hardware Minimum:1268W
Peak Permitted :2322W
BB#00
Permitted AC power consumption:5000W
Actual AC power consumption :1719W
```

Note - The measurement values of the power monitor and airflow indicator are reference
values. Their values vary depending on the system load.

11.1.4　Checking Failed/Degraded Components

By using the showstatus command, you can check some failed or degraded units and
components among the FRUs that make up the system. A unit or component whose
status is failure is marked with an asterisk (*).

There are five types of status as shown in Table 11-5.

Table 11-5　　Component Status

Component	Meaning
Faulted	The part in question has failed, so the unit is not operating.
Degraded	There is a partial failure within the unit, but the unit is continuing to operate.
Deconfigured	As a result of failure or degradation in another unit, the unit, including lower-level components, is in the state of degradation, even though it is operating normally.
Maintenance	The unit is under maintenance. The replacefru, addfru, or initbb command is running.
Normal	The unit is normal.

Operation Procedure

1. **Execute the showstatus command to check the component status.**
   A unit whose status is failure is marked with an asterisk (*).

   The following example shows that a CPU and memory on the CPU memory unit
   (lower) of BB#00 and the PSU of XBBOX#80 have been degraded because of

failures.

```
XSCF> showstatus
   BB#00;
      CMUL Status:Normal;
*        CPU#0 Status:Faulted;
*        MEM#00A Status:Faulted;
   XBBOX#80;
*     PSU#0 Status:Faulted;
```

The following example shows that memory on the motherboard unit has been degraded because of a failure.

```
XSCF> showstatus
   MBU Status:Normal;
*       MEM#0A Status:Faulted;
```

The following example shows that a CPU memory unit has been degraded because of the degradation of the crossbar unit.

```
XSCF> showstatus
   BB#00
      CMUU Status:Normal;
*        CPU#1 Status:Deconfigured;
*     XBU#0 Status:Degraded;
```

The following example shows that no units are degraded.

```
XSCF> showstatus
No failures found in System Initialization.
```

Note - The failure and degradation information about a failed/degraded component is cleared by the replacement of the relevant part. For parts replacement work, contact a field engineer.

11.1.5   Displaying the PCI Expansion Unit Status

This section describes how to check the PCI expansion unit connected to the system, the parts in the PCI expansion unit, a link card mounted in a built-in PCI slot of the system, and the PCI expansion unit status.

You can check the PCI expansion unit status and settings by using the ioxadm command.

Note - For details of the PCI expansion unit hardware configuration, see "Chapter 2

Understanding the PCI Expansion Unit Components" in the *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*. For details or usage examples of the ioxadm command, see the ioxadm(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Displayed Information

Table 11-6 outlines the information displayed by the executed ioxadm command.

Table 11-6   Displayed PCI Expansion Unit Information

Display Item	Description
List display (list)	- List of paths (host_path) between the PCI expansion unit and link cards mounted in chassis slots - Detailed information on the PCI expansion unit - Detailed information on FRUs (I/O board, power supply unit, etc.) in the PCI expansion unit The displayed information includes the FRU type, firmware version, serial number, part number, and status.

Environment display (env)	- Environmental conditions according to sensor measurement values of the specified PCI expansion unit or link card
	- Environment information on FRUs in the PCI expansion unit or cards mounted in PCI slots
	The displayed information includes the following:
	  - Current (A)
	  - Voltage (V)
	  - Fan speed (RPM)
	  - Temperature (C)
	  - LED status
	  - SWITCH

Locator LED display (locator)	- Locator LED states of the specified PCI expansion unit and each part in the PCI expansion unit
	The locator LED states are as follows:
	  - Blinking
	  - On
	  - Off

Version comparison result (versionlist)	Displays the PCI expansion unit firmware version, connection destination link card firmware version, and the result of comparing these firmware.
	The comparison results are as follows.
	  - equal
	  - mismatch

List Display

The procedure for displaying a list of the PCI expansion unit, I/O boards, link cards, and power supply units is described below.

1. **Execute the ioxadm command to check the PCI expansion unit and link cards.**
   In the following example, a list of all PCI expansion units and link cards is displayed.

```
XSCF> ioxadm list
PCIBOX      Link
PCIBOX#0033 BB#00-PCI#1
PCIBOX#12B4 BB#01-PCI#0
```

The following example displays a single PCI expansion unit.

```
XSCF> ioxadm list PCIBOX#12B4
PCIBOX      Link
PCIBOX#12B4 BB#01-PCI#0
```

The following example uses host_path to display cards in detailed output mode with the headers hidden.

```
XSCF> ioxadm -A -v list BB#00-PCI#1
BB#00-PCI#1 F20 - 000004 5111500-01 On
```

Environment Display

The procedure for displaying the environment by using sensor measurement values is described below.

1. **Execute the ioxadm command to check environment information.**
   The following example displays the sensor measurement values of temperature, voltage, current, fan speed, etc.

```
XSCF> ioxadm env -te PCIBOX#A3B4
Location Sensor Value Res Units

PCIBOX#A3B4/PSU#0 FAN 3224.324 - RPM
PCIBOX#A3B4/PSU#1 FAN 3224.324 - RPM
PCIBOX#A3B4/FAN#0 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#1 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#2 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#0 FAN 3522.314 - RPM
PCIBOX#A3B4/IOBT T_INTAKE 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO1 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO2 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO3 32.000 - C
PCIBOX#A3B4/IOBT V_12_0V 12.400 - V
PCIBOX#A3B4/IOBT V_3_3_NO0 3.320 - V
PCIBOX#A3B4/IOBT V_3_3_NO1 3.310 - V
PCIBOX#A3B4/IOBT V_3_3_NO2 3.310 - V
PCIBOX#A3B4/IOBT V_3_3_NO3 3.320 - V
PCIBOX#A3B4/IOBT V_1_8V 1.820 - V
PCIBOX#A3B4/IOBT V_0_9V 0.910 - V
```

The following example displays all the sensor measurement values relating to one link.

```
XSCF> ioxadm -A env BB#00-PCI#1
BB#00-PCI#1 LINK On - LED
BB#00-PCI#1 MGMT On - LED
```

Location Display

The procedure for displaying the locator LED states of the PCI expansion unit and specified parts is described below.

1. **Execute the ioxadm command to check the PCI expansion unit status.**
   The following example displays the locator LED state of the PCI expansion unit.

```
XSCF> ioxadm locator PCIBOX#12B4
Location            Sensor     Value Resolution Units
PCIBOX#12B4         LOCATE     Blink -           LED
```

Version Comparison Result

The method of displaying the PCI expansion unit firmware version, connection destination link card firmware version, and the comparison result is as follows.

1. **Execute the ioxadm command to confirm the PCI expansion unit firmware version, connection destination link card firmware version, and the comparison result.**
   In the following example, the result of comparing all PCI expansion units and link cards is displayed.

```
XSCF> ioxadm versionlist
  PCIBOX       Ver. Link        Ver. Info
  PCIBOX#0033 1010 BB#00-PCI#1 1010 equal
* PCIBOX#12B4 1010 BB#00-PCI#0 1011 mismatch
```

11.2 Checking a Physical Partition

11.2.1 Checking the Items and Commands Related to the Configuration/Status of Physical Partitions and Logical Domains

Table 11-7 lists the items and XSCF shell commands for checking the physical partition configuration/status, building block (PSB) status, and logical domain status. For details of individual items, see the subsequent sections.

Table 11-7   Commands for Checking the Configuration and Status

Check Item	Related Command
Checking physical partition configuration information - PPAR-ID - LSB number - PSB number - Configuration policy - Availability of I/O - Availability of memory	showpcl(8)
Checking the physical partition operation status	showpparstatus(8), showpcl(8)
Checking the PSB setting - Location (PSB, CPU) - Memory mirror mode	showfru(8)
Checking the PSB status	showboards(8)
Checking the logical domain status	showdomainstatus(8) Commands of Oracle VM Server for SPARC

Note - For details of the physical partition settings/configuration/status and configuring logical domains from a physical partition, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

11.2.2   Checking the Physical Partition Configuration

The showpcl command displays the configuration information for each physical partition or each logical system board that makes up the physical partition. The system administrator refers to a PCL (physical partition configuration list) when incorporating a logical system board into a physical partition.
You can check the PCL of the specified physical partition by using the showpcl command.

The mapping between the logical system boards (LSBs) on the physical partition and the physical system boards (PSBs) is determined by the PCL information. Figure 11-1 shows an example of a PCL mapping.
PSB refers to a hardware resource to configure a physical partition. Specify (or display) a PSB in xx-y format. xx is BB-ID, and y is fixed at 0.

Figure 11-1   Image of the Mapping Between Logical System Boards and System Boards
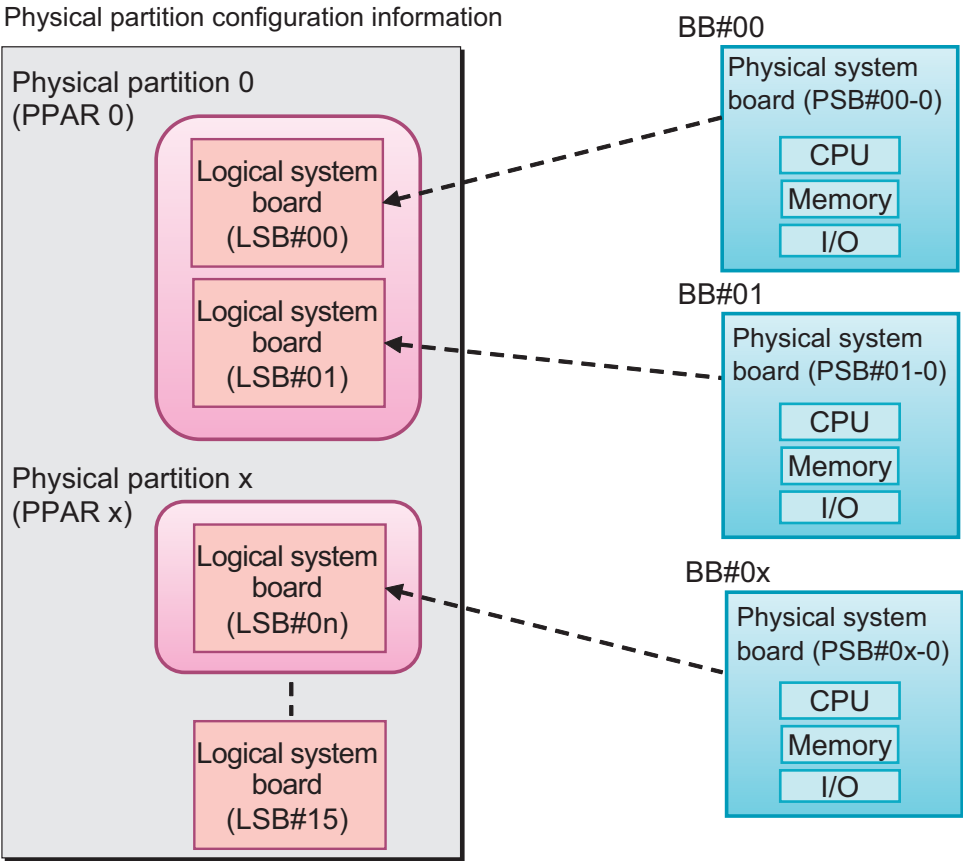
Table 11-8 describes terms related to physical partitions.

Table 11-8   Terms Related to Physical Partitions

Term	Description
Physical system board (PSB)	PSB stands for physical system board. The PSB consists of physical components (CPU, memory, and I/O) mounted in one SPARC M12/M10 chassis. In the SPARC M12-1/M10-1, a physical system board is a motherboard unit. In the SPARC M12-2/M12-2S/M10-4/M10-4S, a physical system board is a CPU memory unit (including lower (CMUL) and higher (CMUU)). A physical system board may be used as the unit representing a chassis, in maintenance for adding/removing/replacing a SPARC M12/M10 chassis. For a system in a building block configuration, a physical system board refers to one building block (BB).

Table 11-8   Terms Related to Physical Partitions *(continued)*

Term	Description
Logical system board (LSB)	LSB stands for logical system board. Logical unit names are assigned to a PSB. Each physical partition has a set of logical system boards assigned to it. With one PSB number assigned to the logical system boards in the physical partition, they can be recognized in the system. LSB numbers are used to control the assignment of resources such as memory to the physical partition.
Physical partition configuration	This term refers to the partitioning of system hardware resources into independent units for software operation. A physical partition is a PSB cluster, and the system consists of one or multiple physical partitions. A physical partition is configured using the XSCF as follows. 1. Assign LSB numbers to the PSB. 2. Assign the PSB to a physical partition. 3. The physical partition operates with LSB resources and the LSB numbers.
Physical partition configuration information	This term refers to the hardware resource information configured for each physical partition or each LSB that makes up the physical partition. The setpcl and showpcl commands can set and display, respectively, the PCL.
Configuration policy	This policy can specify the unit of logical resources to be degraded for each physical partition when an error is detected in an initial hardware diagnosis. The configuration policy specifies a PSB or discrete resources as the degradation range.
I/O disabled (no-io)	This term refers to when the logical use of the I/O unit on the PSB is disabled in the physical partition.
Memory disabled (no-mem)	This term refers to when the logical use of the memory on the PSB is disabled in the physical partition.
PSB status	This status of each PSB shows the power status (power), diagnosis status (test), assignment status (assignment), incorporation status (connection), operation status (configuration), and degradation status (fault). You can learn the progress of PSB status change in the physical partition. You can refer to PSB status information by using the showpcl and showboards commands.
System board pool (SP)	This term refers to the state of BBs (PSBs) that do not belong to any physical partition. For a physical partition with a high CPU or memory load, a BB (PSB) can be added to this physical partition. At the point when the system board is no longer needed, it can be returned to the system board pool.

A PCL is a definition list for setting the information for one LSB. You can set LSB information for up to 16 LSBs per physical partition.

Table 11-9 lists details of physical partition configuration information. The configuration policy can be set only in the SPARC M12-2/M10-1/M10-4 systems.

Table 11-9   PCL

Term	Description
PPAR-ID	ID of a PPAR
LSB number	LSB number
PSB number	PSB number assigned to an LSB. The same PSB number cannot be assigned to another LSB within the same physical partition.
no-mem (Memory nullification option)	True: Memory cannot be used False: Memory can be used (Default)
no-io (I/O nullification option)	True: I/O not incorporated False: I/O incorporated (Default)
Configuration policy	FRU: Degradation is performed in units of field replaceable units (FRUs). (Default) PSB: Degradation is performed in units of PSBs. System: Physical partitions are powered off, in units of physical partitions, without degradation.
Physical partition status	This indicates the physical partition operation status, such as whether the power is off or whether POST initialization has completed. For detailed definitions, see the showpcl(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operation Procedure

1. **Execute the showpcl command to check PCL information.**
    The following example displays the set PCL information for PPAR-ID 00.

```
XSCF> showpcl -p 0
PPAR-ID   LSB     PSB    Status
00                       Running
          00      00-0
          04      01-0
          08      02-0
          12      03-0
```

The following example displays the set PCL information for PPAR-ID 00 in detail.

```
XSCF> showpcl -v -p 0
PPAR-ID   LSB     PSB    Status  No-Mem   No-IO   Cfg-policy
00                       Running
                                                  System
          00      -
          01      -
          02      -
```

```
                          03      -
                          04      01-0            False     False
                          05      -
                          06      -
                          07      -
                          08      02-0            True      False
                          09      -
                          10      -
                          11      -
                          12      03-0            False     True
                          13      -
                          14      -
                          15      -
```

Note - For details of physical partition configurations, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide.*

11.2.3 Checking the Physical Partition Operation Status

You can check the physical partition operation status, including the power disconnection status or initialization status, by using the showpparstatus command. You can obtain the same information by using "Status" of the showpcl command.

Note - For details of the physical partition operation status, see the showpparstatus(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

Note - You can check the status of the logical domains in a physical partition by using the showdomainstatus command. For details, see "11.2.6   Checking the Logical Domain Status."

Note - For details of the physical partition status, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide.*

Operation Procedure

The procedure for checking the physical partition operation status is described below.
1. **Execute the showpparstatus command to check the physical partition status.**
   The following example displays the operation status of all physical partitions.

```
XSCF> showpparstatus -a
PPAR-ID PPAR Status
00          Powered Off
01          Initialization Phase
02          Initialization Phase
03          Running
```

11.2.4 Checking the Memory Mirror Mode Settings

Use the showfru command to check the memory mirror mode settings. You can check the following content with respect to a PSB used to configure a physical partition.

- Device
  sb: You can check the BB (PSB).

    Example: 00-0: PSB of BB-ID 0

  cpu: You can check the CPU mounted on the BB.

    Example: 00-0-2: CPU#2 on the PSB of BB-ID 0

- Memory mirror mode
  You can check the status of the memory mirror mode settings, which can be set for each CPU.

  yes: Memory mirror mode

  no: Non memory mirror mode

Note - For the settings/details of memory mirror mode, see "Chapter 14   Configuring a Highly Reliable System."

Operation Procedure

1. **Execute the showfru command to check device information.**
   The following example displays the set information for all devices.

```
XSCF> showfru -a
Device    Location    Memory Mirror Mode
sb        00-0
    cpu   00-0-0      yes
    cpu   00-0-1      yes
    cpu   00-0-2      yes
    cpu   00-0-3      yes
sb        01-0
    cpu   01-0-0      yes
    cpu   01-0-1      yes
    cpu   01-0-2      yes
    cpu   01-0-3      yes
sb        02-0
    cpu   02-0-0      no
    cpu   02-0-1      no
    cpu   02-0-2      no
    cpu   02-0-3      no
sb        03-0
    cpu   03-0-0      yes
    cpu   03-0-1      yes
    cpu   03-0-2      no
    cpu   03-0-3      no
```

```
  :
```

The following example specifies the sb operand to display the set information for the specific PSB.

```
XSCF> showfru sb 01-0
Device   Location    Memory Mirror Mode
sb       01-0
    cpu  01-0-0      yes
    cpu  01-0-1      yes
    cpu  01-0-2      yes
    cpu  01-0-3      yes
```

The following example specifies the cpu operand to display the set information for the specific CPU.

```
XSCF> showfru cpu 01-0-3
Device   Location    Memory Mirror Mode
sb       01-0
    cpu  01-0-3      yes
```

11.2.5   Checking the PSB Status

A system board (PSB) refers to a SPARC M12/SPARC M10 chassis.
You can check the PSB power status (power), diagnosis status (test), and degradation status (fault) by executing the showboards command. In a building block configuration, after executing the addboard or deleteboard command to configure or disconnect, respectively, a PSB in a physical partition, you can learn the progress of that operation, such as whether the operation succeeded or failed, with the showboards command. The progress is a status such as PSB assignment to the physical partition (assignment), configuration/disconnection, status (connection), or operation status (configuration).

By using the showboards command, you can check the PSB power status (power), diagnosis status (test), assignment status (assignment), configuration status (connection), operation status (configuration), and degradation status (fault).

Note - For details of the PSB status, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*, the showboards(8) command man page, or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operation Procedure

The procedure for checking the PSB status is described below.
1. **Execute the showboards command to check the PSB status.**
   The following example displays the status of all PSBs.

```
XSCF> showboards -a
PSB  PPAR-ID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- ------------ ----------- ---- ---- ---- ------- --------
00-0 00(00)       Assigned    y    y    y    Passed  Normal
01-0 SP           Unavailable n    n    n    Testing Normal
02-0 Other        Assigned    y    y    n    Passed  Degraded
03-0 SP           Unavailable n    n    n    Failed  Faulted
```

The following example displays detailed information for PSB 00-0.

```
XSCF> showboards 00-0
PSB  PPAR-ID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- ------------ ----------- ---- ---- ---- ------- --------
00-0 00(00)       Assigned    y    y    y    Passed  Normal
```

The following example displays the PSB that is in the system board pool and defined for PPAR-ID 00.

```
XSCF> showboards -p 0 -c sp
PSB  PPAR-ID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- ------------ ----------- ---- ---- ---- ------- --------
01-0 SP           Available   n    n    n    Passed  Normal
```

11.2.6   Checking the Logical Domain Status

You can check the operation status of Oracle Solaris on the control domain in a
physical partition, the OpenBoot PROM status on the control domain, etc. by using
the showdomainstatus command.

Note - For detailed definitions of the logical domain operation status, see the
showdomainstatus(8) command man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC
M10 XSCF Reference Manual*. You can check the logical domain status with the ldm
list-domain command of Oracle VM Server for SPARC too. For details of the ldm command,
see the *Oracle VM Server for SPARC Reference Manual* of the version used.

Operation Procedure

The procedure for checking the logical domain operation status is described below.

1. **Execute the showdomainstatus command to check the operation status of the
   logical domains belonging to the specified physical partition.**
   The following example displays the operation status of all the logical domains of
   PPAR-ID 0.

```
XSCF> showdomainstatus -p 0
Logical Domain Name    Status
primary                Solaris running
```

```
guest00                 Solaris running
guest01                 Solaris booting
guest02                 Solaris powering down
guest03                 Solaris panicking
guest04                 Shutdown Started
guest05                 OpenBoot initializing
guest06                 OpenBoot Primary Boot Loader
```

The following example displays the operation status of the logical domain named "guest01" of PPAR-ID 0.

```
XSCF> showdomainstatus -p 0 -g guest01
Logical Domain Name   Status
guest01               Solaris powering down
```

Chapter 12

Checking Logs and Messages

This chapter describes the types of logs and messages displayed and stored on the systems, and the commands for referencing the logs and messages.

- Checking a Log Saved by the XSCF
- Checking Warning and Notification Messages

12.1 Checking a Log Saved by the XSCF

This section describes how to check XSCF log information.

XSCF log information is used to investigate system problems. The system administrator, domain administrators, and field engineers can refer to the log information. They can learn the server operation status and usage status, as well as the details concerning any abnormalities that occurred.

12.1.1 Checking the Log Types and Reference Commands

The logs that are collected/managed by the system include fault information-related logs, logs for recording events, security-related logs, and server environment-related logs.

This section describes the various log types.

Log Type

These systems collect the following types of logs, which can be referenced by the system administrator.

- Fault information-related logs
  - Fault Management log (FM log) (*1)

  - Error log

- Syslog (*1)

- Monitoring message log

*1 The log can be referenced only on Oracle Solaris. For details, see Oracle Solaris related manuals.

- Logs for recording events
  - Power log

  - Event log

  - Console log

  - Panic log

  - IPL log

- Security- and authentication-related logs
  - Audit log

  - COD log

  - Active Directory log

  - LDAP over SSL log

- Server environment-related log
  - Temperature history log

Overviews and Reference Methods of Logs

Table 12-1 lists types, overviews, and reference methods of fault information-related logs. For details of XSCF commands, see the man page of each command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*. For details of each log type, see the subsequent sections.

Table 12-1   Fault Information-Related Logs

Log Type	Description	Size (Entry Size)/ <Standard Storage Period> Archiving	Output Display Destination/ Reference Method
Fault Management log (FM log)	Log for errors, notifications, and failures that occurred in the system.		Domain/ fmdump
Error log	Log for errors, notifications, and failures that occurred in the system. The log display format is specific to the platform.	About 1,024 generations (variable length) <Amount for about 1 month> Archived	XSCF/ showlogs(8) XSCF Web
Syslog (SYSLOG)	Log for recording output Oracle Solaris messages. If a failure occurs, an overview of the failure is output.		Domain/ Use an Oracle Solaris command to refer to it.

Table 12-1   Fault Information-Related Logs *(continued)*

Log Type	Description	Size (Entry Size)/ <Standard Storage Period> Archiving	Output Display Destination/ Reference Method
Monitoring message log (Monitor message log)	Log for recording messages from the XSCF reporting failures	512 KB, about 10,000 lines	XSCF/ showlogs(8) XSCF Web

Note - The logs displayed by Oracle Solaris commands are not archived.

Table 12-2 lists types, overviews, and reference methods of the logs for recording events.

Table 12-2   Logs for recording events

Log Type	Description	Size (Entry Size)/ <Standard Storage Period> Archiving	Reference Method
Power log (Power Log)	Log for recording server power events	1,920 generations (x 16 B) <Amount for about 1 month> Archived	showlogs(8) XSCF Web
Event log (XSCF Event Log)	Log for recording system operations, operation panel operations, and event notifications issued to Oracle Solaris.	4,096 generations (x 48 B) <Amount for about 1 month> Archived	showlogs(8) XSCF Web
Console log (Console Log)	Log for recording control domain console messages. Turning off the input power clears the log.	512 KB/PPAR, about 10,000 lines/PPAR <Amount for about 1 week> Archived	showlogs(8) XSCF Web
Panic log (Panic Log)	Console log for any panic occurrences	1 generation, 64 KB/PPAR (about 1,200 lines) <Amount for 1 time> Archived	showlogs(8) XSCF Web

Table 12-2 Logs for recording events *(continued)*

Log Type	Description	Size (Entry Size)/ <Standard Storage Period> Archiving	Reference Method
IPL log (IPL Log)	Log for the period from power-on to Oracle Solaris startup completion	1 generation, 32 KB/PPAR, about 600 lines/PPAR <Amount for 1 time> Archived	showlogs(8) XSCF Web

Table 12-3 lists types, overviews, and reference methods of security-related logs.

Table 12-3 Security-related Logs

Log type	Description	Size (Entry Size)/ <Standard Storage Period> Archiving	Reference Method
Audit log (Audit Log)	XSCF audit-related log	4 MB <Amount for about 1 month> Archived	viewaudit(8) XSCF Web
COD log (CoD activation log)	Log for CPU Activation additions and deletions	1,024 generations (x 32 KB) License per core Archived	showcodactivationhistory(8) XSCF Web
Active Directory log	A message log for diagnosing the authentication and authorization of the Active Directory.	250 KB (about 3000 lines) Not Archived	showad(8) XSCF Web
LDAP over SSL log (LDAP over SSL Log)	A message log for diagnosing the authentication and authorization of the LDAP over SSL.	250 KB (about 3000 lines) Not Archived	showldapssl(8) XSCF Web

Table 12-4 lists types, overviews, and reference methods of server environment-related logs.

Table 12-4   Server environment-related log

Log Type	Description	Size (Entry Size)/ <Standard Storage Period> Archiving	Reference Method
Temperature history log (Thermal and humidity History)	Environment-related log with a server temperature history	16,384 generations (x 16 B) (Every 10 minutes) <Amount for about 1 year> Archived	showlogs(8) XSCF Web

Note - When the log is full, the log is overwritten, beginning with the oldest log data.

12.1.2   How to View the Log

This section describes how to view the information in each XSCF log.

Checking the Log on the XSCF Shell or XSCF Web

The common procedure for referencing each log is described below.

1. **Check the user privileges required for referencing logs.**
   The user privileges for each log are as in Table 12-5.

Table 12-5   User Privileges Required for Referencing Logs

Log Type	Required User Privilege
Error log	platadm, platop, fieldeng
Monitoring message log	platadm, platop, fieldeng
Power log	platadm, platop, pparadm, pparmgr, fieldeng
Event log	platadm, platop, fieldeng
Console log	platadm, platop, pparadm, pparmgr, pparop, fieldeng
Panic log	platadm, platop, pparadm, pparmgr, pparop, fieldeng
IPL log	platadm, platop, pparadm, pparmgr, pparop, fieldeng
Audit log	auditadm, auditop
COD log	platadm, platop, fieldeng
Temperature history log	platadm, platop, fieldeng
Active Directory log	useradm
LDAP over SSL log	useradm

2. **Specify the host name or IP address to connect to the XSCF shell terminal or XSCF Web.**

3. **Specify an XSCF user account that has the required user privilege, and a password to log in to the XSCF.**

4. **Execute the command for referring to the relevant log, or select this operation from the menu.**

5. **Refer to the log.**

Note - For details of the XSCF Web menu, see "Appendix C   List of the XSCF Web Pages."

12.1.3   Checking the Error Log

The error log is a fault information-related log. Use the showlogs command with the error operand specified to refer to the log for a notification or failure that occurred in the system.

Use Scenarios

The scenarios for using the error log on the XSCF are described below.

- A message was output to the domain console, the XSCF shell terminal, or XSCF Web, so the log is used to check whether a failure occurred.

- Notification was sent to the already registered e-mail address, so the log is used to check for fault information.

- A trap was generated by the SNMP manager, so the log is used to check for fault information.

Operation Procedure

1. **Execute the showlogs command with the error operand specified on the XSCF shell.**

```
XSCF> showlogs error
Date: Oct 20 17:45:31 JST 2012
      Code: 00112233-444555666777-888999aaabbbcccdddeeefff
      Status: Warning Occurred: Oct 20 17:45:31.000 JST 2012
      FRU: /PSU#1
      Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Date: Oct 20 17:45:31 JST 2012
      Code: 00112233-444555666777-888999aaabbbcccdddeee000
      Status: Alarm Occurred: Oct 20 17:45:31.000 JST 2012
      FRU: /PSU#1
      Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
```

The following content is displayed in the above example.

- Registered time (Date) as logged for the problem

It is shown in local time.

- DIAGCODE, which field engineers and service engineers use for troubleshooting (Code)

Note - Users are requested to report this code to a field engineer or service engineer. The code helps in finding an early solution to the problem.

- Failure level (Status) of the part
  One of the following is displayed:

  Alarm: Failure or error of the relevant part

  Warning: Partial degradation or warning of the relevant part

  Information: Notification

  Notice: System status notification

- Time that the problem occurred (Occurred)
  It is shown in local time.

- Replacement part possibly faulty (FRU)
  If the first, second, and third most likely faulty parts are displayed, they are delimited by a comma (,). If there are additional likely faulty parts, an asterisk (*) is displayed after the last comma (,). Each part is shown hierarchically in the format of the mounting path of the part. The determination of whether to display the second and subsequent most likely faulty parts depends on the detected fault location.

  The following cases show the meaning of the displayed "FRU:" content.

  a. "/PSU#0,/PSU#1" is displayed.
  PSU#0 and PSU#1 have been detected as the first and second most likely faulty parts, respectively. This means each of the parts may need to be replaced depending on its condition.

  b. "/BB#1/XBU#0/CBL#0R,/XBBOX#80/XBU#0,/BB#1/XBU#0,*" is displayed.
  CBL#0R between BB#1 and XBBOX#80, XBU#0 in XBBOX#80, and XBU#0 in BB#1 have been detected as the first, second, and third most likely faulty parts, respectively, along with other parts also detected as such. This means each of the parts may need to be replaced depending on its condition.

  c. "/BB#0/PCI#3" is displayed.
  BB#0/PCI#3 has been detected as a likely faulty part, and PCI slot 3 of BB-ID 0 has a problem. This means the device connected to PCI slot 3 may need to be replaced depending on its condition.

  d. "/MBU/MEM#02A" is displayed.
  /MBU/MEM#02A has been detected as a likely faulty part, and memory slot 02A of the motherboard unit has a problem. This means memory slot 02A may need to be replaced depending on its condition.

  e. "/BB#0/CMUL/MEM#02A" is displayed.
  /BB#0/CMUL/MEM#02A has been detected as a likely faulty part, and memory slot 02A of the CPU memory unit (lower) of BB-ID 0 has a problem. This means memory slot 02A may need to be replaced depending on its

condition.

f. "/BB#0/CMUL/MEM#02A-03A" is displayed.
/BB#0/CMUL/MEM#02A-03A has been detected as a likely faulty part, and memory slots 02A and 02B of the CPU memory unit (lower) of BB-ID 0 have problems. This means the memory in memory slots 02A and 02B may need to be replaced as a pair, depending on their condition.

- One-row message outlining a problem (Msg)

Note - For details of the showlogs(8) command, see the man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

12.1.4   Checking the Monitoring Message Log

Events that have occurred on the system are displayed in real time as monitoring messages for the users who have logged in to the XSCF. The XSCF firmware collects these messages in the monitoring message log. Use the showlogs command with the monitor operand specified to refer to the monitoring message log.

Operation Procedure

1. **Execute the showlogs command with the monitor operand specified on the XSCF shell.**

```
XSCF> showlogs monitor
Oct 20 17:45:31 monitor message: xxxxxxx
Oct 20 17:55:31 monitor message: xxxxxxx
```

The following content is displayed.
- Monitoring message log collection time (Date)
     It is shown in local time.

- Monitoring message (Message)

12.1.5   Checking the Power Log

The power log is collected when a power operation or reset operation is performed on these systems. Use the showlogs command with the power operand specified to refer to the power log.

Operation Procedure

1. **Execute the showlogs command with the power operand specified on the XSCF shell.**
The following example displays the power log.

```
XSCF> showlogs power
Date                    Event            Cause          ID Switch
Oct 20 17:25:31 JST 2012 Cabinet Power On  Operator       00 Service
Oct 20 17:35:31 JST 2012 PPAR Power On     Operator       00 Locked
Oct 20 17:45:31 JST 2012 PPAR Power Off    Software Request 00 Locked
Oct 20 17:50:31 JST 2012 Cabinet Power Off Self Reset      00 Service
```

The following example specifies start and end times to display the power log in a list ordered by newest to oldest.

```
XSCF> showlogs power -t Oct2017:302012 -T Oct2017:492012 -r
Date                    Event            Cause          ID Switch
Oct 20 17:45:31 JST 2012 PPAR Power Off    Software Request 00 Locked
Oct 20 17:35:31 JST 2012 PPAR Power On     Operator       00 Locked
```

Note - The layout of the command example is subject to change without prior notice for functional improvement.

The following content is displayed in the above example.

- Power log collection time (Date)
  It is shown in local time.

- Type of power event that occurred (Event)
  The following table lists power events (Event) and their meanings.

Event	Meaning
SCF Reset:	The XSCF reboot or reset was performed.
PPAR Power On:	The physical partition was powered on.
PPAR Power Off:	The physical partition was powered off.
PPAR Reset:	The physical partition was reset.
Cabinet Power On:	The server was powered on.
Cabinet Power Off:	The server was powered off.
XIR:	An XIR reset was performed.

- Factor causing a power event instruction (Cause)
  The following table lists causes (Cause) and their meanings.

Cause	Meaning
Self Reset:	The XSCF reboot was performed.
Power On:	An XSCF reboot was performed because the input power was turned on.
System Reset:	An XSCF reset was performed because of a detected failure.

Cause	Meaning
Panel:	The operation of a switch on the operation panel caused a power event.
Scheduled:	A TOD timer setting caused a power event.
IPMI:	An I/O device connected to RCIL caused a power event.
Power Recover:	The power was turned on because of power recovery.
Operator:	An operator instruction caused a power event.
Power Failure:	The power was turned off because of a power outage.
Software Request:	An Oracle Solaris instruction caused a power event.
Alarm:	The server environment or a hardware failure caused a power event.
Fatal:	A "Fatal" error caused a power event.

- PPAR-ID or BB-ID of a power event (ID)

  If Event is System Power On or System Power Off, a BB-ID is displayed.

  If Event is PPAR Power On, PPAR Power off, or PPAR Reset, a PPAR-ID is displayed.

  If Event is the cause on all the SPARC M12/M10 systems or all the physical partitions, "--" is displayed.

- Mode switch state on the operation panel (Switch)

  The following lists the switch states and their meanings.

Switch state	Meaning
Locked:	The Mode switch is set to Locked.
Service:	The Mode switch is set to Service.

12.1.6   Checking the Event Log

In these systems, the event log is collected when an event such as the following occurs in the system or a physical partition: the system status changes, the configuration is changed, the operation panel is operated, or Oracle Solaris is notified of an event. Use the showlogs command with the event operand specified to refer to the event log.

Operation Procedure

1. **Execute the showlogs command with the event operand specified on the XSCF shell.**

```
XSCF> showlogs event
Date                      Message
Oct 20 17:45:31 JST 2012   System power on
Oct 20 17:55:31 JST 2012   System power off
```

The following content is displayed.
- Event log collection time (Date)
  It is shown in local time.
- Event message (Message)

12.1.7 Checking the Console Log

The XSCF writes control domain console messages to the console log. The console log contains one message entry per line. In some cases, the console log may be called a console message log. Use the showlogs command with the console operand specified to refer to the console log.

Operation Procedure

1. **Execute the showlogs command with the console operand specified on the XSCF shell.**

```
XSCF> showlogs console -p 0
PPAR-ID: 00
Oct 20 17:45:31 JST 2012   console message: xxxxxxx
Oct 20 17:55:31 JST 2012   console message: xxxxxxx
```

The following content is displayed.
- Physical partition ID (PPAR ID)
- Console log collection time (Date)
  It is shown in local time.
- Console message (Message)

12.1.8 Checking the Panic Log

A console message is output to the domain console when a panic occurs. These output console messages are collected in the panic log. In some cases, the panic log may be called a panic message log. Use the showlogs command with the panic operand specified to refer to the panic log.

Operation Procedure

1. **Execute the showlogs command with the panic operand specified on the XSCF shell.**

```
XSCF> showlogs panic -p 0
<<panic>>
Date: Oct 20 18:45:31 JST 2012      PPAR-ID: 00
Oct 20 17:45:31 JST 2012    panic message: xxxxxxx
Oct 20 17:55:31 JST 2012    panic message: xxxxxxx
```

The following content is displayed.

- Physical partition ID (PPAR-ID)

- Panic log collection time (Date)
  It is shown in local time.

- Panic message (Message)

12.1.9 Checking the IPL Log

After a physical partition is powered on, console messages are output to the control domain console until the status becomes Running. These console messages are collected in the IPL log. In some cases, the IPL log may be called an IPL message log. Use the showlogs command with the ipl operand specified to refer to the IPL log.

Operation Procedure

1. **Execute the showlogs command with the ipl operand specified on the XSCF shell.**

```
XSCF> showlogs ipl -p 0
<<ipl>>
Date: Oct 20 18:45:31 JST 2012      PPAR-ID: 00
Oct 20 17:45:31 JST 2012    ipl message: xxxxxxx
Oct 20 17:55:31 JST 2012    ipl message: xxxxxxx
```

The following content is displayed.

- Physical partition ID (PPAR-ID)

- IPL log collection time (Date)
  It is shown in local time.

- IPL message (Message)

12.1.10 Checking the Audit Log

The audit log is collected when the audit function is used in these systems. Use the viewaudit command to refer to the audit log.

Operation Procedure

1. **Execute the viewaudit command on the XSCF shell.**
   The following example displays all audit records.

```
XSCF> viewaudit
file,1,2012-04-26 21:37:25.626
+00:00,20120426213725.0000000000.SCF-4-0
header,20,1,audit - start,0.0.0.0,2012-04-26 21:37:25.660 +00:00
header,43,1,authenticate,0.0.0.0,2012-04-26 22:01:28.902 +00:00
authentication,failure,,unknown user,telnet 27652 0.0.197.33
header,37,1,login - telnet,0.0.0.0,2012-04-26 22:02:26.459 +00:
00
subject,1,opl,normal,telnet 50466 10.18.108.4
header,78,1,command - setprivileges,0.0.0.0,2012-04-26
22:02:43.246
+00:00
subject,1,opl,normal,telnet 50466 10.18.108.4
command,setprivileges,opl,useradm
platform access,granted
return,0
```

As shown in the above example, records are displayed in text format by default. One token is displayed per line, with a comma as the field delimiter character.

The token types and their fields are shown in Table 12-6 (in the display order).

Table 12-6   Token Types and Their Fields (in the Display Order)

Token Type	Field (Display Order)
File Token	Label, version, time, file name
Header Token	Label, record byte count, version, event type, machine address, time (event recording time)
Subject Token	Label, audit session ID, UID, mode of operation, terminal type, remote IP address, remote port
Upriv Token	Label, success/failure
Udpriv Token	Label, success/failure, user privilege, domain ID 1, ..., domain ID N
Command Token	Label, command name, operand 1, ..., operand N
Authentication Token	Label, authentication result, user name, message, terminal type, remote IP address, remote port
Return Token	Label, return value
Text Token	Label, text string

Note - Some fields might not be output depending on the environment.

The main audit events and tokens are as follows:

- Login telnet
  header
  subject

text
return

- Login SSH
  Same as for Login telnet

- Login BUI
  Same as for Login telnet

- Logout
  Header
  Subject

- Audit start
  Header

- Audit stop
  Header

- Shell command
  Header
  Subject
  Command
  Text
  Upriv | Updpriv
  Return

Note - Some tokens might not be output depending on the environment. Also, this information is subject to change without prior notice for functional improvement.

Note - For details of the log options, audit classes, and audit events of the viewaudit(8) command, see the man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

12.1.11 Checking the COD Log

The COD log is collected when there is a CPU Activation addition or deletion. COD log is also referred to as CPU Activation log. Use the showcodactivationhistory command to refer to the COD log.

Operation Procedure

1. **Execute the showcodactivationhistory command on the XSCF shell.**
   The following example displays the COD log.

```
XSCF> showcodactivationhistory
11/30/2012 01:42:41PM PST: Report Generated M10-1 SN: 843a996d
10/02/2012 02:08:49PM PST: Activation history initialized: PROC 0 cores
10/15/2012 01:36:13PM PST: Capacity added: PROC 2 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 2 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 2 cores
```

```
11/27/2012 01:46:23PM PST: Configuration backup created: PROC 2 cores
11/27/2012 21:26:22PM PST: Configuration restored: PROC 2 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 2 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 2 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 2 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 2 cores
11/30/2011 01:42:41PM PST: Summary: PROC 10 cores
Signature: yU27yb0oth41UL7hleA2vHL7S1aX4pmkBTIxesD1XEs
```

Note - For details of the showcodactivationhistory(8) command, see the man pages or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

12.1.12 Checking the Active Directory Logs

This section explains the reference method of the Active Directory logs using the showad command. For details on the log options of the showad command, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual* or the man pages for the showad(8) command. For the size and generation number of each log, see Table 12-3.

Referencing the Active Directory Logs Using the showad Command

When user authentication and authorization are performed using the Active Directory function, diagnosis message logs are collected. The logs are used to deal with a failure and are cleared when rebooting the XSCF. The Active Directory logs can be referenced by executing the showad command with the log operand on the XSCF shell. The following items are displayed.
- Time when the Active Directory logs were collected
- Diagnosis messages

12.1.13 Checking the LDAP over SSL Logs

This section describes the reference method of the LDAP over SSL logs using the showldapssl command.   For details on the log options of the showldapssl command, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual* or the man pages for the showldapssl(8) command. For the size and generation number of each log, see Table 12-3.

Referencing the LDAP over SSL logs using the showldapssl command

When user authentication and authorization are performed using the LDAP over SSL function, diagnosis message logs are collected. The logs are used to deal with a failure and cleared when rebooting the XSCF.   The LDAP over SSL logs can be referenced by specifying the log operand on the XSCF shell and executing the showldapssl command. The following items are displayed.
- LDAP over SSL log collection time

- Diagnosis messages

12.1.14 Checking the Temperature History Log

The temperature history log is a log of the intake temperatures of the server. The intake temperature is recorded every 10 minutes. Use the showlogs command with the env operand specified to refer to the temperature history log.

Operation Procedure

1. **Execute the showlogs command with the env operand specified on the XSCF shell.**

```
XSCF> showlogs env
BB#00
Date                          Temperature   Power
Oct 20 17:45:31 JST 2012      32.56(C)      Cabinet Power On
Oct 20 17:55:31 JST 2012      32.56(C)      Cabinet Power Off
 :
```

The following content is displayed.
- Temperature history log collection time (Date). It is shown in local time.
- Temperature (Temperature)
- Chassis power status (On or Off) (Power)

12.1.15 Saving a Log to a File With Snapshot

This section describes how to save XSCF log information to a file.

To save log information, execute the snapshot command on the XSCF shell. Alternatively, select this operation from the snapshot menu on XSCF Web. All XSCF log information is saved to the specified location.

A field engineer or service engineer saves the log information. The system administrator may also be asked to do so.

Method of Saving a Log

The method of saving a log is described below. For details of the save method, see the subsequent section.
- Save the log information locally by connecting a USB device to a USB port of the XSCF unit mounted on the rear panel of the master XSCF chassis.
- Save the log information via the network on the terminals that use XSCF Web. The data transfer at this time uses an encryption protocol.
- Save the log information via the network, on the servers specified with the snapshot command.

The data transfer at this time uses an encryption protocol.

Note - The USB device needs to be formatted with the FAT32 file system. For points to note about the capacity and any handling of the USB device used to save the log locally, ask a service engineer.

Note - The saved data can be encrypted by specifying the option for the snapshot on the XSCF. For information on handling or sending encrypted log files, ask a service engineer.

Note - In systems with multiple XSCFs, the log of another chassis, such as that of the standby XSCF, can be collected from the master XSCF.

Log File Output Format

The output format when saving a log file is as follows.

- File name: This name is automatically generated from the XSCF host name, IP address, and log save time.
  The log file cannot be generated with a user-specified file name.

- File format: zip

In the systems with multiple XSCFs, a single generated zip file consists of the information on each chassis of SPARC M12-2S/SPARC M10-4S and crossbar box that compose the building block. If a single chassis number is specified, the logs specific to the specified chassis are saved in addition to the logs common to the system. If all chassis are specified, the logs for all chassis are saved in addition to the logs common to the system.

12.1.16 Saving a Log to a Local USB Device

This section describes how to save log information to a USB device by using XSCF Web or the XSCF shell.

Operating Procedure on the XSCF Shell

1. **Connect a USB device to a USB port on the XSCF unit on the rear panel of the server.**
2. **Execute the snapshot command with the USB device specified for the output file, on the XSCF shell.**

```
XSCF> snapshot -d usb0 -a
```

Data is transferred.

3. **Confirm that the saving of the log has completed.**
   After the saving is completed, if required, contact a service engineer.

> **Note -** The snapshot command can be used to encrypt data, and then output it. For details of the encryption option of the snapshot command, see its man page or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Operating Procedure on XSCF Web

1. **Connect a USB device to a USB port on the XSCF unit on the rear panel of the server.**

2. **Display the save operation page by selecting this operation from the snapshot menu.**

3. **Select the USB device as the save location, in the Web browser window.**

4. **If the output log file needs to be encrypted, check [Encrypt Output File] and specify the encryption password.**
   Click the [Download] button to transfer the data.

5. **Confirm that the saving of the log has completed.**
   After the saving is completed, if required, contact a service engineer.

12.1.17 Saving the Log via the Network on the Terminals That Use XSCF Web

The procedure for saving the log via the network, in a terminal that uses XSCF Web is described below.

1. **Display the save operation page by selecting the [Snapshot] menu.**

2. **Specify the target directory as the save location, in the Web browser window.**

3. **If the output log file needs to be encrypted, check [Encrypt Output File] and specify the encryption password.**
   Click the [Download] button to transfer the data.

4. **Confirm that the saving of the log has completed.**
   After the saving is completed, if required, contact a service engineer.

12.1.18 Saving the Log via the Network, on the Servers Specified With Snapshot

The procedure for saving the log via the network, on the server specified with the snapshot command is described below.

1. **Specify the full target directory, such as the SSH server and directory on the XSCF shell, and execute the snapshot command.**

```
XSCF> snapshot -t user@host:directory
```

Data is transferred.

2. **Confirm that the saving of the log has completed.**
   After the saving is completed, if required, contact a service engineer.

Note - The snapshot command can be used to encrypt data, and then output it. For details of the encryption option of the snapshot command, see the man page of the snapshot(8) command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual.*

12.2 Checking Warning and Notification Messages

This section describes how to check the failure and notification messages that are output primarily to the control domain console and reported by e-mail and the SNMP agent function.

12.2.1 Checking the Message Types and Reference Methods

Message Type

The following messages are the most common ones seen by users when notified of a server failure and the server status:

- syslog message (*1)
- FMA message (*1)
- IPL message
- Panic message
- Console message
- Monitoring message
- Other notification messages
  *1 The message can be referenced only on Oracle Solaris. For details, see Oracle Solaris related manuals.

Overviews and Reference Methods of Messages

Table 12-7 lists types, overviews, and reference methods of individual messages.

Table 12-7   Overview of Each Message

Message Type	Description	Output Display Destination/ Reference Method
syslog message	This message is a notification from Oracle Solaris.	Domain/ Can be viewed on the control domain console.
FMA message	This message has the results of an automatic diagnosis of a hardware or software failure. The Fault Management Architecture (FMA) of Oracle Solaris makes the diagnosis. The user can thus learn about which parts of the system correspond to the failure notification. The FMA message is stored as log information (in a fault log or the error log). The fmdump command of Oracle Solaris and the showlogs command of the XSCF shell can display its contents for a more detailed investigation. The user can also check the contents at the specified URL based on the MSG-ID displayed on the control domain console.	Domain/ Can be viewed on the control domain console.
IPL message	This message is output at Oracle Solaris startup on the control domain. The IPL message is output to the control domain console and stored as log information (in the IPL log) in the XSCF. The IPL log only retains information about the most recent system startup, for each control domain. The showlogs command of the XSCF shell can display the IPL log.	Domain/ Can be viewed on the control domain console.
Panic message	This message is output when a panic occurs. The panic message is output to the domain console and stored as log information (in the panic log) in the XSCF. The panic log retains information for a single panic event, the most recent one, for each control domain. The showlogs command of the XSCF shell can display the panic log.	Domain/ Can be viewed on the control domain console.

Table 12-7　　Overview of Each Message *(continued)*

Message Type	Description	Output Display Destination/ Reference Method
Console message	Console message is a general term for syslog messages, FMA messages, panic messages, IPL messages, and other messages output by POST, OpenBoot PROM, and Oracle Solaris. Those console messages that are output to the domain console of each control domain are stored as log information (in the console log) in the XSCF. The showlogs command of the XSCF shell can display the console log. Note that Logical Domains Manager manages the console messages that are on guest domains. For details, see "8.10 Domain Console Logging Function." The overwriting of console messages begins with the oldest message. System startup messages are retained in the IPL log, and the respective log information about panic times is retained in the panic log, even when their console messages have been overwritten. In the systems with multiple XSCFs, the console messages stored on the master XSCF are not copied to the standby XSCF. Accordingly, after XSCF switching, the console messages on the previous master side cannot be referenced.	Domain/ Can be viewed on the control domain console.
Monitoring message	The XSCF outputs this message for a system failure or notification. The monitoring message is output using the showmonitorlog command. It is stored as log information (in the monitoring message log or error log) in the XSCF. The showlogs command of the XSCF shell can display the monitoring message log and error log for a more detailed investigation. Also, a service engineer uses the DIAGCODE output in the message to acquire detailed information. The overwriting of monitoring messages begin with the oldest message. In the systems with multiple XSCFs, monitoring messages output by the master XSCF are also managed on the standby XSCF. Even after XSCF switching, the monitoring messages on the previous master side can be referenced.	Domain, XSCF/ Can be viewed on the control domain console. Can be viewed with the showmonito r-log command.
Other notification messages	In addition to the above messages, notification messages are displayed on the domain console for a normal power-off, a reset operation, and some other events.	Domain/ Can be viewed on the control domain console.

12.2.2 Taking Action for Notification Messages

This section describes, along with messages, what action to take after recognizing a message on Oracle Solaris or a notification message from each XSCF function.

Recognizing/Taking Action for a Notification or Failure in a Message on the Control Domain Console

1. **The user recognizes the notification or failure in a console message, such as a syslog message or FMA message, output to the control domain console.**
   The following example shows an FMA message on the control domain console.

```
SUNW-MSG-ID: SUNOS-8000-J0, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Thu Apr 19 10:48:39 JST 2012
PLATFORM: ORCL,SPARC64-X, CSN: PP115300MX, HOSTNAME: 4S-LGA12-D0
SOURCE: eft, REV: 1.16
EVENT-ID: fcbb42a5-47c3-c9c5-f0b0-f782d69afb01
DESC: The diagnosis engine encountered telemetry from the listed devices for
which it was unable to perform a diagnosis - ereport.io.pciex.rc.epkt@
chassis0/cpuboard0/chip0/hostbridge0/pciexrc0 class and path are incompatible.
AUTO-RESPONSE: Error reports have been logged for examination.
IMPACT: Automated diagnosis and response for these events will not occur.
REC-ACTION: Use 'fmadm faulty' to provide a more detailed view of this event.
Use 'fmdump -eV' to view the unexpected telemetry. Please refer to the
associated reference document at http://support.oracle.com/msg/SUNOS-8000-J0
for the latest service procedures and policies regarding this diagnosis.
```

Note - The message example is subject to change without prior notice.

2. **Fault information in the FMA message is stored in a log, so refer to the log file on the control domain console. At this time, execute an Oracle Solaris command, such as the syslog reference command or fmdump command, on the control domain console.**
   For details on how to identify fault information by using these commands, see the reference manual of Oracle Solaris.

3. **Check the notification or failure details by accessing the specified URL based on the message ID (SUNW-MSG-ID) displayed on the control domain console.**
   If there is no message ID (MSG-ID), obtain detailed information from syslog information.

4. **To acquire more detailed information, log in to the XSCF and execute the showlogs command to identify fault information.**

5. **Take action based on what is recommended in the information at the specified URL.**

Note - For the latest URL information, see the website about messages mentioned in the latest *Product Notes* for your server.

The user may be able to recognize a failure not just from a syslog message or FMA message but also by referring to a console message, panic message, IPL message, or monitoring message stored as log information in the XSCF. The user can refer to this log information by executing the showlogs command of the XSCF shell with each log option specified.

For details on the showlogs command, see "12.1　Checking a Log Saved by the XSCF."

Recognizing/Taking Action for a Failure Reported by a Message via E-mail

1. **The user recognizes a notification or failure from the Subject line or the body of the message in a reported XSCF e-mail.**
   For an example of an e-mail for a failure occurrence, see "10.2　Receiving Notification by E-mail When a Failure Occurs."

2. **To learn more detailed information, log in to the XSCF, and execute the showlogs command to identify fault information.**

3. **Check the log information. If required, notify a service engineer of the DIAGCODE output in the e-mail message or log.**
   The service engineer can use the DIAGCODE to acquire detailed information.

Recognizing/Taking Action for a Notification or Failure in an SNMP Trap Message

1. **The user recognizes a notification or failure in trap information issued from the XSCF by the SNMP manager.**
   For a trap example, see "10.3　Monitoring/Managing the System Status With the SNMP Agent."

2. **To learn more detailed information, log in to the XSCF, and execute the showlogs command to identify fault information.**

3. **Check the log information. If required, notify a service engineer of the DIAGCODE output in the log.**

Recognizing/Taking Action for a Notification or Failure in a Monitoring Message on the XSCF Shell

1. **The user executes the showmonitorlog command and recognizes a notification or failure in the output XSCF monitoring message.**
   The following example displays a monitoring message.

```
XSCF> showmonitorlog
PAPL2-5-0:Alarm:/BB#0/CPU#0:XSCF:Uncorrectable
error ( 80006000-20010000-0108000112345678):
```

Note - The command example is subject to change without prior notice for functional improvement.

2. **To learn more detailed information, log in to the XSCF, and execute the showlogs command to identify fault information.**

3. **Check the log information. If required, notify a service engineer of the DIAGCODE output in the log.**

Chapter 13

Switching to Locked Mode/Service Mode

This chapter describes differences between Locked mode and Service mode, which is used for maintenance work, and how to switch between them.

- Understanding the Differences Between Locked Mode and Service Mode
- Switching the Operating Mode

13.1 Understanding the Differences Between Locked Mode and Service Mode

The SPARC M12/M10 systems have two operating modes: Locked mode and Service mode.

- Locked mode
  Locked mode is dedicated to regular operation. In this mode, the Mode switch has been slid to the "Locked" position.

  The user accounts configured with the XSCF are used for work. The range of work varies depending on the user account.

  In Locked mode, power cannot easily be turned off since a mechanism prevents mistaken power-off by users. The POWER switch on the operation panel can be used to turn on but not turn off the power.

- Service mode
  Service mode is dedicated to maintenance work. In this mode, the Mode switch has been slid to the "Service" position. Maintenance that requires the stopping of the whole system has to be performed in Service mode.

Control for power-on and power-off in Locked mode and Service mode affects not only operations from the POWER switch but also power control from a remote location, automatic power control, and other control. Table 13-1 shows differences in power control between the two modes.

Table 13-1   Differences in Power Control Between Locked Mode and Service Mode

Item	Operating Mode	
	Locked Mode	Service Mode
Power-on by POWER switch	Power-on permitted	Power-on not permitted
Power-off by POWER switch	Power-off not permitted	Power-off permitted A long press (4 seconds or longer) starts power-off processing.
Break signal	Depends on the setting (The default is enabled.)	Signal sent to the control domain
Power-on during recovery	Power turned on	Power not turned on
Alive Check	Depends on the setting (The default is enabled.)	Disabled
Reaction when Host Watchdog times out	Depends on the setting (The default is PPAR reset.)	Depends on the setting (The default is PPAR reset.)
Automatic start-stop of Oracle Solaris	Depends on the setting (The default is automatic start.)	Depends on the setting (The default is automatic start.) (*1)
Automatic scheduled power-on	Power-on permitted	Power-on not permitted
Automatic scheduled power-off	Power-off permitted	Power-off not permitted
Remote power management	Control permitted	Control with other hosts not permitted

*1 For details of the automatic start-stop of Oracle Solaris, see "6.4 Suppressing Starting Oracle Solaris at Power-on."

Of the items controlled in Locked mode and Service mode, the ones shown with "Depends on the setting" can be configured by the setpparmode command of the XSCF firmware.

13.2 Switching the Operating Mode

To switch the operating mode in the SPARC M12/M10 systems, use the Mode switch on the operation panel.

Figure 13-1   Operation Panel Mode Switch (SPARC M12-1/M10-1)

(3) (1) (2)

No.	Component
1	Mode switch
2	Locked mode
3	Service mode

Figure 13-2   Operation Panel Mode Switch (SPARC M12-2/M10-4)

(2)

(1)   (3)
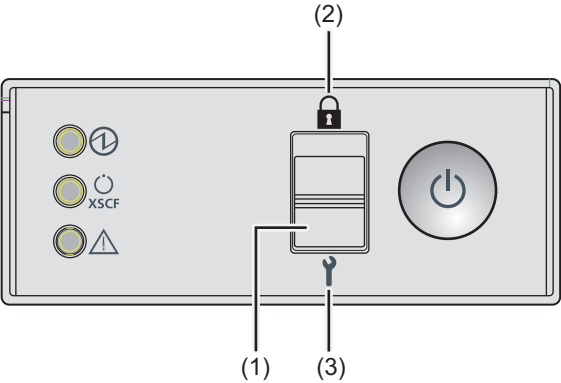
No.	Component
1	Mode switch
2	Locked mode
3	Service mode

Figure 13-3   Operation Panel Mode Switch (SPARC M12-2S/M10-4S)
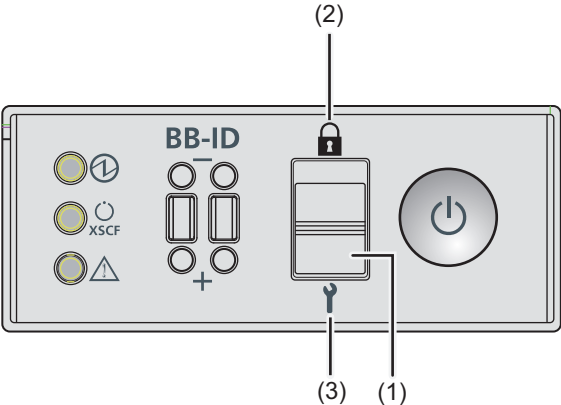
No.	Component
1	Mode switch
2	Locked mode
3	Service mode

For each SPARC M12-2S or SPARC M10-4S in a building block configuration, switch the mode by sliding the Mode switch on the operation panel of the SPARC M12-2S or SPARC M10-4S that has the master XSCF or standby XSCF. If the configuration has no crossbar boxes, the set master XSCF is BB#00 or BB#01. If the configuration has crossbar boxes, the set master XSCF is XBBOX#80 or XBBOX#81.

Note - For the SPARC M12-2S or SPARC M10-4S in a building block configuration, set the Mode switches of the master XSCF and standby XSCF to the same mode. If the master XSCF and the XSCF in the standby state are switched using the switchscf command when the settings are different, the status of the service switch that recognizes each SPARC M12-2S or SPARC M10-4S chassis is changed.
To report this state, an asterisk (*), indicating a failed component, is shown in the showhardconf and showstatus command output.

The procedures described below show how to switch from Locked mode to Service mode and from Service mode to Locked mode.

Switching to Service Mode

To perform cold system maintenance work or make the initial XSCF settings on the SPARC M12/M10 system, set Service mode.

The procedure for switching from Locked mode to Service mode is described below.

1. **Move the Mode switch on the operation panel to Service ( ).**

Switching to Locked Mode

The procedure for switching from Service mode to Locked mode on the SPARC M12/M10 systems is described below.

1. **Move the Mode switch on the operation panel to Locked (🔒).**

Chapter 14

Configuring a Highly Reliable System

This chapter describes methods for configuring highly reliable and secure SPARC M12/M10 systems.

- Configuring Memory Mirroring
- Configuring Hardware RAID
- Using the LDAP Service
- Using SAN Boot
- Using iSCSI
- Remote Power Management for the SPARC M12/M10 and I/O Devices
- Using an Uninterruptible Power Supply
- Using Verified Boot

14.1 Configuring Memory Mirroring

This section describes how to configure the memory mirroring supported by the SPARC M12/M10.

14.1.1 Overview of Memory Mirroring

The SPARC M12/M10 supports memory mirroring configurations to protect data through memory duplication. Data reliability increases, but the available memory capacity is halved.

The memory access controller controls writing of data to memory and reading of data from memory. The SPARC M12/M10 configures the mirroring by grouping the memory into sets controlled by two memory access controllers.

Note - The memory grouped together in a mirroring configuration must all have the same capacity and be the same rank.

For the rules on the physical configuration of memory, see "Checking the Memory Configuration Rules" in the *Service Manual* for your server.

14.1.2 Configuring Memory Mirroring

Use the setupfru command of the XSCF firmware to configure the mirroring of memory mounted in the SPARC M12/M10.
Execute the command with a user account that has the platadm or fieldeng privilege.

Note - To configure memory mirroring, the physical partition to which the PSB belongs must be powered off.

Memory Mirroring Configuration

- **SPARC M12**
  To configure memory mirroring in the SPARC M12, specify -c mirror=yes.

```
XSCF> setupfru [[-q] -{y|n}] -c function=mode device location
```

- **SPARC M10**
  To configure memory mirroring in the SPARC M10, specify -m y. The -c mirror option cannot be used.

```
XSCF> setupfru [-m {y|n}] device location
```

Operation Procedure

1. **Execute the setupfru command to configure memory mirroring.**
   The following example shows all the CPUs mounted in physical system board (PSB) 00-0 being set to memory mirror mode in the SPARC M12.

```
XSCF> setupfru -c mirror=yes sb 00-0
Notice:
- Logical domain config_name will be set to "factory-default".
Memory mirror mode setting will be changed, Continue? [y|n] :y
```

Note - For the SPARC M10, specify the following.
XSCF> setupfru -m y sb 00-0

The following example shows that the CPU of CPU chip #1 in PSB 02-0 is set to memory mirror mode.

```
XSCF> setupfru -m y cpu 02-0-1
```

14.2 Configuring Hardware RAID

This section describes hardware RAID configurations supported by the SPARC M12/M10, and how to configure and manage hardware RAID.

You can select from the following two utilities for the environment for creating and managing hardware RAID volumes on the SPARC M12/M10.

- FCode utility
  This utility consists of a set of special commands for displaying the targets and managing the logical volumes on the server. Use these commands in the OpenBoot PROM environment.

- SAS-2 Integrated RAID Configuration Utility (SAS2IRCU)
  You can configure and manage RAID volumes on the system by using SAS-2 Integrated RAID Configuration Utility (SAS2IRCU) (referred to below as SAS2IRCU utility) version 14.00.00.00 or later from Broadcom Limited.

  SAS-2 Integrated RAID Configuration Utility (SAS2IRCU) is the copyrighted work of Broadcom Limited and its affiliated companies.

  Obtain the SAS2IRCU utility and detailed documentation from Broadcom Limited at the following URL:

  https://www.broadcom.com/support/download-search/?dk=SAS2IRCU

In this chapter, from the above, an example using the FCode utility is shown.
For an example of SAS2IRCU utility output, see "Appendix F   SAS2IRCU Utility Command Display Examples."

To create a system (boot) volume in a hardware RAID configuration, use the FCode utility. The FCode utility and SAS2IRCU utility can support the following tasks.

Table 14-1   Tasks Supported by Hardware RAID Utilities

Task Description	Fcode Utility	SAS2IRCU Utility
Creating system (boot) volume	Supported	Not Supported
Creating data volume	Supported	Supported
Creating hot spare	Not Supported	Supported

14.2.1 Basics of Hardware RAID

Hardware RAID is technology that accelerates the data access speed and increases the reliability of data protection by collectively managing at least two internal disk drives.

The SPARC M12/M10 provides hardware RAID through the Integrated RAID function of the built-in on-board SAS controller. Of the hardware RAID types, RAID0, RAID1, RAID10, and RAID1E are supported. You can configure up to two

RAID volumes per SAS controller.

Table 14-2   Supported RAID Types

Model	Number of SAS Controllers per Chassis	Supported RAID Type
SPARC M12-1	1	RAID0/RAID1/RAID10/RAID1E
SPARC M12-2/M12-2S	2	RAID0/RAID1/RAID10/RAID1E
SPARC M10-1/M10-4/M10-4S	1	RAID0/RAID1/RAID1E

In the SPARC M12/M10, you can configure up to two RAID volumes per chassis for the SPARC M10, or up to four RAID volumes for the SPARC M12 by combining the above RAID types.

Note - You cannot configure a RAID volume spanning SAS controllers in the SPARC M12-2/M12-2S or in multiple SPARC M12-2S/M10-4S units.

Supported Disk Drives

To configure hardware RAID in the SPARC M12/M10, use disk drives of the same capacity and speed for each RAID volume in the configuration.
Solid state drives (SSDs) are not supported. Also, external disk drives connected to the SAS port are not supported.

Next, mechanisms of RAID0, RAID1, RAID10, and RAID1E are described.

- RAID0 (striping)
  In this technique, data writing and reading are decentralized to multiple internal disk drives to process them in parallel. RAID0 increases the data access speed, so it is used for work requiring disk acceleration.

  In the SPARC M12/M10, you can configure a RAID0 volume using two to eight disk drives.

Table 14-3   Number of Disk Drives That Can Configure a RAID0 Volume

Model	Number of Disk Drives to Configure
SPARC M12-1/M10-1/M10-4/M10-4S	2 to 8
SPARC M12-2/M12-2S	2 to 4

Figure 14-1　　Mechanism of RAID0

RAID0

1	2
3	4
5	6
7	8
⋮	⋮
HDD1	HDD2
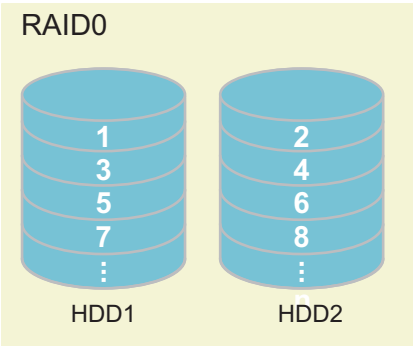
Note - Since RAID0 has no redundancy, a failure of only one disk drive making up RAID0 causes the RAID volume to fail, resulting in the loss of all data.
If a RAID volume failure occurs, it is necessary to reconfigure the RAID volume and then restore it from backup data.

■ RAID1 (mirroring)
This technique duplicates internal disk drives and writes the same data to the duplicated drives to increase data fault tolerance. Even if one of the internal disk drives fails, operation can continue by using the other drive. Moreover, the failed internal disk drive can be replaced while operation continues. However, the disk capacity for saving data is halved.

In the SPARC M12/M10, you can configure a RAID1 volume using two disk drives.

Table 14-4　　Number of Disk Drives That Can Configure a RAID1 Volume

Model	Number of Disk Drives to Configure
SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S	2

Figure 14-2　　Mechanism of RAID1

RAID1

1	1
2	2
3	3
4	4
⋮	⋮
HDD1	HDD2
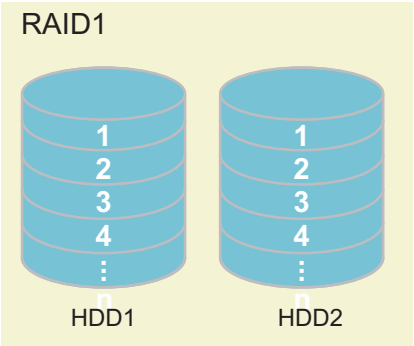
Note - With RAID1, even when one disk drive fails, the system operation continues in the degraded state. However, a failure of both the disk drives causes a RAID volume failure, resulting in the loss of all data.
If the RAID volume enters the degraded state, replace the failed disk drive as soon as possible and recover redundancy.

- RAID10 (mirroring + striping)
  This technique duplicates internal disk drives and splits the data to be written to multiple duplicated groups. RAID10 enables use of four or more internal disk drives.

  In the SPARC M12, you can configure a RAID10 volume using four, six, or eight disk drives.

  The SPARC M10 does not support RAID10.

Note - With RAID10, even when one of the mirrored disk drives fails, system operation continues in the degraded state. However, a failure of both the mirrored disk drives causes a RAID volume failure, resulting in the loss of all data.
If the RAID volume enters the degraded state, replace the failed disk drive as soon as possible and recover redundancy.

Table 14-5   Number of Disk Drives That Can Configure a RAID10 Volume

Model	Number of Disk Drives to Configure
SPARC M12-1	4, 6, or 8
SPARC M12-2/M12-2S	4

Figure 14-3   Mechanism of RAID10
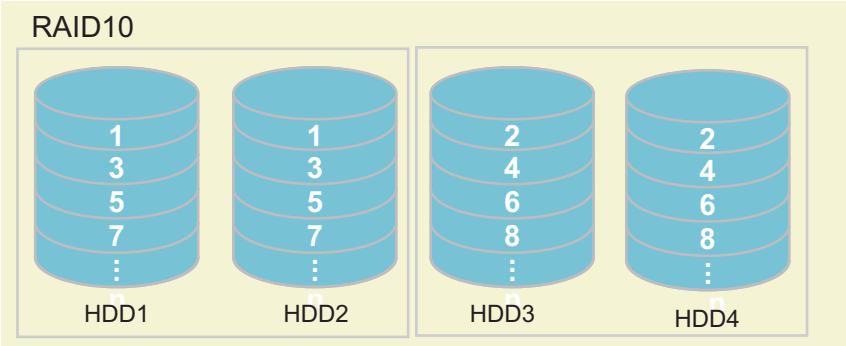
- RAID1E (extended mirroring)
  This technique splits and duplicates data, and then writes the data to multiple internal storage units. RAID1E is an extended type of RAID1, enabling use of three or more internal disk drives.

  In the SPARC M12/M10, you can configure a RAID1E volume using three, five, or seven disk drives.

Table 14-6   Number of Disk Drives That Can Configure a RAID1E Volume

Model	Number of Disk Drives to Configure
SPARC M12-2/M12-2S	3
SPARC M12-1/M10-1/M10-4/M10-4S	3, 5, or 7

Figure 14-4   Mechanism of RAID1E
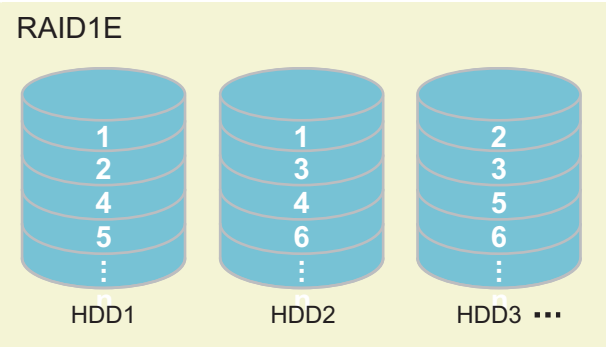
Note - With RAID1E, even when one disk drive fails, system operation continues in the degraded state. However, a failure of two or more disk drives causes a RAID volume failure, resulting in the loss of all data.
If the RAID volume enters the degraded state, replace the failed disk drive as soon as possible and recover redundancy.

14.2.2   FCode Utility Commands

The FCode utility is used to configure hardware RAID. The utility provides the following commands.

Table 14-7   FCode Utility Command List

FCode Command	Description
show-children	Lists all the connected logical drives and logical volumes.
show-volumes	Lists the details of all the connected logical volumes.
create-raid0-volume	Creates a RAID0 volume. Specify at least 2 targets.
create-raid1-volume	Creates a RAID1 volume. Specify 2 targets.
create-raid1e-volume	Creates a RAID1E volume. Specify at least 3 targets. **Note -** If this command is used with an even number of targets (at least 4 targets) specified, the command configures the hardware RAID as RAID10.

Table 14-7   FCode Utility Command List *(continued)*

FCode Command	Description
create-raid10-volume	Creates a RAID10 volume. Specify at least 4 targets. **Note -** If this command is used with an odd number of targets (at least 5 targets) specified, the command configures the hardware RAID as RAID1E.
delete-volume	Deletes a RAID volume.
activate-volume	Enable a RAID volume again after replacing CPU memory units (lower) of the SPARC M12-2/M12-2S/M10-4/M10-4S and motherboard units of the SPARC M12-1/M10-1 systems.

14.2.3   Precautions Concerning Hardware RAID

This section describes the precautions when you use hardware RAID.

Notes When Using Hardware RAID

- Perform backup of important data and programs on a regular basis. For some errors, you may need to restore data or programs from backup media by reconfiguring the hardware RAID.

- We recommend using an uninterruptible power supply (UPS) to ensure that the data in the system can be secured in the case of a power outage.

- If high availability such as duplication of controllers or data paths is required for the hardware RAID function, install a dedicated RAID system.

- Disk redundancy using hardware RAID is possible only under one SAS controller.

SAS2IRCU Utility

- When you manage the hardware RAID environment of the SPARC M12/M10, we recommend using the SAS2IRCU utility (sas2ircu: SAS-2 Integrated RAID Configuration Utility) provided by Broadcom Limited for the following reasons.
  - SAS2IRCU: You can configure and manage a hardware RAID while logical domains are running.

  - OpenBoot PROM environment: You can configure a hardware RAID only when logical domains are stopped, but cannot manage it.

Note - If you use or plan to use the DR function in the SPARC M12-2S/M10-4S, be sure to install the SAS2IRCU utility. After DR integration, the SAS2IRCU utility is needed to enable RAID volumes.

- For details on how to obtain the SAS2IRCU utility, see the Broadcom Limited website described in "14.2   Configuring Hardware RAID." For details on how to use this, see *SAS-2 Integrated RAID Configuration Utility User Guide* on the same website.

- If the RAID volume fails, you can specify the failed disk by using the SAS2IRCU utility.
- The SAS2IRCU utility is used in the Oracle Solaris environment and requires root account privileges. Therefore, the SAS2IRCU utility should be operated by a system administrator.
- The SAS2IRCU utility is used in the logical domain where the SAS controller is assigned. Therefore, install the SAS2IRCU utility in the I/O root domain where the SAS controller on the motherboard is assigned.

Note - The assignment function for PCIe endpoint devices is not supported on the SAS controller in the SPARC M12/M10.

Notes When Configuring/Removing Hardware RAID

- When configuring or removing the hardware RAID, data reliability on a disk is not guaranteed. Be sure to back up data before you initially configure the hardware RAID for the system or remove an installed hardware RAID. After configuring the hardware RAID, you may need to install new data or restore data from backup media.
- Execution of hardware RAID reconfiguration changes the RAID volume-specific information (WWID value). So, if you perform an operation like activation device specification or Oracle Solaris mounting processing, the setting needs to be changed.
- The following table shows the standard time for synchronizing a 600 GB, 900 GB, or 1.2 TB disk drive in the unloaded state due to the configuration or maintenance of the hardware RAID. The synchronization time varies widely depending on the generation and usage state of the disk drives or the load state of systems.

Table 14-8   Standard Synchronization Time for the Hardware RAID

RAID	Number of Disk Drives	Synchronization Time		
		600 GB Disk Drive	900 GB Disk Drive	1.2 TB Disk Drive
1	2	6 hours	8 hours	10 hours
10 (*1)	4	10 hours	15 hours	21 hours
	6	16 hours	21 hours	29 hours
	8	21 hours	31 hours	44 hours
1E	3	20 hours	29 hours	25 hours
	5	35 hours	45 hours	32 hours
	7	54 hours	65 hours	38 hours

*1 Only the SPARC M12 supports RAID10.

- Do not perform tasks which require you to access disk drives, such as Oracle Solaris installation or data restore, while the disk drives are configuring or synchronizing the hardware RAID. From the point of view of RAID volume

safety, we do not recommend rewriting the contents of disk drives before completing the RAID volume configuration. Be sure to perform these tasks after completing RAID volume configuration.

- Only one RAID volume can be configured at a time per SAS controller. When another set of commands to configure the RAID volume are issued for an SAS controller where RAID volume configuration is in process, completion of the first configuration task is followed by the next RAID volume configuration.

- When you configure the hardware RAID, the RAID volume becomes smaller in size than the original disk.

- If the system is restarted or a power outage has occurred and power is recovered while the hardware RAID is being configured or synchronized, start the configuration/synchronization procedure again for the SPARC M10. For the SPARC M12, the configuration/synchronization procedure is restarted from the point when the outage occurred.

Notes about Operating Hardware RAID

Your system may slow down because the hardware RAID controller cannot completely judge whether a disk has a failure. If your system has this problem, follow the procedures below. Be sure to first back up your data before performing the procedures because the hardware RAID will be removed.

1. **Stop applications from using internal storage.**
2. **Remove the hardware RAID.**
3. **Identify whether the problem is related to the disk.**
4. **If the problem is not solved, replace all disks used for the hardware RAID.**
5. **Reconfigure the hardware RAID.**
6. **Restore data from backup media.**

Next, the operation procedures for hardware RAID volumes are described. See the appropriate item indicated depending on the operation you will perform.

Table 14-9   Hardware RAID Operations and References

RAID Volume Operation	References
Configuring a RAID volume	"14.2.4 Preparation Before Hardware RAID Operation" "14.2.5 Creating a Hardware RAID Volume" "14.2.7 Managing a Hot Spare of a Hardware RAID Volume"
Deleting a RAID volume	"14.2.4 Preparation Before Hardware RAID Operation" "14.2.6 Deleting a Hardware RAID Volume"
Replacing disk drives that make up a RAID volume	"14.2.9 Checking for a Failed Disk Drive" "14.2.10 Replacing a Failed Disk Drive"
Re-enabling a hardware RAID after replacing CPU memory units (lower) of the SPARC M12-2/M12-2S/ M10-4/M10-4S and motherboard units of the SPARC M12-1/M10-1 systems	"14.2.11 Re-enabling a Hardware RAID Volume" "14.2.12 Specifying a Hardware RAID Volume as a Boot Device"

14.2.4 Preparation Before Hardware RAID Operation

Use the FCode utility to prepare for hardware RAID operation. Perform this work from xterm or an equivalent terminal that supports scrolling.

Operation Procedure

1. **Power on the system.**
   If powered on already, reboot the system and disable auto boot in OpenBoot PROM.

2. **Confirm that the ok prompt is displayed.**

3. **Execute the show-devs command, and display a list of the server device paths.**
   The following shows an example of the SPARC M10.

```
{0} ok show-devs
      .
      .
/pci@8000/pci@4/pci@0/pci@0/scsi@0
/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
/pci@8000/pci@4/pci@0/pci@0/scsi@0/tape
      .
      .
{0} ok
```

4. **Execute the select command to select the controller for creating a hardware RAID volume.**
   For details on the relationship between device paths and internal HDD slot locations, see "Appendix A   Lists of SPARC M12/M10 System Device Paths."

Note - After executing the select command, you need to execute the unselect-dev command. After the procedure is finished, execute the unselect-dev command according to the directions in 14.2.5 or 14.2.6.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

5. **Execute the .properties command to check the SAS address of the internal SAS controller.**

```
{0} ok .properties
assigned-addresses 81030010 00000000 00000000 00000000 00000100
83030014 00000001 00000000 00000000 00010000
8303001c 00000001 00040000 00000000 00040000
```

```
82030030 00000000 00200000 00000000 00100000
firmware-version 17.00.00.00
mpt-version 2.00
local-wwid 50 00 00 e0 e0 45 00 00  <- SAS address
  :
 Omitted
  :
{0} ok
```

Note - The output result of the .properties command is information that is needed for maintenance of the RAID volume. Be sure to make a note of this information.

6. **Execute the show-children command to display the SAS addresses of the connected drives.**

```
{0} ok show-children

FCode   Version   1.00.56,   MPT   Version   2.00,   Firmware   Version   13.
00.66.00

Target  a
   Unit   0      Disk      TOSHIBA     MBF2600RC                    3706
 1172123568  Blocks,   600   GB
   SASDeviceName   50000393c813ae74    SASAddress   50000393c813ae76
PhyNum   0
Target  b
   Unit   0      Disk      TOSHIBA     MBF2600RC                    3706
 1172123568  Blocks,   600   GB
   SASDeviceName   50000393b81b24ec    SASAddress   50000393b81b24ee
PhyNum   1
   :
  Omitted
   :
Target  12
   Unit   0      Encl   Serv   device      FUJITSU     NBBEXP
         0d32
   SASAddress    500000e0e04d003d     PhyNum   14
```

Note - The output result of the show-children command is information that is needed for maintenance of the RAID volume. Be sure to make a note of this information.

Execute the show-children command to display the SAS addresses of the connected drives.

14.2.5   Creating a Hardware RAID Volume

Use one of the following commands to create a hardware RAID volume, depending on the hardware RAID configuration being created.

- To create a RAID0 volume

```
{0} ok target1 target2 create-raid0-volume
```

- To create a RAID1 volume

```
{0} ok target1 target2 create-raid1-volume
```

- To create a RAID10 volume

```
{0} ok target1 target2 target3 target4 create-raid10-volume
```

Note - RAID10 is not supported on the SPARC M10-4/M10-4S/M10-1.

- To create a RAID1E volume

```
{0} ok target1 target2 target3 create-raid1e-volume
```

The following settings are common to all of these commands.
Specify a target number that can be checked with the show-children command to target 1, target 2, target 3, and target 4. A target cannot belong to multiple volumes. These commands are interactive, so a volume capacity in MB and a volume name of up to 15 characters can be specified. When the volume capacity is not specified, then it is created with the maximum capacity.

Operation Procedure

1. **Prepare for creating a hardware RAID volume.**
   For details, see "14.2.4   Preparation Before Hardware RAID Operation."

2. **From the execution results of the show-children command, determine the targets for creating a hardware RAID volume.**

3. **Execute create-raid0-volume, create-raid1-volume, create-raid10-volume, or create-raid1e-volume to create a hardware RAID volume using physical disks.**
   In the following example, a and b are specified as the targets and a RAID0 volume is created with the maximum capacity volume and without specifying a volume name.

```
{0} ok a b create-raid0-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 1142500 MB
What size do you want?  [1142500]                [Enter]
Volume size will be 2339840000 Blocks, 1197 GB
Enter a volume name:  [0 to 15 characters]       [Enter]
Volume has been created
```

In the following example, a and b are specified as the targets and a RAID1 volume is created with the maximum capacity volume and without specifying a volume name.

```
{0} ok a b create-raid1-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 571250 MB
What size do you want?  [571250]                    [Enter]
Volume size will be 1169920000 Blocks, 598 GB
Enter a volume name:  [0 to 15 characters]          [Enter]
Volume has been created
```

In the following example, a, b, c, and d are specified as the targets and a RAID10 volume is created with the maximum capacity volume and without specifying a volume name.

```
{0} ok a b c d create-raid10-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
Target c size is 1169920000 Blocks, 598 GB
Target d size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 1142500 MB
What size do you want?  [1142500 ]                  [Enter]
Volume size will be 2339840000 Blocks, 1197 GB
Enter a volume name:  [0 to 15 characters]          [Enter]
Volume has been created
```

In the following example, a, b, and c are specified as the targets and a RAID1E volume is created with the maximum capacity volume and without specifying a volume name.

```
{0} ok a b c create-raid1e-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
Target c size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 856875 MB
What size do you want?  [856875]                    [Enter]
Volume size will be 1754880000 Blocks, 898 GB
Enter a volume name:  [0 to 15 characters]          [Enter]
Volume has been created
```

4. **Execute the show-volumes command, and confirm that synchronization of the created RAID volume has completed.**
   The following example checks the contents of the RAID 1 volume.

   ■ Example where synchronization has completed

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  WWID 0d061173730f12d5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                      1169920000 Blocks, 598 GB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2600RC      3706  PhyNum 0
  Disk 1
    Secondary  Optimal
    Target b      TOSHIBA  MBF2600RC      3706  PhyNum 1
{0} ok
```

- Example where synchronization is in progress

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  WWID 0d061173730f12d5
  Optimal  Enabled  Background Init In Progress
  2 Members                                      1169920000 Blocks, 598 GB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2600RC      3706  PhyNum 0
  Disk 1
    Secondary  Optimal
    Target b      TOSHIBA  MBF2600RC      3706  PhyNum 1
{0} ok
```

Note - Confirm that the synchronization has completed, before going to step 5. If you execute
the unselect-dev command while synchronization is in progress, the synchronization
processing stops.

Note - When two RAID volumes are created under the same SAS controller, the RAID
volume created first is numbered as "1", and the RAID volume created second is numbered
as "0".

1. **Execute the unselect-dev command to unselect the controller that was
    selected during preparation.**

```
{0} ok unselect-dev
{0} ok
```

Note - On Oracle Solaris, it is recognized as one disk drive (Vendor is "LSI", Product is
"Logical Volume") per created RAID volume. In addition, incorporating the RAID volume
changes the device path as follows.
Device path of disk drive not incorporated in the hardware RAID:
/device path of the sas controller/iport@f/disk@w[*SAS address of the disk drive*] (or, /scsi_vhci/
disk@g[*SAS device name of the disk drive*])

is changed to:
Device path of the RAID volume:
/*device path of the sas controller*/iport@v0/disk@w[*device name of the RAID volume*]

The following shows output examples when the format command is executed in an environment where both [Disk drives not incorporated in the hardware RAID] and [Hardware RAID volume] exist.

- Example of output message 1
  At Oracle Solaris installation and right after Oracle Solaris installation

```
root# format
Searching for disks... done

AVAILABLE DISK SELECTIONS:
[Disk drive not incorporated in the hardware RAID]
      0. c2t50000394882899F6d0 <TOSHIBA-AL13SEB600-3702 cyl 64986 alt 2 hd 27
sec 668>
          /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394882899f6,0
          /dev/chassis/FUJITSU-BBEXP.500000e0e06d257f/013P_HDD00/disk
[RAID volume]
      1. c3t3DF694DFC21FFDA9d0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
sec 557>
          /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3df694dfc21ffda9,0
```

- Example of output message 2
  Environment where setting to make the built-in disk drive an MPxIO was executed (or Enhanced Support Facility 5.0 or later is applied)

```
root# format
Searching for disks... done

AVAILABLE DISK SELECTIONS:
[Disk drive not incorporated in the hardware RAID]
      0. c0t50000394882899F4d0 <TOSHIBA-AL13SEB600-3702 cyl 64986 alt 2 hd 27
sec 668>
          /scsi_vhci/disk@g50000394882899f4
          /dev/chassis/FUJITSU-BBEXP.500000e0e06d257f/013P_HDD00/disk
[RAID volume]
      1. c3t3DF694DFC21FFDA9d0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
sec 557>
          /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3df694dfc21ffda9,0
```

Note - The following messages may be displayed when Oracle Solaris is started. This indicates that there is no label information on the RAID volume. A RAID volume in this state cannot be used on Oracle Solaris. It is usable on Oracle Solaris after executing the format command, selecting the appropriate RAID volume, and then labeling it.

- Example of output message

```
Jan 16 02:46:48 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:48 solaris          Corrupt label; wrong magic number
```

- Example of executing the format command

```
root@solaris:/root# format
Searching for disks...
Jan 16 02:46:35 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:35 solaris          Corrupt label; wrong magic number
Jan 16 02:46:35 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:35 solaris          Corrupt label; wrong magic number
done
c2t3AA6D102F1BF517Ad0: configured with capacity of 556.97GB
AVAILABLE DISK SELECTIONS:
       0. c2t3AA6D102F1BF517Ad0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
 sec 557>
          /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3aa6d102f1bf517a,0
Specify disk (enter its number): 0
selecting c2t3AA6D102F1BF517Ad0
[disk formatted]
Jan 16 02:46:48 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:48 solaris          Corrupt label; wrong magic number
Jan 16 02:46:54 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:54 solaris          Corrupt label; wrong magic number
Disk not labeled.  Label it now? yes
```

14.2.6   Deleting a Hardware RAID Volume

Use the delete-volume command of the FCode utility to delete a hardware RAID
volume that was created.

```
 {0} ok volume_number delete-volume
```

For volume_number, specify a volume number that is output by the show-volumes
command.
Execution of the command displays a confirmation message asking whether to delete
the RAID volume. Select "yes" or "no" as appropriate.

Operation Procedure

1. **Prepare for deleting a hardware RAID volume.**
   For details, see "14.2.4   Preparation Before Hardware RAID Operation."

2. **Execute the show-volumes command to check for the RAID volume to delete.**

The following example shows that the RAID1 volume was created with volume number 0.

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                 1169920000 Blocks, 598 GB
  Disk 0
    Primary  Optimal
    Target a     TOSHIBA  MBF2600RC      3706  PhyNum 0
  Disk 1
    Secondary  Optimal
    Target b     TOSHIBA  MBF2600RC      3706  PhyNum 1
{0} ok
```

3. **Execute the delete-volume command to delete a RAID volume.**
   The following example deletes the RAID volume with volume number 0.

```
{0} ok 0 delete-volume
The volume and its data will be deleted
Are you sure (yes/no)?  [no] yes
Volume 0 has been deleted
{0} ok
```

4. **Execute the show-volumes command, and confirm that the RAID volume was deleted.**

```
{0} ok show-volumes
No volumes to show
{0} ok
```

5. **Execute the unselect-dev command to unselect the controller that was selected during preparation.**

```
{0} ok unselect-dev
{0} ok
```

14.2.7 Managing a Hot Spare of a Hardware RAID Volume

With a hot spare drive already created, if one of the disk drives of a mirrored RAID volume (RAID1, RAID10, or RAID1E) fails, the on-board RAID controller replaces the failed disk drive with the hot spare drive and resynchronizes data.

Use the SAS2IRCU utility to create or delete a hot spare of a RAID volume. For

details on the SAS2IRCU utility, see the beginning of "14.2   Configuring Hardware RAID." Or, for output examples, see "Appendix F   SAS2IRCU Utility Command Display Examples."

Note - If you configure two RAID volumes with different disk drive capacities, we do not recommend creating a hot spare for the following reasons.
- When the disk drive capacity of a hot spare is smaller than the disk drive configuring the RAID volume
  Re-synchronization is not executed because the hot spare drive cannot replace the failed disk drive.
- When the disk drive capacity of a hot spare is larger than the disk drive configuring the RAID volume
  The hot spare drive replaces the failed disk drive and re-synchronization is executed. However, the RAID disk volume is configured with a different disk drive capacity. (This configuration is not supported.)

14.2.8   Checking the Status of a Hardware RAID Volume and a Disk Drive

This section describes how to check the status of a hardware RAID volume and an internal disk drive within the hardware RAID volume.

To check the status of a hardware RAID volume and a disk drive within the hardware RAID volume, use the Fcode utility or the SAS2IRCU utility with the following commands.

Table 14-10   Status Display Commands of Hardware RAID

Utility Name	Command Name
FCode utility	show-volumes command
SAS2IRCU utility	STATUS command DISPLAY command

The following describes the main status and the description when each utility command is executed.

Table 14-11   Statuses Displayed by Utility Commands of the Hardware RAID

Item	Output Value		Description
	FCode Utility show-volume Command	**SAS2IRCU Utility STATUS Command DISPLAY Command**	
RAID level	RAID0 (Striping)	RAID0	RAID0 (Striping) volume
	RAID1 (Mirroring)	RAID1	RAID1 (Mirroring) volume
	RAID10 (Striped Mirroring)	RAID10	RAID10 (Mirroring + Striping) volume

Item	Output Value		Description
	FCode Utility show-volume Command	**SAS2IRCU Utility STATUS Command DISPLAY Command**	
	RAID1E (Mirroring Extended)	RAID1E	RAID1E (Mirroring Extended) volume
Hardware RAID volume status (typical example)	Optimal	Optimal	Hardware RAID volume operating normally
	Degraded	Degraded	Hardware RAID volume degraded
	Missing	Missing	Hardware RAID volume not found
	Failed	Failed	Hardware RAID volume failed
	Enabled	Enabled	Hardware RAID volume active
	Inactive	Inactive	Hardware RAID volume inactive
	Data Scrub In Progress	None	Data scrub status of a hardware RAID volume This indication is not a problem because the hardware RAID firmware performs automatically.
	Background Init In Progress	Background Init	Hardware RAID volume configuration in process The hardware RAID volume is not fully configured.
	Resync In Progress	Synchronize	Resynchronization of a RAID volume is in process. The hardware RAID volume is not fully configured.
	Consistency Check In Progress	Consistency Check	Hardware RAID volume consistency being checked
Disk drive status (typical example)	Optimal	Optimal (OPT)	Target disk drive incorporated into a hardware RAID volume
	Offline	Failed (FLD)	Target disk drive not incorporated into a hardware RAID volume
	Degraded	Degraded (DGD)	Target disk drive degraded
	Rebuilding	Rebuilding (RBLD)	Target disk drive being incorporated into a hardware RAID volume
	Out Of Sync	Out of Sync (OSY)	Target disk drive out of synchronization with hardware RAID volume

Displaying the Status With the FCode Utility

To check the status of a hardware RAID volume and an internal disk drive within the hardware RAID volume, stop the system and execute the show-volumes command

with the FCode utility.

1. **Confirm that the ok prompt is displayed.**

2. **Execute the select command with the controller name to display its hardware RAID volumes.**

Note - After executing the select command, you need to execute the unselect-dev command. After the procedure is finished, execute the unselect-dev command according to the instruction in step 4.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

3. **Execute the show-volumes command to check RAID volumes.**
   The following example shows the following:

   (1) The RAID type of the hardware RAID volume is "RAID1 (Mirroring)."

   (2) The hardware RAID volume is "Degraded" and "Enabled."

   (3) Of the disk drives that make up the hardware RAID volume, Disk 0 is "incorporated as Primary (Optimal)."

   (4) Of the disk drives that make up the hardware RAID volume, Disk 1 is "not incorporated as the Secondary (Offline)" and is "out of synchronization (Out Of Sync)."

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring) <-- (1)
  Name raid1-volume  WWID 0c233a838262c6c5
  Degraded  Enabled <-- (2)
  2 Members                                1169920000 Blocks, 598 GB
  Disk 0
    Primary  Optimal <-- (3)
    Target a     TOSHIBA  MBF2600RC       3706  PhyNum 0
  Disk 1
    Secondary  Offline  Out Of Sync <-- (4)
    Target b     TOSHIBA  MBF2600RC       3706  PhyNum 1
{0} ok
```

Note - The error status of the disk drive itself can be displayed after it is released from the hardware RAID.

---

4. **Use the unselect-dev command to unselect the controller that was selected during preparation.**

```
{0} ok unselect-dev
{0} ok
```

Displaying the Status With the SAS2IRCU Utility

You can also use the SAS2IRCU utility to check the status of a hardware RAID volume and an internal disk drive within the hardware RAID volume.
For details on the SAS2IRCU utility, see the beginning of "14.2   Configuring Hardware RAID."

14.2.9   Checking for a Failed Disk Drive

This section describes how to check for a failure in the internal disk drives that make up a RAID volume.
You can confirm faulty disk drives using any of the methods or combination of the methods listed below.

Checking the LEDs of Disk Drives

If a failure occurs in any of the disk drives in the system, the CHECK LED (amber) on the front of that disk drive goes on. With this CHECK LED, you can identify the disk drive where the failure occurred in the system. For the locations and detailed descriptions of these LEDs, see "Understanding the System Components" in the *Service Manual* for your server.

Checking an Error Message

If a failure occurs in a disk drive, the console screen displays an error message. You can also check for such a message by opening the /var/adm/messages file.

This procedure describes how to check for the slot of a failed disk drive within the hardware RAID volume or a failed hot spare disk drive.

(1)   Check the DevHandle value of the failed disk drive.
In the following example of an error message, the value is "11" (DevHandle 0x11).

```
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now offline Jun 10 16:33:33 A4U4S429-D0 scsi: /
pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now , active, out of sync, write cache enabled
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now , active, out of sync Jun 10 16:33:33
A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded Jun 10 16:33:33 A4U4S429-D0
 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now degraded Jun 10 16:33:33
A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded Jun 10 16:33:33 A4U4S429-D0
 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
```

```
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now , enabled, active, data scrub in
progress Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/
pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded Jun 10 16:33:33 A4U4S429-D0
 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now , enabled, active, data scrub in
progress
```

(2) Check the output results from the show-children command, which were recorded beforehand.
The PhyNum value of the Target value matching the DevHandle value obtained from the check in step (1) indicates the slot of the failed disk drive.
In the following example, the PhyNum value of Target 11 is 7, so it can be determined that the failed disk drive is in slot 7.

```
    {0} ok show-children
        :
      Omitted
        :
Target   11
     Unit   0       Disk        TOSHIBA     MBF2600RC                    3706
 1172123568   Blocks,    600    GB
     SASDeviceName   50000393c813ae72    SASAddress   50000393c813ae74
PhyNum   7
        :
      Omitted
        :
```

Note - A change of the disk drive mounting status also changes the DevHandle value.

Displaying the Status With the FCode Utility

To check for a disk drive failure, stop the system, and use the show-volumes command of the FCode utility command.

For details, see "14.2.8   Checking the Status of a Hardware RAID Volume and a Disk Drive."

Displaying the status with the SAS2IRCU utility

You can also use the SAS2IRCU utility to check for a disk drive failure.
For details on the SAS2IRCU utility, see the beginning of "14.2   Configuring Hardware RAID." Also, for the display status with SAS2IRCU utility, see "14.2.8 Checking the Status of a Hardware RAID Volume and a Disk Drive" and for display examples, see "Appendix F   SAS2IRCU Utility Command Display Examples."

14.2.10 Replacing a Failed Disk Drive

This section describes how to replace a failed disk drive among the disk drives that make up a RAID volume.

RAID0

If a disk drive in a RAID0 volume fails, all the data in the volume is lost. Replace the failed disk drive with a new disk drive of the same capacity, re-create the RAID0 volume, and restore the data from a backup.

RAID1/RAID10/RAID1E

Replace the failed disk drive with a new disk drive of the same capacity. Synchronization begins when the new disk drive is incorporated into the RAID volume.

Note - If two disk drives fail at the same time, the RAID volume enters the failed state (Failed).
Replace the failed disk drive, re-create the RAID volume, and then restore the data from backup.

In a hot spare configuration, the hot spare disk drive is automatically re-synchronized to restore data. Replace the faulty disk drive immediately without booting or rebooting Oracle Solaris or starting OpenBoot PROM.
Otherwise, if you replace the faulty disk drive after booting or rebooting Oracle Solaris or starting OpenBoot PROM, switching to the hot spare disk drive does not occur when the disk drive fails again.
In this case, after replacing the faulty disk drive, delete the hot spare setting of the disk drive and create one again to enable recovery.

Use the SAS2IRCU utility to delete/create a hot spare. See the Appendixes "F.6 Deleting a Hot Spare of a Hardware RAID Volume" and "F.5   Creating a Hot Spare of a Hardware RAID Volume."

14.2.11 Re-enabling a Hardware RAID Volume

This section describes how to re-enable a hardware RAID volume after replacing the CPU memory unit (lower) of the SPARC M12-2/M12-2S/M10-4/M10-4S or the SPARC M12-1/M10-1 motherboard unit.
After replacing the unit mentioned above, the hardware RAID volume is inactive because there is no hardware RAID information on the SAS controller (hardware RAID controller). Therefore, you need to re-enable the hardware RAID volume by using the following procedures.

1. **Select the device, display its volume information, and confirm that it is not enabled.**

Note - After executing the select command, you need to execute the unselect-dev command.

After the procedure is finished, execute the unselect-dev command according to the instruction in step 4.

In the following example, the indication Inactive is shown, meaning that the RAID volume is inactive.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Inactive  Consistent
  2 Members                                  1169920000 Blocks, 598 GB
  Disk 0
    Primary  Optimal
    Target a     TOSHIBA  MBF2600RC      3706 PhyNum 0
  Disk 1
    Secondary  Optimal
    Target b     TOSHIBA  MBF2600RC      3706 PhyNum 1
{0} ok
```

2. **Execute the activate-volume command to enable the RAID volume.**
   The following example shows that the RAID volume with volume number 0 is re-enabled.

```
{0} ok 0 activate-volume
Volume 0 is now activated
{0} ok
```

3. **Execute the show-volumes command, and confirm that the RAID volume is enabled.**
   In the following example, the indication Data Scrub in Progress is shown, meaning that the RAID volume is active.

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                  1169920000 Blocks, 598 GB
  Disk 0
    Primary  Optimal
    Target a     TOSHIBA  MBF2600RC      3706 PhyNum 0
  Disk 1
    Secondary  Optimal
    Target b     TOSHIBA  MBF2600RC      3706 PhyNum 1
{0} ok
```

4. **Execute the unselect-dev command to unselect the controller that was selected during preparation.**

```
{0} ok unselect-dev
{0} ok
```

Note - Perform the shutdown processing correctly before replacing the CPU memory unit (lower) of SPARC M12-2/M12-2S/M10-4/M10-4S or the SPARC M12-1/M10-1 motherboard unit. Then, confirm that the system stopped, and replace the part.

If the system stops without the shutdown processing due to a blackout, etc., an unintended media check may be executed after the RAID volume is enabled.

During a media check, you cannot get the media check status from the Fcode utility or the SAS2IRCU utility. During this time, the RAID volume state becomes Optimal. Check whether the LED of the disk drive is blinking to confirm the media check execution status. When the LED of the disk drive changes from blinking to on, it means that the media check has ended.

During the media check, you can access the hardware RAID volume as is normally done, but the I/O performance may be insufficient, compared to the hardware RAID volume when the media check is not being executed.

The required media check time is the same as the synchronization time for hardware RAID configuration or maintenance. For the standard required time, see "Table 14-8   Standard Synchronization Time for the Hardware RAID."

14.2.12   Specifying a Hardware RAID Volume as a Boot Device

This section describes how to specify a hardware RAID volume as a boot-device.

For details on specifying a boot device, see "Appendix I   How to Specify the Boot Device."

1.   **Select the device and display its volume information.**
     Check the WWID of the RAID volume.

     The following is an example of the SPARC M10. Check the WWID of the RAID volume.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                       1169920000 Blocks, 598 GB
  Disk 1
    Primary  Optimal
    Target a      TOSHIBA  MBF2600RC       3706 PhyNum 0
  Disk 0
    Secondary  Optimal
    Target b      TOSHIBA  MBF2600RC       3706 PhyNum 1
{0} ok unselect-dev
{0} ok
```

2. **Specify the RAID volume that was confirmed in step 1 as the boot device.**
   Follow the rules below when specifying the RAID volume.
   a. Replace the number "0" at the beginning of WWID of the RAID volume with "3".
      Since the WWID of the RAID volume that was confirmed in Step 1 is "0c233a838262c6c5," it becomes "3c233a838262c6c5."
   b. To the WWID of the RAID volume in step 2a, (the one in which you replaced a digit), add "disk@w" to the beginning of it, and append ",0:a" to its end.
   c. Specify the full pathname of the RAID boot device as the argument to the setenv boot-device command below. The full pathname is the device path selected in step 1, "/pci@8000/pci@4/pci@0/pci@0/scsi@0/", followed by the RAID boot device name from step 2b, "disk@w3c233a838262c6c5,0:a".

```
{0} ok setenv boot-device /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@
w3c233a838262c6c5,0:a
```

14.3 Using the LDAP Service

Lightweight Directory Access Protocol (LDAP) is a protocol that is used to access a directory service on a network. Normally, user authentication and user privileges of an XSCF user account on the SPARC M12/M10 are managed by the local master XSCF. However, by using LDAP, they can be managed by a directory service (LDAP server) on a network. In addition, if multiple SPARC M12/M10 systems are installed, the XSCF user account common to all systems can be used with LDAP.
To manage the XSCF user account settings, such as user authentication and user privileges, using LDAP, configure the XSCF as an LDAP client.

For details on how to manage the XSCF user account settings through a directory service on a network using LDAP, see "3.5.12 Managing XSCF User Accounts Using LDAP."

14.4 Using SAN Boot

The SPARC M12/M10 supports SAN boot.

SAN boot is a system with external storage, rather than a built-in internal disk drive in the server, configured as the startup disk.

The SPARC M12/M10 uses a Fibre Channel card for connections between external storage devices, and the system can be configured to use SAN boot with the Fcode function of OpenBoot PROM.

For details about building a system using SAN boot, see the following Oracle document:

- Oracle Solaris Administration: SAN Configuration and Multipathing

14.5 Using iSCSI

iSCSI is a protocol used to exchange SCSI commands via an IP network. The commands are used for communication between the server and external storage.

In the SPARC M12/M10, you can configure the system to use iSCSI. Once the system is configured to use iSCSI, multiple servers can share large-capacity storage connected over a TCP/IP network.

14.6 Remote Power Management for the SPARC M12/M10 and I/O Devices

This section provides an outline of the remote power management function and a description of its settings for the SPARC M12/M10.

14.6.1 Remote Power Management Function for the SPARC M12/M10

The remote power management function for the SPARC M12/M10 system (Remote Cabinet Interface over LAN: RCIL) is an interface which controls the remote power management function for the power supply between SPARC M12/M10 systems or I/O devices. RCIL employs a proprietary interface based on IPMI over LAN. If the following functions of general IPMI are supported, RCIL can be set as the target of remote power management without regard to differences in the controlled hardware or operating systems. RCIL uses the XSCF-LAN on the SPARC M12/M10.

- Power on and off: Chassis Control
- Obtaining power supply status: Get Chassis Status

Table 14-12 shows the terms and definitions that are used with the remote power management function for the SPARC M12/M10.

Table 14-12   Terms and Definitions Used for Remote Power Management

Term	Definition
Host node	A SPARC M12/M10 chassis that supports the remote power management function. SPARC M12-2, M12-2S, M10-1, M10-4, and M10-4S support the remote power management function for the system. The host node set as master when setting a remote power management group is referred to as the master host node. The master host node is a host node that monitors connections with other host nodes and I/O nodes.
Sub node	A physical partition in the SPARC M12/M10
I/O node	An I/O device or a power supply control box that supports the remote power management function for the SPARC M12/M10
Remote power management group	Group obtained from the grouping of remote power management targets, such as a host node, subnode, and I/O node. A unique group ID is assigned to a remote power management group.
Controller	A mechanism to control the remote power management function. A controller needs to be mounted in each node. In the SPARC M12/M10, the XSCF is a controller.

If the remote power management function is used, create a remote power management group in combination with power-interlocked nodes. You can control remote power management per created remote power management group.

Note - Each host node, sub node, or I/O node can be set in only one remote power management group.

Figure 14-5   Example of a Remote Power Management Group of the SPARC M12/M10

Table 14-12   Terms and Definitions Used for Remote Power Management

Term	Definition
Host node	A SPARC M12/M10 chassis that supports the remote power management function. SPARC M12-2, M12-2S, M10-1, M10-4, and M10-4S support the remote power management function for the system. The host node set as master when setting a remote power management group is referred to as the master host node. The master host node is a host node that monitors connections with other host nodes and I/O nodes.
Sub node	A physical partition in the SPARC M12/M10
I/O node	An I/O device or a power supply control box that supports the remote power management function for the SPARC M12/M10
Remote power management group	Group obtained from the grouping of remote power management targets, such as a host node, subnode, and I/O node. A unique group ID is assigned to a remote power management group.
Controller	A mechanism to control the remote power management function. A controller needs to be mounted in each node. In the SPARC M12/M10, the XSCF is a controller.

If the remote power management function is used, create a remote power management group in combination with power-interlocked nodes. You can control remote power management per created remote power management group.

Note - Each host node, sub node, or I/O node can be set in only one remote power management group.

Figure 14-5   Example of a Remote Power Management Group of the SPARC M12/M10

14.6.2 Understanding Forms of Connection for Remote Power Management

Connect through a LAN the host nodes, sub nodes, and I/O nodes that support the remote power management function for the SPARC M12/M10.

The connection specifications are as follows.

Table 14-13   Power Supply Control Connection Specifications

Item	Description
Forms of connection	LAN connection The connection takes either of the following forms: - Using XSCF-LAN#0 - Using XSCF-LAN#0 and XSCF-LAN#1
Transmission rate	100 Mbps or more
Internet protocol	IPv4
DHCP	Not supported If the remote power management function for the SPARC M12/M10 is used, you must set a fixed IP address for a connection target.
Connection protocol	IPMI(*1) over LAN (Intelligent Platform Management Interface)

*1 The supported IPMI version is IPMI 2.0.
   In a SPARC M12/M10, IPMI can be used only internally by the remote power management function. IPMI cannot be used by ipmitool or any function other than the remote power management function of the SPARC M12/M10.

Standard Connection for Remote Power Management

Connect through an identical LAN the host nodes, sub nodes, and I/O nodes that are equipped with a controller that supports the remote power management function for the SPARC M12/M10.

Figure 14-6   Forms of Connection for Remote Power Management
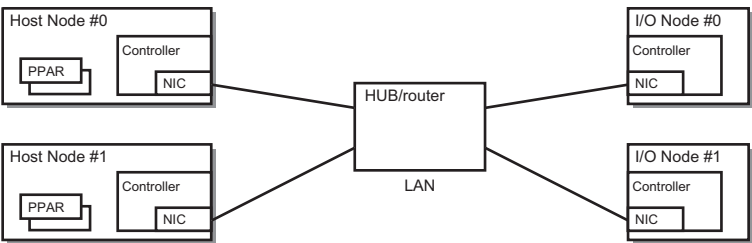
Connection in the Case of Duplexed Controllers

If the controllers of a host node are duplexed, each controller can be connected to an identical LAN. Operation of the remote power management is performed from the master XSCF.

Figure 14-7   Forms of Connection for Remote Power Management When the Controllers are Duplicated
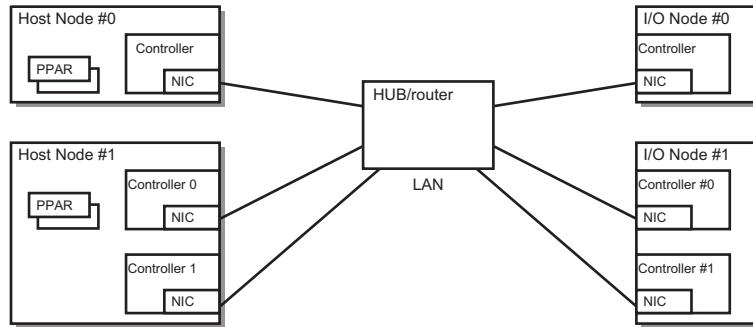
Note - We recommend setting a takeover IP address on the I/O nodes that can set a takeover IP address between controllers. In this case, set controller 0 and controller 1 to the same IP address in the management file for configuring the remote power management group. For specific settings, see "3.1.1   System That is Configured with a Host Node and an I/O Node" in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide.*

Connection in the Case of Duplexed Paths

If the following conditions are met, the connection paths for remote power management can be duplexed.

- When two LAN cards can be installed on each controller of all nodes

- When two LAN cards can be installed on a controller of a host node, and an I/O node has either of the following configurations
  - Controllers of an I/O node are duplexed
  - Two LAN cards can be installed on a controller of an I/O node

Figure 14-8   Forms of Connection for Remote Power Management in the Case of Duplexed Paths
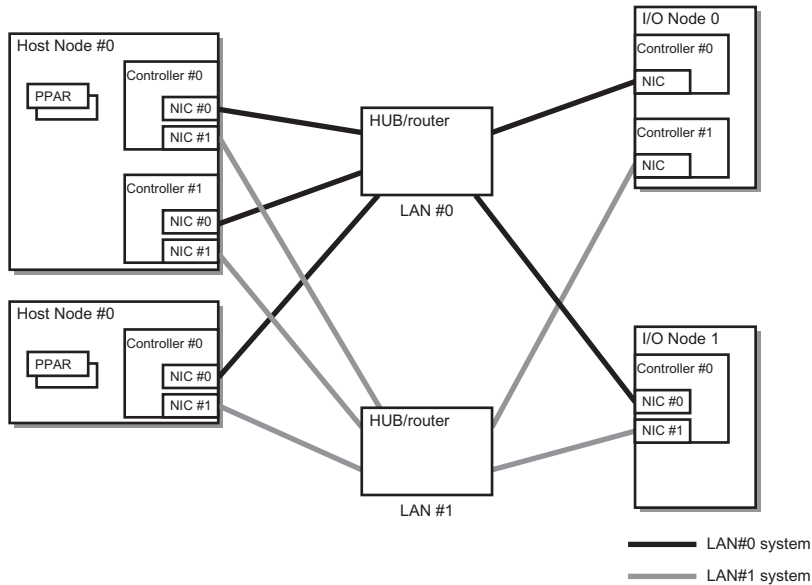
14.6.3   Remote Power Management Structure

Remote power management for the SPARC M12/M10 is controlled per the remote power management group.

Of the host nodes in a group, the host nodes with the remote power management function enabled are targeted for remote power management. The power supply status of a remote power management group is determined depending on the host node status in the group.

- On status
  When the status of the power supply of any one of the host nodes in the remote power management group is on

- Off status
  When the status of the power supplies of all host nodes in the remote power management group is off

This section describes remote power-on and power-off management structures based on the following settings.

Table 14-14   Remote Power Management Structure (Example)

Setting Item	Host Node#0	Host Node#1	Host Node#2	I/O Node#0	I/O Node#1
Remote management setting	Disable	Enable	Enable	Setting disabled	Setting disabled
Master node	Yes	No	Yes	Setting disabled	Setting disabled

Mechanism of Interlocking When Powering On

If any of the host nodes in a remote power management group is powered on, then all of the host nodes, subnodes, and I/O nodes in the group are powered on. Host nodes are powered on, followed by I/O nodes.

Note - You can set a time for host nodes to wait until I/O node devices are accessible. Use the setpowerupdelay command of the XSCF firmware to make the setting. For details, see "4.2.2 Setting/Checking the Wait Time for Air Conditioning."
If you do not set the wait time, the system may fail to start when a host node attempts to access an I/O node device that is inaccessible.
In addition, if I/O nodes are switched or the setting is changed, the time to access the devices changes. So, the devices may not be accessed when a host node attempts to access one.
If you have switched I/O nodes or changed the setting, use the setpowerupdelay command to set a new wait time.

Remote Power-off Management Structure

All the host nodes in a remote power management group are powered off, followed by all the I/O nodes in the group.

Remote Power Management by Wake on LAN

Generally, the target nodes of the remote power management function of the SPARC M12/M10 are the hosts and I/O devices on which a controller is mounted. The controller allows IPMI communication even while the power of the hosts and I/O devices is turned off.
When all of the following conditions are satisfied, those devices on which such a controller is not mounted can also remotely manage power using the remote power management function of the SPARC M12/M10.

- Device conditions
  - Wake on LAN is supported.
    Power-on is performed with Wake on LAN.

  - IPMI communication can be performed.
    After power-on using Wake on LAN, IPMI communication through the LAN is used for performing power-off and obtaining the power state.

Note - A host node where Wake on LAN is set cannot become a master node.

Note - Wake on LAN cannot be set for the SPARC M12/M10 chassis. Therefore, Wake on LAN cannot be used to power on the SPARC M12/M10 chassis.

Note - The Wake on LAN setting varies depending on the node. See the manuals for each node.

Interlocking at the Failure Recovery Time

If a node in a remote power management group cannot communicate when recovered from a failure or other problem, operation is as follows.

- In the case of an I/O node failure
  If the power supply status of a remote power management group is on, the master host node issues an instruction to power on.

- In the case of host node failure
  Even if the power supply status of a remote power management group is on, the master host node does not issue an instruction to power on.

14.6.4 Before Setting Remote Power Management

If you set remote power management, connect the LAN cables and configure the network settings in advance on the XSCF-LAN and I/O devices that perform remote power management.

14.6.5 Flow for Setting Remote Power Management

This section describes the flow for setting remote power management, divided into the following cases:

- Setting the remote power management function for the first time
- Adding, deleting, or replacing nodes in an existing remote power management group

Setting Remote Power Management for the First Time

The following figure describes the flow for setting remote power management for the first time.

Note - If an existing remote power management setting is enabled, initialize the remote power management setting.

Figure 14-9   Flow for Setting Remote Power Management for the First Time

```
┌─────────────────────────────────────────────┐
│         Create the management file.          │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│  Enable the IPMI service used by the remote  │
│     power management function of the XSCF.    │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│   Configure a remote power management group   │
│         by using the management file.         │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│  Enable the remote power management function. │
└─────────────────────────────────────────────┘
```
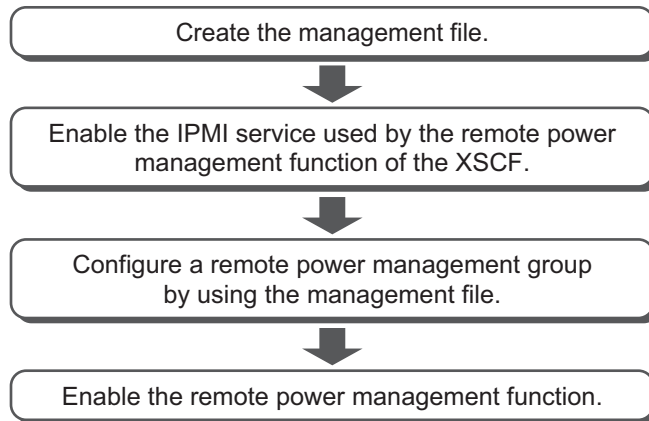
Note - XCP 2290 and later support the enable/disable setting for the IPMI service.

Adding, Deleting, or Replacing Nodes in an Existing Remote Power Management Group

The following figure describes the flow for adding, deleting, or replacing nodes in an existing remote power management group.

Figure 14-10   Flow for Adding, Deleting, or Replacing Nodes in an Existing Remote Power Management Group

```
┌─────────────────────────────────────────────┐
│   Acquire the setting information of the existing  │
│       remote power management group.          │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│       Update the acquired management file.    │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│  Disable the remote power management function. │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│    Set the remote power management group      │
│         using the management file.            │
└─────────────────────────────────────────────┘
                      ▼
┌─────────────────────────────────────────────┐
│  Enable the remote power management function. │
└─────────────────────────────────────────────┘
```
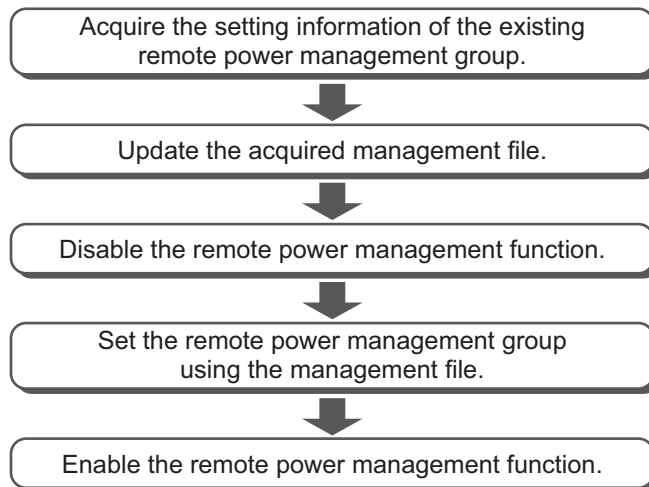
14.6.6 Checking the Remote Power Management Setting

Use the showremotepwrmgmt command of the XSCF firmware to check the remote power management setting.

```
XSCF> showremotepwrmgmt [-a|-G groupid [-N gnodeid]]
```

To check all the remote power management settings, specify -a. To specify a remote power management group, specify -G groupid. To specify a node in a remote power management group, specify -N gnodeid.

14.6.7 Initializing the Remote Power Management Setting

Use the clearremotepwrmgmt command of the XSCF firmware to initialize the remote power management setting.

```
XSCF> clearremotepwrmgmt [-a|-G groupid]
```

To initialize the settings of all the remote power management groups, specify -a. To specify a remote power management group, specify a group ID with the -G option. If -a and -G are omitted, the system assumes -a is specified.

14.6.8 Enabling/Disabling the Remote Power Management Function

Use the setremotepwrmgmt command of the XSCF firmware to enable/disable the remote power management function.

```
XSCF> setremotepwrmgmt -c enable|disable
```

To enable the remote power management function, specify -c enable. To disable it, specify -c disable.

14.6.9 Creating a Management File

Create a management file in csv format for setting remote power management groups. You can create the management file and store it by using a URL that is accessible with the http, https, ftp, or file scheme.
The management file description format is as follows.

```
1,1,0x01,8a041209b35947899e7bfa5d578dbd3f,0x03,0x00,default,,10.
24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,,"4,5,6,7,8,9,10,11,12"
 1,2,0x00,8a041209b35947899e7bfa5d578dbd40,0x03,0x00,default,,
10.
24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,,
1,3,0x10,8a041209b35947899e7bfa5d578dbd41,0x03,0x00,default,,10.
24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,,  (Omitted)
1,128,0x20,8a041209b35947899e7bfa5d578dbd42,0x03,0x00,default,,1
0.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,,
```

For each row, specify the following in the order shown: GroupID, NodeID,
NodeType, NodeIdentName, Linkage, Operation, User, Password, IP0-0, Slave0-0,
MAC0-0, IP0-1, Slave0-1, MAC0-1, IP1-0, Slave1-0, MAC1-0, IP1-1, Slave1-1, MAC1-1,
and SubNode.

The setting item details are as follows.

Table 14-15 Setting Items for the Management File for Remote Power Management

Item	Description
GroupID	Group ID of remote power management group You can specify an integer (decimal) from 1 to 32. All the group IDs in one management file must be identical.
NodeID	Node ID of remote power management device You can specify an integer (decimal) from 1 to 128. The node IDs in one management file must be unique.
NodeType	Node type of remote power management device Specify any of the following values. 0x00: host node, 0x01: master host node, 0x10: I/O node, 0x20: remote power management box
NodeIdentName	Distinguished name of remote power management device You can specify a System GUID or any unique character string. As shown in the example, System GUID is specified as 32 consecutive digits. The value is handled as hexadecimal with case ignored. In the case of any character string, you can specify the value in hexadecimal using up to 32 digits.
Linkage	Value representing remote power-on management (hexadecimal) Specify any of the following values. 0x00: Disable, 0x01: Enable (On), 0x02: Enable (Off), 0x03: Enable (On+Off)
Operation	Value representing power-on method Specify it using either of the following ways. 0x00:IPMI, 0x01:WakeOnLAN
User	IPMI user name Leave it blank without specifying anything. If it is not blank, operation is not guaranteed.
Password	IPMI password Leave it blank without specifying anything.

Table 14-15　　Setting Items for the Management File for Remote Power Management
(continued)

Item	Description
IPAddress	IP address of IPMI port of controller You can specify an IPv4 address with a character string.
SlaveAddress	Value representing IPMI slave address of controller (hexadecimal) Specify "0x20".
SubNodeID	Character string representing a sub node ID that is control target 0 to 31, or blank. You can specify the target sub node IDs (decimal) by separating them with a comma (,), and enclosing everything in double quotation marks ("). A blank indicates that the entire node is the control target.

14.6.10　Enabling/Disabling the IPMI Service Used by the Remote Power Management Function of the XSCF

To use the remote power management function, you must enable the IPMI service.
The IPMI service can be used only by the remote power management function.
Enable/disable the IPMI service by using the setpacketfilters command on the XSCF.

```
XSCF> setpacketfilters -c ipmi_port [enable|disable]
```

To enable the IPMI service, specify -c ipmi_port enable. To disable it, specify -c ipmi_port disable.
The default value is disable.

Note - XCP 2290 and later support the enable/disable setting for the IPMI service.
In XCP 2280 and earlier, the IPMI service is enabled, and you cannot disable it.
If the firmware is updated from XCP 2280 or earlier to XCP 2290 or later, the IPMI service will be set as follows:
- When the remote power management function is used: enable
- When the remote power management function is not used: disable

14.6.11　Obtaining Setting Information on a Remote Power Management Group

Use the getremotepwrmgmt command of the XSCF firmware to obtain the setting information on a remote power management group.

```
XSCF> getremotepwrmgmt -G groupid configuration_file
```

For groupid, you can specify the ID of a remote power management group whose

setting information is obtained. For a configuration file, you can specify the name of the management file that stores the obtained setting information.

14.6.12 Setting a Remote Power Management Group

Use the setremotepwrmgmt command to configure a remote power management group by using the management file.

```
XSCF> setremotepwrmgmt -c config configuration_file
```

You can specify -c config if you configure a remote power management group. For configuration_file, you can specify the name of the management file used for configuring.

14.7 Using an Uninterruptible Power Supply

The SPARC M12/M10 supports connection of an uninterruptible power supply (UPS) as an option.

Using an uninterruptible power supply (UPS) enables a stable supply of electrical power to the system in the event of a power failure, power outage, etc. An APC-manufactured uninterruptible power supply (UPS) is supported, and a LAN is used as the interface between the domains and UPS.

For details on how to connect an uninterruptible power supply, see "Uninterruptible power supply (UPS) connection (optional)" in the *Installation Guide* for your server.

14.8 Using Verified Boot

This section describes the verified boot function that provides security protection when Oracle Solaris is started.

14.8.1 Basics of Verified Boot

Verified boot is a function that secures the SPARC M12/M10 from threats that can be present in drivers, modules, or other programs loaded when Oracle Solaris is started.

The boot process of a system is verified and secured from the following threats:
- Damaging a kernel module
- Inserting a malicious program (Trojan horse virus, spyware, rootkit, etc.) that pretends to be a legitimate kernel module, or replacing a program with such a

program
- Loading an unapproved third-party kernel module

Oracle Solaris 11.2 provides two types of methods for configuring the verified boot function: using an XSCF and using Oracle Solaris. In Oracle Solaris 11.3 or later, only the configuration method using an XSCF is available.
This section describes the method for configuring the function with an XSCF. For the method for configuring the function with Oracle Solaris, see "How to Enable Verified Boot on Legacy SPARC Systems and x86 Systems" in the *Securing Systems and Attached Devices in Oracle Solaris 11.2* of Oracle Solaris.

14.8.2 Mechanism of Boot Verification by Verified Boot

Boot verification by verified boot requires X.509 public key certificates registered with the XSCF. The system boot process performs boot verification by using public keys contained in the X.509 public key certificates.

The mechanism to perform boot verification is as follows:
- A user configures verified boot with the XSCF that supports the verified boot function. In this configuration work, the user registers or selects an X.509 public key certificate and sets policies that control the behavior of boot verification. Configuration information is saved in the master XSCF.
- Suppose that the verified boot configuration information in the XSCF is changed. The changed configuration information becomes valid for the boot verification of all modules the next time that OpenBoot PROM is started.
- When a physical partition is started, the configuration information is reported to the OpenBoot PROM firmware and Oracle Solaris via the XSCF, and they perform boot verification. Boot verification is also performed when a physical partition, the OpenBoot PROM firmware, or Oracle Solaris is restarted.

Boot verification by the OpenBoot PROM firmware and Oracle Solaris is performed in the order shown in Figure 14-11.

Figure 14-11   Order of Boot Verification
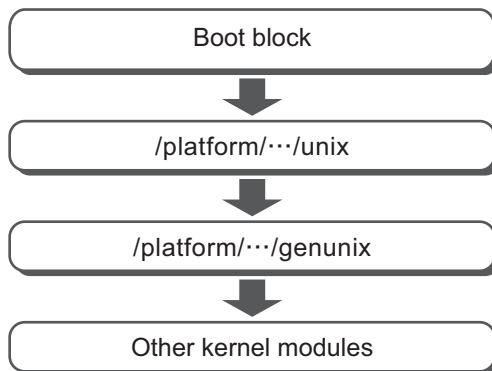
14.8.3 X.509 Public Key Certificates for Verified Boot

Table 14-16 shows the two types of X.509 public key certificates used for verified boot.

Table 14-16   X.509 Public Key Certificates Used for Verified Boot

Certificate Type	Description
System default certificate (System default)	System default certificate that the XSCF has The XSCF has the same certificate as the public key certificate (/etc/certs/*SE) contained in Oracle Solaris. The XSCF has 1 or 2 system default certificates, which are replaced with the latest public key certificates at the time of firmware update. Therefore, system default certificates are not subject to save/restore from the system. In addition, they are not certificates that users can manipulate.
User's certificate	Certificate registered by a user A certificate issued by a third party is registered as a user's certificate with XSCF. Up to 5 user's certificates can be registered with the XSCF for each physical partition. When enabled, a registered certificate can be used for boot verification. User's certificates are subject to save/restore on the system. However, saved certificates cannot be restored in other SPARC M12/M10.

Boot verification is performed by using the system default certificate(s) and enabled user's certificates.

14.8.4 Verified Boot Policies

Table 14-17 lists the two policies that control verified boot.

Table 14-17   Verified Boot Policies

OS Version	Policy	Description
Oracle Solaris 11.2	Boot policy (boot_policy)	Sets boot verification for the boot block, unix, and genunix. These modules are loaded first during a boot process.
	Module policy (module_policy)	Sets boot verification for kernel modules that need to be loaded after genunix.
Oracle Solaris 11.3 or later	Boot policy (boot_policy)	Sets boot verification for the boot block and unix. These modules are loaded first during a boot process.
	Module policy (module_policy)	Sets boot verification for genunix and kernel modules.

Use the setvbootconfig command of the XSCF firmware to set each policy.
Users can set the behavior of the boot process at the time of boot verification failure by setting the policies.
Table 14-18 lists values that can be set as each of the boot and module policies. The set value determines the verification operation.

Table 14-18   Policy Setting Values

Policy Setting Value	Operation
none	Boot verification is not performed. (Default)
warning	Boot verification is performed. Verification is performed before the target of the verification is loaded. Even if the verification fails, the target of the verification is loaded and boot processing continues. If verification of the boot block and unix fails, the failure of the verification is recorded on the system console. It is not recorded in the system log and XSCF error log. If verification of genunix and other kernel modules fails, the failure of the verification is recorded on the system console and in the system log. It is not recorded in the XSCF error log.
enforce	Boot verification is performed. Verification is performed before the target of the verification is loaded. If verification of the boot block and unix fails, boot processing stops. At this time, the failure of the verification is recorded on the system console and the XSCF error log. It is not recorded in the system log. If verification of genunix fails, boot processing stops. At this time, the failure of the verification is recorded on the system console. It is not recorded in the XSCF error log and the system log. If verification of other kernel modules fails, the boot continues without loading the module. At this time, the failure of the verification is recorded on the system console and in the system log. It is not recorded in the XSCF error log.

Note - In Oracle Solaris 11.2 SRU11.2.8.4.0 or later, if the policy setting value is enforce, the operation after verification of genunix fails is different. If the OpenBoot PROM environment variable auto-boot? is true, a panic occurs repeatedly. If this phenomenon persists, execute the sendbreak command for the control domain, the ldm stop command for a guest domain, or the zoneadm halt command for a kernel zone to stop it.

Table 14-19 shows an example of the messages output when boot verification fails.

Table 14-19   Example of Messages Output When Boot Verification Fails

Policy Setting Value	Message
none	Boot verification is not performed.

warning	The following warning message appears, but the start of Oracle Solaris continues.
	 - System console message in the case of genunix
	    WARNING: module /platform/sun4v/kernel/sparcv9/genunix failed elfsign verification.
	 - System console or system log message in the case of other kernel modules
	    WARNING: module /kernel/drv/sparcv9/*module* failed elfsign verification.

Policy Setting Value	Message

enforce	- In the case of the boot block
	    The following error message appears, and the boot stops at the ok prompt.
	    - System console message
	      FATAL: Bootblk signature verification failed, verified boot policy = enforce, halting boot
	    - XSCF error log
	      boot process failed
	- System console or system log message in the case of other kernel modules
	    The following error message appears, but the start of Oracle Solaris continues.
	    Module /kernel/drv/sparcv9/*module* failed elfsign verification; "module-policy enforce" requested.

14.8.5   Versions of Oracle Solaris and XCP That Support Verified Boot

Table 14-20 lists the versions of Oracle Solaris and XCP that support verified boot. Verified boot can be used when both conditions in Table 14-20 are met.

Table 14-20   Versions of Oracle Solaris and XCP With Which Verified Boot Can be Used

Oracle Solaris and XCP	Version
Oracle Solaris	11.2 or later
XCP	2250 or later

Verified boot from an Oracle Solaris setting is available only with the combination of XCP 2240 or earlier and Oracle Solaris 11.2.
In XCP 2250 or later, operation is based on the configuration information in the XSCF. A firmware update from XCP 2240 or earlier to XCP 2250 or later will set the default of "none" for the verified boot policy of the XSCF. This setting is given priority, even over the Oracle Solaris configuration settings. To use verified boot, set the policy with the XSCF.

14.8.6   Range of Verified Boot Support

Verified Boot on Guest Domains and Kernel Zones

Verified boot is supported only for global zones in Oracle Solaris 11.2. In addition to this, verified boot is supported for kernel zones in Oracle Solaris 11.3 or later. For details on configuring verified boot in kernel zones, see *Creating and Using Oracle Solaris Kernel Zones*. For details on configuring verified boot in guest domains, see "Using Verified Boot" in the *Oracle VM Server for SPARC 3.4 Administration Guide*.

Boot Device and Verified Boot Policy Settings

The verified boot supports booting from a hard disk drive (HDD) and booting from the network. For other boot methods, set the verified boot policy to "none."

Also, when performing verified boot, be sure to perform boot from a signed device. Otherwise, boot verification by verified boot fails.

Table 14-21 shows the range of verified boot support.

Table 14-21　　Range of verified boot support

	Control Domain		Guest Domain	
	Global Zone	Kernel Zone	Global Zone	Kernel Zone
Boot from HDD	Oracle Solaris 11.2 or later (*1) XCP 2250 or later	Oracle Solaris 11.3 or later XCP 2250 or later	Control domain: Oracle Solaris 11.4 or later Oracle Solaris 11.3 SRU11.3.8.7.0 or later Guest domain: Oracle Solaris 11.2 or later XCP 2280 or later	Oracle Solaris 11.3 or later XCP 2250 or later
Boot from network	Oracle Solaris 11.2 or later (*1) XCP 2320 or later	-	Control domain: Oracle Solaris 11.4 or later Oracle Solaris 11.3 SRU11.3.8.7.0 or later Guest domain: Oracle Solaris 11.2 or later XCP 2320 or later	-

*1 Settings in the XSCF are used, and settings in Oracle Solaris are ignored.

14.8.7　　Notes and Restrictions

Note the following when using verified boot.

Setting Value of the OpenBoot PROM Environment Variable use-nvramrc?

To use verified boot, set the value of the OpenBoot PROM environment variable use-nvramrc? to "false." If you use verified boot with the variable set to "true," boot verification fails. Operations listed in Table 14-22 can be performed when boot verification fails, according to the boot policy setting value.

Table 14-22　　Boot Verification Operation When use-nvramrc? is "true"

Boot Policy Setting Value	Operation
none	Boot verification is not performed.

Boot Policy Setting Value	Operation
warning	The following message appears, and Oracle Solaris is started. use-nvramrc? variable is set, continuing with signature verification
enforce	The following message appears, and the boot stops at the ok prompt. In addition, the "boot process failed" error log is registered with the XSCF. use-nvramrc? variable is set, verified boot policy = enforce, halting boot

Setting the Verified Boot Configuration at the OpenBoot PROM ok Prompt

Suppose that you change the verified boot configuration information in the XSCF from the OpenBoot PROM ok prompt and then start Oracle Solaris. The changed configuration information becomes valid only for genunix and other kernel modules. The changed configuration information becomes valid for all modules the next time that OpenBoot PROM is started.

14.8.8 Checking the Setting Items and Commands Related to Verified Boot

Table 14-23 lists the setting items related to verified boot and the corresponding XSCF shell commands. Configure verified boot for each physical partition.

Table 14-23   Commands Related to Configuring Verified Boot

Setting Item	Related Command
Registering/Deleting/Displaying a certificate	addvbootcerts(8), deletevbootcerts(8), showvbootcerts(8)
Setting/Displaying configuration information - Selecting a certificate - Setting boot and module policies	setvbootconfig(8), showvbootconfig(8)

Note - Do not execute the setvbootconfig command while power-on or power-off processing for the physical partition is in progress. Otherwise, the command ends with an error.

14.8.9 Verified Boot Setting Flow

Figure 14-12 shows the flow for making settings to use verified boot.

Figure 14-12   Setting Flow When Using Boot Verification
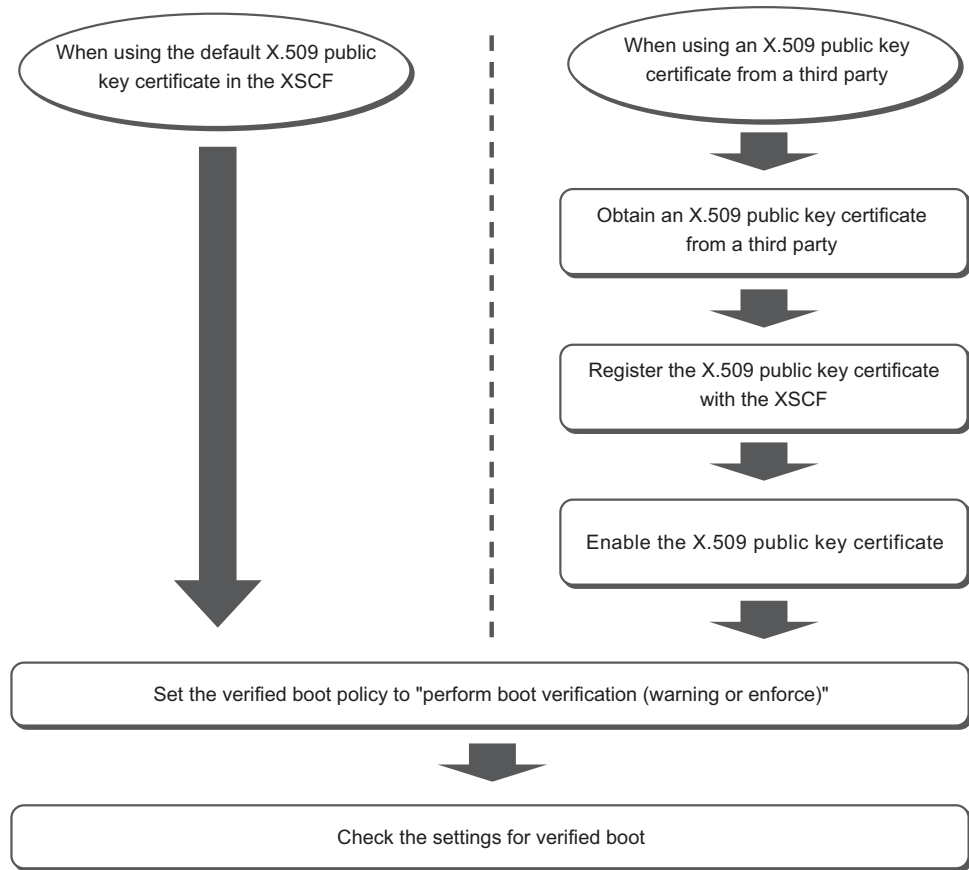
Figure 14-13 shows the setting flow when you do not use boot verification by verified boot.

Figure 14-13   Setting Flow When You Do Not Perform Boot Verification
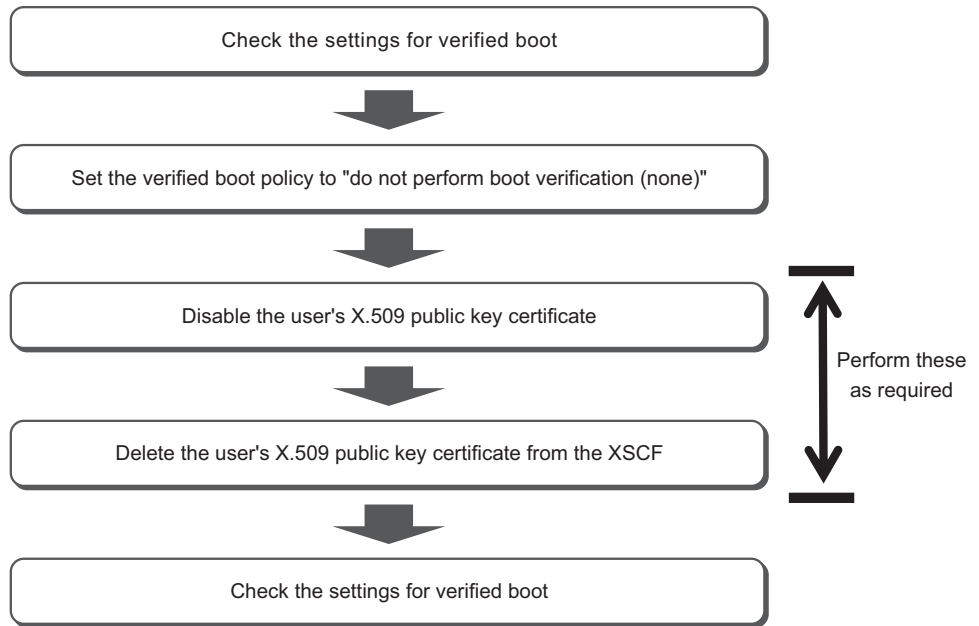
14.8.10   Registering an X.509 Public Key Certificate

Use the addvbootcerts command to register an X.509 public key certificate with the XSCF. Execute the addvbootcerts command with a user account that has the platadm or pparadm privilege.

```
XSCF> addvbootcerts -p ppar_id certname {-F URL | signature}
```

For ppar_id, specify the destination physical partition. For certname, specify the name of the X.509 public key certificate to be registered. To specify a public key certificate, copy and paste the contents of the public key certificate, or read it from a USB medium or http/https server by specifying the -F option.

The public key certificate is registered with the XSCF as a user's certificate. Up to five public key certificates can be registered.

In the following example, a public key certificate stored in a USB medium is specified.

```
XSCF> addvbootcerts -p ppar_id certname -F file:///media/usb_msd/file
```

Note - You can also register an X.509 public key certificate by using XSCF Web.

Note - Register X.509 public key certificates by specifying them one by one. You cannot

specify multiple public key certificates at a time.

> **Note -** In cases such as if the data format of the public key certificate to be registered is other than X.509 and if the data is corrupted, the public key certificate cannot be registered with the XSCF. The addvbootcerts command results in an error.

> **Note -** A system default certificate is a public key certificate the XSCF has by default. X.509 public key certificates cannot be registered as system default certificates.

Operation Procedure

1. **Log in to the XSCF.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the addvbootcerts command to register a user's certificate with the XSCF.**
   In the following example, an X.509 public key certificate stored on USB media is added to PPAR-ID 4 under the name "CUSTOM_CERT_2". The confirmation message is responded to with "y (yes)."

```
XSCF> addvbootcerts -p 4 CUSTOM_CERT_2 -F file:///media/usb_msd/vboot/3rd_perty_
cert_xyz
The above elfsign X.509 key certificate will be added to PPAR-ID 4,
Continue?[y|n]:y
.... done.
successfully added this certificate to PPAR-ID 4 as index 2.
```

3. **Execute the showvbootcerts command to confirm that the X.509 public key certificate was properly registered with the XSCF.**
   In the following example, the detailed information of the X.509 public key certificate registered as index number 2 in PPAR-ID 4 is displayed.

```
XSCF> showvbootcerts -v -p 4 -u -i 2
-------------------------------------------------------------------------------
PPAR-ID 4 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution,
CN=www.example.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:de:f0:2c:45:61:7f:10:c7:16:56:a9:14:b4:a4:
```

```
        39:44:b9:2f:65:4f:7e:a7:c0:15:89:b0:e2:1d:c0:
        25:4c:a6:31:75:14:a3:c4:cd:11:d2:87:b7:1a:7c:
        b2:0d:41:99:4f:a6:e9:d4:8e:77:55:19:ce:f1:a4:
        3c:cf:00:8d:e6:d1:c6:bc:06:f7:71:85:28:a4:c5:
        e0:8d:b3:e1:62:25:d5:df:93:d2:d9:1c:5b:48:35:
        70:e1:8a:9b:bf:9d:8b:41:b3:be:b6:c0:50:66:3b:
        d8:9d:2f:82:49:11:f7:6d:43:95:6e:ea:bc:57:dc:
        1c:90:6b:7e:8b:e3:0f:89:bd:32:3a:88:50:f0:48:
        d3:98:8c:bc:eb:7f:44:31:2b:86:01:d0:80:4c:a2:
        36:6e:24:47:48:d5:86:8e:86:06:c3:8e:df:5f:fb:
        6b:fe:6a:aa:0c:a8:ca:b6:ed:60:47:ea:8e:5d:63:
        b1:4f:ff:94:00:34:52:82:cf:a6:6a:84:69:4c:26:
        ac:a3:dc:d7:45:eb:7c:4e:fc:fc:92:4a:73:12:9f:
        31:7a:75:b9:de:33:54:34:af:0b:cf:46:c0:ac:2f:
        ec:28:af:0d:f7:c6:50:c0:e7:4c:88:16:13:95:54:
        0e:01:6e:1a:b6:33:bf:20:52:34:f4:69:a6:9e:bf:
        02:95
    Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
    44:65:95:e1:33:a4:ce:d1:c1:02:1a:ce:b3:2c:fa:c0:b2:34:
    4e:12:d0:86:c7:09:23:9d:5b:46:f4:b2:bf:88:8b:5b:5d:d7:
    57:c3:f9:9a:ba:95:bc:ed:4b:29:4b:19:97:ca:6c:bc:e1:44:
    e0:e1:89:a3:ed:bd:29:ad:a7:91:c8:76:ea:62:d2:2c:e3:ff:
    50:01:0a:3b:5a:28:53:38:53:82:ea:de:bc:24:84:bc:31:63:
    ab:b2:10:81:81:73:f4:02:46:5f:2d:6d:22:b0:af:d7:70:c0:
    db:de:ea:b9:23:87:3c:19:ef:c0:24:de:05:77:eb:89:d2:36:
    d0:85:8a:ed:d1:7f:12:b0:58:5f:f5:53:f1:db:0b:44:53:a0:
    72:8c:1a:e6:4a:fd:e8:8e:f8:ee:9e:7e:4e:85:59:42:44:fa:
    1f:d3:70:4f:81:95:8e:a9:0f:83:49:a2:b0:fd:5b:f4:2d:5e:
    86:ef:f3:56:b3:31:f3:58:3a:37:42:bb:39:c4:c1:b5:8c:e9:
    b4:01:d2:2e:e8:7d:86:1a:66:88:34:1e:e5:36:ee:6d:6c:90:
    78:45:a0:5b:a9:50:84:62:a8:88:ee:a6:70:fa:7c:ad:81:b7:
    89:f1:d6:64:94:c4:17:69:c8:35:81:b2:f3:79:ad:a2:5a:a0:
    02:28:a9:7f
--------------------------------------------------------------------------------
```

4. **Execute the exit command to log out from the XSCF shell.**
    If you do not have any further work with the XSCF shell, log out from the XSCF.
    To proceed to configuring another setting, go to the relevant step.

Note - If the information of an X.509 public key certificate is corrupted because of an unexpected operation, the public key certificate may be required by the XSCF. Ensure that public key certificates are safely stored for recovery.

14.8.11 Enabling/Disabling a Registered X.509 Public Key Certificate

To use a user's X.509 public key certificate that has been registered, execute the setvbootconfig command from the XSCF shell to enable the public key certificate.

Execute the setvbootconfig command with a user account that has the platadm or pparadm privilege.

In the following example, a disabled public key certificate is enabled.

```
XSCF> setvbootconfig -p ppar_id -i index -c enable
```

For ppar_id, specify the destination physical partition. For index, specify the index number of the user's certificate to be enabled.

You can use a list of user's certificates to check index numbers and whether a public key certificate is enabled/disabled. To display a list of user's certificates, execute the showvbootcerts command with the -a option specified.

```
XSCF> showvbootcerts -p ppar_id -a
```

In the following example, an enabled public key certificate is disabled.

```
XSCF> setvbootconfig -p ppar_id -i index -c disable
```

For ppar_id, specify the destination physical partition. For index, specify the index number of the user's certificate to be disabled.

Note - You can also use XSCF Web to enable/disable an X.509 public key certificate.

Note - You can enable/disable an X.509 public key certificate while the physical partition is powered off or Oracle Solaris on the logical domain is running. If the physical partition or logical domain is in the startup or stop procedure, an error occurs. Perform the operation again after the startup or stop is completed.

Note - A system default certificate is a public key certificate the XSCF has by default. System default certificates cannot be enabled/disabled.

Operation Procedure

1. **Log in to the XSCF.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the showvbootcerts command to check the index number of the user's certificate to be used and whether the certificate is enabled.**
   If the registered public key certificate is already enabled, the subsequent steps are not required.

   In the following example, all the X.509 public key certificates registered in PPAR-ID 2 are displayed.

```
XSCF> showvbootcerts -p 2 -a
-------------------------------------------------------------------------------
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
```

```
--------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
--------------------------------------------------------------------------------
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
--------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
--------------------------------------------------------------------------------
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Disable]
--------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
--------------------------------------------------------------------------------
```

3. **Execute the setvbootconfig command to enable the public key certificate.**
   In the following example, the X.509 public key certificate registered as index
   number 5 in PPAR-ID 2 is enabled. The confirmation message is responded to
   with "y (yes)."

```
XSCF> setvbootconfig -p 2 -i 5 -c enable
Index 5, CUSTOM_CERT_5 on PPAR-ID 2 will be enabled,
Continue?[y|n]: y
```

4. **Execute the showvbootcerts command to confirm that the public key
   certificate was enabled.**
   In the following example, it is confirmed that the X.509 public key certificate
   registered as index number 5 in PPAR-ID 2 is enabled.

```
XSCF> showvbootcerts -p 2 -a
-----------------------------------------------------------------------------
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----------------------------------------------------------------------------
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----------------------------------------------------------------------------
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Enable]
-----------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----------------------------------------------------------------------------
```

5. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.
   To proceed to configuring another setting, go to the relevant step.

14.8.12   Deleting a Registered X.509 Public Key Certificate

To delete an X.509 public key certificate from the system, use the deletevbootcerts command in the XSCF shell. Executed the deletevbootcerts command with a user account that has the platadm or pparadm privilege.
You can delete a public key certificate when the public key certificate is disabled.

```
XSCF> deletevbootcerts -p ppar_id -i index
```

For ppar_id, specify the destination physical partition. For index, specify the index

number of the user's certificate to be deleted.

You can check the index number from a list of user's certificates that is output by executing the showvbootcerts command with the -a option specified.

```
XSCF> showvbootcerts -p ppar_id -a
```

Note - You cannot delete a public key certificate while it is enabled. Delete it after disabling it by using the setvbootconfig command. See "14.8.11　Enabling/Disabling a Registered X.509 Public Key Certificate."

Note - You can also use XSCF Web to enable/disable an X.509 public key certificate.

Note - A system default certificate is a public key certificate the XSCF has by default. System default certificates cannot be deleted.

Operation Procedure

1. **Log in to the XSCF.**
   For details, see "2.2　Logging In to the XSCF Shell."

2. **Execute the showvbootcerts command to check the index number of the user's certificate to be deleted and whether the certificate is disabled.**
   You cannot delete a public key certificate while it is enabled. Execute the setvbootconfig command to disable it.

   In the following example, all the X.509 public key certificates registered in PPAR-ID 2 are displayed.

```
XSCF> showvbootcerts -p 2 -a
------------------------------------------------------------------------------
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
------------------------------------------------------------------------------
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
```

```
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
--------------------------------------------------------------------------------
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Enable]
--------------------------------------------------------------------------------
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
--------------------------------------------------------------------------------
```

3. **Execute the deletevbootcerts command to delete the public key certificate.**
   In the following example, the X.509 public key certificate registered as index
   number 5 in PPAR-ID 2 is deleted. The confirmation message is responded to
   with "y (yes)."

```
XSCF> deletevbootcerts -p 2 -i 5
Index 5, CUSTOM_CERT_5 will be deleted from PPAR-ID 2,
Continue?[y|n]: y
```

4. **Execute the showvbootcerts command to confirm that the public key
   certificate was deleted.**
   In the following example, all the X.509 public key certificates registered in
   PPAR-ID 2 are displayed. You can see that the public key certificate with index
   number 5 has been deleted.

```
XSCF> showvbootcerts -p 2 -a
--------------------------------------------------------------------------------
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
--------------------------------------------------------------------------------
Data:
Version: 3 (0x2)
Serial Number:
0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris Signed
Execution, CN=Solaris 11
--------------------------------------------------------------------------------
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
--------------------------------------------------------------------------------
Data:
Version: 3 (0x2)
Serial Number:
```

```
07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----------------------------------------------------------------------------
```

5. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF.
   To proceed to configuring another setting, go to the relevant step.

14.8.13 Displaying a Registered X.509 Public Key Certificate

Use the showvbootcerts command to display the information of an X.509 public key certificate registered with the XSCF.

If you want to display a list of all registered X.509 public key certificates, specify the destination physical partition and the -a option. This displays a list of system default certificates and user's certificates. You can also display detailed information by specifying the -v option.

```
XSCF> showvbootcerts -p ppar_id -a
```

To display the information for a system default certificate, specify the target physical partition, the -s option, and the index number of the system default certificate. You can also display detailed information by specifying the -v option.

```
XSCF> showvbootcerts -p ppar_id -s -i index
```

To display the information of a user's certificate registered with the addvbootcerts command, specify the destination physical partition, the -u option, and the index number of the user's certificate. You can also display detailed information by specifying the -v option.

```
XSCF> showvbootcerts -p ppar_id -u -i index
```

Note - You can also use XSCF Web to display an X.509 public key certificate.

14.8.14 Setting Verified Boot Policies

Use the setvbootconfig command in the XSCF shell to set verified boot policies.
Execute the command with a user account that has the platadm or pparadm privilege.

```
XSCF> setvbootconfig -p ppar_id -s policy=value
```

For ppar_id, specify the target physical partition. For policy, specify the boot policy "boot_policy" or module policy "module_policy". For value, specify "none", "warning", or "enforce". For details, see "14.8.4   Verified Boot Policies."

Operation Procedure

1. **Log in to the XSCF.**
   For details, see "2.2   Logging In to the XSCF Shell."

2. **Execute the showvbootconfig command to check the setting values for verified boot policies.**
   If the policy setting is set to a desired value, setting a policy is not required.

```
XSCF> showvbootconfig -p ppar_id
```

3. **Execute the showvbootconfig command to set verified boot policies. Enter "y" for the confirmation message.**
   In the following example, the boot policy (boot_policy) is set to "warning" and the module policy (module_policy) is set to "enforce" in PPAR-ID 2.

```
XSCF> setvbootconfig -p 2 -s boot_policy=warning
XSCF> setvbootconfig -p 2 -s module_policy=enforce
```

4. **Execute the showvbootcerts command to confirm that the setting values for verified boot policies were changed.**

```
XSCF> showvbootconfig -p ppar_id
```

5. **Execute the exit command to log out from the XSCF shell.**
   If you do not have any further work with the XSCF shell, log out from the XSCF. To proceed to configuring another setting, go to the relevant step.

14.8.15   Displaying Verified Boot Policies

Use the showvbootconfig command to display verified boot policies set for the physical partition.

```
XSCF> showvbootconfig -p ppar_id
```

For ppar_id, specify the target physical partition where policies are to be displayed.

Note - You can also use XSCF Web to display verified boot policies.

Chapter 15

Expanding the System Configuration

This chapter describes how to change the configuration of the I/O devices and hardware resources such as virtual CPUs and memory in the system.

- Changing the Virtual CPU Configuration
- Changing the Memory Configuration
- Dynamic Reconfiguration Function for PCIe Endpoint Devices
- Using the PCI Expansion Unit
- Expanding the SPARC M12-2S/M10-4S

15.1 Changing the Virtual CPU Configuration

This section describes how to change the virtual CPU configuration by using the dynamic reconfiguration (DR) function of Oracle VM Server for SPARC.

Note - To dynamically change logical domain resources, the Logical Domain Dynamic Reconfiguration (drd) daemon must be running on the target domain.

On the SPARC M12/M10 systems, various business processes run on each logical domain. The virtual CPU configuration can be flexibly changed according to the system operation status. In some active processes, the load is concentrated into a given logical domain, so performance with only the configured virtual CPUs used can be considered to be lower. In such a situation, the logical domains in the same physical partition can keep the system operating. This is done by dynamically assigning the virtual CPUs of domains that have a relatively low load.

The virtual CPU configuration can be changed for each thread.

To change the virtual CPU configuration, first use the ldm remove-vcpu command of Oracle VM Server for SPARC to delete virtual CPUs from logical domains that have a relatively low load. Then, use the ldm add-vcpu command of Oracle VM Server for

SPARC to add virtual CPUs to logical domains that present concerns about lower performance due to increased load. Execute these commands with the root privilege.

Deleting a Virtual CPU

```
primary# ldm remove-vcpu number ldom
```

For number, specify the number of virtual CPUs to delete. You can specify it in units of threads. For ldom, specify the logical domain from which to delete the virtual CPUs.

Adding a Virtual CPU

```
primary# ldm add-vcpu number ldom
```

For number, specify the number of virtual CPUs to add. You can specify it in units of threads. For ldom, specify the logical domain to which to add the virtual CPUs.

Operation Procedure

1. **Switch from the XSCF console to the control domain console to which the target logical domain belongs.**
   For details on how to switch to the control domain console, see "8.3 Switching to the Control Domain Console From the XSCF Shell."

2. **Check the number of virtual CPUs in each domain with the ldm list-domain command.**
   The following example checks the status of the primary, ldom1, ldom2, and ldom3 logical domains.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 16 2G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 24 4G 17% 17h 48m
```

3. **Delete a virtual CPU from a domain with the ldm remove-vcpu command.**
   The following example deletes eight virtual CPUs from ldom3.

```
primary# ldm remove-vcpu 8 ldom3
```

4. **Add a virtual CPU to a domain with the ldm add-vcpu command.**
   The following example adds eight virtual CPUs to ldom1.

```
primary# ldm add-vcpu 8 ldom1
```

5. **Check for a configuration change in the number of virtual CPUs in each domain by using the ldm list-domain command.**
   In the following example, check for configuration changes in the primary, ldom1, ldom2, and ldom3 logical domains.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 24 2G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 16 4G 17% 17h 48m
```

   You can see that virtual CPUs have been deleted from ldom3 and added to ldom1.

6. **Log out from the control domain console to return to the XSCF console.**
   For details on how to return to the XSCF console from the control domain console, see "8.4   Returning to the XSCF Shell From the Control Domain Console."

15.2   Changing the Memory Configuration

This section describes how to change the memory configuration by using the dynamic reconfiguration (DR) function of Oracle VM Server for SPARC.

Note - To dynamically change logical domain resources, the Logical Domain Dynamic Reconfiguration (drd) daemon must be running on the target domain.

On the SPARC M12/M10 systems, various business processes run on each logical domain. The memory configuration can be flexibly changed according to the system operation status. In some active processes, load is concentrated into a given logical domain, so performance with only the configured memory used can be considered to be lower. In such a situation, the logical domains in the same physical partition can be reallocated. This is done by dynamically assigning the memory of domains that have a relatively low load.

The memory configuration can be changed in units of 256 MB.

To change the memory configuration, first use the ldm remove-memory command of Oracle VM Server for SPARC to delete memory from logical domains that have a relatively low load. Then, use the ldm add-memory command of Oracle VM Server for SPARC to add memory to logical domains that present concerns about lower performance due to increased load.

Deleting Memory

```
primary# ldm remove-memory size[unit] ldom
```

For size, specify the size of the memory to delete. For unit, specify the unit of memory. For ldom, specify the logical domain from which to delete the memory.

Adding Memory

```
primary# ldm add-memory size[unit] ldom
```

For size, specify the size of memory to add. For unit, specify the unit of memory. For ldom, specify the logical domain to which to add the memory.

Operation Procedure

1. **Switch from the XSCF console to the control domain console to which the target logical domain belongs.**
   For details on how to switch to the control domain console, see "8.3　Switching to the Control Domain Console From the XSCF Shell."

2. **Check the memory capacity of each domain with the ldm list-domain command.**
   The following example checks the status of the primary, ldom1, ldom2, and ldom3 logical domains.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 16 2G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 24 4G 17% 17h 48m
```

3. **Delete memory from a domain with the ldm remove-memory command.**
   The following example deletes 1 GB of memory from ldom3.

```
primary# ldm remove-memory 1G ldom3
```

4. **Add memory to a domain with the ldm add-memory command.**
   The following example adds 1 GB of memory to ldom1.

```
primary# ldm add-memory 1G ldom1
```

5. **Check for a configuration change in the memory capacity of each domain with the ldm list-domain command.**
   In the following example, check for configuration changes in the primary, ldom1, ldom2, and ldom3 logical domains.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
```

```
ldom1 active -n---- 5001 16 3G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 16 3G 17% 17h 48m
```

You can see that memory has been deleted from the domain ldom3 and added to ldom1.

6. **Log out from the control domain console to return to the XSCF console.**
   For details on how to return to the XSCF console from the control domain console, see "8.4   Returning to the XSCF Shell From the Control Domain Console."

15.3   Dynamic Reconfiguration Function for PCIe Endpoint Devices

The dynamic reconfiguration function for PCIe endpoint devices is supported from Oracle VM Server for SPARC 3.1.1.1 onwards. This allows you to assign or delete PCIe endpoint devices without reconfiguring the root domain or stopping the I/O domain.
To use this function, check the corresponding card in "Cards That Support the Dynamic Reassignment Function for the PCIe End Point Device (PCIe Card)" in the *PCI Card Installation Guide* for your server.

The following table shows the required XCP/Oracle Solaris version and essential SRU/patch for executing the dynamic reconfiguration of PCIe endpoint devices.

Table 15-1   XCP and Oracle Solaris Versions Essential for Executing Dynamic Reconfiguration of PCIe Endpoint Devices (SPARC M10)

Server	XCP	Oracle Solaris	Essential Package Essential Product	Essential SRU Essential Patch
SPARC M10-1 SPARC M10-4 SPARC M10-4S	2230 or later	Oracle Solaris 11.3 or later	system/ldoms (*1) system/ldoms/ldomsmanager (*2)	None
		Oracle Solaris 11.2	system/ldoms (*1) system/ldoms/ldomsmanager (*2)	SRU 11.2.2.5.0 or later
		Oracle Solaris 11.1 (*4)	system/ldoms (*1)	SRU 11.1.17.5.0 or later (*3)
		Oracle Solaris 10 1/13	Oracle VM for SPARC 3.1 (*5)(*6)	150817-03 or later (*5)

*1 Essential for the control domain or other domains. Included in group/system/solaris-large-server and group/system/solaris-small-server.
*2 Essential only for the control domain. Included in group/system/solaris-large-server and group/system/solaris-small-server.
*3 Essential for the control domain or other domains.
*4 Can be used only with domains other than the control domain.
*5 Essential only for the control domain.
*6 There are required patches other than the Oracle VM Server for SPARC patch. For details, see "Required Oracle Solaris OS Versions for Oracle VM Server for SPARC 3.1.1.1" in the *Oracle VM Server for SPARC 3.1.1.1, 3.1.1, and 3.1 Release Notes*.

Table 15-2　Oracle Solaris Version Essential for Executing Dynamic Reconfiguration of PCIe Endpoint Devices (SPARC M12)

OS Version	Domain Type		
	Control Domain Non Virtualization Environment	Root Domain (With I/O Rental)	I/O Domain
Oracle Solaris 11	Oracle Solaris 11.4 (*1)	Oracle Solaris 11.4 or later (*2)	Oracle Solaris 11.4 or later (*2)
	Oracle Solaris 11.3 (*1) SRU 11.3.17.5.0 or later	Oracle Solaris 11.3 or later (*2)	Oracle Solaris 11.3 or later (*2)
	Oracle Solaris 11.2 (*1) 　SRU11.2.15.5.1	Oracle Solaris 11.2 or later (*2)	Oracle Solaris 11.2 or later (*2)
			Oracle Solaris 11.1 SRU 11.1.17.5.0 or later
Oracle Solaris 10	Oracle Solaris 10 1/13 (*3) Oracle VM Server for SPARC 3.2 (*4) 151934-03 or later	—	—

*1 The system/ldoms and system/ldoms/ldomsmanager packages are required. These packages are included in group/system/solaris-large-server and group/system/solaris-small-server.
*2 The system/ldoms package is required. This package is included in group/system/solaris-large-server and group/system/solaris-small-server.
*3 When Oracle Solaris 10 1/13 is operated in the control domain, CPUs with the LSB number 0 to 7 mounted on the logical system board can be assigned to the control domain.
*4 This is not included in Oracle Solaris 10 1/13. Install it separately.

To use this function, the hotplug service of the target logical domain must be enabled in advance.

```
# svcadm enable svc:/system/hotplug:default
```

15.3.1　Adding a Physical I/O Device to an I/O Domain

This section describes the procedure for adding a physical I/O device to an I/O domain by using the dynamic reconfiguration function for PCIe endpoint devices.

1. **Remove the physical I/O device from the root domain.**

```
# ldm remove-io device root_domain
```

2. **Assign the physical I/O device removed in step 1 to the I/O domain.**

```
# ldm add-io device io_domain
```

3. **Set the physical I/O device on the I/O domain.**
   The procedure for making this setting varies depending on the Oracle Solaris

version of the target I/O domain, and the physical I/O device. For details, see the following Oracle Solaris related manuals.

- For Ethernet card

  - For Oracle Solaris 11.2
    Configuring and Administering Network Components in Oracle Solaris 11.2
    Managing Network Datalinks in Oracle Solaris 11.2
    Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2

  - For Oracle Solaris 11.1
    Connecting Systems Using Fixed Network Configuration in Oracle Solaris 11.1
    Managing Oracle Solaris 11.1 Network Performance

  - For Oracle Solaris 10
    Oracle Solaris Administration: IP Services

- For SAS card or Fibre Channel card

  - For Oracle Solaris 11.2
    Managing SAN Devices and Multipathing in Oracle Solaris 11.2

  - For Oracle Solaris 11.1
    Oracle Solaris SAN Configuration and Multipathing Guide

  - For Oracle Solaris 10
    Oracle Solaris SAN Configuration and Multipathing Guide

15.3.2 Removing a Physical I/O Device From an I/O Domain

This section describes the procedure for removing a physical I/O device from an I/O domain by using the dynamic reconfiguration function for PCIe endpoint devices.

1. **Cancel the physical I/O physical I/O setting on the I/O domain.**
    Before the removal of the physical I/O device can be enabled, the physical I/O device setting on the I/O domain must be canceled.

    The procedure for making this setting varies depending on the Oracle Solaris version of the target I/O domain, and the physical I/O device. For details, see the following Oracle Solaris related manuals.

    - For Ethernet card

      - For Oracle Solaris 11.2
        Configuring and Administering Network Components in Oracle Solaris 11.2
        Managing Network Datalinks in Oracle Solaris 11.2
        Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2

      - For Oracle Solaris 11.1
        Connecting Systems Using Fixed Network Configuration in Oracle Solaris 11.1
        Managing Oracle Solaris 11.1 Network Performance

      - For Oracle Solaris 10
        Oracle Solaris Administration: IP Services

    - For SAS card or Fibre Channel card

      - For Oracle Solaris 11.2

Managing SAN Devices and Multipathing in Oracle Solaris 11.2

- For Oracle Solaris 11.1
  Oracle Solaris SAN Configuration and Multipathing Guide

- For Oracle Solaris 10
  Oracle Solaris SAN Configuration and Multipathing Guide

2. **Remove the physical I/O device from the I/O domain.**

```
# ldm remove-io device io_domain
```

3. **To perform active maintenance of the PCIe card by using PCI hot plug (PHP), etc., reassign the physical I/O device removed in step 2 to the root domain.**

```
# ldm add-io device root_domain
```

15.4 Using the PCI Expansion Unit

This section provides an overview of the PCI expansion unit, which is an option for the SPARC M12/M10.

The PCI expansion unit is a rack-mounted device that enables expansion of up to 11 PCI-Express slots. The unit can be mounted in the same rack as the SPARC M12/M10. Suppose there is a shortage of the built-in PCI-Express slots for the SPARC M12/M10. In such cases, installing the PCI expansion unit can flexibly expand the system.

You can check the status of the PCI expansion unit and power it on/off by using the ioxadm command of the XSCF firmware. For details of the ioxadm command, see the man page of the command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

If you are considering the installation of the PCI expansion unit, contact a sales representative.

For details of mounting the PCI extension unit, see "Mounting the PCI expansion unit in a rack" in the *Installation Guide* for your server.

15.4.1 Checking the PCI Expansion Unit

You can check, among others, a list about the PCI expansion unit managed by the system and the temperature, voltage, current, measured values of fan speed sensors, status of locator LEDs, and firmware status of the unit.

For details on how to check it, see "11.1.5 Displaying the PCI Expansion Unit Status."

15.4.2 Controlling the Power to the PCI Expansion Unit

This section describes how to turn on/off the power to remove the PCI expansion unit, an I/O board, a power supply unit, etc.

Power-on and power-off must be performed with a user account that has the platadm or fieldeng privilege.

Operation Procedure

1. **Power off the power supply unit in the PCI expansion unit with the ioxadm command.**
   The following example powers off the specified parts, including a power supply unit, so that they can be removed.

```
XSCF> ioxadm -f poweroff PCIBOX#12B4/PSU#1
```

Note - To forcibly turn off the power, specify the -f option. Note that use of the -f option may damage the domain.

2. **Restore power to the power supply unit in the PCI expansion unit with the ioxadm command.**
   The following example turns on the power again to the powered-off parts.

```
XSCF> ioxadm poweron PCIBOX#12B4/PSU#1
```

Note - To remove a power supply unit or I/O board, power off the specified part. To turn on the power again when the POWER switch is set to on, execute the ioxadm command.

15.4.3 Notes on the Configuration in Which the System is Connected to a PCI Expansion Unit

SPARC M12-2/M12-2S/M10-4/M10-4S

Suppose that one of the following operations is performed with the setpciboxdio command in the SPARC M12-2/M12-2S or using the following firmware on other systems: XCP 2044 or later on the SPARC M10-4 or XCP 2050 or later on the SPARC M10-4S. Then, the logical domain configuration of the physical partition will return to the factory-default state at the next control domain start time. Also, the OpenBoot PROM environment variables of the control domain can be initialized.
- Changing the enable/disable setting of the direct I/O function for the PCI expansion

unit
- When a PCI expansion unit is added to/removed from/replaced on a PCI slot of a
  SPARC M12/M10 with a PCI expansion unit whose direct I/O function is enabled
You can execute the setpciboxdio command regardless of whether there is a PCI
expansion unit. Before doing so, save the logical domain configuration information
from Oracle Solaris to an XML file. Also, write down the setting information for the
OpenBoot PROM environment variables of the control domain to set it again.

Table 15-3 indicates what information may need to be saved/restored when changing
the enable/disable setting of the direct I/O function for the PCI expansion unit by
executing the setpciboxdio command.

Table 15-3   Required Operations to Toggle the Enable/Disable Setting for Direct I/O
              Functions

Configuration of PCI Expansion Unit	Current Domain Configuration	Rebuilding Oracle VM Server for SPARC Configuration	Setting OpenBoot PROM Environment Variable Again
No	factory-default (Control domain only)	Not required	Not required
No	With logical domains other than control domain	Required (XML file)	Required (*1)
Yes	factory-default (Control domain only)	Not required	Not required
Yes	With logical domains other than control domain	Required (XML file)	Required (*1)

*1 This is not required in XCP 2230 or later or the SPARC M12-2/M12-2S.

Table 15-4 indicates what information may need to be saved/restored when
adding/removing/replacing a PCI expansion unit in a PCI slot of a SPARC M12/M10
where the direct I/O function for the PCI expansion unit is enabled. Here, the
setpciboxdio command has been executed to enable the function.

Note - In PCI expansion unit maintenance using the PCI hot plug (PHP) function, the direct
I/O function is disabled, so the above information does not need to be saved/restored.

Table 15-4 Required Operations for the Addition/Removal/Replacement of a PCI Expansion Unit in a PCI Slot of a SPARC M12/M10 Where the Direct I/O Function is Enabled

Maintenance Environment	Current Domain Configuration	Rebuilding Oracle VM Server for SPARC Configuration	Setting OpenBoot PROM Environment Variable Again
Addition/Removal with PPAR stopped	factory-default (Control domain only)	Not required	Not required
	With logical domains other than control domain	Required (XML file)	Required (*2)
Replacement of faulty PCI expansion unit (*1) with PPAR stopped	factory-default (Control domain only)	Not required	Not required
	With logical domains other than control domain	Required (XML file)	Required (*2)
Replacement of normal PCI expansion unit (*1) with PPAR stopped	factory-default (Control domain only)	Not required	Not required
	With logical domains other than control domain	Not required	Not required

*1 This includes even the replacement of a link card, link cable, management cable, and link board.
*2 This is not required in XCP 2230 or later or the SPARC M12-2/M12-2S.

Note - Execute the ldm list-constraints -x command to save to an XML file, and execute the ldm init-system -i command to restore from an XML file. To display the OpenBoot PROM environment variables, execute the printenv command from the ok prompt. For a detailed procedure, see "1.7.3   How to Save/Restore the Logical Domain Configuration Information and the OpenBoot PROM Environment Variable" in the *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

SPARC M12-1/M10-1

If a PCI expansion unit is added to or removed from the SPARC M12-1, or if one of the following operations is performed on the SPARC M10-1, the logical domain configuration of the physical partition will return to the factory-default state at the next control domain start time. Also, the OpenBoot PROM environment variables of the control domain can be initialized.
- Updating the firmware from XCP 2043 or earlier to XCP 2044 or later in a system connected to a PCI expansion unit
- Adding/Removing a PCI expansion unit in a system to which the firmware XCP 2044 or later is applied

Before the operation, save the logical domain configuration information from Oracle Solaris to an XML file. Also, write down the setting information for the OpenBoot

PROM environment variables of the control domain in advance to set it again.

Table 15-5 indicates what information may need to be saved/restored when updating the firmware from XCP 2043 or earlier to XCP 2044 or later in a system connected to a PCI expansion unit.

Table 15-5 Required Operations When Updating the Firmware From XCP 2043 or Earlier to XCP 2044 or Later

PCI Expansion Unit Connection	Current Domain Configuration	Rebuilding Oracle VM Server for SPARC Configuration	Setting OpenBoot PROM Environment Variable Again
No	factory-default (Control domain only)	Not required	Not required
No	With logical domains other than control domain	Not required	Not required
Yes	factory-default (Control domain only)	Not required	Not required
Yes	With logical domains other than control domain	Required (XML file)	Required

Table 15-6 indicates what information may need to be saved/restored when adding/removing a PCI expansion unit in a system to which the firmware XCP 2044 or later is applied.

Table 15-6 Required Operations When Adding/Removing a PCI Expansion Unit in a System to Which the Firmware XCP 2044 or Later is Applied

PCI Expansion Unit Connection	Current Domain Configuration	Rebuilding Oracle VM Server for SPARC Configuration	Setting OpenBoot PROM Environment Variable Again
No (adding)	factory-default (Control domain only)	Not required	Not required
No (adding)	With logical domains other than control domain	Required (XML file)	Required (*1)
Yes (adding/removing)	factory-default (Control domain only)	Not required	Not required
Yes (adding/removing)	With logical domains other than control domain	Required (XML file)	Required (*1)

*1 This is not required in XCP 2230 or later or the SPARC M12-1.

Note - Execute the ldm list-constraints -x command to save to an XML file, and execute the ldm init-system -i command to restore from an XML file. To display the OpenBoot PROM environment variables, execute the printenv command from the ok prompt. For a detailed procedure, see "1.7.3   How to Save/Restore the Logical Domain Configuration Information and the OpenBoot PROM Environment Variable" in the *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

15.5 Expanding the SPARC M12-2S/M10-4S

For the workflow for adding the SPARC M12-2S/M10-4S to expand the system as well as the preparation and addition procedures in detail, see "Chapter 8 Expanding a System With a Building Block Configuration" in the *Fujitsu SPARC M12-2S Installation Guide* or "Chapter 8   Before Expanding/Reducing a System with a Building Block Configuration" in the *Fujitsu M10-4S/SPARC M10-4S Installation Guide*.

For details on how to add an added SPARC M12-2S/M10-4S chassis to a physical partition and how to assign it to a logical domain, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Chapter 16

Updating the XCP Firmware

This chapter describes how to update the current firmware to the latest firmware by downloading the program (XCP) that manages the SPARC M12/M10 systems firmware.

- Basics of Firmware Update
- Before Updating Firmware
- Update Flow
- Preparing an XCP Image File
- Updating Firmware
- Updating Firmware From XSCF Web
- Firmware Version Matching with Parts Addition/Replacement
- Trouble During Firmware Update
- FAQ Relating to Firmware Update

The system administrator and field engineers update the firmware.

16.1 Basics of Firmware Update

16.1.1 Types of Firmware to Update

These systems have multiple pieces of firmware for controlling hardware/software. The program module that packages together that firmware is called XCP (XSCF Control Package).

Downloading the XCP firmware from our site, for example, and performing an update makes the functions of new firmware available to users.

The XCP firmware includes the following types.

- POST firmware, OpenBoot PROM firmware, and Hypervisor firmware (hereinafter referred to as CMU firmware)

These three pieces of firmware are grouped as one bundle of the firmware to update on the CPU memory unit, and to manage their versions. In this manual, these three pieces of firmware are collectively called the CMU firmware.

- XSCF firmware
  This firmware is updated on the XSCF unit.

Users can select to update the firmware as a whole (referred to below as XCP firmware) or update only the XSCF firmware.

16.1.2 Features of Firmware Update

The XCP firmware update has the following features.

- A new firmware update can be performed without powering off a physical partition. The physical partition must be powered off and on when updating the CMU firmware.

- If a part has been replaced using the maintenance menu in a building block configuration, the firmware on the replacement part is automatically matched to the version of the firmware in operation.

Note - For details on the automatic matching of firmware versions, see "16.7   Firmware Version Matching with Parts Addition/Replacement."

- Firmware can be updated to the latest firmware with no effect on other physical partitions even if the system consists of multiple physical partitions.

16.1.3 Mechanism of Firmware Update

Figure 16-1 is a conceptual diagram showing the mechanism of firmware update.

Figure 16-1   Concept of Firmware Update
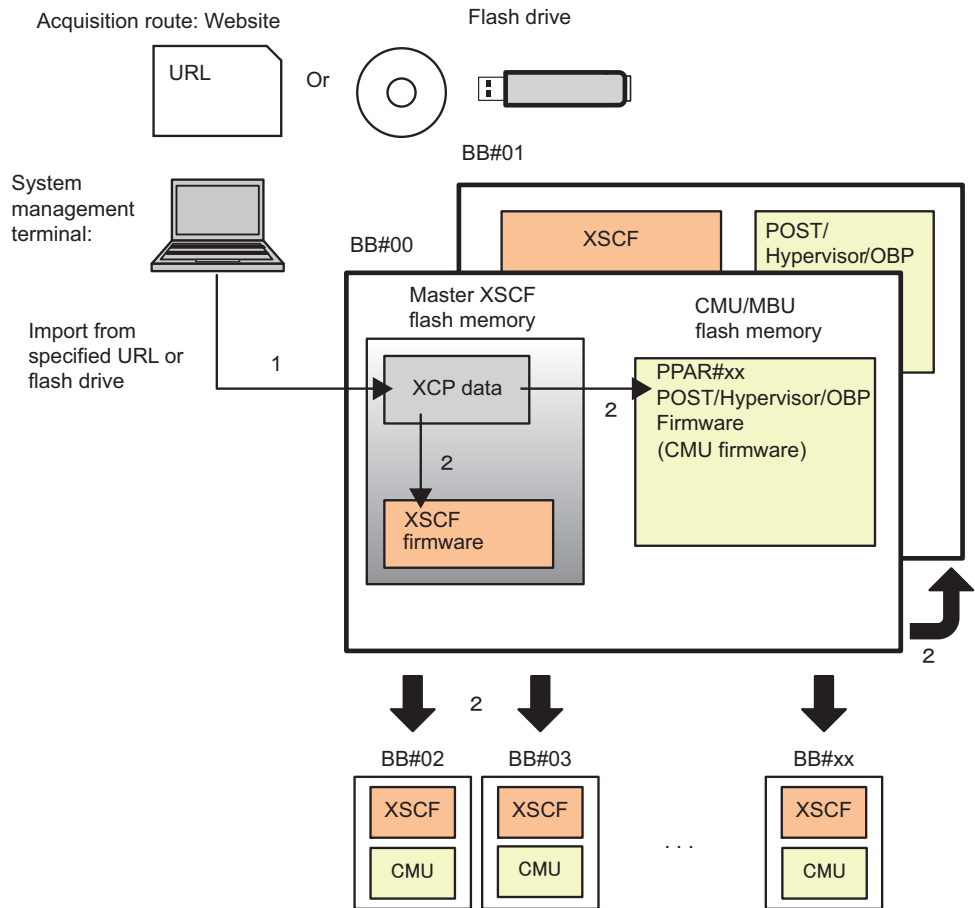
| 1 | XCP import |
| 2 | Update |

The following two operations (XCP import and update) provide firmware updates for these systems.

1. **XCP import (download)**
   Saving a decompressed XCP image file obtained from a website, for example, to any of these systems is called "XCP import." When XCP is just imported, the firmware in operation is not yet updated.

2. **Update**
   Writing the image file of the imported XCP to the flash memory in any of these systems is called "update." Updates of the XSCF firmware and the CMU firmware when the power is off are completed in this update.

Note - To complete the CMU firmware update on the target physical partitions that are

powered on, power off and on the physical partitions.

In the SPARC M10-1/M10-4/M10-4S, the flash memory with the written firmware has two areas: Current bank and Reserve bank. Update of firmware is controlled with these two banks. With CMU firmware, the firmware update is controlled by using only the current bank.

Note - With the CMU firmware on the SPARC M10 system, the reserve bank is also displayed. With the CMU firmware, where control is handled only by the current bank, there is no problem with an outdated version of the reserve bank.

16.1.4 Version Matching

In any of the following cases, these systems automatically match the firmware version.

- Suppose that multiple building blocks (system boards) in a physical partition have different CMU firmware versions. In this case, the firmware versions are automatically matched when the physical partition is powered on.

- If maintenance parts (XSCF unit or CPU memory unit (lower)) have been replaced or added using the maintenance menu, their firmware versions are automatically matched to the version of the firmware in operation.

- If the flashupdate -c sync command has been executed, all of the XSCF firmware versions are matched to the master XSCF.

16.1.5 Update When Using Multiple XSCFs

In the systems with multiple XSCFs, the master XSCF updates firmware. Firmware is automatically updated in order, beginning with the standby XSCF and followed by the master XSCF. In this case, the XSCF reboots itself or switches the master and standby XSCF networks. As a result, the network is disconnected once. Therefore, the user needs to log in again.

For details on update, see "."

16.2 Before Updating Firmware

16.2.1 Notes on Update

- Along with an XCP release, product notes for that version are also made publicly available. The product notes describe the following: added functions, software

patch information, the correspondence between new hardware and firmware, bug information, document corrections, etc. Also, the latest product notes contain corrections of past product notes. Be sure to read the product notes for both the firmware version applied and the latest version.

- A problem described in "Problems With XCP and Workarounds" in the *Product Notes* for your server may occur when the firmware is updated. In such cases, take the actions described as workarounds, and then update the firmware again.

- Do not apply a version older than the XCP firmware on the system currently in operation. If an older version is applied, system operation is not guaranteed. However, there is no problem with returning to the pre-update version of the firmware, unless any of the settings for the XSCF and Oracle VM Server for SPARC has changed after the firmware update.
  The procedure for returning to the earlier version is similar to the update procedure.

- No firmware update is possible where there is failed hardware. Before update, be sure to confirm that there is no failed hardware. If there is failed hardware, recover it from a failure and then update firmware. Check the hardware status with the showhardconf command. Confirm that no hardware is marked with an asterisk (*).

- XSCF communication is disconnected once during an update of the entire XCP firmware and the XSCF firmware because the XSCF is rebooted. In this case, connect and log in to the XSCF again.
  Also, the following warning message may be output to the control domain console during the XSCF reboot.

  PICL snmpplugin: cannot fetch object value (err=5, OID=<1.3.6.1.2.1.47.1.4.1>,row=0)

  If cluster software is in use, the following warning message may be output to the logical domain console during the XSCF reboot.

  SA SA_xscf***.so to test host *** failed

  7240 Connection to the XSCF is refused. (node:*** ipadress:*** detail:***)

- To safely update firmware, do not perform the operations described below until you have confirmed the "XCP update has been completed" message on the completion of the XCP firmware update. The same also applies to the XSCF Web operations corresponding to XSCF commands.
  - Turning off the input power

  - Executing the poweron, testsb, diagxbu, or reset command, or operating the POWER switch on the operation panel

  - Executing the setdate, switchscf, rebootxscf, initbb, restoreconfig, or restoredefaults command, or operating the RESET switch on the rear panel

  - Executing the getflashimage -d command

  - Executing the flashupdate -c update command

  Also, in a building block configuration system with XCP 2050 or later, after the XCP firmware update is completed, the master and standby XSCFs are automatically switched. Do not perform the above operations until you have confirmed that the master/standby switching has completed.

- To check whether the CMU firmware has been revised, see "Latest Information" and "Existing XCP Firmware Versions and Support Information" in the latest *Product Notes*. For the method of checking the CMU firmware version, see "16.2.3 Method of Checking the Firmware Version."

- To complete an update of revised CMU firmware when the power of the target physical partition is on, power off and on the physical partition.
  Also, in a building block configuration, if CMU firmware update has not been applied after the previous firmware update, then the message "flashupdate canceled cause PPAR is running" may appear at the next firmware update time. If this message appears, power off and on the relevant physical partition, and then update the firmware again.

- The CMU firmware in the SPARC M10 has a current bank and a reserve bank. If the firmware is updated by powering on a physical partition, only the current bank is updated by the completion of CMU firmware application.
  With the CMU firmware, where control is handled only by the current bank, there is no problem with an outdated firmware version of the reserve bank.

  If the firmware is updated by stopping the power of a physical partition, then both the reserve bank and current bank of the CMU firmware are updated.

- After updating the firmware, save the XSCF setting information again. For details, see "10.10 Saving/Restoring XSCF Settings Information."

- In the SPARC M12-1/M10-1, if the XSCF startup mode function is set to "fast" mode, set it to "normal" (default) mode again to update the firmware.
  For details on how to change the startup mode of the XSCF startup mode function, see the xscfstartupmode command in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

16.2.2 Update File Delivery Method and Format

The image files of the XCP firmware are provided in the following formats at the following locations.

- Delivery method: Website
  For details of the website, see the descriptions relating to firmware download in the latest *Product Notes* for your server. Field engineers may perform this work with a CD-ROM, DVD-ROM, or flash drive.

- Format: Compressed tar file (tar.gz) or Windows executable file (exe)
  Example: XCP2020.tar.gz

16.2.3 Method of Checking the Firmware Version

The firmware version on these systems is called "XCP version." The higher the version number, the newer the firmware. Before updating firmware, be sure to check the XCP version of the current system.

In the following example, use the version command with the -c xcp option specified

to display the XCP version.

```
XSCF> version -c xcp
BB#00-XSCF#0 (Master)
XCP0 (Current): 2044
XCP1 (Reserve): 2044
BB#01-XSCF#0 (Standby)
XCP0 (Current): 2044
XCP1 (Reserve): 2044
BB#02-XSCF#0
XCP0 (Current): 2044
XCP1 (Reserve): 2044
```

You can also check the version of each firmware in XCP by using the version command.

Four digits like "xyyz" represent the XCP version. Each number has the following meaning:

- x: Major release number

- yy: Minor release number

- z: Micro release number

There may be more micro release revisions than document revisions. For this reason, the document may show the micro release number as a variable.
Example: XCP201x

You can confirm the individual versions of the XSCF firmware and CMU firmware in XCP by using the -c xcp -v option with the version command.

The following example displays the XCP firmware version of the SPARC M10-1.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU            : 02.04.0001
POST           : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor     : 0.26.9
XSCF           : 02.04.0001
XCP1 (Reserve): 2041
CMU            : 02.04.0001
POST           : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor     : 0.26.9
XSCF           : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..
```

The following example displays the XCP firmware version of the SPARC M12-2. In the SPARC M12-1/M12-2/M12-2S, there is no CMU reserve area.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF          : 03.01.0000
XCP1 (Current): 3010
XSCF          : 03.01.0000
CMU           : 03.01.0000
    POST          : X.X.X
    OpenBoot PROM : X.XX.X+X.XX.X
    Hypervisor    : X.X.X
CMU BACKUP
#0: 03.01.0000
#1: ..
```

The CMU firmware may be different from the XCP version.
Example: When the XCP version is 2042, the XSCF firmware version is 02.04.0002
while the CMU firmware version is 02.04.0001.

For the CMU firmware version that corresponds to the XCP version, see "Existing XCP Firmware Versions and Support Information" in the latest *Product Notes* for your server.

16.2.4 Update Methods and Work Times

Table 16-1 lists update methods and rough work times.

Table 16-1   Update Methods and Work Times

Update Method	System Status	Time
In a system with one XSCF, update XCP.	Physical partition power is off or on.	About 45 minutes
In a building block configuration system with multiple XSCFs, update XCP. The following firmware is updated: the CMU firmware on all physical partitions, and the XSCF firmware on all XSCF units. Only the master XSCF firmware can also be updated. However, to complete the update of the CMU firmware on the target physical partitions that are powered on, power off and on the physical partitions.	Physical partition power is off or on.	About 120 minutes
In a building block configuration, firmware is automatically updated during replacement of parts or addition of the SPARC M12-2S/M10-4S in order to match firmware versions in the system. The following parts are targets: - XSCF unit in the SPARC M12-2S - CPU memory unit lower in the SPARC M10-4S - XSCF unit in the crossbar box	Physical partition power is off or on.	About 5 minutes

Note - Replace/Add units one by one. If multiple SPARC M12-2S/M10-4S units are replaced/added at the same time, firmware is not automatically updated to match firmware versions. Update the firmware manually.

Note - In some situations with the SPARC M10-4S, the input power is turned off and the maintenance menu is not used when replacing the CPU memory unit lower (CMUL), replacing the XSCF unit, adding the SPARC M10-4S, or adding the crossbar box. For support information on the function automatically matching firmware versions in these situations, see the latest *Fujitsu M10/SPARC M10 Systems Product Notes*.

16.3 Update Flow

The order of firmware update with the XSCF shell or XSCF Web is 1) XCP import and 2) XCP update.

The basic firmware update procedure is described below.

1. **Obtain the XCP firmware program file (tar.gz format) from the site, and place it on your USB device or in a network directory.**

2. **Decompress the XCP firmware program file.**

3. **Log in to the XSCF with a user account that has the platadm or fieldeng user privilege. If the systems has multiple XSCFs, log in to the master XSCF.**

4. **Import the XCP firmware image file (BBXCPxxxx.tar.gz) from your USB device or the network directory to the system (see getflashimage(8)).**
   XCP can be imported to the system while Oracle Solaris is active or stopped.

5. **Update XCP or the XSCF firmware (see flashupdate(8)).**

6. **Set the XSCF time (see "6.1.2 Setting the XSCF Time Before System Startup").**

7. **For the CMU firmware on the target physical partitions that are powered on, power off and on the physical partitions (see poweroff(8) and poweron(8)).**

Note - In the case of a logical domain configuration, execute the ldm add-spconfig command of Oracle VM Server for SPARC in the control domain to save the latest configuration information in the XSCF before powering off the physical partition.
For details, see "6.2.2 Saving the Logical Domain Configuration Information before System Stop" and "10.11.1 Saving/Displaying Logical Domain Configuration Information."

8. **Confirm the firmware version (see version(8)).**

For details of these five commands, see the man page of each command or the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*. For details on the associated XSCF Web menu, see "Appendix C List of the XSCF Web Pages."

16.4 Preparing an XCP Image File

This section describes how to prepare an XCP image file.

1. **Download the XCP firmware program file (XCPxxxx.tar.gz or XCPxxxx.exe) from the website into any folder on a PC connected to this system.**

2. **Check the XCP version.**
   For the XCP version, see the 4-digit number in the file name of the firmware program (tar.gz format).

   Example: The XCP version of XCP2044.tar.gz is 2044.

3. **Decompress the downloaded XCP firmware program.**
   The XCP image file to import to the system is expanded.

   Example: If XCP2044.tar.gz is decompressed, BBXCP2044.tar.gz is expanded.

16.5 Updating Firmware

This section describes how to update firmware with the XSCF shell. With XSCF Web, the procedure is identical. For details of the procedure on XSCF Web, see "16.6 Updating Firmware From XSCF Web."

16.5.1 Updating XCP on a System With One XSCF

1. **Log in to the XSCF.**

2. **Execute the showhardconf command, and confirm that the XSCF status (MBU Status) is Normal.**
   The following shows examples of the SPARC M10-1.

```
XSCF> showhardconf
SPARC M10-1;
    + Serial:2101151019A; Operator_Panel_Switch:Service;
    + System_Power:Off; System_Phase:Cabinet Power Off;
    Partition#0 PPAR_Status:Powered Off;
    MBU Status:Normal; Ver:2046h; Serial:USDA-P00008 ;
        + FRU-Part-Number:CA20366-B10X 002AB/LGA-MBU -01 ;
        + Power_Supply_System: ;
        + Memory_Size:32 GB;
```

3. **Execute the version command to check the version of the firmware in operation.**

```
XSCF> version -c xcp -v
    BB#00-XSCF#0 (Master)
    XCP0 (Current): 2041
    CMU           : 02.04.0001
        POST          : 1.42.0
        OpenBoot PROM : 4.34.0+1.16.0
        Hypervisor    : 0.26.9
    XSCF          : 02.04.0001
    XCP1 (Reserve): 2041
    CMU           : 02.04.0001
        POST          : 1.42.0
        OpenBoot PROM : 4.34.0+1.16.0
        Hypervisor    : 0.26.9
    XSCF          : 02.04.0001
    CMU BACKUP
    #0: 02.04.0001
    #1: ..
```

For the SPARC M12-1/M12-2, there is no reserve bank of the CMU firmware. The
following shows a display example.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF          : 03.01.0000
XCP1 (Current): 3010
XSCF          : 03.01.0000
CMU           : 03.01.0000
    POST          : X.X.X
    OpenBoot PROM : X.XX.X+X.XX.X
    Hypervisor    : X.X.X
CMU BACKUP
#0: 03.01.0000
#1: ..
```

4. **Execute the getflashimage command to import the XCP image file.**
   The following example imports the XSCF image file from a USB device
   connected to a USB port (where "MAINTENANCE ONLY" is printed) on the
   XSCF unit panel (rear panel).

```
XSCF> getflashimage file:///media/usb_msd/xxxx/BBXCP2044.tar.gz
Existing versions:
        Version                 Size   Date
        BBXCP2041.tar.gz    90004045  Tue Apr 09 04:40:12 JST 2013
Mounted USB device
0MB received
1MB received
...
44MB received
45MB received
Download successful: 46827 Kbytes in 109 secs (430.094 Kbytes/sec)
Checking file...
```

```
MD5: e619e6dd367c888507427e58cdb8e0a4
XSCF>
```

XCP image file importing is completed when the normal end messages "Download successful: ..." and "MD5: ..." appear.

Note - If the following error occurs during XCP import, there may be a problem with the XCP file: "Error: File is invalid or corrupt." Check the XCP file.
The possible cause, for example, is that an unauthorized XCP image file was obtained or that the XCP image file downloaded by the customer was subsequently changed through unauthorized access. In such cases, obtain the correct XCP image file and import XCP again.

Note - If a message such as "An internal error has occurred" or "Error: insufficient free space" appears during XCP import, an XSCF firmware error or parts failure may have occurred. In this case, see "16.8 Trouble During Firmware Update" and solve the problem.

---

5. **Use the getflashimage -l command to check the version of the imported XCP image file.**

```
XSCF> getflashimage -l
Existing versions:
        Version                   Size   Date
        BBXCP2044.tar.gz     90005045   Wed May 29 13:56:50 JST 2013
```

6. **Execute the flashupdate -c check command to check whether the imported XCP image file can be used for the update.**
   Immediately after executing the flashupdate command, execute the showresult command. If the returned end value is 0, you can use the file for the update.

```
XSCF> flashupdate -c check -m xcp -s 2044
XSCF> showresult
0
XSCF>
```

7. **Execute the flashupdate command to update the firmware.**

Note - The update takes about 30 minutes.

Note - To safely update the firmware, do not perform power operations for physical partitions and do not reboot the XSCF during the work (steps 7 to 9). For details, see "16.2.1 Notes on Update."

Note - If a message such as "An internal error has occurred" or "Internal error" appears during firmware update, an XSCF firmware error or parts failure may have occurred. In this case, see "16.8 Trouble During Firmware Update" and solve the problem.

```
XSCF> flashupdate -c update -m xcp -s 2044
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [3600sec]
  0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....
:
```

Here, the XSCF is rebooted, and the XSCF session is disconnected.

At this point in time, the XCP firmware update is not yet complete.

8. **Connect to the XSCF again.**

9. **Execute the showlogs monitor command to check the completion of the XCP firmware update.**

```
XSCF> showlogs monitor
May 29 14:30:09 M10-1-0 Event: SCF:XCP update is started (XCP version=2044:
last version=2041)
May 29 14:31:59 M10-1-0 Event: SCF:XSCF update is started (BBID=0, bank=1)
May 29 14:32:18 M10-1-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 14:39:27 M10-1-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=1)
May 29 14:39:28 M10-1-0 Event: SCF:XSCF bank apply has been completed (BBID=0,
 bank=1, XCP version=2044:last version=2041)
May 29 14:47:12 M10-1-0 Event: SCF:XSCF ready
May 29 14:48:32 M10-1-0 Event: SCF:XSCF update is started (BBID=0, bank=0)
May 29 14:48:52 M10-1-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 14:55:51 M10-1-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=0)
May 29 14:57:04 M10-1-0 Event: SCF:CMU update is started (BBID=0)
May 29 14:57:07 M10-1-0 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 14:59:07 M10-1-0 Event: SCF:CMU update has been completed (BBID=0)
May 29 15:00:19 M10-1-0 Event: SCF:CMU update is started (BBID=0)
May 29 15:00:20 M10-1-0 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 15:02:18 M10-1-0 Event: SCF:CMU update has been completed (BBID=0)
May 29 15:02:20 M10-1-0 Event: SCF:XCP update has been completed (XCP
version=2044:last version=2041)
```

The following example displays messages on the SPARC M12-2.

```
XSCF> showlogs monitor
Mar 15 15:29:34 M12-2-0 Event: SCF:XCP update is started (XCP version=3010:
last version=3009)
Mar 15 15:39:20 M12-2-0 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Mar 15 15:42:59 M12-2-0 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Mar 15 15:43:13 M12-2-0 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=0)
Mar 15 15:43:20 M12-2-0 Event: SCF:Updating XCP:XSCF bank has changed (BBID=0,
```

```
 bank=0, XCP version=3010:last version=3009)
Mar 15 16:02:49 M12-2-0 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=1)
Mar 15 16:04:18 M12-2-0 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Mar 15 16:04:22 M12-2-0 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=1)
Mar 15 16:04:47 M12-2-0 Event: SCF:XSCF ready
Mar 15 16:07:47 M12-2-0 Event: SCF:Updating XCP:Preparing to update CMU (BBID=0)
Mar 15 16:08:17 M12-2-0 Event: SCF:Updating XCP:Updating CMU (BBID=0, CMU
version=03010000)
Mar 15 16:08:28 M12-2-0 Event: SCF:Updating XCP:CMU updated (BBID=0)
Mar 15 16:08:31 M12-2-0 Event: SCF:XCP update has been completed (XCP
version=3010:last version=3009)
```

If the message "XCP update has been completed" appears, the XCP firmware update has completed.

Note - A message similar to "XSCF update has been completed" or "CMU update has been completed" will appear on the SPARC M10. However, the update of all the XCP firmware will not have completed by the time the message appears.

Note - To safely update the firmware, do not perform power operations for physical partitions, reboot the XSCF, etc. until you have confirmed the "XCP update has been completed" message on the completion of the XCP firmware update. For details, see "16.2.1 Notes on Update."

If the message "XCP update has been completed" does not appear, the update is not yet complete. Execute the showlogs monitor command again to check the completion of the update. Usually, the update is completed about 20 minutes after the "XSCF ready" message appears.

10. **Set the XSCF time.**
    If the XSCF time has shifted, the logical domain time may shift when the physical partition is powered on.

    For details on how to set the XSCF time, see "6.1.2 Setting the XSCF Time Before System Startup."

11. **To complete the CMU firmware update, power off and on the physical partition.**
    If the power of the physical partition is on, the target CMU firmware has not been updated at this point in time. Therefore, the message does not appear for the CMU firmware.

    If the power of the physical partition is off, go to step 12.

Note - In the case of a logical domain configuration, execute the ldm add-spconfig command of Oracle VM Server for SPARC in the control domain to save the latest configuration information in the XSCF before powering off the physical partition.
For details, see "6.2.2 Saving the Logical Domain Configuration Information before System Stop" and "10.11.1 Saving/Displaying Logical Domain Configuration Information."

Execute the poweroff command to power off the physical partition.

```
XSCF> poweroff -p 0
```

Execute the showpparstatus power command, and confirm that the power of the physical partition is off.

```
XSCF> showpparstatus -p 0
PPAR-ID         PPAR Status
00              Powered Off
```

Execute the poweron command to power on the physical partition.

```
XSCF> poweron -p 0
```

Execute the showpparstatus command, and confirm that PPAR Status is "Running."

```
XSCF> showpparstatus -p 0
PPAR-ID         PPAR Status
00              Running
```

12. **Execute the version command, and confirm that the firmware version is up to date.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU           : 02.04.0004
    POST          : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044
CMU           : 02.04.0004
    POST          : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF          : 02.04.0004
CMU BACKUP
#0: 02.04.0004
#1: ..
```

Note - On the SPARC M10, if firmware is updated by powering on the physical partition, only the current bank of the CMU firmware is updated.
With the CMU firmware, where control is handled only by the current bank, there is no problem with an outdated version of the reserve bank.

If the firmware is updated by stopping the power of a physical partition, then both the reserve bank and current bank of the CMU firmware are updated.
For the CMU firmware version that corresponds to the XCP version, see "Existing XCP Firmware Versions and Support Information" in the latest *Product Notes* for your server.

16.5.2 Updating XCP on a Building Block Configuration System With Multiple XSCFs

1. **Log in to the master XSCF.**

2. **Execute the showhardconf command, and confirm that Status is Normal for both the master XSCF and standby XSCF.**
   The following shows examples of the SPARC M10-4S.

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

3. **Execute the version command to check the version of the firmware in operation.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU           : 02.04.0001
    POST         : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor   : 0.26.9
XSCF          : 02.04.0001
XCP1 (Reserve): 2041
CMU           : 02.04.0001
    POST         : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor   : 0.26.9
XSCF          : 02.04.0001
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2041
CMU           : 02.04.0001
    POST         : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor   : 0.26.9
XSCF          : 02.04.0001
```

```
XCP1 (Current): 2041
CMU            : 02.04.0001
    POST           : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor    : 0.26.9
XSCF           : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..
```

For the SPARC M12-2S, there is no reserve bank of the CMU firmware. The
following shows a display example.

```
XSCF# version -c xcp -v
BB#00-XSCF#0 (Standby)
XCP0 (Reserve): 3010
XSCF           : 03.01.0000
XCP1 (Current): 3010
XSCF           : 03.01.0000
CMU            : 03.01.0000
    POST           :
    OpenBoot PROM :
    Hypervisor    :
BB#01-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF           : 03.01.0000
XCP1 (Current): 3010
XSCF           : 03.01.0000
CMU            : 03.01.0000
    POST           :
    OpenBoot PROM :
    Hypervisor    :
CMU BACKUP
#0: 03.01.0000
#1: ..
XSCF#
```

4. **Execute the getflashimage command to import the XCP image file.**
    The following example imports the XSCF image file from a USB device
    connected to a USB port (where "MAINTENANCE ONLY" is printed) on the
    XSCF unit panel (rear panel) of the master XSCF.

```
XSCF> getflashimage file:///media/usb_msd/xxxx/BBXCP2044.tar.gz
Existing versions:
        Version                 Size    Date
        BBXCP2041.tar.gz    90004045  Tue Apr 09 04:40:12 JST 2013
Mounted USB device
0MB received
1MB received
...
44MB received
45MB received
```

```
Download successful: 46827 Kbytes in 109 secs (430.094 Kbytes/sec)
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a4
XSCF>
```

XCP image file importing is completed when the normal end messages "Download successful: ..." and "MD5: ..." appear.

> **Note -** If the following error occurs during XCP import, there may be a problem with the XCP file: "Error: File is invalid or corrupt." Check the XCP file.
> The possible cause, for example, is that an unauthorized XCP image file was obtained or that the XCP image file downloaded by the customer was subsequently changed through unauthorized access. In such cases, obtain the correct XCP image file and import XCP again.

> **Note -** If a message such as "An internal error has occurred" or "Error: insufficient free space" appears during XCP import, an XSCF firmware error or parts failure may have occurred. In this case, see "16.8   Trouble During Firmware Update" and solve the problem.

5. **Use the getflashimage -l command to check the version of the imported XCP image file.**

```
XSCF> getflashimage -l
Existing versions:
        Version                   Size  Date
        BBXCP2044.tar.gz    90005045  Wed May 29 09:11:40 JST 2013
```

6 **Execute the flashupdate -c check command to check whether the imported XCP image file can be used for the update.**
   Immediately after executing the flashupdate command, execute the showresult command. If the returned end value is 0, you can use the file for the update.

```
XSCF> flashupdate -c check -m xcp -s 2044
XSCF> showresult
0
XSCF>
```

7. **Execute the flashupdate command to update the firmware.**

> **Note -** The update takes about 60 minutes.

> **Note -** To safely update the firmware, do not perform power operations for physical partitions and do not reboot the XSCF during the work (steps 7 to 11). For details, see "16.2.1 Notes on Update."

> **Note -** If a message such as "An internal error has occurred" or "Internal error" appears during firmware update, an XSCF firmware error or parts failure may have occurred. In this case, see "16.8   Trouble During Firmware Update" and solve the problem.

```
XSCF> flashupdate -c update -m xcp -s 2044
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [3600sec]
  0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....|
540.....570.....600.....630.....660.....690.....720.....750.....780.....-
810.....840.....870.....900.....930
:
```

Here, the XSCF is rebooted, the XSCF session is disconnected.

At this point in time, the XCP firmware update is not yet complete.

8. **Connect to the master XSCF again.**
   Immediately after the XSCF reboot, the states of the master and standby XSCFs are reversed from their original states. For example, when the firmware update is executed with BB-ID number 0 on master XSCF, reconnecting to XSCF will change the status of BB-ID number 1 to master and BB-ID number 0 to standby. In this example, the master XSCF (BB-ID 1) is connected.

Note - For customers who have set the takeover IP address, the machines are automatically connected to the master XSCF when connected using the takeover IP address.

---

9. **Execute the showbbstatus command, and confirm that you are logged in to the master XSCF. If you are logged in to the standby XSCF, reconnect to the master XSCF.**

Note - If the firmware is updated to version XCP 2050 or later, when the XCP firmware update is completed, the switched master/standby XSCF will return to the original state. In such cases, connect to the master XSCF again because the XSCF is rebooted and the XSCF session is disconnected.

```
XSCF> showbbstatus
BB#01 (Master)
```

10. **Execute the showlogs monitor command to check the completion of the XCP firmware update.**

```
XSCF> showlogs monitor
May 29 09:38:05 M10-4S-0 Event: SCF:XCP update is started (XCP version=2044:
last version=2041)
May 29 09:40:31 M10-4S-0 Event: SCF:XSCF update is started (BBID=0, bank=0)
May 29 09:40:46 M10-4S-0 Event: SCF:XSCF update is started (BBID=1, bank=0)
May 29 09:41:03 M10-4S-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 09:41:12 M10-4S-0 Event: SCF:XSCF writing is performed (BBID=1, XSCF
version=02040004)
May 29 09:48:18 M10-4S-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=0)
```

```
May 29 09:50:39 M10-4S-0 Event: SCF:XSCF update has been completed (BBID=1,
bank=0)
May 29 09:50:41 M10-4S-0 Event: SCF:XSCF bank apply has been completed
(BBID=1, bank=0, XCP version=2044:last version=2041)
May 29 10:01:50 M10-4S-0 Event: SCF:XSCF bank apply has been completed
(BBID=0, bank=0, XCP version=2044:last version=2041)
May 29 10:01:51 M10-4S-0 Event: SCF:Change Master Start(BB#01)
May 29 10:03:26 M10-4S-1 Event: SCF:Change Master Complete(BB#01)
May 29 10:05:00 M10-4S-1 Event: SCF:Standby XSCF Ready (BBID#00)
May 29 10:12:56 M10-4S-1 Event: SCF:XSCF update is started (BBID=1, bank=1)
May 29 10:13:23 M10-4S-1 Event: SCF:XSCF update is started (BBID=0, bank=1)
May 29 10:13:24 M10-4S-1 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 10:13:42 M10-4S-1 Event: SCF:XSCF writing is performed (BBID=1, XSCF
version=02040004)
May 29 10:20:22 M10-4S-1 Event: SCF:XSCF update has been completed (BBID=0,
bank=1)
May 29 10:23:34 M10-4S-1 Event: SCF:XSCF update has been completed (BBID=1,
bank=1)
May 29 10:24:42 M10-4S-1 Event: SCF:CMU update is started (BBID=0)
May 29 10:24:58 M10-4S-1 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 10:25:44 M10-4S-1 Event: SCF:CMU update is started (BBID=1)
May 29 10:25:46 M10-4S-1 Event: SCF:CMU writing is performed (BBID=1, CMU
version=02040004)
May 29 10:26:44 M10-4S-1 Event: SCF:CMU update has been completed (BBID=0)
May 29 10:27:51 M10-4S-1 Event: SCF:CMU update has been completed (BBID=1)
May 29 10:29:30 M10-4S-1 Event: SCF:CMU update is started (BBID=0)
May 29 10:29:36 M10-4S-1 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 10:29:45 M10-4S-1 Event: SCF:CMU update is started (BBID=1)
May 29 10:30:04 M10-4S-1 Event: SCF:CMU writing is performed (BBID=1, CMU
version=02040004)
May 29 10:31:18 M10-4S-1 Event: SCF:CMU update has been completed (BBID=0)
May 29 10:31:51 M10-4S-1 Event: SCF:CMU update has been completed (BBID=1)
May 29 10:32:38 M10-4S-1 Event: SCF:XCP update has been completed (XCP
version=2044:last version=2041)
May 29 10:32:39 M10-4S-1 Event: SCF:This XSCF will be switched back to standby
 mode after completion of firmware update
May 29 10:32:39 M10-4S-1 Event: SCF:Change Master Start(BB#00)
May 29 10:33:29 M10-4S-1 Event: SCF:Change Master Complete(BB#00)
May 29 10:42:29 M10-4S-1 Event: SCF:Standby XSCF Ready (BBID#01)
```

The following example displays messages on the SPARC M12-2S.

```
XSCF> showlogs monitor
Apr  5 06:51:06 M12-2S-1 Event: SCF:XCP update is started (XCP version=3010:
last version=3009)
Apr  5 07:01:41 M12-2S-1 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=1, bank=1)
Apr  5 07:03:46 M12-2S-1 Event: SCF:Updating XCP:Updating XSCF (BBID=1, XSCF
version=03010000)
Apr  5 07:03:54 M12-2S-1 Event: SCF:Updating XCP:XSCF updated (BBID=1, bank=1)
Apr  5 07:06:58 M12-2S-1 Event: SCF:Updating XCP:Preparing to update XSCF
```

```
(BBID=0, bank=0)
Apr  5 07:09:22 M12-2S-1 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Apr  5 07:10:39 M12-2S-1 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=0)
Apr  5 07:12:50 M12-2S-1 Event: SCF:Updating XCP:XSCF bank has changed
(BBID=1, bank=1, XCP version=3010:last version=3009)
Apr  5 07:20:06 M12-2S-1 Event: SCF:Updating XCP:XSCF bank has changed
(BBID=0, bank=0, XCP version=3010:last version=3009)
Apr  5 07:21:27 M12-2S-1 Event: SCF:Change Master Start(BB#01)
Apr  5 07:22:28 M12-2S-2 Event: SCF:Standby XSCF Ready(BB#01)
Apr  5 07:24:05 M12-2S-2 Event: SCF:Change Master Complete(BB#01)
Apr  5 07:30:08 M12-2S-2 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=1, bank=0)
Apr  5 07:30:35 M12-2S-2 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Apr  5 07:34:41 M12-2S-2 Event: SCF:Standby XSCF Ready(BB#00)
Apr  5 07:35:21 M12-2S-2 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Apr  5 07:40:32 M12-2S-2 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=1)
Apr  5 07:40:39 M12-2S-2 Event: SCF:Updating XCP:Updating XSCF (BBID=1, XSCF
version=03010000)
Apr  5 07:45:49 M12-2S-2 Event: SCF:Updating XCP:XSCF updated (BBID=1, bank=0)
Apr  5 07:46:18 M12-2S-2 Event: SCF:Updating XCP:Preparing to update CMU
(BBID=0)
Apr  5 07:46:41 M12-2S-2 Event: SCF:Updating XCP:Updating CMU (BBID=0, CMU
version=03010000)
Apr  5 07:48:21 M12-2S-2 Event: SCF:Updating XCP:CMU updated (BBID=0)
Apr  5 07:49:00 M12-2S-2 Event: SCF:Updating XCP:Preparing to update CMU
(BBID=1)
Apr  5 07:49:30 M12-2S-2 Event: SCF:Updating XCP:Updating CMU (BBID=1, CMU
version=03010000)
Apr  5 07:51:24 M12-2S-2 Event: SCF:Updating XCP:CMU updated (BBID=1)
Apr  5 07:51:25 M12-2S-2 Event: SCF:XCP update has been completed (XCP
version=3010:last version=3009)
Apr  5 07:51:26 M12-2S-2 Event: SCF:This XSCF will be switched back to standby
 mode after completion of firmware update
Apr  5 07:51:57 M12-2S-1 Event: SCF:Change Master Complete(BB#00)
```

If the message "XCP update has been completed" appears, the XCP firmware update
has completed.

Note - A message similar to "XSCF update has been completed" or "CMU update has been
completed" will appear on the SPARC M10. However, the update of all the XCP firmware
will not have completed by the time the message appears.

Note - To safely update the firmware, do not perform power operations for physical
partitions, reboot the XSCF, etc. until you have confirmed the "XCP update has been
completed" message on the completion of the XCP firmware update. For details, see "16.2.1
Notes on Update."

If the message "XCP update has been completed" does not appear, the update
is not yet complete. Execute the showlogs monitor command again to check
the completion of the update.

Usually, the update is completed about 40 minutes after an XSCF reboot.

- If the power of the physical partition is on

The update of the target CMU firmware has not yet begun at the point in time where the flashupdate command is executed and update completion is checked. Therefore, the message does not appear for the CMU firmware. The update of the target CMU firmware begins when the physical partition is powered off and on in step 13.

- If the firmware is updated to version XCP 2050 or later

After the firmware update is completed, the master and standby XSCFs are automatically switched. The automatic switching takes about 10 minutes.

If the messages "This XSCF will be switched back to standby mode after completion of firmware update," "Change Master Complete," and "Standby XSCF Ready" appear, the switching has been completed.

To check the completion of the switching, execute the showhardconf command, and confirm that Status is Normal for both the master XSCF and standby XSCF.

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

After confirming that the switching has completed, go to step 12.

Note - If execution of the showhardconf command displays "Cannot communicate with the other XSCF. Check the other XSCF's state.", the switching of the master and standby XSCFs has not been completed. Execute the showhardconf command again to check the completion of the switching.

Note - Firmware update processing switches the master and standby XSCFs twice. As a result, the XSCF where you executed the flashupdate command returns to being the master XSCF. Switching the master and standby XSCFs may disconnect the XSCF session. If the XSCF session is disconnected, reconnect.

Note - Do not perform power operations for physical partitions, reboot the XSCF, etc. until the switching of the master and standby XSCFs has completed. For details, see "16.2.1 Notes on Update."

- If the firmware is updated to version XCP 2044 or earlier

Firmware update processing switches the master and standby XSCFs. As a result, the other XSCF paired with the XSCF where you executed the flashupdate command becomes the master XSCF.

11. **Execute the switchscf command to return the master and standby XSCFs to their pre-update states.**

Note - When updating the firmware to version XCP 2050 or later, you do not have to perform this work because the XSCFs have already been switched.

```
XSCF> switchscf -t Standby
The XSCF unit switch between the Active and Standby states.
Continue? [y|n] :y
```

Since an XSCF reboot disconnects the XSCF session, the master XSCF is connected again.

To check the completion of the switching, execute the showhardconf command, and confirm that Status is Normal for both the master XSCF and standby XSCF.

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

Note - If execution of the showhardconf command displays "Cannot communicate with the other XSCF. Check the other XSCF's state.", the switching of the master and standby XSCFs has not been completed. Execute the showhardconf command again to check the completion of the switching.

---

12. **Set the XSCF time.**
    If the XSCF time has shifted, the logical domain time may shift when the physical partition is powered on.

    For details on how to set the XSCF time, see "6.1.2   Setting the XSCF Time Before System Startup."

13. **To complete the CMU firmware update when the power of the physical partition is on, power off and on the physical partition.**
    If the power of the physical partition is off, go to step 14.

If the power of the physical partition is on, execute the poweroff command to power off the physical partition.

```
XSCF> poweroff -p xx
```

Execute the showpparstatus power command, and confirm that the power of the physical partition is off.

```
XSCF> showpparstatus -p xx
PPAR-ID         PPAR Status
xx              Powered Off
```

Execute the poweron command to power on the physical partition.

```
XSCF> poweron -p xx
```

Execute the showpparstatus command, and confirm that PPAR Status is "Running."

```
XSCF> showpparstatus -p xx
PPAR-ID         PPAR Status
xx              Running
```

14. **Execute the version command, and confirm that the firmware version is up to date.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
    POST         : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
    POST         : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF          : 02.04.0004
```

```
BB#01-XSCF#0 (Standby)
XCP0 (Current): 2044
CMU           : 02.04.0004
    POST          : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF          : 02.04.0004
XCP1 (Reserve): 2044
CMU           : 02.04.0004
    POST          : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF          : 02.04.0004
CMU BACKUP
#0: 02.04.0004
#1: ..
```

Note - On the SPARC M10, if firmware is updated by powering on the physical partition, only the current bank of the CMU firmware is updated.
With the CMU firmware, where control is handled only by the current bank, there is no problem with an outdated version of the reserve bank.
If the firmware is updated by stopping the power of a physical partition, then both the reserve bank and current bank of the CMU firmware are updated.
For the CMU firmware version that corresponds to the XCP version, see "Existing XCP Firmware Versions and Support Information" in the latest *Product Notes* for your server.

16.6 Updating Firmware From XSCF Web

This section describes how to update firmware from XSCF Web with an example for the SPARC M12-1.

1. **Log in to XSCF Web.**

2. **Select [menu] - [XSCF] - [Settings] - [Autologout] menu, and set a value of 30 minutes or longer for the [Time-out value] value.**
   If you will need to restore the original value, make a note of the current setting value.

Note - If the XSCF shell timeout time is too short during XCP import or firmware update, "Session is invalid" may appear in the Web browser. For a building block configuration, set a value of 60 minutes or longer.

3. **Select [Physical] - [MBU].**

4. **Confirm that Status is Normal for the MBU on the [MBU Detail] screen as shown in Figure 16-2.**

Figure 16-2　　[MBU Detail] Screen

5. **Select [Menu] - [Maintenance] - [Firmware Update].**

6. **Confirm the version of the XCP firmware in operation, on the [Display Firmware Version] screen shown in Figure 16-3.**

Figure 16-3　　[Display Firmware Version] Screen

7. **Import an XCP image file from the [Import Firmware] screen shown in Figure 16-4.**

Specify the path of the XCP image file, and click the [Upload] button. Importing takes about five minutes.

Note - If the overwrite warning message "An existing file will be overwritten, continue to process?" appears, click the [OK] button.

Note - If a message such as "An internal error has occurred" or "Error: insufficient free space" appears during XCP import, an XSCF firmware error or parts failure may have occurred. In this case, see "16.8   Trouble During Firmware Update" and solve the problem.

Figure 16-4   [Import Firmware] Screen
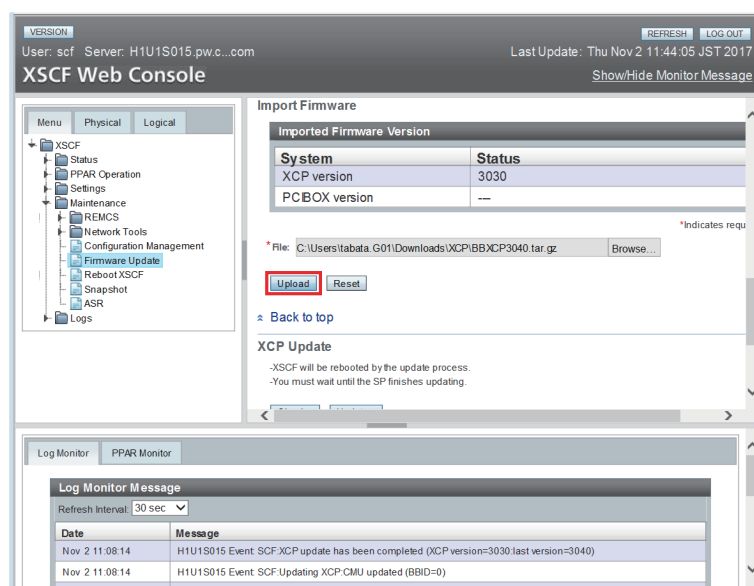
Importing is completed when "The file has been uploaded successfully." appears. The XCP Version line on the [Import Firmware] screen shown in Figure 16-5 is updated. Confirm that it displays the firmware version of the imported XCP image file.

Figure 16-5   [Import Firmware] Screen After Importing Ends
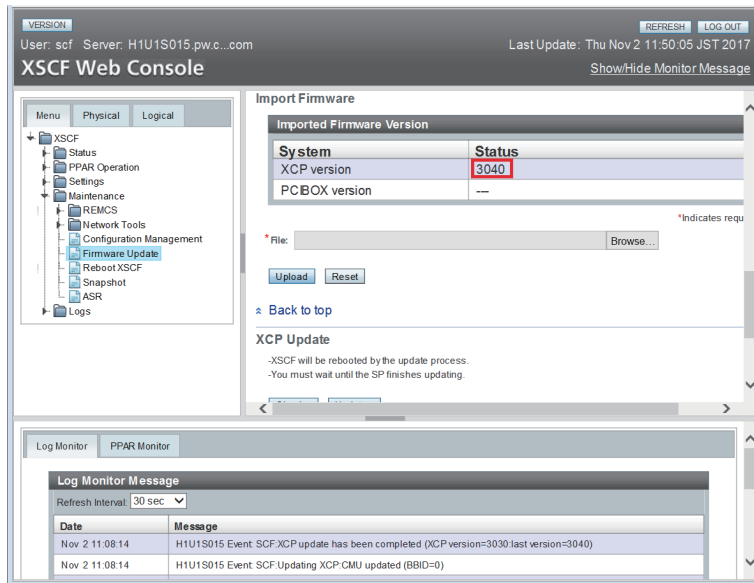
8. **Check the [XCP Update] screen shown in Figure 16-6 to see whether the imported XCP image file can be used to update the firmware.**
    Click the [Check] button and specify the firmware version in the pop-up window to start the file check. If "The XCP file has been checked successfully." appears, the file can be used for the firmware update.

Figure 16-6   XCP Image File Check From the [XCP Update] Screen
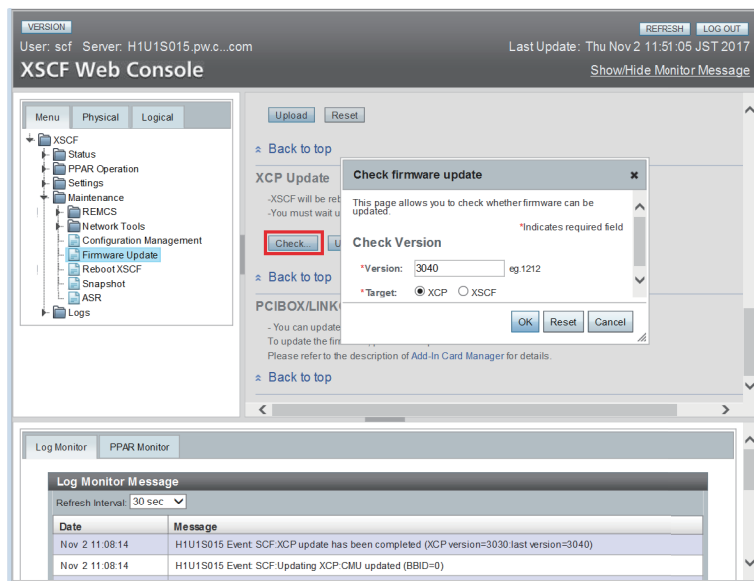
9. **Update the firmware from the [XCP Update] screen shown in Figure 16-7.**
   Click the [Update] button and specify the firmware version in the pop-up window to start the firmware update. The update takes about 30 minutes.

Note - In a building block configuration, the update tales about 60 minutes.

Note - If a message such as "An internal error has occurred" or "Internal error" appears during firmware update, an XSCF firmware error or parts failure may have occurred. In this case, see "16.8   Trouble During Firmware Update" and solve the problem.

Figure 16-7   Firmware Update From the [XCP Update] Screen
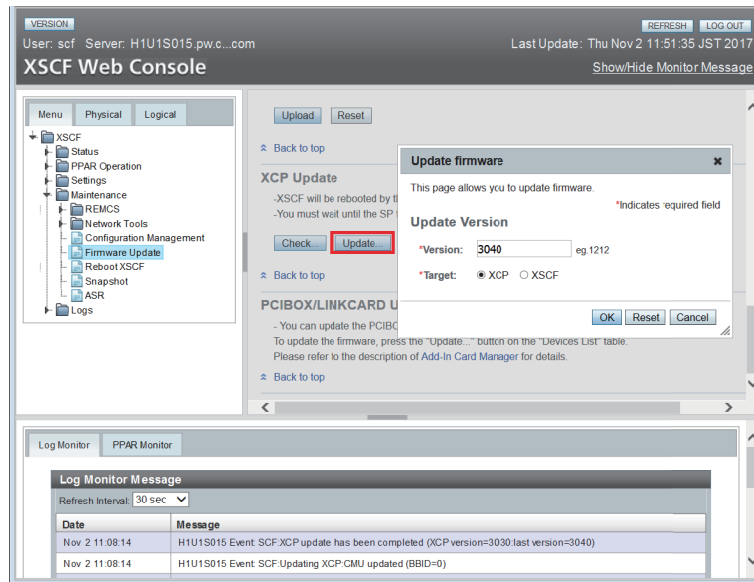
Partway through the update, the XSCF is rebooted, and the XSCF session is disconnected.
The message shown in Figure 16-8 is output.

Figure 16-8   XSCF reboot message
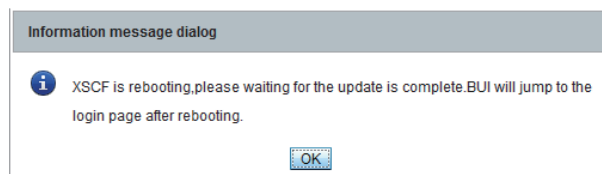
The message "The file has been updated successfully" shown in Figure 16-9 also appears partway through the update. At this point in time, the firmware update is not yet complete.

Figure 16-9   Message During the Update
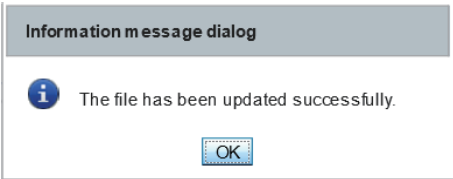
10. **Log in to XSCF Web again.**

11. **Check the firmware update message on the [Log Monitor Message] screen in the bottom frame of the window shown in Figure 16-10.**

Figure 16-10   [Log Monitor Message] Screen
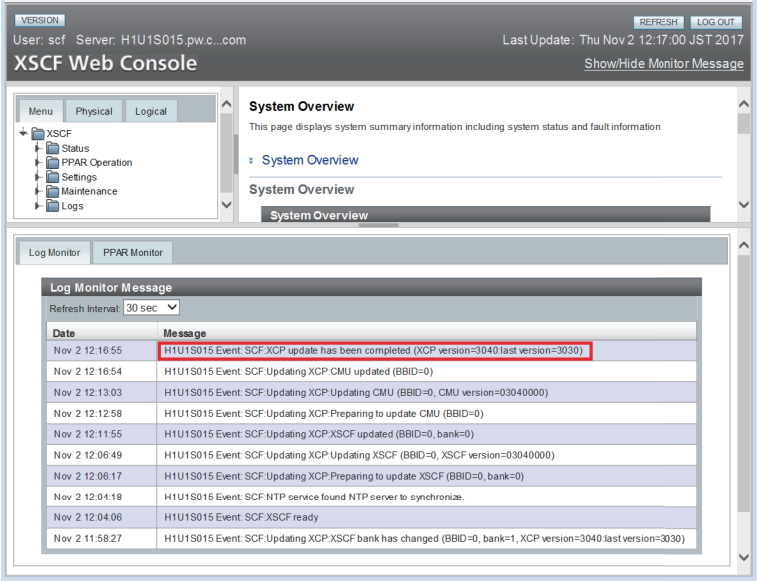
If the message "XCP update has been completed" appears, the XCP firmware update has completed.

Note - A message similar to "XSCF update has been completed" or "CMU update has been completed" will appear on the SPARC M10. However, the update of all the XCP firmware will not have completed by the time the message appears.

Note - To safely update the firmware, do not perform power operations for physical partitions, reboot the XSCF, etc. until you have confirmed the "XCP update has been completed" message on the completion of the XCP firmware update. For details, see "16.2.1 Notes on Update."

Note - In a building block configuration: The states of the master and standby XSCFs in a building block configuration immediately after the XCP firmware update is completed have been inverted from their pre-update states. The master and standby XSCFs are switched to

return them to their original states. The automatic switching takes about 10 minutes.

12. **Set the XSCF time.**
    If the XSCF time has shifted, the logical domain time may shift when the physical partition is powered on.

    For details on how to set the XSCF time, see "6.1.2   Setting the XSCF Time Before System Startup." Take action from the associated XSCF Web menu.

13. **Confirm that the firmware version is up to date on the [Display Firmware Version] screen as shown in Figure 16-11.**

Figure 16-11   [Display Firmware Version] Screen
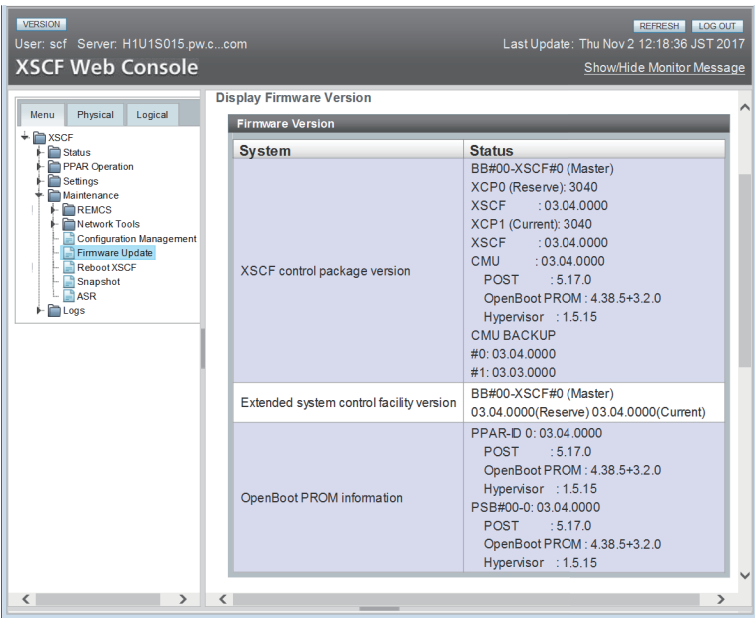
Note - Power of the physical partition is on: The target CMU firmware has not been updated at this point in time. Therefore, the message does not appear for the CMU firmware. To complete the CMU firmware update after the XCP firmware update is completed, power off and on the physical partition.

Note - In the case of a logical domain configuration, execute the ldm add-spconfig command of Oracle VM Server for SPARC in the control domain to save the latest configuration information in the XSCF before powering off the physical partition.
For details, see "6.2.2   Saving the Logical Domain Configuration Information before System Stop" and "10.11.1   Saving/Displaying Logical Domain Configuration Information."

Note - On the SPARC M10, if firmware is updated by powering on the physical partition, only the current bank of the CMU firmware is updated.
With the CMU firmware, where control is handled only by the current bank, there is

no problem with an outdated version of the reserve bank.
If the firmware is updated by stopping the power of a physical partition, then both the reserve bank and current bank of the CMU firmware are updated.
For the CMU firmware version that corresponds to the XCP version, see "Existing XCP Firmware Versions and Support Information" in the latest *Product Notes* for your server.

14. **If the auto logout time has been changed, select [menu] - [XSCF] - [Settings] - [Autologout] menu, and restore the original value in [Time-out value].**

16.7 Firmware Version Matching with Parts Addition/Replacement

This section describes the firmware version matching when parts are added/replaced. In a building block configuration, firmware is automatically updated during replacement of parts or addition of the SPARC M12-2S/M10-4S in order to match firmware versions in the system.
The following parts are targets:

- XSCF unit in the SPARC M12-2S

- CPU memory unit lower in the SPARC M10-4S

- XSCF unit in the crossbar box

Note - Replace/Add parts one by one. If multiple SPARC M12-2S/M10-4S servers are replaced/added at the same time, firmware is not automatically updated to match firmware versions. Update the firmware manually.

When parts are replaced or added in the systems described below, firmware is not automatically updated to match firmware versions. Update the firmware manually.

- System not in a building block configuration

- System with a crossbar box added

- SPARC M10-4S with an XCP version that does not support automatic update, and the maintenance menu is not used

For information on automatic update support for the SPARC M10-4S, see the *Fujitsu M10/SPARC M10 Systems Product Notes* for the latest XCP version.

16.7.1 Firmware Version Matching in Addition/ Replacement With the Input Power Turned On

This section describes how to match the version when replacing CPU memory units (lower) (CMUL), replacing XSCF units, adding the SPARC M12-2S/M10-4S, or adding the crossbar box with the input power turned on.

1. **After the addfru command or replacefru command is executed, if addition/replacement work is done using the maintenance menu, the XSCF firmware version is automatically matched.**
   If the addfru command, replacefru command, or testsb command performs a diagnosis test, the CMU firmware version is automatically matched.

2. **After the completion of the addfru, replacefru, or testsb command, execute the version command to check the XCP firmware version.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
    POST         : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
    POST         : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF         : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
    POST         : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
    POST         : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF         : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..
```

16.7.2 Firmware Version Matching in Addition/Replacement With the Input Power Turned Off

This section describes how to match the version when replacing CPU memory units (lower) (CMUL), replacing XSCF units, adding the SPARC M12-2S/M10-4S, or adding the crossbar box with the input power turned off.

1. **After replacing CPU memory units (lower) (CMUL), replacing XSCF units, adding the SPARC M10-4S, or adding the crossbar box, log in to the XSCF and execute the version command to check the XCP firmware version.**

The following example shows that, after addition/replacement work done without using the maintenance menu, the firmware version of BB#01 does not match.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU            : 02.04.0004
    POST           : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF           : 02.04.0004
XCP1 (Current): 2044
CMU            : 02.04.0004
    POST           : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF           : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2041
CMU            : 02.04.0001
    POST           : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor    : 0.26.9
XSCF           : 02.04.0001
XCP1 (Current): 2041
CMU            : 02.04.0001
    POST           : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor    : 0.26.9
XSCF           : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..
```

2. **If a firmware version does not match, execute the flashupdate -c sync command to match it to the master XSCF firmware version.**

```
XSCF> flashupdate -c sync
XCP update is started. [3600sec]
  0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
```

```
270.....300.....330.....360.....390.....420.....450.....480.....510.....|
540.....570.....600.....630.....660.....690.....720.....750.....780.....-
810.....840.....870.....900.....930.....960.....990.....1020.....1050.....\
1080.....1110.....1140.....1170.....1200.....1230.....1260.....1290.....
1320..../
1350.....1380.....1410.....1440.....1470.....1500.....1530.....1560.....15
90.....\
1620.....1650.....1680.....1710.....1740.....1770.....1800.....1830.....
1860..../
1890.....1920.....1950.....1980.....2010.....2040.....2070.....2100.....
2130.....\
2160.....2190..XSCF>
XSCF>
```

3. **Execute the version command, and confirm that the XCP firmware version matches the XSCF firmware version.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU             : 02.04.0004
    POST            : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF            : 02.04.0004
XCP1 (Current): 2044
CMU             : 02.04.0004
    POST            : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor    : 0.27.3
XSCF            : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU             : 02.04.0001
    POST            : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor    : 0.26.9
XSCF            : 02.04.0004
XCP1 (Current): 2044
CMU             : 02.04.0001
    POST            : 1.42.0
    OpenBoot PROM : 4.34.0+1.16.0
    Hypervisor    : 0.26.9
XSCF            : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..
```

The target CMU firmware is not updated at this point in time.

4. **Set the XSCF time.**
    If the XSCF time has shifted, the logical domain time may shift when the physical partition is powered on.

For details on how to set the XSCF time, see "6.1.2   Setting the XSCF Time Before System Startup."

5. **Power on the target physical partition so that the CMU firmware version matches.**
Execute the poweron command to power on the physical partition.

```
XSCF> poweron -p xx
```

Execute the showpparstatus command, and confirm that PPAR Status is "Running."

```
XSCF> showpparstatus -p xx
PPAR-ID        PPAR Status
XX             Running
```

6. **Execute the version command to check the CMU firmware version of the target physical partition.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU         : 02.04.0004
    POST        : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU         : 02.04.0004
    POST        : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF        : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU         : 02.04.0004
    POST        : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU         : 02.04.0004
    POST        : 1.43.0
    OpenBoot PROM : 4.34.0+1.19.0
    Hypervisor   : 0.27.3
XSCF        : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..
```

16.8 Trouble During Firmware Update

This section describes problems that occur during firmware update and their corrective actions.

- Problems that occur due to XSCF unit defects
  If a write-related error, including those listed below, or a reboot failure-related error occurs, a parts failure has occurred.

  Contact a field engineer or service engineer to solve the problem.

  - Firm update failure

  - XSCF data write error

- Problems that occur in importing
  - The following error may occur during XCP importing on XSCF Web: "File upload failed. This mostly caused by network unstable, please try again later." There may be a problem with the network environment or browser settings. Check whether cookies are accepted in the network environment and the Web browser settings.

  - If the following error occurs during XCP import, there may be a problem with the XCP file: "Error: File is invalid or corrupt." Check the XCP file.
    The possible cause, for example, is that an unauthorized XCP image file was obtained or that the XCP image file downloaded by the customer was subsequently changed through unauthorized access. In such cases, obtain the correct XCP image file and import XCP again.

  After the check, try again. If the retry also does not end normally, contact a field engineer or service engineer to solve the problem.

- Problems that occur in importing or when updating firmware
  Errors, including those listed below, may occur during XCP importing or firmware updating. In such cases, an XSCF firmware error or parts failure may have occurred.

  In this situation, contact a field engineer or service engineer to solve the problem.

  - An internal error has occurred

  - Error: insufficient free space

  - Internal error

- Other errors
  If a failure other than the above occurs during firmware update, try the firmware update again.

  The second attempt at the firmware update may end normally.

  If the retry also does not end normally, contact a field engineer or service engineer to solve the problem.

16.9 FAQ Relating to Firmware Update

Q: Is it okay to reboot twice when updating the CMU firmware?

A: That would not be a problem.

Q: In the systems with multiple XSCFs, why are the master XSCF and standby XSCF switched partway through an update?

A: The master XSCF exercises control to apply the firmware update to the standby XSCF. Upon completion of the firmware update on the standby side, the standby side has new firmware. The standby side is switched with the master side to apply the firmware update to the XSCF again on the standby side (old master side).

Q: Can the CMU firmware be updated on all physical partitions at one time?

A: Yes. If the power of all physical partitions is off, the firmware can be updated at one time. If the power of a physical partition is on, you can update it to the new firmware by executing the poweroff -a command and then the poweron -a command with all the physical partitions specified.

Chapter 17

Updating Oracle Solaris and Oracle VM Server for SPARC

This chapter describes how to update Oracle Solaris installed on a logical domain.

Each of the logical domains configured for a physical partition already has Oracle Solaris installed. You can update Oracle Solaris individually on each logical domain.

Before Update

Before updating Oracle Solaris on the control domain, save the data listed below in advance. Restore the data after the update.

- Autosave configuration directories
  /var/opt/SUNWldm/autosave-*

- Logical Domains constraints database files
  /var/opt/SUNWldm/ldom-db.xml provides a reference to the Logical Domains constraints database files.

For details, see "Installing and Enabling Software" in the *Oracle VM Server for SPARC Administration Guide* of the version used.

Updating

Use the latest SRU (Support Repository Update) when updating Oracle Solaris. For the supported versions of Oracle Solaris and the latest SRU-related information, see the latest *Product Notes* for your server.

For details on how to update Oracle Solaris and Oracle VM Server for SPARC, see Oracle Solaris related manuals and "Installing and Enabling Software" in the *Oracle VM Server for SPARC Administration Guide* of the version used.

Chapter 18

Troubleshooting

This chapter describes problems that may occur during use of the XSCF or while the system is running, and how to solve the problems.

- Troubleshooting for the XSCF
- Precautions Concerning Using the RESET Switch
- Frequently Asked Questions / FAQ
- System Troubleshooting With the XSCF

18.1 Troubleshooting for the XSCF

This section describes problems that may occur during use of the XSCF, and how to solve the problems.

Login to the XSCF Not Possible

- Check whether the user name entered for login is correct.
- Check whether the password used is correct.
- Check the number of the users currently connected to the XSCF. For details of the number of users, see "2.6 Number of Connectable Users."

Forgotten Login Password for the XSCF

- Ask the system administrator to reset the password. A system administrator who has the platadm or useradm user privilege can reset the password by using the password command.
- If the system administrator forgets the login password, log in using the "default" account, and set the password again by using the password command. For details on login authentication with the "default" account, see "Performing an Initial System Diagnosis" in the *Installation Guide* for your server.

XSCF Cannot be Connected via the Serial Port

- Check whether the terminal software is connected to the serial port.
- Check the terminal software setting (baud rate of 9600 bps, delay of other than 0, etc.) For details of settings, see "2.2.1   How to Log In to the XSCF Shell With a Serial Connection."

Note - If the XSCF connection fails even after you have performed the measures above, the problem could be solved by pressing the RESET switch on the rear panel. For details, see "18.2   Precautions Concerning Using the RESET Switch."

XSCF Cannot be Connected Using Telnet via the XSCF-LAN

- Check whether the LAN cable between the XSCF shell terminal and server is correctly connected.
- Check whether the terminal software is connected to the Telnet port.
- Use the shownetwork command to check whether the XSCF-LAN is enabled.
- Use the showtelnet command to check whether the Telnet service is enabled.
- Confirm that the entered IP address and port number do not differ from the settings.
- Confirm that the number of connections via Telnet/SSH does not exceed the upper limit. For details of the upper limit, see "2.6   Number of Connectable Users."
- If necessary, use the console on a PC connected directly to the XSCF through the serial port to log in to the XSCF shell, and check the XSCF-LAN settings by using the shownetwork command.

Note - If the XSCF connection fails even after you have performed the measures above, the problem could be solved by pressing the RESET switch on the rear panel. For details, see "18.2   Precautions Concerning Using the RESET Switch."

XSCF Cannot be Connected Using SSH via the XSCF-LAN

- Confirm that the LAN cable between the XSCF shell terminal and the server is correctly connected.
- Execute the shownetwork command to confirm that the XSCF-LAN setting is enabled.
- Execute the showssh command to confirm that the SSH service is enabled.
- Confirm that the entered IP address and port number do not differ from the settings.
- Confirm that the number of connections via Telnet/SSH does not exceed the upper limit. For details of the upper limit, see "2.6   Number of Connectable Users."
- If necessary, use the console on a PC connected directly to the XSCF through the serial port to log in to the XSCF shell, and check the XSCF-LAN settings by

executing the shownetwork command.

- Confirm that the host key setting is correct. Note that replacing an XSCF unit returns the host key to the preset key on the XSCF.

- Confirm that the client software has the correct settings.

Note - If the XSCF connection fails even after you have performed the measures above, the problem could be solved by pressing the RESET switch on the rear panel. For details, see "18.2 Precautions Concerning Using the RESET Switch."

Unknown XSCF IP Address

- Use the shownetwork command to check the current network configuration. If the address has not been set, notify the network administrator to check the settings.

- If necessary, use the console on a PC connected directly to the XSCF through the serial port to log in to the XSCF shell, and check the XSCF-LAN settings by using the shownetwork command.

XSCF Shell Terminal or Domain Console Suddenly Disconnected

- After the setnetwork, setroute, sethostname, setnameserver, and setsscp commands related to the XSCF network were executed by another user, the applynetwork and rebootxscf commands may have been executed. Alternatively, the flashupdate command may have been executed. To use the XSCF, establish another connection, and log in again.

- The setdate or switchscf command with respect to the XSCF may have been executed by another user. To use the XSCF, establish another connection, and log in again.

- If the XSCF shell is left unused for a specific duration after login, the XSCF automatically terminates the shell. This forced termination occurs after that length of time has elapsed, only if the time monitoring function is enabled and the length of time is set for this function in the XSCF settings.

- Oracle Solaris Secure Shell or the SSH client of OpenSSH is disconnected by the input of the escape character (e.g., "#") and "." (period) key that were set by the client. If the escape character of Oracle Solaris Secure Shell or the SSH client of OpenSSH has the same setting as the escape character that has been set by the console command, the terminal is disconnected. Therefore, change either of the setting values. For details, see the SSH client manual.

Server Power-on/off Operation Not Possible

- The power-on/off operations for the whole system are not available for operations with a user privilege other than the platadm or fieldeng privilege. For details of user privileges, see "3.5.3 Types of User Privilege."

XSCF User Cannot be Added

- Check the registered number of XSCF users. For details of the registered number,

see "2.6　Number of Connectable Users." Alternatively, notify the system administrator.

No E-mail Notification From the XSCF

- The XSCF does not necessarily report all events. It sends e-mails for parts failures, authentication failure events, etc. To check for the intended notification in the error log or among the reported events in the event log, see "12.1　Checking a Log Saved by the XSCF."
- Use the showemailreport command to check whether enabled is the setting. If no e-mail has arrived, check whether an error e-mail was sent to the error e-mail notification recipient, or check the errors recorded in the error log.
- If a mobile phone is used to receive such e-mails, check the mobile phone settings for any receiving limit on its e-mail address.

Top Page of XSCF Web Not Accessible

- Use the showhttps command to check whether XSCF Web is enabled.
- Check whether the entered URL is correct. (Examples include a missing "s" for https.)
- Check with the system administrator about permission settings for the IP address.
- Check whether the connection setting with TLS 1.0 of the Web browser is enabled.

XSCF Web Window Not Displayed

- If the individual windows of XSCF Web do not appear after login from the top page of XSCF Web, JavaScript may be disabled in the Web browser settings. Enable JavaScript in the Web browser settings, and log in again.
- If pop-up windows are blocked by the Web browser settings, XSCF Web windows cannot appear. Check the Web browser settings.

Forgotten Password for XSCF Web

- XSCF Web authentication is the same as XSCF shell authentication. See the above "Forgotten Login Password for the XSCF."

Initial Access Failed After Login With XSCF Web

- Check whether cookies are accepted in the Web browser settings.

XSCF Web Not Displayed Correctly in the Web Browser Window

- Some versions of Web browsers may not correctly show the XSCF in their windows. See the supported browsers in "2.4　Logging In to XSCF Web," and update the Web browser to the latest version.

Warning Displayed on XSCF Web

- Check the contents of the security warning, and stop the use of XSCF Web. Take appropriate action according to the contents of the checked warning. If the expiration time has passed, configure the HTTPS service of the XSCF again. For details of HTTPS service settings, see "3.8   Configuring the HTTPS Service for Login to the XSCF."

Displayed Message Regarding the NTP Server

- The following message regarding the NTP server might appear when the XSCF starts. It means there may be a time deviation from the XSCF because time synchronization failed between the NTP server and the XSCF.

```
NTP service failed to reach appropriate NTP server.
```

If the physical partition starts in this situation, the logical domain time may shift.

Set the XSCF time before starting the physical partition.

For details, see "6.1.2   Setting the XSCF Time Before System Startup."

Other Troubles

- Notify the system administrator. If you need to collect/save an XSCF log, use XSCF shell commands to save the XSCF log. For details on how to save a log, see "12.1.15 Saving a Log to a File With Snapshot."

18.2   Precautions Concerning Using the RESET Switch

The RESET switch is an emergency switch, which is on the rear panel of the SPARC M12/M10 and crossbar box, to reboot the XSCF.
Use the RESET switch as an emergency measure when the XSCF does not start and access cannot be made to the XSCF after applying the measures introduced in this section.
When using the RESET switch, note the following.

- Use the RESET switch as a last resort to start the XSCF.

- If the XSCF does not start even after pressing the RESET switch, ask a service engineer.

- Do not press the RESET switch many times while the XSCF is operating. If you press the RESET switch repeatedly, the CHECK LED goes on and the XSCF READY LED goes out. Then, the XSCF stops. If that happens, you need to turn off/on the input power to connect to the XSCF.

For the RESET switch location, see the *Service Manual* for your server or "Appendix C External Interface Specifications" in the *Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

18.3 Frequently Asked Questions / FAQ

This section contains frequently asked questions about using the XSCF.

Q: Are IP addresses assigned by default to the LAN ports used with the XSCF-LAN?

A: No XSCF-LAN IP address is assigned by default for the IP addresses. For details on XSCF-LAN IP addresses, see "3.9.2 Understanding the XSCF Network Interfaces."

Q: Is a default IP address assigned for SSCP?

A: An IP address is assigned by default. For the default SSCP IP address, see "3.9.5 Understanding the IP Addresses that are Set with SSCP." If the default IP address may affect the user LAN environment, change it.

Q: If Oracle Solaris hangs up during Oracle Solaris startup after the server is powered on, can the server be powered off from the XSCF?

A: If a guest domain hangs up, collect an Oracle Solaris dump by using the ldm panic-domain command. For details of the ldm command, see the *Oracle VM Server for SPARC Reference Manual* of the version used.
If a control domain hangs up, do the following.

1. **Execute the reset command with the panic option specified in the XSCF shell to give an instruction for an Oracle Solaris dump.**

2. **If the Oracle Solaris dump failed even though step 1. was performed, execute the poweroff command in the XSCF shell to turn off the power.**

Q: What kind of processing is executed by the XSCF after input power is supplied to the server until Oracle Solaris starts?

A: The processing flow until the system starts is as follows. For details, see "Chapter 6 Starting/Stopping the System."

1. **The operator turns on the input power.**

2. **The XSCF starts.**

3. **The operator powers on the server.**

4. **The XSCF initializes hardware.**

5. **POST starts and performs an initial hardware diagnosis.**

6. **OpenBoot PROM starts.**

7. **OpenBoot PROM starts the boot process.**

8. **Oracle Solaris starts.**

Q: What kind of messages appear on the terminal during normal XSCF login or logout?

A: XSCF login success/failure is described below.
The following example shows login has succeeded.

```
login: jsmith
Password: xxxxxxxx
XSCF>
```

The following example shows login failed.

```
login: jsmith
Password: xxxxxxxx
Login incorrect
```

A: XSCF logout success/failure is described below.
The following example shows logout has succeeded.

```
XSCF> exit
Logout
```

The following example shows logout failed.

```
XSCF> exit
Not supported in this system.
```

Note - The above examples vary depending on the client software on the terminal.

Q: What is the relationship between the XSCF error log and the error information in a MIB definition file?

A: The error information reflected in a MIB definition file is the latest XSCF error log.

18.4 System Troubleshooting With the XSCF

This section describes how to effectively use the XSCF when the server is not responding, which means that a problem or panic occurred in the system.

Before Notifying a Service Engineer

Follow the process below before contacting a service engineer. The procedure may not only help in solving the problem but also eliminate the need to make an inquiry.

1. **If the server does not respond, set the Mode switch on the operation panel to Service mode.**

2. **Check the system status with either of the following methods.**

- Method when the XSCF shell cannot be used via SSH/Telnet

  a. Connect a terminal to the serial port of the XSCF.

  b. Enter your user account and password to log in to the XSCF shell.

  c. Use the XSCF shell to check the error log and other information.

- Method when the XSCF shell can be used via SSH/Telnet and the serial port

  a. Log in to the XSCF with your XSCF user account.

  b. Connect to the XSCF-LAN port, and use the XSCF shell to check the error log and other information.
  For details of the error log, see "12.1   Checking a Log Saved by the XSCF." Check and take action accordingly.

  c. Alternatively, check the XSCF event log and server status by using the XSCF shell via the serial port.
  Execute the following commands to check the events that happened at the time the problem occurred:

  showlogs error

  showlogs event

  showlogs power

  showlogs monitor

  showlogs console

  If you find a failure, see "12.1   Checking a Log Saved by the XSCF." Check and take action accordingly.

  d. Check the XSCF console log or panic log for the latest messages.
  Oracle Solaris may have detected a problem and displayed a message. Also, for cases involving a panic, use the showlogs command with the panic option to check the events that happened at the time the panic occurred.

3. **When the above check does not find any problem, restart the system.**

4. **If a failure occurs, see "12.1   Checking a Log Saved by the XSCF." Take action accordingly, such as regarding a part by following the maintenance guidance for XSCF shell commands.**

Appendix A

Lists of SPARC M12/M10 System Device Paths

This appendix describes the device paths of the SPARC M12/M10 systems.

- SPARC M12-1 Device Paths
- SPARC M12-2 Device Paths
- SPARC M12-2S Device Paths
- SPARC M10-1 Device Paths
- SPARC M10-4 Device Paths
- SPARC M10-4S Device Paths

A.1 SPARC M12-1 Device Paths

Device paths which are recognized by the SPARC M12-1, and the hardware block diagram corresponding to device paths are as follows.

Table A-1   I/O Device Paths in the SPARC M12-1 Chassis and on the PCI Expansion Unit Side

Instance Priority	Device	Device Path	Number in Diagram
1	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@1/network@0	1
2	Internal LAN#1	/pci@8000/pci@4/pci@0/pci@1/network@0,1	2
3	Internal SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0	3
-	Internal HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	4
-	Internal HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	5
-	Internal HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	6
-	Internal HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	7
-	Internal HDD#4	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p4	8
-	Internal HDD#5	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5	9
-	Internal HDD#6	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p6	10

Table A-1   I/O Device Paths in the SPARC M12-1 Chassis and on the PCI Expansion Unit Side *(continued)*

Instance Priority	Device	Device Path	Number in Diagram
-	Internal HDD#7	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p7	11
-	External SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	12
4	Internal USB port (rear: USB 3.0)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/****@1	13
	Internal USB port (rear: USB 2.0/1.1)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/****@1	14
5	Internal USB port (front: USB 2.0/1.1)	/pci@8100/pci@4/pci@0/pci@8/usb@0/****@6	15
6	Remote storage	/pci@8100/pci@4/pci@0/pci@8/usb@0/storage@7	16
7	PCI#0	/pci@8100/pci@4/pci@0/pci@9/****@0	17
	PCI expansion units under PCI#0		
8	PCI#1	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@0/****@0	
9	PCI#2	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@1/****@0	
10	PCI#3	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@8/****@0	
11	PCI#4	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
12	PCI#5	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
13	PCI#6	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
14	PCI#7	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
15	PCI#8	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
16	PCI#9	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
17	PCI#10	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
18	PCI#11	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
19	Internal LAN#2	/pci@8200/pci@4/pci@0/pci@0/network@0	18
20	Internal LAN#3	/pci@8200/pci@4/pci@0/pci@0/network@0,1	19
21	PCI#1 PCI expansion units under PCI#1	/pci@8200/pci@4/pci@0/pci@8/****@0	20

Instance Priority	Device	Device Path	Number in Diagram
22	PCI#1	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
23	PCI#2	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
24	PCI#3	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
25	PCI#4	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
26	PCI#5	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
27	PCI#6	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
28	PCI#7	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
29	PCI#8	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
30	PCI#9	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
31	PCI#10	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
32	PCI#11	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
33	PCI#2	/pci@8300/pci@4/pci@0/pci@1/****@0	21
	PCI expansion units under PCI#2		
34	PCI#1	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
35	PCI#2	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
36	PCI#3	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
37	PCI#4	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
38	PCI#5	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
39	PCI#6	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
40	PCI#7	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	

Instance Priority	Device	Device Path	Number in Diagram
41	PCI#8	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
42	PCI#9	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
43	PCI#10	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
44	PCI#11	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@11/****@0	

Figure A-1   SPARC M12-1 Block Diagram
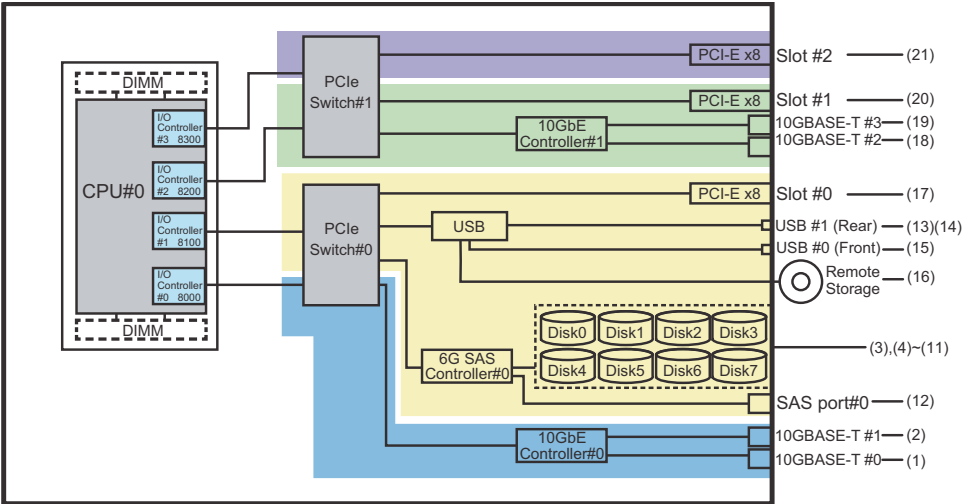
A.2   SPARC M12-2 Device Paths

Device paths which are recognized by the SPARC M12-2, and the hardware block diagram corresponding to device paths are as follows.

A.2.1   For a 1-CPU Configuration at the Initial Installation Time

Device paths for a 1-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

I/O Device Paths in the SPARC M12-2 Chassis

Table A-2   I/O Device Paths in the SPARC M12-2 Chassis (Initial Installation Time: 1 CPU)

Instance Priority	Device	Device Path	Number in Diagram
1	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	Internal LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#8	/pci@8000/pci@4/pci@0/pci@1/****@0	3
4	PCI#3	/pci@8000/pci@4/pci@0/pci@10/****@0	4
5	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	5
6	Internal SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	6
-	Internal HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	7
-	Internal HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	8
-	Internal HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	9
-	Internal HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	10
-	External SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	11
7	Internal USB port (rear:USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	12
8	Internal USB port (rear:USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	13
9	Internal USB port (front:USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	14
10	Remote storage	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	15
11	PCI#1	/pci@8100/pci@4/pci@0/pci@10/****@0	16
12	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	17
13	Internal LAN#2	/pci@8200/pci@4/pci@0/pci@0/network@0	18
14	Internal LAN#3	/pci@8200/pci@4/pci@0/pci@0/network@0,1	19
15	PCI#6	/pci@8200/pci@4/pci@0/pci@1/****@0	20

Instance Priority	Device	Device Path	Number in Diagram
16	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	21
17	PCI#10	/pci@8200/pci@4/pci@0/pci@9/****@0	22
18	Internal SAS#1	/pci@8300/pci@4/pci@0/pci@0/scsi@0	23
-	Internal HDD#4	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p4	24
-	Internal HDD#5	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p5	25
-	Internal HDD#6	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p6	26
-	Internal HDD#7	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p7	27
19	PCI#4	/pci@8300/pci@4/pci@0/pci@1/****@0	28
20	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	29
21	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	30

*1 If a USB3.0 device is used, it works as USB2.0.

Figure A-2   SPARC M12-2 Block Diagram (1 CPU)
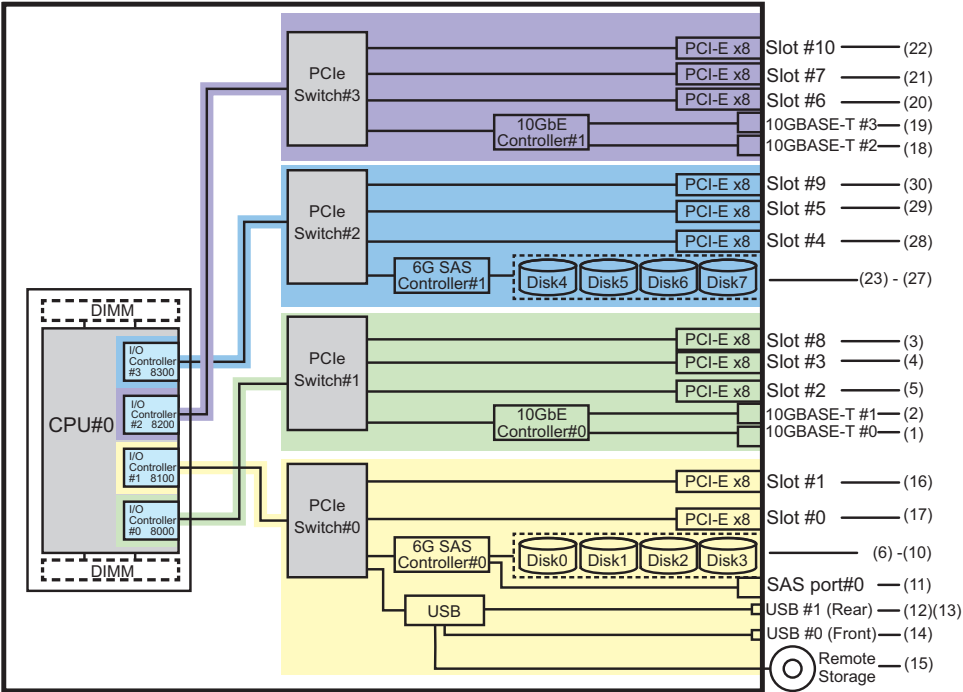
I/O Device Paths on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in

the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-2.

Table A-3   I/O Device Paths on the PCI Expansion Unit Side (1 CPU)

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.2.2   For a 2-CPU Configuration at the Initial Installation Time

Device paths for a 2-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

Note - If you disable I/O bus reconfiguration (ioreconfigure) by using the setpparmode command, the following device paths also apply to cases of removal that reduce a 2-CPU configuration to a 1-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
If you enable I/O bus reconfiguration (ioreconfigure) and reduce a 2-CPU configuration to a 1-CPU configuration, the device paths change to the 1-CPU configuration (Table A-2) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.
In addition, you may need to reinstall Oracle Solaris or set it again.
If you want to keep the logical domain configuration, disable I/O bus reconfiguration and

I/O Device Paths in the SPARC M12-2 Chassis

Table A-4   I/O Device Paths in the SPARC M12-2 Chassis (Initial Installation Time: 2 CPUs)

Instance Priority	Device	Device Path	Number in Diagram
1	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	Internal LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	3
4	Internal SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	4
-	Internal HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	5
-	Internal HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	6
-	Internal HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	7
-	Internal HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	8
-	External SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	9
5	Internal USB port (rear:USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	10
6	Internal USB port (rear:USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	11
7	Internal USB port (front:3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	12
8	Remote storage	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	13
9	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	14
10	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	15
11	PCI#10	/pci@8200/pci@4/pci@0/pci@9/****@0	16
12	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	17
13	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	18
14	Internal LAN#2	/pci@8400/pci@4/pci@0/pci@0/network@0	19
15	Internal LAN#3	/pci@8400/pci@4/pci@0/pci@0/network@0,1	20
16	PCI#6	/pci@8400/pci@4/pci@0/pci@1/****@0	21
17	Internal SAS#1	/pci@8500/pci@4/pci@0/pci@0/scsi@0	22
-	Internal HDD#4	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p4	23
-	Internal HDD#5	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p5	24
-	Internal HDD#6	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p6	25
-	Internal HDD#7	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p7	26
18	PCI#4	/pci@8500/pci@4/pci@0/pci@1/****@0	27

Instance Priority	Device	Device Path	Number in Diagram
19	PCI#8	/pci@8600/pci@4/pci@0/pci@1/****@0	28
20	PCI#3	/pci@8600/pci@4/pci@0/pci@10/****@0	29
21	PCI#1	/pci@8700/pci@4/pci@0/pci@10/****@0	30

*1 If a USB3.0 device is used, it works as USB2.0.

Figure A-3   SPARC M12-2 Block Diagram (2 CPUs)
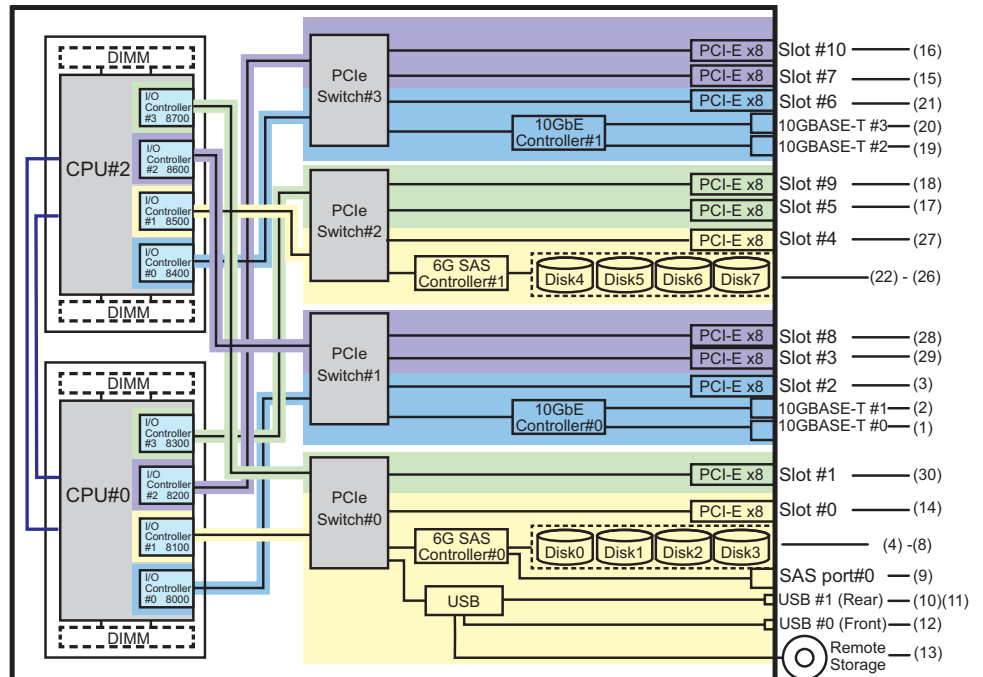
I/O Device Paths on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-4.

Table A-5   I/O Device Paths on the PCI Expansion Unit Side (2 CPUs)

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@1/pci@0/pci@1/****@0

Instance Priority	Device	Device Path
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.3   SPARC M12-2S Device Paths

Device paths which are recognized by the SPARC M12-2S, and the hardware block diagram corresponding to device paths are as follows.

A.3.1   For a 1-CPU Configuration at the Initial Installation Time

Device paths for a 1-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

Note - If you disable I/O bus reconfiguration (ioreconfigure) by using the setpparmode command, the following device paths also apply to cases of addition that expand a 1-CPU configuration to a 2-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
If you enable I/O bus reconfiguration (ioreconfigure) and expand a 1-CPU configuration to a 2-CPU configuration, the device paths change to the 2-CPU configuration (Table A-9) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.

In addition, you may need to reinstall Oracle Solaris or set it again.
If you want to keep the logical domain configuration, disable I/O bus reconfiguration and expand the configuration.

I/O Device Paths in the SPARC M12-2S Chassis

Table A-6   I/O Device Paths in the SPARC M12-2S Chassis (Initial Installation Time: 1 CPU)

Instance Priority	Device		Device Path	Number in Diagram
1	LSB#0	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2		Internal LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3		PCI#3	/pci@8000/pci@4/pci@0/pci@10/****@0	3
4		PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	4
5		Internal SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	5
-		Internal HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	6
-		Internal HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	7
-		Internal HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	8
-		Internal HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	9
-		External SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
6		Internal USB port (rear:USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	11
7		Internal USB port (rear:USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	12
8		Internal USB port (front:USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	13
9		Remote storage	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	14
10		PCI#1	/pci@8100/pci@4/pci@0/pci@10/****@0	15
11		PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	16
12		Internal LAN#2	/pci@8200/pci@4/pci@0/pci@0/network@0	17

Table A-6   I/O Device Paths in the SPARC M12-2S Chassis (Initial Installation Time: 1 CPU) *(continued)*

Instance Priority	Device	Device Path	Number in Diagram
13	Internal LAN#3	/pci@8200/pci@4/pci@0/pci@0/network@0,1	18
14	PCI#6	/pci@8200/pci@4/pci@0/pci@1/****@0	19
15	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	20
16	Internal SAS#1	/pci@8300/pci@4/pci@0/pci@0/scsi@0	21
-	Internal HDD#4	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p4	22
-	Internal HDD#5	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p5	23
-	Internal HDD#6	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p6	24
-	Internal HDD#7	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p7	25
17	PCI#4	/pci@8300/pci@4/pci@0/pci@1/****@0	26
18	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	27

*1 If a USB3.0 device is used, it works as USB2.0.

Figure A-4   SPARC M12-2S Block Diagram
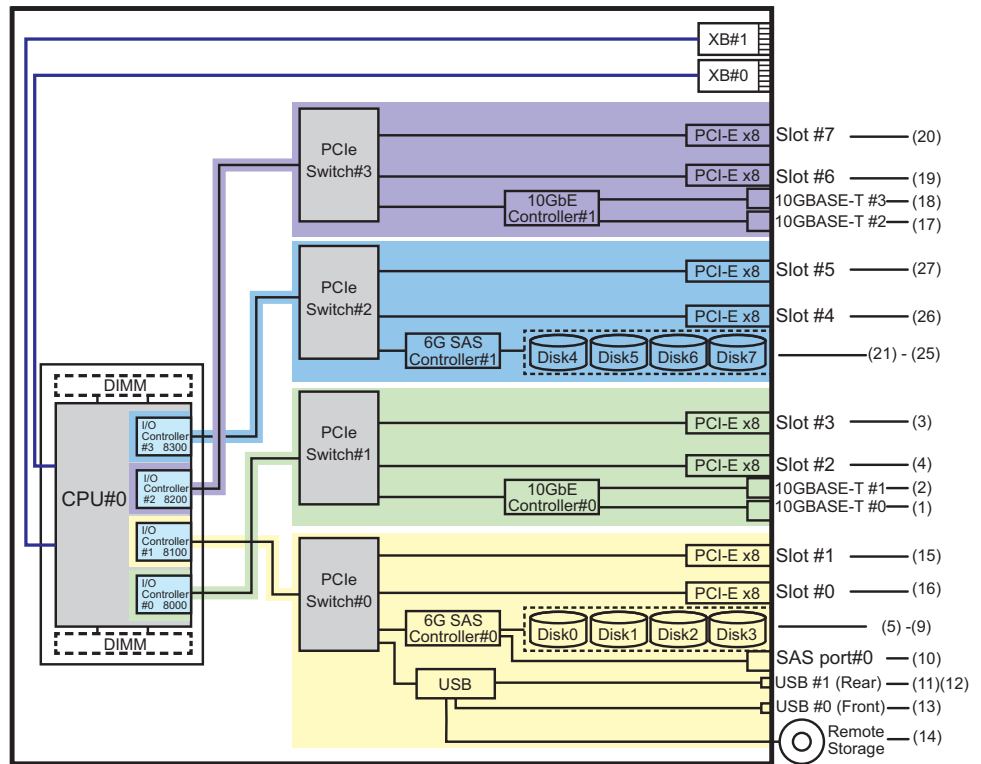
I/O Device Paths on the PCI Expansion Unit Side

If the server side PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-6.

Table A-7   I/O Device Paths on the PCI Expansion Unit Side

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0

Instance Priority	Device	Device Path
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

I/O Device Paths of Logical System Boards

For the I/O device paths of LSB#1 to LSB#15, the device nodes (/pci@vvvv) at the beginning of the I/O device paths in Table A-7 become those shown in Table A-8. The other device nodes are the same as in Table A-7.
As an example, for LSB#1, interpret the node values in Table A-7 as shown below. Also interpret the node values for LSB#2 to LSB#15 in the same way.
/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00

Table A-8   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 1 CPU)

LSB No.	Device Path
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ...
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ...
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ...
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ...
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ...

Table A-8   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 1 CPU) *(continued)*

LSB No.	Device Path
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/… /pci@eb00/…
LSB#14	/pci@f000/… /pci@f100/… /pci@f200/… /pci@f300/…
LSB#15	/pci@f800/… /pci@f900/… /pci@fa00/… /pci@fb00/…

A.3.2 For a 2-CPU Configuration at the Initial Installation Time

Device paths for a 2-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

> **Note -** If you disable I/O bus reconfiguration (ioreconfigure) by using the setpparmode command, the following device paths also apply to cases of removal that reduce a 2-CPU configuration to a 1-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
> If you enable I/O bus reconfiguration (ioreconfigure) and reduce a 2-CPU configuration to a 1-CPU configuration, the device paths change to the 1-CPU configuration (Table A-6) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.
> In addition, you may need to reinstall Oracle Solaris or set it again.
> If you want to keep the logical domain configuration, disable I/O bus reconfiguration and reduce the configuration.

I/O Device Paths in the SPARC M12-2S Chassis

Table A-9   I/O Device Paths in the SPARC M12-2S Chassis (Initial Installation Time: 2 CPUs)

Instance Priority	Device		Device Path	Number in Diagram
1	LSB#0	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2		Internal LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3		PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	3
4		Internal SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	4
-		Internal HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	5
-		Internal HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	6
-		Internal HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	7
-		Internal HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	8
-		External SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	9
5		Internal USB port (rear:USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	10

Instance Priority	Device	Device Path	Number in Diagram
6	Internal USB port (rear:USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	11
7	Internal USB port (front:USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	12
8	Remote storage	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	13
9	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	14
10	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	15
11	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	16
12	Internal LAN#2	/pci@8400/pci@4/pci@0/pci@0/network@0	17
13	Internal LAN#3	/pci@8400/pci@4/pci@0/pci@0/network@0,1	18
14	PCI#6	/pci@8400/pci@4/pci@0/pci@1/****@0	19
15	Internal SAS#1	/pci@8500/pci@4/pci@0/pci@0/scsi@0	20
-	Internal HDD#4	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p4	21
-	Internal HDD#5	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p5	22
-	Internal HDD#6	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p6	23
-	Internal HDD#7	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p7	24
16	PCI#4	/pci@8500/pci@4/pci@0/pci@1/****@0	25
17	PCI#3	/pci@8600/pci@4/pci@0/pci@10/****@0	26
18	PCI#1	/pci@8700/pci@4/pci@0/pci@10/****@0	27

*1 If a USB3.0 device is used, it works as USB2.0.

Figure A-5   SPARC M12-2S Block Diagram
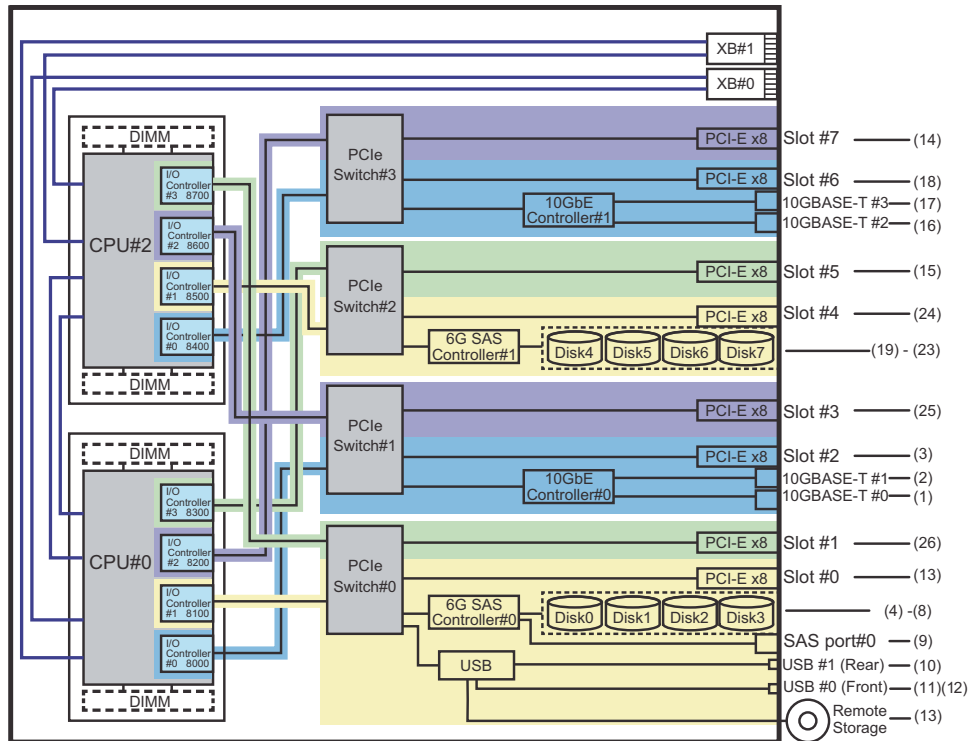
I/O Device Paths on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-9.

Table A-10   I/O Device Paths on the PCI Expansion Unit Side

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0

Instance Priority	Device	Device Path
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

I/O Device Paths of Logical System Boards

Device paths for LSB#1 to LSB#15 have the instance priority in ascending order of LSB# like LSB#0. The device nodes (/pci@vvvv in Table A-10) at the beginning become those shown in Table A-11. The other device nodes are the same as in Table A-10.
As an example, for LSB#1, interpret the node values in Table A-11 as shown below. Also interpret the node values for LSB#2 to LSB#15 in the same way.
/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00
/pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00, /pci@8700->/pci@8f00

Table A-11   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 2 CPUs)

LSB No.	Device Path
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ... /pci@8c00/… /pci@8d00/… /pci@8e00/… /pci@8f00/...
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ... /pci@9400/… /pci@9500/… /pci@9600/… /pci@9700/...

Table A-11   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 2 CPUs)
(continued)

LSB No.	Device Path
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ... /pci@9c00/… /pci@9d00/… /pci@9e00/… /pci@9f00/...
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ... /pci@a400/… /pci@a500/… /pci@a600/… /pci@a700/...
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ... /pci@ac00/… /pci@ad00/… /pci@ae00/… /pci@af00/...
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ... /pci@b400/… /pci@b500/… /pci@b600/… /pci@b700/...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ... /pci@bc00/… /pci@bd00/… /pci@be00/… /pci@bf00/...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ... /pci@c400/… /pci@c500/… /pci@c600/… /pci@c700/...

Table A-11   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 2 CPUs)
(continued)

LSB No.	Device Path
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ... /pci@cc00/… /pci@cd00/… /pci@ce00/… /pci@cf00/...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ... /pci@d400/… /pci@d500/… /pci@d600/… /pci@d700/...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ... /pci@dc00/… /pci@dd00/… /pci@de00/… /pci@df00/...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ... /pci@e400/… /pci@e500/… /pci@e600/… /pci@e700/...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/… /pci@eb00/… /pci@ec00/… /pci@ed00/… /pci@ee00/… /pci@ef00/...
LSB#14	/pci@f000/… /pci@f100/… /pci@f200/… /pci@f300/… /pci@f400/… /pci@f500/… /pci@f600/… /pci@f700/...

LSB No.	Device Path
LSB#15	/pci@f800/…
	/pci@f900/…
	/pci@fa00/…
	/pci@fb00/…
	/pci@fc00/…
	/pci@fd00/…
	/pci@fe00/…
	/pci@ff00/...

A.4   SPARC M10-1 Device Paths

Device paths which are recognized by the SPARC M10-1, and the hardware block diagram corresponding to device paths are as follows.

Table A-12   I/O Device Paths in the SPARC M10-1 Chassis and on the PCI Expansion Unit Side

Instance Priority	Device	Device Path	Number in Diagram
1	Internal SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-	Internal HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-	Internal HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	Internal HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	Internal HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	Internal HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	Internal HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	Internal HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	Internal HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	External SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@1/network@0	11
3	Internal LAN#1	/pci@8000/pci@4/pci@0/pci@1/network@0,1	12
4	Internal USB port (rear: USB 1.1)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4/****@1	13
5	Internal USB port (front: USB 1.1)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4/****@2	14
6	Internal USB port (rear: USB 2.0)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/****@1	13

Instance Priority	Device	Device Path	Number in Diagram
7	Internal USB port (front: USB 2.0)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/****@2	14
8	Remote storage	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3	15
9	PCI#0	/pci@8000/pci@4/pci@0/pci@8/****@0	16
	PCI expansion units under PCI#0		
10	PCI#1	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
11	PCI#2	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
12	PCI#3	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
13	PCI#4	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
14	PCI#5	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
15	PCI#6	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
16	PCI#7	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
17	PCI#8	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
18	PCI#9	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
19	PCI#10	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
20	PCI#11	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
21	Internal LAN#2	/pci@8100/pci@4/pci@0/pci@0/network@0	17
22	Internal LAN#3	/pci@8100/pci@4/pci@0/pci@0/network@0,1	18
23	PCI#1	/pci@8100/pci@4/pci@0/pci@1/****@0	19
	PCI expansion units under PCI#1		
24	PCI#1	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
25	PCI#2	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
26	PCI#3	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
27	PCI#4	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
28	PCI#5	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
29	PCI#6	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	

Table A-12   I/O Device Paths in the SPARC M10-1 Chassis and on the PCI Expansion Unit Side *(continued)*

Instance Priority	Device	Device Path	Number in Diagram
30	PCI#7	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
31	PCI#8	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
32	PCI#9	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
33	PCI#10	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
34	PCI#11	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
35	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
	PCI expansion units under PCI#2		
36	PCI#1	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
37	PCI#2	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
38	PCI#3	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
39	PCI#4	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
40	PCI#5	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
41	PCI#6	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
42	PCI#7	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
43	PCI#8	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
44	PCI#9	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
45	PCI#10	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
46	PCI#11	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
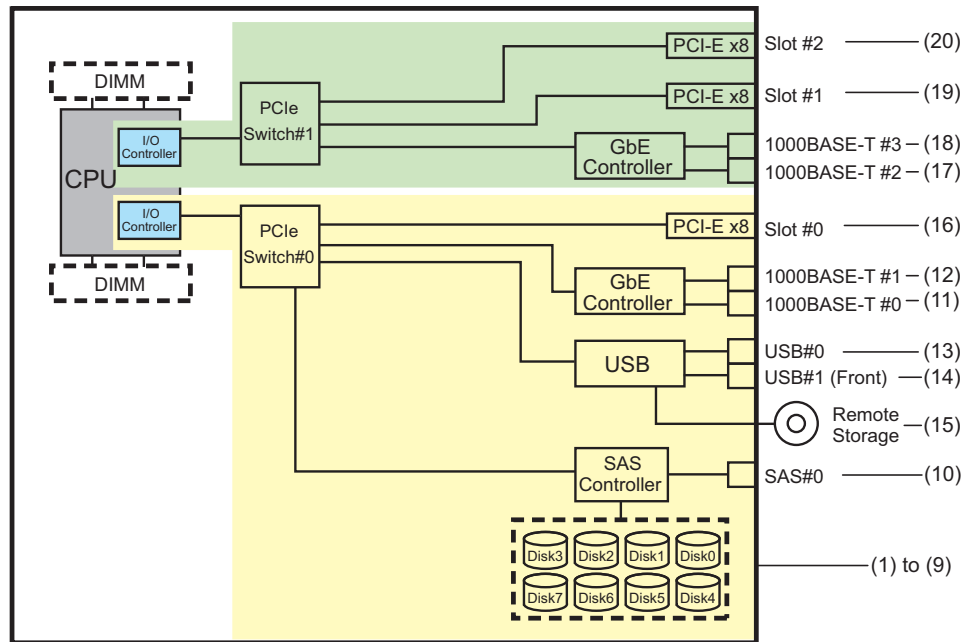
A.5   SPARC M10-4 Device Paths

Device paths which are recognized by the SPARC M10-4, and the hardware block diagram corresponding to device paths are as follows.

A.5.1   For a 2-CPU Configuration at the Initial Installation Time

Device paths for a 2-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

Note - If you disable I/O bus reconfiguration (ioreconfigure) by using the setpparmode command, the following device paths also apply to cases of addition that expand a 2-CPU configuration to a 4-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
If you enable I/O bus reconfiguration (ioreconfigure) and expand a 2-CPU configuration to a 4-CPU configuration, the device paths change to the 4-CPU configuration (Table A-16) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.
In addition, you may need to reinstall Oracle Solaris or set it again.
If you want to keep the logical domain configuration, disable I/O bus reconfiguration and

---

I/O Device Paths in the SPARC M10-4 Chassis

Table A-13   I/O Device Paths in the SPARC M10-4 Chassis (Initial Installation Time: 2 CPUs)

Instance Priority	Device		Device Path	Number in Diagram
1	LSB#0	Internal SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		Internal HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		Internal HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		Internal HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-		Internal HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-		Internal HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-		Internal HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-		Internal HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-		Internal HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-		External SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2		Internal USB port (rear: USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3		Internal USB port (rear: USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4		Internal USB port (front: USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5		Remote storage	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6		Internal LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7		Internal LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8		Internal LAN#2	/pci@8000/pci@4/pci@0/pci@a/network@0	16

Instance Priority	Device	Device Path	Number in Diagram
9	Internal LAN#3	/pci@8000/pci@4/pci@0/pci@a/network@0,1	17
10	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	18
11	PCI#1	/pci@8100/pci@4/pci@0/pci@8/****@0	19
12	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
13	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	21
14	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	22
15	PCI#5	/pci@8200/pci@4/pci@0/pci@9/****@0	23
16	PCI#6	/pci@8200/pci@4/pci@0/pci@11/****@0	24
17	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	25
18	PCI#8	/pci@8300/pci@4/pci@0/pci@8/****@0	26
19	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	27
20	PCI#10	/pci@8300/pci@4/pci@0/pci@11/****@0	28

Figure A-7   SPARC M10-4 Block Diagram (2 CPUs)
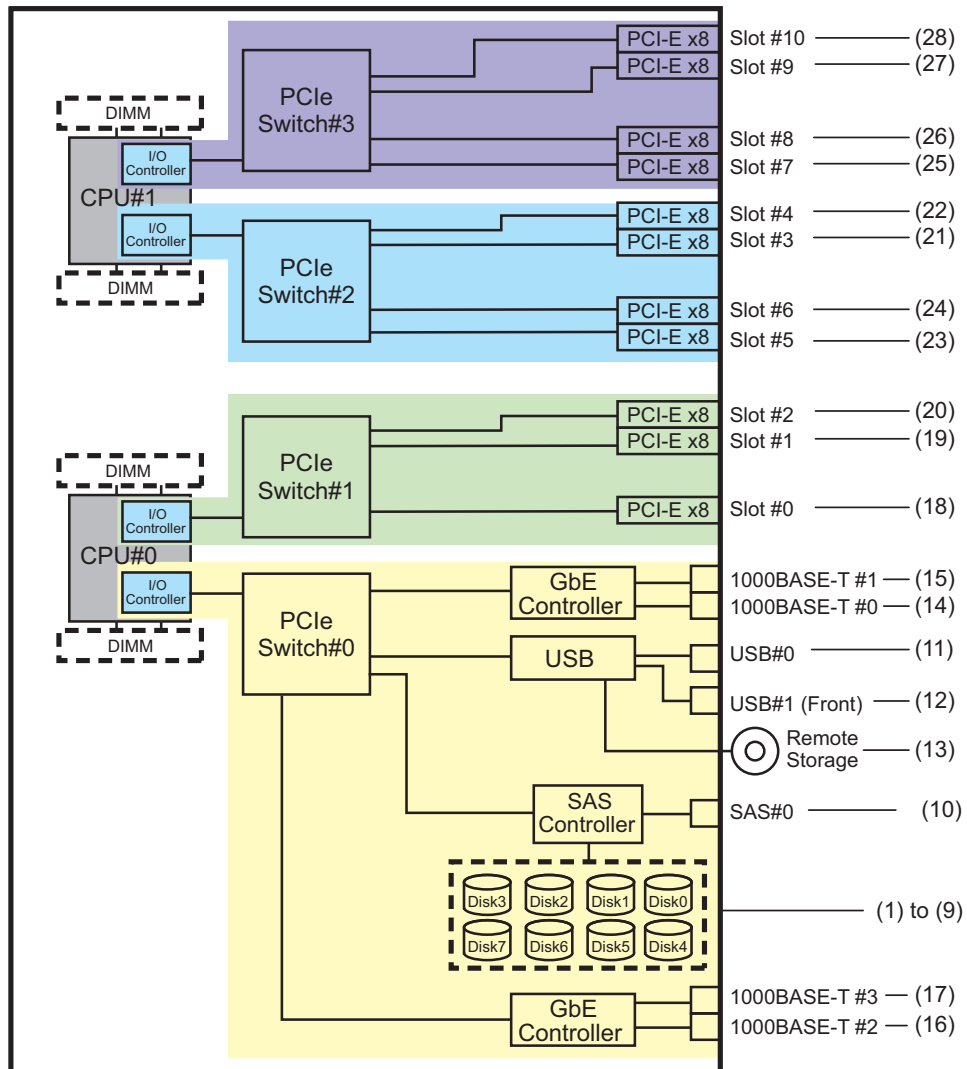
I/O Device Paths on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-13.

Table A-14   I/O Device Paths on the PCI Expansion Unit Side (Initial Installation Time: 2 CPUs)

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0

Instance Priority	Device	Device Path
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.5.2   For a 4-CPU Configuration at the Initial Installation Time

Device paths for a 4-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

Note - If you disable I/O bus reconfiguration (ioreconfigure) by using the setpparmode command, the following device paths also apply to cases of removal that reduce a 4-CPU configuration to a 2-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
If you enable I/O bus reconfiguration (ioreconfigure) and reduce a 4-CPU configuration to a 2-CPU configuration, the device paths change to the 2-CPU configuration (Table A-13) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.
In addition, you may need to reinstall Oracle Solaris or set it again.
If you want to keep the logical domain configuration, disable I/O bus reconfiguration and reduce the configuration.

I/O Devices in the SPARC M10-4 Chassis

Table A-15   I/O Devices in the SPARC M10-4 Chassis (Initial Installation Time: 4 CPUs)

Instance Priority	Device		Device Path	Number in Diagram
1	LSB#0	Internal SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		Internal HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2

Table A-15   I/O Devices in the SPARC M10-4 Chassis (Initial Installation Time: 4 CPUs) *(continued)*

Instance Priority	Device	Device Path	Number in Diagram
-	Internal HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	Internal HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	Internal HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	Internal HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	Internal HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	Internal HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	Internal HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	External SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	Internal USB port (rear: USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	Internal USB port (rear: USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	Internal USB port (front: USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	Remote storage	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	Internal LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	16
9	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	17
10	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	18
11	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	19
12	PCI#8	/pci@8300/pci@4/pci@0/pci@8/****@0	20
13	Internal LAN#2	/pci@8400/pci@4/pci@0/pci@a/network@0	21
14	Internal LAN#3	/pci@8400/pci@4/pci@0/pci@a/network@0,1	22

Instance Priority	Device	Device Path	Number in Diagram
15	PCI#1	/pci@8500/pci@4/pci@0/pci@8/****@0	23
16	PCI#2	/pci@8500/pci@4/pci@0/pci@9/****@0	24
17	PCI#5	/pci@8600/pci@4/pci@0/pci@9/****@0	25
18	PCI#6	/pci@8600/pci@4/pci@0/pci@11/****@0	26
19	PCI#9	/pci@8700/pci@4/pci@0/pci@9/****@0	27
20	PCI#10	/pci@8700/pci@4/pci@0/pci@11/****@0	28

Figure A-8   SPARC M10-4 Block Diagram (4 CPUs)
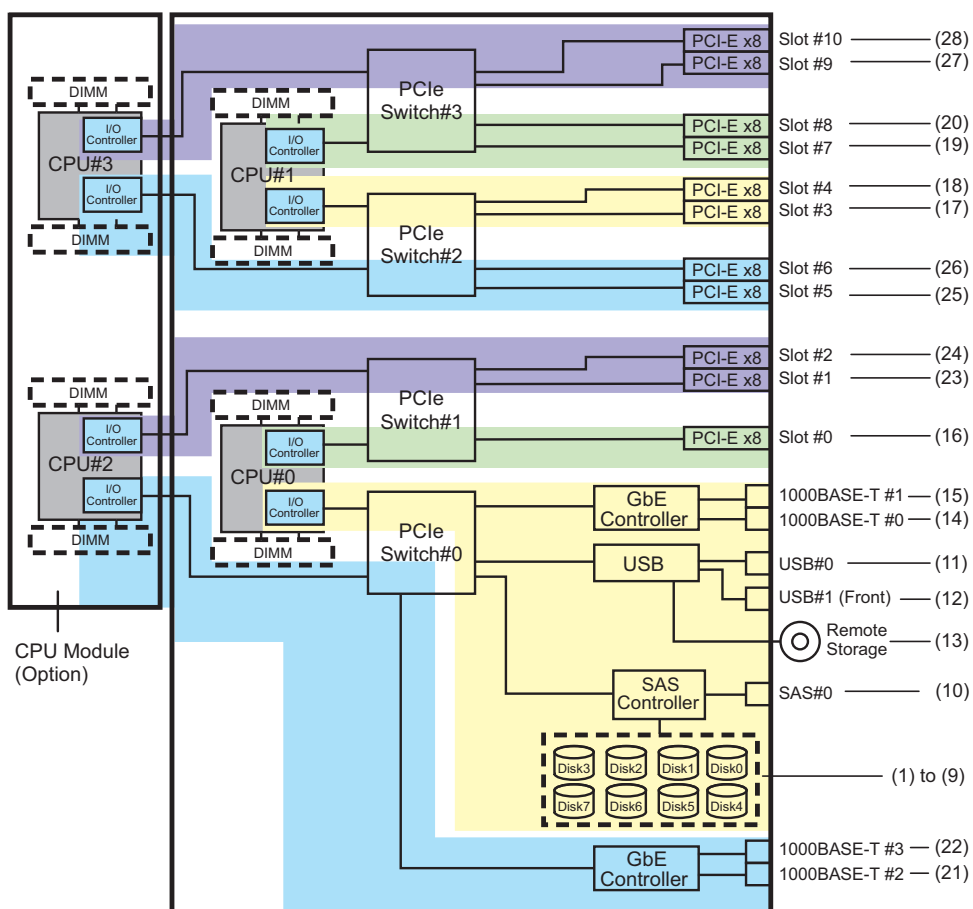
I/O Devices on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X,

the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-15.

Table A-16   I/O Device Paths on the PCI Expansion Unit Side (Initial Installation Time: 4 CPUs)

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.6   SPARC M10-4S Device Paths

Device paths which are recognized by the SPARC M10-4S, and the hardware block diagram corresponding to device paths are as follows.

A.6.1   For a 2-CPU Configuration at the Initial Installation Time

Device paths for a 2-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

Note - If you set the I/O bus reconfiguration (ioreconfigure) to the disabled status (default) by using the setpparmode command, the following device paths also apply to cases of installation that expand a 2-CPU configuration to a 4-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
If you enable I/O bus reconfiguration (ioreconfigure) and expand a 2-CPU configuration to a 4-CPU configuration, the device paths change to the 4-CPU configuration (Table A-20) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.
In addition, you may need to reinstall Oracle Solaris or set it again.

If you want to keep the logical domain configuration, disable I/O bus reconfiguration and expand the configuration.

I/O Device Paths in the SPARC M10-4S Chassis

Table A-17   I/O Device Paths in the SPARC M10-4S Chassis (Initial Installation Time: 2 CPUs)

Instance Priority	Device		Device Path	Number in Diagram
1	LSB#0	Internal SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		Internal HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		Internal HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		Internal HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-		Internal HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-		Internal HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-		Internal HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-		Internal HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-		Internal HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-		External SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2		Internal USB port (rear: USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3		Internal USB port (rear: USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4		Internal USB port (front: USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5		Remote storage	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6		Internal LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7		Internal LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15

Instance Priority	Device	Device Path	Number in Diagram
8	Internal LAN#2	/pci@8000/pci@4/pci@0/pci@a/network@0	16
9	Internal LAN#3	/pci@8000/pci@4/pci@0/pci@a/network@0,1	17
10	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	18
11	PCI#1	/pci@8100/pci@4/pci@0/pci@8/****@0	19
12	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
13	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	21
14	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	22
15	PCI#5	/pci@8200/pci@4/pci@0/pci@9/****@0	23
16	PCI#6	/pci@8200/pci@4/pci@0/pci@11/****@0	24
17	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	25

Table A-17   I/O Device Paths in the SPARC M10-4S Chassis (Initial Installation Time: 2 CPUs) *(continued)*

Figure A-9   SPARC M10-4S Block Diagram (2 CPUs)
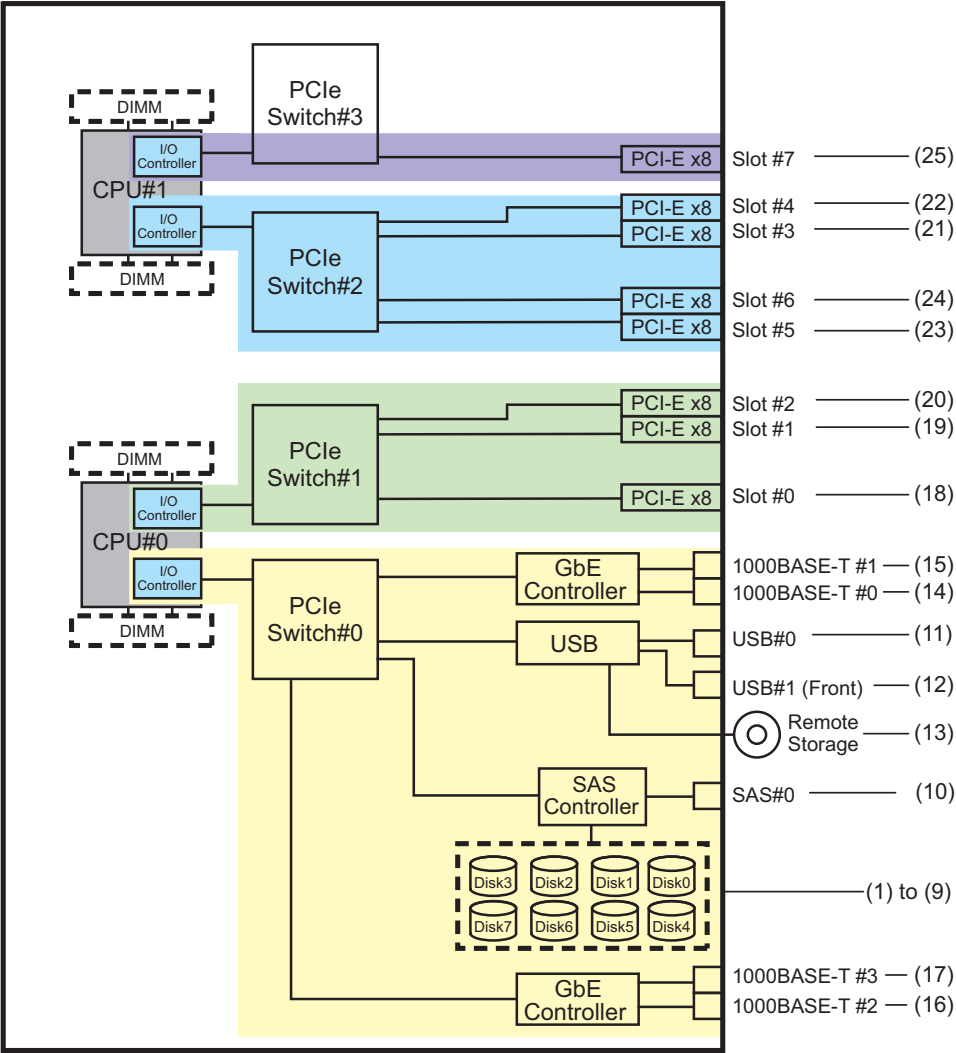
I/O Device Paths on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-17.

Table A-18   I/O Device Paths on the PCI Expansion Unit Side (Initial Installation Time: 2 CPUs)

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0

Instance Priority	Device	Device Path
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

I/O Device Paths of Logical System Boards

Device paths for LSB#1 to LSB#15 have the instance priority in ascending order of LSB# like LSB#0. The device nodes (Table A-18/pci@vvvv) at the beginning become those shown in Table A-19. The other device nodes are the same as in Table A-18. As an example, for LSB#1, interpret the node values in Table A-19 as shown below. Also interpret the node values for LSB#2 to LSB#15 in the same way.
/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00, /pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00, /pci@8700->/pci@8f00

Table A-19   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 2 CPUs)

LSB No.	Device Path
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ...
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ...
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ...
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ...

Table A-19   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 2 CPUs)
(continued)

LSB No.	Device Path
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ...
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/… /pci@eb00/…
LSB#14	/pci@f000/… /pci@f100/… /pci@f200/… /pci@f300/…
LSB#15	/pci@f800/… /pci@f900/… /pci@fa00/… /pci@fb00/…

A.6.2 For a 4-CPU Configuration at the Initial Installation Time

Device paths for a 4-CPU configuration at initial installation and the hardware block diagram corresponding to device paths are as follows.

> **Note -** If you disable I/O bus reconfiguration (ioreconfigure) by using the setpparmode command, the following device paths also apply to cases of removal that reduce a 4-CPU configuration to a 2-CPU configuration. In this case, you do not need to reconfigure the logical domains, reinstall Oracle Solaris, and set it again.
>
> If you enable I/O bus reconfiguration (ioreconfigure) and reduce a 4-CPU configuration to a 2-CPU configuration, the device paths change to the 2-CPU configuration (Table A-17) at the time of PPAR reset. At this time, the system changes to the factory-default configuration. In this case, the logical domains need to be reconfigured.
>
> In addition, you may need to reinstall Oracle Solaris or set it again.
>
> If you want to keep the logical domain configuration, disable I/O bus reconfiguration and reduce the configuration.

I/O Devices in the SPARC M10-4S Chassis

Table A-20   I/O Devices in the SPARC M10-4S Chassis (Initial Installation Time: 4 CPUs)

Instance Priority	Device		Device Path	Number in Diagram
1	LSB#0	Internal SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		Internal HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		Internal HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		Internal HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-		Internal HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-		Internal HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-		Internal HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-		Internal HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-		Internal HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-		External SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10

Instance Priority	Device	Device Path	Number in Diagram
2	Internal USB port (rear: USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	Internal USB port (rear: USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	Internal USB port (front: USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	Remote storage	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	Internal LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	Internal LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	16
9	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	17
10	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	18
11	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	19
12	Internal LAN#2	/pci@8400/pci@4/pci@0/pci@a/network@0	20
13	Internal LAN#3	/pci@8400/pci@4/pci@0/pci@a/network@0,1	21
14	PCI#1	/pci@8500/pci@4/pci@0/pci@8/****@0	22
15	PCI#2	/pci@8500/pci@4/pci@0/pci@9/****@0	23
16	PCI#5	/pci@8600/pci@4/pci@0/pci@9/****@0	24
17	PCI#6	/pci@8600/pci@4/pci@0/pci@11/****@0	25

Figure A-10　SPARC M10-4S Block Diagram (4 CPUs)
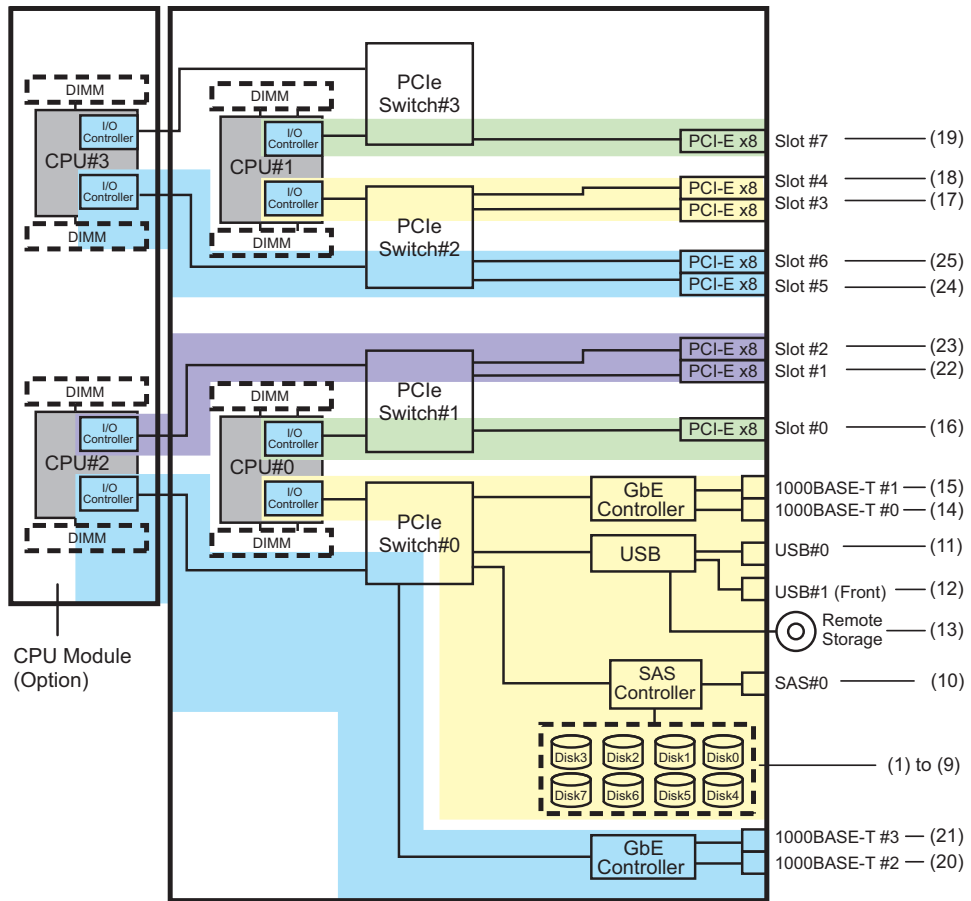
I/O Devices on the PCI Expansion Unit Side

If the server PCI slot having a link card connected to the PCI expansion unit is PCI#X, the following device paths are created with the corresponding vvvv and u shown in the PCI#X device path /pci@vvvv/pci@4/pci@0/pci@u/****@0 in Table A-20.

Table A-21　I/O Device Paths on the PCI Expansion Unit Side (Initial Installation Time: 4 CPUs)

Instance Priority	Device	Device Path
		PCI expansion units under PCI#X
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0

Table A-21   I/O Device Paths on the PCI Expansion Unit Side (Initial Installation Time: 4 CPUs) *(continued)*

Instance Priority	Device	Device Path
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

I/O Devices of Logical System Boards

For the I/O device paths of LSB#1 to LSB#15, the device nodes (/pci@vvvv) at the beginning of the I/O device paths in Table A-20 become those shown in Table A-22. The other device nodes are the same as in Table A-20.
As an example, for LSB#1, interpret the node values in Table A-20 as shown below. Also interpret the node values for LSB#2 to LSB#15 in the same way.
/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00
/pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00

Table A-22   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 4 CPUs)

LSB No.	Device Path
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ... /pci@8c00/… /pci@8d00/… /pci@8e00/…
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ... /pci@9400/… /pci@9500/… /pci@9600/…
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ... /pci@9c00/… /pci@9d00/… /pci@9e00/…

Table A-22   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 4 CPUs)
(continued)

LSB No.	Device Path
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ... /pci@a400/… /pci@a500/… /pci@a600/…
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ... /pci@ac00/… /pci@ad00/… /pci@ae00/…
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ... /pci@b400/… /pci@b500/… /pci@b600/…
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ... /pci@bc00/… /pci@bd00/… /pci@be00/…
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ... /pci@c400/… /pci@c500/… /pci@c600/…
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ... /pci@cc00/… /pci@cd00/… /pci@ce00/…

Table A-22   I/O Device Paths of LSB#1 to LSB#15 (Initial Installation Time: 4 CPUs)
(continued)

LSB No.	Device Path
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ... /pci@d400/… /pci@d500/… /pci@d600/…
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ... /pci@dc00/… /pci@dd00/… /pci@de00/…
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ... /pci@e400/… /pci@e500/… /pci@e600/…
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/… /pci@eb00/… /pci@ec00/… /pci@ed00/… /pci@ee00/…
LSB#14	/pci@f000/… /pci@f100/… /pci@f200/… /pci@f300/… /pci@f400/… /pci@f500/… /pci@f600/…
LSB#15	/pci@f800/… /pci@f900/… /pci@fa00/… /pci@fb00/… /pci@fc00/… /pci@fd00/… /pci@fe00/…

Appendix B

Identifying an SAS2 Device Based on a WWN

This appendix describes how to identify an SAS2 device based on a WWN value.

- World Wide Name (WWN) Syntax
- Overview of probe-scsi-all Command Output
- Identifying a Disk Slot by Using the probe-scsi-all Command
- Identifying Disk Slot

B.1   World Wide Name (WWN) Syntax

Oracle Solaris now uses the World Wide Name (WWN) syntax for logical device names. This section describes how to map a WWN-based device name to a given SCSI device.

As an example, a boot device is used to show the difference in notation between the former device names (tn; target ID) and WWN-based device names.

Table B-1   Difference in Notation Between Device Names

Boot Device Name Using WWN Value	Former Boot Device Name (Using Target ID)
c#t*WWN*d# A WWN is a globally unique hexadecimal number for this device. The manufacturer assigns the number to the device.	c0t0d0

WWN values do not conform to the structure of the former logical device names, so a target device cannot be directly identified from a c#tWWNd# value.

To map a WWN-based device name to a given physical device, use the probe-scsi-all command of OpenBoot PROM. For details, see "B.3   Identifying a Disk Slot by Using the probe-scsi-all Command."

B.2　Overview of probe-scsi-all Command Output

The output of the probe-scsi-all command of OpenBoot PROM displays a list of all SCSI devices in the system and basic information on each device. The following table lists the displayed items.

Table B-2　probe-scsi-all Command Configuration

Entity Name	Description
Target	Unique target ID assigned to each SAS device
SASDeviceName	WWN value assigned to an SAS device by the manufacturer. Oracle Solaris recognizes it.
SASAddress	WWN value recognized by the OpenBoot PROM firmware and assigned to a SCSI device
PhyNum	Hexadecimal number ID of the controller port connected to the target drive
VolumeDeviceName (when configuring a RAID volume)	WWN value recognized by Oracle Solaris and assigned to a RAID volume. It replaces the SASDeviceName of each SCSI device included in the RAID volume.
VolumeWWID (when a configuring a RAID volume)	WWN-based value recognized by the OpenBoot PROM firmware and assigned to a RAID volume. It replaces the SASAddress of each SCSI device included in the RAID volume.

B.3　Identifying a Disk Slot by Using the probe-scsi-all Command

This section describes how to identify a disk slot by using the probe-scsi-all command of OpenBoot PROM.
In this way, you can associate the disk slot with the corresponding WWN value.

B.3.1 Example of Identifying a Disk Slot by Using the probe-scsi-all Command (SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S)

This section describes the correspondence between PhyNum, which is connected to the on-board SAS controller, and disk slots.

In the SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S, the SAS controller is connected to the HDD backplane. The following table shows the mapping between PhyNum of the HDD backplane and disk slots.

Table B-3   Mapping of PhyNum and Disk Slots (SPARC M12-1/M10-1/M10-4/M10-4S)

PhyNum	Disk Slot
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table B-4   Mapping of PhyNum and Disk Slots (SPARC M12-2/M12-2S)

PhyNum	SAS Controller Number	Disk Slot
0	0	0
1		1
2		2
3		3
4	1	4
5		5
6		6
7		7

Note - For the physical locations of disk slots in the SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S, see "Maintaining the Internal Storage" in the *Service Manual* for your server.

Example of probe-scsi-all Command Output

The procedure for identifying a disk slot is described below, in a case where eight internal disk drives are mounted in the SPARC M12-2S/M10-1.

1. **Execute the probe-scsi-all command.**
   In the following example of the SPARC M10-1, the PhyNum of the internal disk drive mounted in disk slot 0 is 0. The internal disk drive is assigned to Target a, and the SASDeviceName value is 50000393c813ae74.

Example of SPARC M10-1

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0  <---- SAS controller

FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.57.00

Target a
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393c813ae74  SASAddress 50000393c813ae76  PhyNum 0
Target b
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b24ec  SASAddress 50000393b81b24ee  PhyNum 1
Target c
   Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81af47c  SASAddress 50000393b81af47e  PhyNum 2
Target d
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81af3c0  SASAddress 50000393b81af3c2  PhyNum 3
Target e
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b0f58  SASAddress 50000393b81b0f5a  PhyNum 4
Target f
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b130c  SASAddress 50000393b81b130e  PhyNum 5
Target 10
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b2420  SASAddress 50000393b81b2422  PhyNum 6
Target 11
  Unit 0   Disk   TOSHIBA  MBF2300RC      3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81acc84  SASAddress 50000393b81acc86  PhyNum 7
Target 12
  Unit 0   Encl Serv device   FUJITSU  NBBEXP         0d32
    SASAddress 500000e0e04d003d  PhyNum 14
{0} ok
```

Example of SPARC M12-2S

```
{0} ok probe-scsi-all
/pci@8500/pci@4/pci@0/pci@0/scsi@0   <---- SAS controller 1
```

```
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 20.00.06.00

Target a
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039678332cc5  SASAddress 5000039678332cc6  PhyNum 4
Target b
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039678332ca9  SASAddress 5000039678332caa  PhyNum 5
Target c
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039678332c59  SASAddress 5000039678332c5a  PhyNum 6
Target d
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039678332c55  SASAddress 5000039678332c56  PhyNum 7
Target e
  Unit 0   Encl Serv device   FUJITSU  BBEXP          0d32
  SASAddress 500000e0e0b0103d  PhyNum 14

/pci@8100/pci@4/pci@0/pci@0/scsi@0   <---- SAS controller 0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 20.00.06.00

Target a
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039698002565  SASAddress 5000039698002566  PhyNum 0
Target b
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 50000396980024b9  SASAddress 50000396980024ba  PhyNum 1
Target c
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039698002495  SASAddress 5000039698002496  PhyNum 2
Target d
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
  SASDeviceName 5000039678332cd1  SASAddress 5000039678332cd2  PhyNum 3
Target e
  Unit 0   Encl Serv device   FUJITSU  BBEXP          0d32
  SASAddress 500000e0e0b0103d  PhyNum 14
```

Note - The above method can also identify a disk slot in the SPARC M12-1/M12-2/M10-4/ M10-4S.

B.4   Identifying Disk Slot

To perform active replacement of internal storage, you need to know the physical device name or the logical device name of the device to be installed or removed. If a disk error occurs in the system, normally, you can check the message related to the disk which is likely to fail or which has already failed. This information is also recorded in the /var/adm/messages file.

This message normally describes the faulty internal disk with its physical device name or logical device name. Also, the slot number of the disk may be reported depending on the application.

The procedures for checking the installation location information of the HDD varies depending on the Oracle Solaris version.
- **In the case of Oracle Solaris 11**
  For details, see "B.4.1   Using the format Command (Oracle Solaris 11)" or "B.4.2 Using the diskinfo Command (Oracle Solaris 11)."
- **In the case of Oracle Solaris 10**
  For details, see "B.4.3   Using the diskinfo Command (Oracle Solaris 10)."

B.4.1   Using the format Command (Oracle Solaris 11)

1. **Execute the showhardconf command, and check the serial number of CMUL of the chassis whose installation location information is displayed.**

```
XSCF> showhardconf
SPARC M10-4S;
    + Serial:2081238017; Operator_Panel_Switch:Service;
    + System_Power:Off; System_Phase:Cabinet Power Off;
    Partition#0 PPAR_Status:Powered Off;
    Partition#1 PPAR_Status:Powered Off;
    BB#00 Status:Normal; Role:Master; Ver:2044h; Serial:2081238017;
        + FRU-Part-Number:CA07361-D202 A1                        ;
        + Power_Supply_System: ;
        + Memory_Size:256 GB;
        CMUL Status:Normal; Ver:0101h; Serial:PP123001Y1  ;
                                            * BB#00 CMUL serial number
            + FRU-Part-Number:CA07361-D941 C3   /7060911            ;
            + Memory_Size:128 GB;
            CPU#0 Status:Normal; Ver:4142h; Serial:00321144;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
            CPU#1 Status:Normal; Ver:4142h; Serial:00322957;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
-----------------------Omitted-----------------------
    BB#01 Status:Normal; Role:Standby; Ver:2044h; Serial:2081230011;
        + FRU-Part-Number:CA07361-D202 A1                        ;
        + Power_Supply_System: ;
        + Memory_Size:256 GB;
        CMUL Status:Normal; Ver:0101h; Serial:PP123203N0  ;
                                            * BB#01 CMUL serial number
            + FRU-Part-Number:CA07361-D941 C3   /7060911            ;
            + Memory_Size:128 GB;
            CPU#0 Status:Normal; Ver:4142h; Serial:00320804;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
            CPU#1 Status:Normal; Ver:4142h; Serial:00321030;
                + Freq:3.000 GHz; Type:0x10;
```

```
                         + Core:16; Strand:2;
             MEM#00A Status:Normal;
                 + Code:2c800118KSF1G72PZ-1G6E1 4531-1A94229F;
                 + Type:04; Size:8 GB;
----------------------Omitted----------------------
```

2. **Execute the format command, and check the physical disk slot.**

   In the examples that follow, (1) to (5) indicate the following:

   (1): Logical path name of the disk

   (2): The disk is installed in the HDD00 slot of BB#01

   (3): The disk is installed in the HDD01 slot of BB#01

   (4): The disk is installed in the HDD00 slot of BB#00

   (5): The disk is installed in the HDD01 slot of BB#00

```
# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
    0. c2t50000394281B5312d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
 668> <-- (1)
        /pci@8800/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b5312,0
        /dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD00/disk <-- (2)
                                              * Last 4 digits of the
BB#1_CMUL serial number
                                                    * HDD00
    1. c2t50000394281B59D6d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
 668> <-- (1)
        /pci@8800/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b59d6,0
        /dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD01/disk <-- (3)
                                                    * HDD01
    2. c0t500003942823C8C6d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
 668> <-- (1)
        /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w500003942823c8c6,0
        /dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD00/disk <-- (4)
                                              * Last 4 digits of the
BB#0_CMUL serial number
                                                    * HDD00
    3. c0t50000394281B517Ad0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
 668> <-- (1)
        /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b517a,0
        /dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD01/disk <-- (5)
                                                    * HDD01
Specify disk (enter its number):
```

B.4.2   Using the diskinfo Command (Oracle Solaris 11)

1. **Execute the showhardconf command, and check the serial number of CMUL of the chassis whose installation location information is displayed.**

```
XSCF> showhardconf
SPARC M10-4S;
    + Serial:2081238017; Operator_Panel_Switch:Service;
    + System_Power:Off; System_Phase:Cabinet Power Off;
    Partition#0 PPAR_Status:Powered Off;
    Partition#1 PPAR_Status:Powered Off;
    BB#00 Status:Normal; Role:Master; Ver:2044h; Serial:2081238017;
        + FRU-Part-Number:CA07361-D202 A1                        ;
        + Power_Supply_System: ;
        + Memory_Size:256 GB;
        CMUL Status:Normal; Ver:0101h; Serial:PP123001Y1  ;
                                            * BB#00 CMUL serial number
            + FRU-Part-Number:CA07361-D941 C3   /7060911             ;
            + Memory_Size:128 GB;
            CPU#0 Status:Normal; Ver:4142h; Serial:00321144;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
            CPU#1 Status:Normal; Ver:4142h; Serial:00322957;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
-----------------------Omitted-----------------------
    BB#01 Status:Normal; Role:Standby; Ver:2044h; Serial:2081230011;
        + FRU-Part-Number:CA07361-D202 A1                        ;
        + Power_Supply_System: ;
        + Memory_Size:256 GB;
        CMUL Status:Normal; Ver:0101h; Serial:PP123203N0  ;
                                            * BB#01 CMUL serial number
            + FRU-Part-Number:CA07361-D941 C3   /7060911             ;
            + Memory_Size:128 GB;
            CPU#0 Status:Normal; Ver:4142h; Serial:00320804;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
            CPU#1 Status:Normal; Ver:4142h; Serial:00321030;
                + Freq:3.000 GHz; Type:0x10;
                + Core:16; Strand:2;
            MEM#00A Status:Normal;
                + Code:2c800118KSF1G72PZ-1G6E1 4531-1A94229F;
                + Type:04; Size:8 GB;
-----------------------Omitted-----------------------
```

2. **Execute the diskinfo command, and check the physical disk slot.**

   In the examples that follow, (1) to (4) indicate the following:

   (1): The device name and logical path name of the disk installed in HDD 0 of BB#01

   (2): The device name and logical path name of the disk installed in HDD 1 of BB#01

   (3): The device name and logical path name of the disk installed in HDD 0 of BB#00

   (4): The device name and logical path name of the disk installed in HDD 1 of BB#00

```
# diskinfo
D:devchassis-path                                                c:occupant-compdev
---------------------------------------------------------------- ------------------
/dev/chassis/SYS/BB0/CMUL/HDD0                                    -
/dev/chassis/SYS/BB0/CMUL/HDD1                                    -
/dev/chassis/SYS/BB0/CMUL/HDD2                                    -
/dev/chassis/SYS/BB0/CMUL/HDD3                                    -
/dev/chassis/SYS/BB0/CMUL/HDD4                                    -
/dev/chassis/SYS/BB0/CMUL/HDD5                                    -
/dev/chassis/SYS/BB0/CMUL/HDD6                                    -
/dev/chassis/SYS/BB0/CMUL/HDD7                                    -
/dev/chassis/SYS/BB1/CMUL/HDD0                                    -
/dev/chassis/SYS/BB1/CMUL/HDD1                                    -
/dev/chassis/SYS/BB1/CMUL/HDD2                                    -
/dev/chassis/SYS/BB1/CMUL/HDD3                                    -
/dev/chassis/SYS/BB1/CMUL/HDD4                                    -
/dev/chassis/SYS/BB1/CMUL/HDD5                                    -
/dev/chassis/SYS/BB1/CMUL/HDD6                                    -
/dev/chassis/SYS/BB1/CMUL/HDD7                                    -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD00/disk
c4t50000394281B5312d0 <-- (1)
                                * Last 4 digits of the BB#01_CMUL serial number
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD01/disk
c4t50000394281B59D6d0 <-- (2)
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD02          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD03          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD04          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD05          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD06          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD07          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD00/disk
c2t500003942823C8C6d0 <-- (3)
                                * Last 4 digits of the BB#00_CMUL serial number
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD01/disk
c2t50000394281B517Ad0 <-- (4)
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD02          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD03          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD04          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD05          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD06          -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD07          -
```

B.4.3   Using the diskinfo Command (Oracle Solaris 10)

1. **Execute the diskinfo command, and check the physical disk slot and the logical system board.**
   In the examples that follow, (1) to (4) indicate the following:

   (1): The logical path name of the disk installed in HDD 0.

   (2): The device path of the disk installed in HDD 0 of LSB#00

   (3): The logical path name of the disk installed in HDD 1.

(4): The device path of the disk installed in HDD 1 of LSB#00

```
# diskinfo -ap

Enclosure path:         2081210007-physical-hba-0
Chassis Serial Number:  2081210007-physical-hba-0
Chassis Model:          ORCL,SPARC64-X

Enclosure path:         /dev/es/ses0
Chassis Serial Number:  500000e0e06d233f
Chassis Model:          FUJITSU-BBEXP

Label    Disk name                Vendor    Product        Vers
-------- ---------------------    -------- -------------- ----
HDD_0    c0t50000393D8289180d0    TOSHIBA  MBF2600RC       3706 <--  (1)
  Physical path
  -------------------------------
  0: /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000393D8289180,0<--(2)
      * LSB#0
HDD_1    c0t50000393D82891D0d0    TOSHIBA  MBF2600RC       3706 <--  (3)
  Physical path
  -------------------------------
  0: /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000393D82891D0,0<--(4)
      * LSB#0
```

The device path notation format of a disk displayed by the diskinfo command is as follows.

<SAS controller device path>/iport@f/disk@wXXXXXXXX,Y:Z

The device path varies depending on the model or system configuration. For details, see "Appendix A   Lists of SPARC M12/M10 System Device Paths."

Appendix C

List of the XSCF Web Pages

This appendix provides an overview of each page of XSCF Web.
For details on how to log in to and log out from XSCF Web, see "Chapter 2   Logging In/Out of the XSCF."

- Overview of the Pages
- Understanding the Menu Configuration
- Available Pages

C.1   Overview of the Pages

Figure C-1 shows the XSCF Web console window displayed after login.

Figure C-1   XSCF Web Console Window
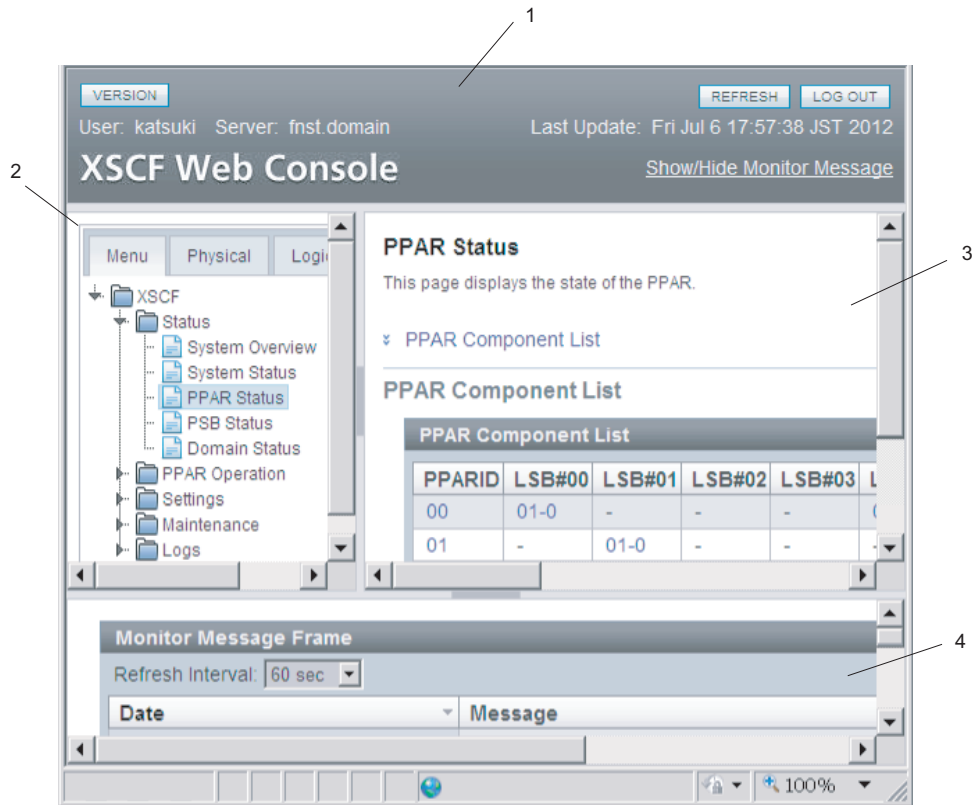
1	Masthead frame
2	Menu frame (tree frame)
3	Main frame
4	Event frame

The XSCF Web console displayed after login consists of four frames. Selecting the necessary item from a menu in the left frame displays information about it in the right frame. Users can thus operate/manage the server.

Table C-1 lists the types of XSCF Web console frames and provides an overview of each frame.

Table C-1   Overviews of Frames

Frame Type	Overview
Masthead frame	Page at the top of the window (1 in Figure C-1). The frame displays the user account name specified at the login time, name of the connected host, and other information. When logging out from this frame, the user is returned to the login page.
Menu frame (tree frame)	Page on the left side of the window (2 in Figure C-1). With a menu item selected there, the main frame on the right can display the relevant information. There are three menu bars. Each menu appears in the form of a tree. - Menu: Displays a menu for various settings, operations, and status display. - Physical: Displays the physical component configuration of the system. - Logical: Displays the logical component configuration for each physical partition.
Main frame	Page on the right side of the window (3 in Figure C-1). Selecting an item from a menu in the tree frame displays the corresponding page.
Event frame (monitoring message frame)	Page at the bottom of the window (4 in Figure C-1). Events in the whole system are displayed in the form of monitoring messages. The frame is regularly refreshed. The interval value can be changed in the same frame. The default value for the refresh interval is 60 seconds.

Table C-2 lists the functions and provides overviews of the main pages displayed by the XSCF Web console.

Table C-2   Overviews of the Main Pages

Page Function	Overview
Login page	This is the XSCF Web console login page. Log in with an XSCF user account from the login page.
Displaying the server status	This page displays the status of the whole system, physical partitions, and logical domains. This includes the status of the PCI expansion unit. From the [Menu] bar, select [Status].
Operating a physical partition	This page is used to operate a physical partition and logical domains. The operations include power operations of the physical partition and system board (PSB) configuration management. From the [Menu] bar, select [PPAR Operation].
Configuring the server	Various settings are made from this page to use the whole system and the XSCF. From the [Menu] bar, select [Settings].

Table C-2	Overviews of the Main Pages *(continued)*
Page Function	**Overview**
Maintaining the server	The operations of this page include saving/restoring data, firmware update, XSCF reboot, XSCF switching, the remote maintenance service, and saving logs. From the [Menu] bar, select [Maintenance].
Displaying a log	The displayed logs include the error log, power log, event log, and console log. From the [Menu] bar, select [Logs].
Standby-side page	This page appears after login to the standby XSCF. It can switch the XSCF, save logs, etc.

C.2 Understanding the Menu Configuration

This section describes the menu configuration.

The configuration when the [Menu] bar is selected in the menu frame is shown below.

```
Menu
+ XSCF
  + Status
    - System Overview
    - System Status
    - PPAR Status
    - PSB Status
    - Domain Status
  + PPAR Operation
    - PPAR Power
    - PPAR Mode Configuration
    - PPAR Configuration
    - PSB Configuration
    - Domain Configuration
    - PPAR Parameter
    - Verified Boot
  + Settings
    + Network
      - Current
      - Reserve
    + Service
      - Service State
      - HTTPS
      - SSH
      - Telnet
      - NTP
      - SMTP
```

```
            - SNMP
            - SNMP Security
        + User Manager
            - Account
            - LDAP
            - LDAP/SSL
            - Active Directory
        - Autologout
        - CoD Reservation
        - CoD Activation
        - Audit
        - Email Reporting
        - Time
        - Power Capping
        - Power Schedule
        - Add-In Card Manager
        - PCIBOX DIO
        - Remote Storage
    + Maintenance
        + Network Tools
            - Ping
            - Traceroute
            - Nslookup
        - Configuration Management
        - Firmware Update
        - Reboot XSCF
        - Switch Over
        - Snapshot
        - ASR
    + Logs
        - Error Log
        - Power Log
        - Event Log
        - Console Log
        - Panic Log
        - Environment Log
        - IPL Message Log
        - Monitor Message Log
        - Audit Log
```

Note - Each menu item is subject to change for functional improvement or other reasons.
Also, the menu may differ depending on the model and conditions.

Selecting a menu item displays the corresponding page in the main frame.

In the systems with multiple XSCFs, the [Switch Over] menu item is available,
enabling XSCF switching. For an overview of the page targeted by each menu item,
see "C.3   Available Pages."

Figure C-2 shows a screen example where the [Physical] bar is selected in the menu

frame.

Figure C-2　　Physical Component Tree
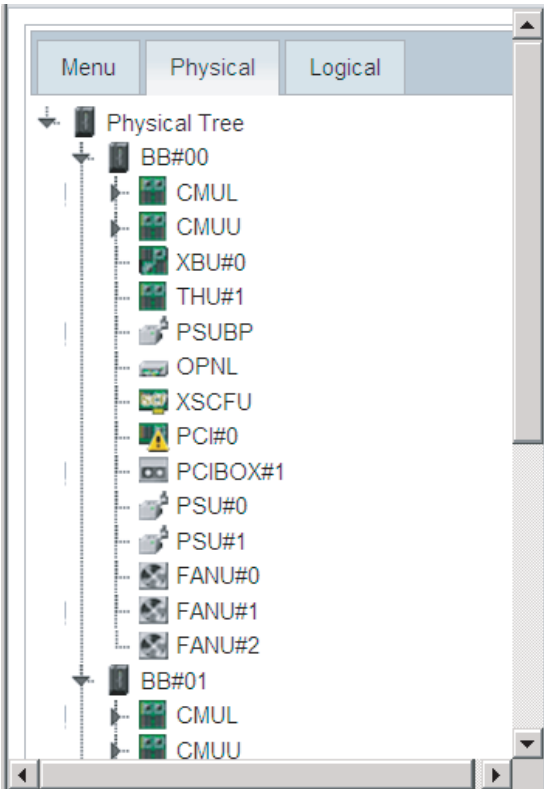
Note - The window layout and displayed content are just one example of the appearance and subject to change for functional improvement or other reasons.

Selecting the [Physical] bar displays the components in this system in the form of a tree. The main frame displays the information/status of the component selected in the tree frame.

If the [Logical] bar is selected, the logical components belonging to the physical partition are displayed in the form of a tree. The main frame displays the information/status of the logical component, which belongs to the physical partition, selected in the tree frame.

The component status display is as follows.

Table C-3　　Component Status Display

Display	Overview
	Operating normally
	Not operating due to failure

Table C-3	Component Status Display *(continued)*
Display	**Overview**
⚠	Any of the statuses below - Continuing operating although some components have failed or are degraded - Although component status is normal, degraded because other components have failed or are degraded - Component undergoing maintenance

C.3   Available Pages

This section provides an overview of the pages available in the main frame. The functions of each page are the same as those of XSCF shell commands. For detailed information on each function, see "Chapter 3   Configuring the System," the chapters describing the relevant commands, or the *Fujitsu SPARC M12 and Fujitsu M10/ SPARC M10 XSCF Reference Manual*.

C.3.1   Pages Displaying the Status of the System, Physical Partitions, and Logical Domains

Table C-4 lists the functions provided to display system information.   Select [Menu] - [Status] - [System Overview].

Table C-4   System Information

Item	Overview	Relevant Command
Product name	Displays the server product name.	showhardconf(8)
Serial number	Displays the system serial number.	
System mode switch state	Displays the state of the Mode switch on the operation panel.	
Input power type	Displays the type of input power supplied.	
Power status	Display the on/off state of input power.	
Power phase	Displays the power-on phase of the system.	
XSCF version	Displays the XSCF firmware version.	version(8)
Chassis status	Displays whether the chassis is the master or standby.	showbbstatus(8)
System time	Displays the system time.	showdate(8)
Failed components	Displays the failed and degraded components.	showstatus(8)

Table C-4   System Information *(continued)*

Item	Overview	Relevant Command
Temperature	Displays the intake air temperature of the chassis.	showenvironment(8)
Exhaust airflow	Display the amount of exhaust airflow of the chassis.	showenvironment(8)
Power capping status	Displays whether the power capping function, which suppresses system power consumption, is enabled or disabled.	showpowercapping (8)

Table C-5 lists the functions provided to display the status of each system component. Select [Menu] - [Status] - [System Status].

Table C-5   Component Status

Item	Overview	Relevant Command
Power consumption Temperature Voltage Fan information	Displays the power consumption, exhaust temperature, voltage, and fan speed of individual components.	showenvironment(8)

Table C-6 lists the functions provided to display the status of each physical partition. Select [Menu] - [Status] - [PPAR Status].

Table C-6   Physical Partition Status

Item	Overview	Relevant Command
PPAR configuration list display	Displays the PSB numbers corresponding to the LSB numbers of each PPAR in the form of a table.	showpcl(8)
PPAR status	Displays the PPAR operation status and configuration policy.	showpcl(8)
PSB information	Displays PSB information.	showboards(8)

Table C-7 lists the function provided to display the PSB status. Select [Menu] - [Status] - [PSB Status].

Table C-7   PSB Status

Item	Overview	Relevant Command
PSB status	Displays a detailed status list, including the PPAR ID where each PSB is currently incorporated.	showboards(8)

Table C-8 lists the function provided to display the logical domain status. Select [Menu] - [Status] - [Domain Status].

Table C-8   Logical Domain Status

Item	Overview	Relevant Command
Logical domain status	Displays the operation status of each logical domain belonging to the specified PPAR.	showdomainstatus(8) showpparstatus(8)

C.3.2   Pages for Operating a Physical Partition

Table C-9 lists the functions provided to operate the power of physical partitions. Select [Menu] - [PPAR Operation] - [PPAR Power].

Table C-9   Physical Partition Power Operations

Item	Overview	Relevant Command
System power-on/off	Specifies whether to power on or off the system (all physical partitions).	showpparstatus(8) poweron(8) poweroff(8)
PPAR power-on/off or reset	Performs the following operations for the specified PPAR: - Power-on/off - Forced power-off - por: PPAR reset - panic: Panic instruction to logical domains - sir: Logical domain reset - xir: CPU reset - Break signal transmission	showpparstatus(8) poweron(8) poweroff(8) reset(8) sendbreak(8)

Table C-10 lists the function provided to set the physical partition operation mode. Select [Menu] - [PPAR Operation] - [PPAR Mode Configuration].

Table C-10   Physical Partition Operation Mode

Item	Overview	Relevant Command
PPAR mode display/setting	Displays/Sets the following modes for the specified PPAR: - Host ID - Hardware diagnosis level - Diagnosis message level - Alive check function enabled/disabled - Operation when Host Watchdog times out - Break signal transmission suppression - Auto boot function enabled/disabled for logical domains - Low-power operation enabled/disabled - I/O path reconfiguration - DR function currently enabled/disabled - DR function enabled/disabled at next start - PPAR Ethernet address (mac address)	showpparmode(8) setpparmode(8)

Note - For support information on the Alive check function and DR function between the XSCF and Hypervisor, see the latest *Product Notes* for your server.

Table C-11 lists the functions provided to configure physical partitions.   Select [Menu] - [PPAR Operation] - [PPAR Configuration].

Table C-11   Physical Partition Settings

Item	Overview	Relevant Command
PPAR configuration list display	Displays the PCL of the specified PPAR system board (PSB). The function also displays/sets the configuration policy of the PPAR. On the SPARC M12-1/M12-2/M10-1/M10-4, it can display information and set the configuration policy for PPAR-ID 00 only.	showpcl(8) setpcl(8)
PCL setting	Sets the PCL. The function associates a PPAR LSB with a PSB and sets configuration information for an LSB. The SPARC M12-1/M12-2/M10-1/M10-4 does not support this function.	showpcl(8) setpcl(8)
PSB addition, deletion, or setting	Instructs that the PSB configuration be changed as follows for a PPAR: - Reserving or incorporating a PSB (BB) for a PPAR - Releasing a PSB (BB) from a PPAR - Moving a PSB (BB) from one PPAR to another PPAR Perform the above operations by following the procedures described in the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*. The SPARC M12-1/M12-2/M10-1/M10-4 does not support this function.	addboard(8) deleteboard(8)

Table C-12 lists the function provided to set memory mirror mode.   Select [Menu] - [PPAR Operation] - [PSB Configuration].

Table C-12   System Board Setting

Item	Overview	Relevant Command
Memory mirror information display/setting	Displays/Sets memory mirror mode information for the CPUs on a system board (PSB).	showfru(8) setupfru(8)

Table C-13 lists the functions provided to set the configuration of a logical domain. Select [Menu] - [PPAR Operation] - [Domain Configuration].

Table C-13   Logical Domain Settings

Item	Overview	Relevant Command
Logical domain configuration information display	Displays the logical domain configuration information for the specified PPAR. The configuration information has the following elements: - Configuration name - Number of constituent logical domains - Date of configuration The function also displays the configuration name of the logical domain currently in operation in the PPAR and the configuration name of the next logical domain to enter operation.	showdomainconfig(8)
Logical domain configuration setting	Sets a logical domain configuration. The function sets the configuration of the next logical domain scheduled to enter operation in the specified PPAR.	setdomainconfig(8)

Table C-14 lists the functions provided to overwrite the OpenBoot PROM environment variables for the control domain of a physical partition. Select [Menu] - [PPAR Operation] - [PPAR Parameter].

Note - For support information on [PPAR Parameter], see the latest *Product Notes*.

Table C-14   Setting OpenBoot PROM Environment Variables

Item	Overview	Relevant Command
Display/setting of PPAR OpenBoot PROM environment variables	Displays/overwrites the following OpenBoot PROM environment variables overwrite settings for the specified PPAR. - use-nvramrc - security-mode - bootscript	showpparparam(8) setpparparam(8)

Table C-15 lists the functions provided to configure verified boot for each physical partition. Select [Menu] - [PPAR Operation] - [Verified Boot].

Table C-15   Configuring Verified Boot

Item	Overview	Relevant Command
Policy displaying/setting	Displays/sets the boot or module policy for verified boot.	showvbootconfig(8) setvbootconfig(8)
System default certificate display	Displays the X.509 public key certificate preinstalled on the system.	showvbootcerts(8)

Table C-15   Configuring Verified Boot *(continued)*

Item	Overview	Relevant Command
Registration/ deletion/enabling/ disabling of an X.509 public key certificate	Registers/deletes a user-specified X.509 public key certificate. Enables/disables/displays a user-specified X.509 public key certificate.	addvbootcerts(8) deletevbootcerts(8) showvbootconfig(8) setvbootconfig(8)

C.3.3   Pages for Configuring the Server

XSCF Network Settings

Table C-16 lists the functions provided to configure an XSCF network.   Select [Menu] - [Setting] - [Network] - [Current]. Alternatively, select [Menu] - [Setting] - [Network] - [Reserve]. The network settings are accessible from either the [Current] or [Reserve] menu. The [Current] menu displays information on the XSCF network currently in operation. You can check the set information from the [Reserve] menu.

After the network is configured with the [Current] menu, there is an automatic transition to the [Reserve] menu. After you configure the network, reflect the settings by clicking [Apply] on the [Reserve] menu and then the [Reboot] button.

Table C-16   XSCF Network Settings

Menu	Item	Overview	Relevant Command
[Current]	XSCF network information/ status display, XSCF network settings	Displays the information and status of the XSCF network currently in operation. The function also sets each host name, domain name, IP address, and net mask of the XSCF network interfaces, and whether to enable or disable them. You can configure the network by clicking the [Edit] button to change to the [Reserve] menu. You can check the set information with the [Reserve] menu.	shownetwork(8) showhostname (8)
	Route display/setting	Displays the current routes. The function also sets routes. You can set a route by clicking the [Edit] button to change to the [Reserve] menu. You can check the set information with the [Reserve] menu.	shownameserve r(8) setnameserver (8)
	DNS display/ setting	Displays the current name servers and search paths. The function also sets name servers and search paths. You can configure the DNS by clicking the [Edit] button to change to the [Reserve] menu. You can check the set information with the [Reserve] menu.	shownameserve r(8) setnameserver (8)

Table C-16   XSCF Network Settings *(continued)*

Menu	Item	Overview	Relevant Command
[Reserve]	XSCF network setting information display, XSCF network settings	Displays XSCF network setting information. The function also sets each host name, domain name, IP address, and net mask of the XSCF network interfaces, and whether to enable or disable them. You can display the information currently used for operation by clicking the [Current Status] button to change to the [Current] menu.	applynetwork(8) setnetwork(8) sethostname(8)
	Route setting information display/route setting	Displays routing setting information. The function also sets routes. You can display the information currently used for operation by clicking the [Current Status] button to change to the [Current] menu.	applynetwork(8) setroute(8)
	DNS setting information display/DNS setting	Displays name server and search path setting information. The function also sets name servers and search paths. You can display the information currently used for operation by clicking the [Current Status] button to change to the [Current] menu.	applynetwork(8) setnameserver(8)
	Reflecting network settings	Displays/Reflects network settings. After the settings are saved, an XSCF reboot is needed to complete the process.	applynetwork(8) rebootxscf(8)

Note - SSCP link addresses cannot be set/displayed from XSCF Web. Use the setsscp and showsscp commands to set/display the addresses.

Note - IP packet filtering rules cannot be set/displayed from XSCF Web. Use the setpacketfilters and showpacketfilters commands to set/display the filtering rules.

Individual Service Function Settings

Table C-17 lists the functions provided to enable/disable individual service functions. Select [Settings] - [Service] - [Service State].

Table C-17   Individual Service Function Enable/Disable Setting

Item	Overview	Relevant Command
Service function status display Enable/Disable setting	Displays the status of the following service functions in a list. The function also enables/disables the service functions. - HTTPS service - SNMPv3 service - SSH service - Telnet service - NTP server service Setting enable/disable for the SNMPv3 service results in the display changing to the SNMP setting menu, where you can configure the SNMP agent. Also, by selecting the NTP server service, you can enable/disable the operation of the XSCF as an NTP server.	showhttps(8) sethttps(8) showsnmp(8) setsnmp(8) showssh(8) setssh(8) showtelnet(8) settelnet(8) showntp(8) setntp(8)

Table C-18 lists the function provided to enable/disable the HTTP service function. Select [Settings] - [Service] - [HTTPS].

Table C-18   HTTP Service Function Enable/Disable Setting

Item	Overview	Relevant Command
HTTP service enable/disable setting	Displays whether the HTTPS service is enabled or disabled, or enables/disables the service.	showhttps(8) sethttps(8)

Note - XSCF Web cannot be used when the HTTPS service is disabled. To enable the HTTPS service, use the sethttps command.

Table C-19 lists the function provided to enable/disable the SSH service function. Select [Settings] - [Service] - [SSH].

Table C-19   SSH Service Function Enable/Disable Setting

Item	Overview	Relevant Command
SSH service enable/disable setting	Displays whether the SSH service is enabled or disabled, or enables/disables the service.	showssh(8) setssh(8)

Note - XSCF Web does not support host key generation, user public key registration/deletion, and XSCF shell timeout setting. Use the showssh and setssh commands for these functions to make settings.

Table C-20 lists the function provided to enable/disable the Telnet service function. Select [Settings] - [Service] - [Telnet].

Table C-20　　Telnet Service Function Enable/Disable Setting

Item	Overview	Relevant Command
Telnet service enable/disable setting	Displays whether the Telnet service is enabled or disabled, or enables/disables the service.	showtelnet(8) settelnet(8)

Table C-21 lists the functions provided to configure the XSCF NTP service function. Select [Settings] - [Service] - [NTP].

Table C-21　　NTP Service Function Settings

Item	Overview	Relevant Command
NTP server enable/disable display/setting	Displays/Sets whether XSCF operation as an NTP server is enabled or disabled.	showntp(8) setntp(8)
NTP client enable/disable display/setting	Displays/Sets whether XSCF operation as an NTP client is enabled or disabled.	
NTP server settings	Displays/Sets the following items for the NTP server settings used by the XSCF network: - NTP server (up to 3) - Priority server (prefer) - stratum value - To complete the local clock address setting of the XSCF itself, an XSCF reboot is needed. An XSCF reboot is needed to complete the setting process.	

Table C-22 lists the function provided to configure the XSCF SMTP service function. Select [Settings] - [Service] - [SMTP].

Table C-22　　SMTP Service Function Settings

Item	Overview	Relevant Command
SMTP server display/setting	Displays/Sets the SMTP server address, authentication algorithm, POP server address, destination e-mail address for error e-mails, and other SMTP server information.	showsmtp(8) setsmtp(8)

Table C-23 lists the functions provided to configure the XSCF SNMP agent function. Select [Settings] - [Service] - [SNMP].

Table C-23   SNMP Agent Function Settings

Item	Overview	Relevant Command
SNMPv3 agent display/setting	Displays/Sets whether the SNMPv3 agent is enabled or disabled. The function also displays/sets an MIB definition file and system management information, etc.	showsnmp(8) setsnmp(8)
SNMPv1/v2c agent display/setting	Displays/Sets whether the SNMPv1/v2c agent is enabled or disabled. The function also displays/sets community strings.	
Trap host display/ setting	Displays the SNMPv1/v2c and SNMPv3 trap hosts in a list. The function also displays/sets trap destination host names, port numbers, and other host information.	

Table C-24 lists the functions provided to configure the security function for SNMPv3.   Select [Settings] - [Service] - [SNMP Security].

Table C-24   SNMP Security Function Settings

Item	Overview	Relevant Command
USM management information display/setting	Displays/Sets USM management information such as the user authentication algorithm. For details of USM management information, see Table 10-5.	showsnmpusm(8) setsnmpusm(8)
SNMPv1/v2c agent display/setting	Displays/Sets VACM management information such as access control groups and access control views. For details of VACM management information, see Table 10-5.	showsnmpvacm(8) setsnmpvacm(8)

User Account Settings

Table C-25 lists the functions provided to configure XSCF local user accounts.   Select [Settings] - [User Manage] - [Account].

Table C-25   User Account Settings

Item	Overview	Relevant Command
User account information display	Displays the information and status of the currently registered user accounts. useradm privilege is required.	showuser(8)
User account addition/deletion	Adds/Deletes user accounts. useradm privilege is required.	adduser(8) deleteuser(8)

Table C-25   User Account Settings *(continued)*

Item	Overview	Relevant Command
User account enabling/disabling	Disables currently registered user accounts, and enables them again. useradm privilege is required.	disableuser(8) enableuser(8)
User account information display/change	Displays information on the specified user account, and changes the password, user privileges, and password policy. useradm privilege is required.	showuser(8) password(8) setprivileges(8)
Local user account information display/password change	With any privilege other than useradm, you can display information on a local user account and change the password.	showuser(8) password(8)
System password policy display/setting	Displays the current system password policy. The function also sets the system password policy to be applied later.	showpasswordpolicy(8) setpasswordpolicy(8)

Note - XSCF Web does not support the lockout function, which locks out a user account after three successive login failures. Use the setloginlockout and showloginlockout commands for the XSCF shell lockout function.

LDAP Service Settings

Table C-26 lists the functions provided to configure an LDAP client. Select [Settings] - [User Manage] - [LDAP].

Table C-26   LDAP Service Settings

Item	Overview	Relevant Command
LDAP server display/registration	Displays/Registers an LDAP server with the XSCF configured as an LDAP client.	showldap(8) setldap(8)
Certificate display/import	Displays/Imports the LDAP server certificate.	

LDAP over SSL Service Settings

Table C-27 lists the functions provided to configure an LDAP over SSL client. Select [Settings] - [User Manage] - [LDAP/SSL].

Table C-27   LDAP over SSL Service Settings

Item	Overview	Relevant Command
LDAP over SSL server display/ registration	Displays/Registers an LDAP over SSL server with the XSCF configured as an LDAP over SSL client.	showldapssl(8) setldapssl(8)

Table C-27   LDAP over SSL Service Settings *(continued)*

Item	Overview	Relevant Command
usermap display/ setting	Displays/Sets usermap.	
Certificate display/setting	Displays/Loads/Deletes the LDAP over SSL server certificates.	
defaultrole display/setting	Displays/Sets the user privilege used by all users that are authenticated via LDAP over SSL.	
Alternate server display/setting	Displays/Sets up to five alternate LDAP over SSL servers.	
Group display/setting	Displays/Sets the administrator group, operator group, and customer group.	
User domain display/setting	Displays/Sets up to five user domains.	

Active Directory Service Settings

Table C-28 lists the functions provided to configure an Active Directory client. Select [Settings] - [User Manage] - [Active Directory].

Table C-28   Active Directory Service Settings

Item	Overview	Relevant Command
Active Directory server display/setting	Enables/Disables Active Directory with the XSCF configured as an Active Directory client. Displays/Sets the server, mode, timeout time, log, default settings, etc.	showad(8) setad(8)
Certificate display/setting	Displays/Loads/Deletes the Active Directory server certificates.	
defaultrole display/setting	Displays/Sets the user privileges used by all users that are authenticated via Active Directory.	
Alternate server display/setting	Displays/Sets up to five alternate Active Directory servers, and displays/loads/deletes the server certificates.	
Group display/setting	Displays/Sets the administrator group, operator group, and customer group.	
User domain display/setting	Displays/Sets up to five user domains.	
DNS locator query display/setting	Displays/Sets up to five DNS locator queries.	

Auto Logout Setting

Table C-29 lists the function provided to set the XSCF Web session timeout (auto logout) time. Select [Settings] - [Autologout] - [Account]. With the auto logout time (minutes) set, users who are logged in to XSCF Web but have not accessed it for a specific duration are automatically logged out from the XSCF.

Table C-29　　Auto Logout Setting

Item	Overview	Relevant Command
Auto logout time display/setting	Displays the currently set auto logout time (minutes) or sets an auto logout time. The default value is 10 minutes. You can specify a value in a range of 1 to 255.	This is supported only on XSCF Web.

Note - XSCF Web does not support the XSCF shell session timeout time setting. Use the showautologout and setautologout commands.

CPU Activation Setting

Table C-30 lists the functions provided to set a CPU Activation. Select [Settings] - [CoD Reservation].

Table C-30　　CPU Activation Setting

Item	Overview	Relevant Command
Usage of CPU core resources	Displays the usage of CPU core resources. The pattern of display is as follows: - Resource (CPU) - Individual PPARs	showcodusage(8)
CPU Activation assignment display/setting	Displays the CPU Activation assignment status for each PPAR. The function also specifies a PPAR to increase or decrease the number of CPU Activations for resources.	showcod(8) setcod(8)

Table C-31 lists the functions provided to register a CPU Activation key. Select [Settings] - [CoD Activation].

Table C-31　　CPU Activation Key Registration

Item	Overview	Relevant Command
CPU Activation key information display/setting	Displays the currently registered CPU Activation key information.	showcodactivation(8)
CPU Activation key addition/deletion	Adds/Deletes CPU Activation keys.	addcodactivation(8) deletecodactivation(8)

Table C-31   CPU Activation Key Registration *(continued)*

Item	Overview	Relevant Command
CPU Activation key registration history	Displays history information about adding and deleting CPU Activation keys.	showcodactivationhistory(8)

Audit Settings

Table C-32 lists the functions provided to configure XSCF auditing.   Select [Settings] - [Audit].

Table C-32   Audit Settings

Item	Overview	Relevant Command
Audit log (audit trail) usage status/data archiving/data deletion	Displays the use capacity of an audit log. The function also archives an audit log (*1) and deletes secondary files.	showaudit(8) setaudit(8)
Auditing enabling/ disabling	Displays/Sets whether auditing is enabled or disabled.	
Audit policy display/setting	Displays/Sets the policy applied when the audit log reaches the full capacity (*2), the warning threshold for the local audit log amount (%), and the warning e-mail destination address.	
Global user policy display/setting	Specifies whether to enable/disable the global user policy.	
User audit record generation policy display/addition/ change	Displays the user-specific audit record generation policies (audit record generation enabled/disabled) in a list. The function also adds audit record generation policies for users. The global user policy is disabled for these users with the added policies. The audit record generation policy is enabled/disabled by the specified user, who specifies whether to enable the global user policy.	
Audit event/audit class display/setting	Displays audit events and audit classes. The function also specifies whether to enable or disable audit events and audit classes.	

*1 Audit log archiving is not currently supported.
*2 When an audit log reaches full capacity, only the default audit policy "count," which discards audit records, is
   currently supported. Therefore, do not specify "suspend."

E-mail Settings

Table C-33 lists the function provided for making XSCF e-mail settings.   Select [Settings] - [Email Reporting].

Table C-33   E-mail Settings

Item	Overview	Relevant Command
E-mail notification function display/ setting	Displays/Sets e-mail notification function setting information. The function enables/ disables the e-mail notification function and displays/sets the destination e-mail address for notification sent to the system administrator.	showemailreport(8) setemailreport(8)

Time Settings

Table C-34 lists the function provided to set the system time and time zone.   Select [Settings] - [Time].

Table C-34   Time Settings

Item	Overview	Relevant Command
System time display/setting	Displays/Sets the current system time and time zone. After a setting is made, the XSCF is rebooted. Log in again. If the system time is synchronized with an NTP server, the time cannot be set.	showdate(8) setdate(8) showtimezone(8) settimezone(8)

Note - Daylight saving time cannot be set from XSCF Web. Use the showtimezone and settimezone commands to set it.

Power Consumption Settings

Table C-35 lists the function provided to set a limit on system power consumption. Select [Settings] - [Power Capping].

Table C-35   Power Consumption Settings

Item	Overview	Relevant Command
Power consumption limit display/setting	Displays the setting for limiting power consumption. The function also enables/ disables the limit and sets the upper limit value of power consumption, etc.	showpowercapping (8) setpowercapping(8)

Power Schedule Setting

Table C-36 lists the functions provided to set a power schedule.   Select [Settings] - [Power Schedule].

Table C-36   Power Schedule Setting

Item	Overview	Relevant Command
Power schedule setting status display	Displays the status of PPAR power schedules in a list.	showpowerschedule (8)
Power schedule setting	Sets a power schedule. The function enables/disables schedules and makes other settings for the following targets: - Individual PPARs - All PPARs	setpowerschedule(8)
Power schedule information display	Displays the next power-on and power-off times by PPAR.	showpowerschedule (8)
Detailed power schedule information	Displays/Sets the details of power schedule information. The function displays/adds/changes/deletes schedules for the following targets: - Individual PPARs - All PPARs	showpowerschedule (8) setpowerschedule(8) addpowerschedule(8) deletepowerschedule (8)

Device Settings

Table C-37 lists the functions provided to set PCI expansion unit information and information about the cards connected to the servers.   Select [Settings] - [Add-In Card Manager].

Table C-37   PCI Expansion Unit Information Setting

Item	Overview	Relevant Command
Card/PCI expansion unit sensor information display	The function displays the sensor information in a list for the following targets: - PCI card (connected to the server) - PCI expansion unit - FRU in the PCI expansion unit	ioxadm(8)
Device information display/power setting	Displays device information about PCI cards, the PCI expansion unit, and link cards in a list. The function also gives power-off/on instructions for the power supply units in the PCI expansion unit.	
Monitoring component initialization	Initializes the monitoring components of the PCI expansion unit.	
Firmware update	Checks, registers, and updates the PCI expansion unit and link card firmware.	
PCI expansion unit LED state display/ setting	Displays/Sets the locator LED states of FRUs in the PCI expansion unit.	

Setting of the Direct I/O Function of the PCI Expansion Unit

Table C-38 lists the function provided to configure the direct I/O function of the PCI expansion unit. Select [Settings] - [PCIBOX DIO].

Table C-38   Setting of the Direct I/O Function of the PCI Expansion Unit

Item	Overview	Relevant Command
Enabling/Disabling direct I/O function	Displays/Sets whether the direct I/O function of the PCI expansion unit is enabled or disabled for each PCI slot of the SPARC M12/M10.	showpciboxdio(8) setpciboxdio(8)

Remote Storage Settings

Table C-39 lists the functions provided to configure remote storage. Select [Settings] - [Remote Storage].

Table C-39   Remote Storage Settings

Item	Overview	Relevant Command
Remote Storage Server start (*1)	Start the Java Runtime Environment to start the Remote Storage Server.	No
Remote storage connection status display/setting	Displays the remote storage connection information in a list. - XSCF-LAN interface - XSCF-LAN, IP address, net mask, gateway - Connection status/IP address of system management terminal Also, select the XSCF-LAN interface, and connect to media/disconnect media/specify an IP address/configure a slave XSCF for the system management terminal.	setremotestorage(8) showremotestorage (8)

*1 None of the XSCF shell commands is a command that starts XSCF Remote Storage Server. However, you can start XSCF Remote Storage Server with the Java command from a terminal. For details, see "Before Using Remote Storage" in "4.6.9   Flow for Using Remote Storage."

C.3.4   Pages for Maintaining the Server

Network Connection Information

Table C-40 lists the functions provided to display network connection information.

Select [Maintenance] - [Network Tools]. When selected, [Ping], [Traceroute], and [Nslookup] menus display the host response, network path to the host, and host name information, respectively.

Table C-40   Network Connection Information Display

Item	Overview	Relevant Command
Host response display	Displays the network response status between the XSCF and the specified host.	ping(8)
Network path display	Displays information on the network path to the specified host or network device.	traceroute(8)
Host name information display	Displays information on the specified host name.	nslookup(8)

XSCF Settings Information Saving/Restoration

Table C-41 lists the function provided to save/restore XSCF settings information. Select [Maintenance] - [Configuration Management].

Table C-41   XSCF settings information saving/restoration

Item	Overview	Relevant Command
Setting information saving/restoration	XSCF settings information or CPU Activation keys are saved/restored. The XSCF is rebooted when the information is saved/restored with the [Run] button. Log in again.	dumpconfig(8) restoreconfig(8) dumpcodactivation(8) restorecodactivation (8)

Firmware Update

Table C-42 lists the functions provided to update the XCP firmware.   Select [Maintenance] - [Firmware Update].

Table C-42   Firmware Update

Item	Overview	Relevant Command
Version display	Displays the following firmware versions: - XCP version - XSCF firmware version - CMU firmware version	version(8)
XCP import	Specifies the following firmware files to import firmware onto the server: - XCP firmware file - PCI expansion unit firmware file	getflashimage(8)
Firmware update	Performs an XCP update. At this time, the XSCF is rebooted, so log in to the XSCF again.	flashupdate(8)

Table C-42   Firmware Update *(continued)*

Item	Overview	Relevant Command
Version matching (for systems with multiple XSCFs)	Matches the XCP firmware versions in a system with multiple XSCFs. Use this function after XSCF unit, CMU, chassis, or other replacement.	flashupdate(8)

XSCF Reboot

Table C-43 lists the functions provided to reboot the XSCF.   Select [Maintenance] - [Reboot XSCF].

Table C-43   XSCF Reboot

Item	Overview	Relevant Command
XSCF reboot	Reboot the local XSCF.	rebootxscf(8)
Target XSCF reboot (for systems with multiple XSCFs)	Specifies the BB-ID of the chassis with the mounted XSCF to restart the chassis. - All chassis - Specified chassis	showbbstatus(8) rebootxscf(8)

XSCF Switching

Table C-44 lists the function provided to switch between XSCFs in a system with multiple XSCFs.   Select [Maintenance] - [Switch Over].

Table C-44   XSCF Switching

Item	Overview	Relevant Command
XSCF switching (for systems with multiple XSCFs)	Switches the XSCF from the master to standby or from the standby to master.	switchscf(8)

Server Information Saving

Table C-45 lists the function provided to collect server information and analyze/solve system problems.   Select [Maintenance] - [Switch Over].

Table C-45   Server Information Saving

Item	Overview	Relevant Command
Server information saving/ target chassis information saving (for systems with multiple XSCFs)	Specifies the target BB-ID for collecting data such as the server configuration, common system logs, and individual chassis logs, and saves the data to a file. - All chassis - Specified chassis	snapshot(8)

Note - In the systems with multiple XSCFs, you can save server information from the page displayed after login to the standby XSCF.

ASR Function Settings

Table C-46 ASR Function Settings

Item	Overview	Relevant Command
Enabling/Disabling ASR function (service tag) (*1)	Displays/Sets whether the service tag is enabled or disabled.	showservicetag(8) setservicetag(8)
Alive test	Generates pseudo errors in Ops Center and the ASR manager, or checks whether they are alive.	

*1 The ASR function is a remote maintenance service that uses the Oracle Auto Service Request software provided by Oracle Corporation. For details of the ASR function, see the *Oracle Auto Service Request Installation and Operations Guide* for the version of the software that you are using.

C.3.5 Pages Displaying Logs

Table C-47 lists the functions provided to refer to log information. Select [Logs]. Select the intended log.

Table C-47 Log Information

Item	Overview	Relevant Command
Error log display	Displays the error log. You can search the log.	showlogs(8) error option
Power log display	Displays the power log. You can search the log.	showlogs(8) power option
Event log display	Displays the event log. You can search the log.	showlogs(8) event option
Console log display	Displays the console log. You can search the log.	showlogs(8) console option
Panic log display	Displays the panic log. You can search the log.	showlogs(8) panic option
Temperature history log display (Environment Log)	Specifies the BB-ID of a chassis to display its temperature history log. You can search the log.	showlogs(8) env option
IPL message log display	Specifies a PPAR to display its IPL log. You can search the log.	showlogs(8) ipl option
Monitoring message log display	Displays the monitoring message log. You can search the log.	showlogs(8) monitor option

Table C-47   Log Information *(continued)*

Item	Overview	Relevant Command
Audit log display	Displays the audit log. You can specify a period, date, user, and class to refer to them in the log.	viewaudit(8)

Appendix D

XSCF MIB Information

This appendix provides an overview of the XSCF extended MIB (Management Information Base), which is supported by the XSCF SNMP agent function.　For details of the SNMP agent function, see "10.3　Monitoring/Managing the System Status With the SNMP Agent."

- MIB Object Identification
- Standard MIB
- Extended MIB
- Traps

D.1　MIB Object Identification

This section shows examples of the MIB object identifiers (OIDs) supported by the XSCF.

internet	OBJECT IDENTIFIER ::=	{ iso org(3) dod(6) 1 }
directory	OBJECT IDENTIFIER ::=	{ internet 1 }
mgmt	OBJECT IDENTIFIER ::=	{ internet 2 }
experimental	OBJECT IDENTIFIER ::=	{ internet 3 }
private	OBJECT IDENTIFIER ::=	{ internet 4 }
mib-2	OBJECT IDENTIFIER ::=	{ mgmt 1 }
system	OBJECT IDENTIFIER ::=	{ mib-2 1 }
interfaces	OBJECT IDENTIFIER ::=	{ mib-2 2 }
at	OBJECT IDENTIFIER ::=	{ mib-2 3 }
ip	OBJECT IDENTIFIER ::=	{ mib-2 4 }

icmp	OBJECT IDENTIFIER ::=	{ mib-2 5 }
tcp	OBJECT IDENTIFIER ::=	{ mib-2 6 }
udp	OBJECT IDENTIFIER ::=	{ mib-2 7 }
snmp	OBJECT IDENTIFIER ::=	{ mib-2 11 }
enterprises	OBJECT IDENTIFIER ::=	{ private 1 }
fujitsu	OBJECT IDENTIFIER ::=	{ enterprises 211 }
product	OBJECT IDENTIFIER ::=	{ fujitsu 1 }
solaris	OBJECT IDENTIFIER ::=	{ product 15 }
sparc	OBJECT IDENTIFIER ::=	{ solaris 4 }
xscfSpMIB	OBJECT IDENTIFIER ::=	{ sparc 1 }
scfObjects	OBJECT IDENTIFIER ::=	{ xscfSpMIB 1 }
scfInfo	OBJECT IDENTIFIER ::=	{ scfObjects 1 }
scfState	OBJECT IDENTIFIER ::=	{ scfObjects 2 }
scfMonitorInfo	OBJECT IDENTIFIER ::=	{ scfObjects 3 }
scfSystemInfo	OBJECT IDENTIFIER ::=	{ scfObjects 4 }
scfPPARInfo	OBJECT IDENTIFIER ::=	{ scfObjects 5 }
scfPsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 6 }
scfLsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 7 }
scfBoardInfo	OBJECT IDENTIFIER ::=	{ scfObjects 8 }
scfCpuInfo	OBJECT IDENTIFIER ::=	{ scfObjects 9 }
scfMemoryInfo	OBJECT IDENTIFIER ::=	{ scfObjects 10 }
scfPciBoxInfo	OBJECT IDENTIFIER ::=	{ scfObjects 11 }
scfComponentInfo	OBJECT IDENTIFIER ::=	{ scfObjects 12 }
scfDomainInfo	OBJECT IDENTIFIER ::=	{ scfObjects 13 }
scfMIBTraps	OBJECT IDENTIFIER ::=	{ xscfSpMIB 2 }
scfMIBTrapPrefix	OBJECT IDENTIFIER ::=	{ scfMIBTraps 0 }
scfMIBTrapData	OBJECT IDENTIFIER ::=	{ scfMIBTraps 1 }
scfMIBConformances	OBJECT IDENTIFIER ::=	{ xscfSpMIB 3 }
scfMIBCompliances	OBJECT IDENTIFIER ::=	{ scfMIBConformances 1 }
scfMIBGroups	OBJECT IDENTIFIER ::=	{ scfMIBConformances 2 }
scfMIBObjectGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 1 }

scfMIBNotifGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 2 }

scfHwCtrlMIB	OBJECT IDENTIFIER ::=	{ sparcEnterprise 2 }
scfHwCtrlMIBObjects	OBJECT IDENTIFIER ::=	{ scfHwCtrlMIB 1 }
scfHwCtrlPowerMgmt	OBJECT IDENTIFIER ::=	{ scfHwCtrlMIBObjects 1 }

D.2 Standard MIB

The standard MIB supported by the XSCF conforms to the following RFCs (Note).
For details of the standard MIB definition files, see the general RFC documents.

Protocols and RFC Examples

MIB II	RFC1213
User-based Security Model (USM)	RFC3414
View-based Access Control Model (VACM)	RFC3415
SNMPv2-MIB	RFC3418

Note - RFC: Stands for Request For Comments. RFCs are technical specifications published
by the Internet Engineering Task Force (IETF), which is an organization that establishes
technical standards related to the Internet.

D.3 Extended MIB

The XSCF in the SPARC M12/M10 systems provides the following information from
the XSCF extended MIB:

- System information, hardware/firmware versions, and system configuration
  information
- Environment information (temperature, voltage, fan speed, etc.)
- Physical partition status and physical partition configuration information
- Parts failure information in the system
- Information related to system power values

D.3.1   XSCF Extended MIB Objects

This section describes the information in each group of the major objects of the XSCF extended MIB.

scfObjects

- scfInfo group
  This group provides general information relating to the XSCF, such as master XSCF and XSCF-LAN information.

- scfState group
  This group provides XSCF status information, the Mode switch state on the operation panel, etc.

- scfMonitorInfo group
  This group provides environment information on various components in the system. Such information includes the component name, temperature, voltage, and fan speed.

- scfSystemInfo group
  This group provides the following system information:
  - Host name, serial number, number of CPUs mounted, and other system product information
  - LED state information
  - System environment information such as system power consumption, exhaust airflow, and intake air temperature

- scfPPARInfo group
  This group provides the following physical partition information:
  - PPAR ID, number of CPUs mounted, memory capacity, and other physical partition hardware information
  - OpenBoot PROM, POST, and Hypervisor version
  - Oracle Solaris information
  - Physical partition operation status and configuration policy

- scfPsbInfo group
  This group provides PSB (BB) information such as the PSB number, PSB power status, and PSB assignment/incorporation status in a physical partition.

- scfLsbInfo group
  This group provides LSB information such as the LSB number, the ID of the PPAR to which the LSB belongs, and PCL information.

- scfBoardInfo group
  This group provides CMU information such as the CPU memory unit (CMUL,

CMUU) name, number, and operation status.

- **scfCpuInfo group**
  This group provides CPU module information such as the CPU number, CPU frequency, and operation status.

- **scfMemoryInfo group**
  This group provides information such as the memory unit number, capacity, and operation status.

- **scfPciBoxInfo group**
  This group provides information on PCI expansion units and their constituent components.   The typical components are I/O boards, PCI cards, link cards, power supply units, fan units, and sensors. For details of the parts, see "Chapter 2 Understanding the PCI Expansion Unit Components" in the *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

- **scfComponentInfo group**
  This group provides FRU information and status information about all the components in the system.

- **scfDomainInfo group**
  This group provides logical domain information such as the ID of the PPAR to which the logical domain belongs, the domain name, and the logical domain status.

D.4 Traps

Traps include standard traps and extended traps. Standard traps are general traps to individual devices defined for SNMP. For details on standard traps, see the general documents. In this manual, traps identifying events specific to these systems are called extended traps.
Extended traps provide a variety of information in the scfMIBTRap object. For an overview of extended traps, see "10.3   Monitoring/Managing the System Status With the SNMP Agent."

Appendix E

SPARC M12/M10 System-specific Functions of Oracle VM Server for SPARC

This appendix describes and provides supplementary information on the functions of Oracle VM Server for SPARC that are specific to the SPARC M12/M10 systems.
For general information relating to software management of Oracle VM Server for SPARC, see the *Oracle VM Server for SPARC Administration Guide* of the version used.

- Ordered Shutdown of Logical Domains
- CPU Activation Support
- Checking Failed Resources
- Automatic Replacement of Failed CPUs
- Hypervisor Dump
- Domain Console Logging Function
- CPU Socket Restrictions

E.1   Ordered Shutdown of Logical Domains

In the SPARC M12/M10 systems, you can perform an ordered shutdown of all the logical domains from the XSCF. For details, see "8.7   Ordered Shutdown of Logical Domains."

E.2   CPU Activation Support

CPU Activation is supported on SPARC M12/M10 systems. You can display a list of CPU Activation information by using the ldm command. For details, see "8.8 Checking CPU Activation Information."

E.3 Checking Failed Resources

The SPARC M12/M10 systems automatically detect and degrade failed memory and CPU resources. The ldm(1M) command can be used to display the status of memory and CPU resources. For details, see "10.6   Checking Failed Hardware Resources."

E.3.1 Confirming Whether or Not There Has been a Memory or CPU Failure Using the list-domain Sub Command

1. **Display the detailed information of a logical domain in a physical partition along with the information on whether or not there has been memory or CPU failure.**

```
primary# ldm list-domain -l -S
```

E.3.2 Displaying Whether or Not There Has been a Memory or CPU Failure Using the list-device Sub Command

1. **Display the resource information of available memory and CPU in a physical partition along with the information on whether or not there has been memory or CPU failure.**

```
primary# ldm list-devices -S memory cpu
```

E.4 Automatic Replacement of Failed CPUs

The SPARC M12/M10 systems automatically detect failed CPUs and place them offline. You can configure Oracle VM Server for SPARC so that a failed CPU is automatically replaced when there is a free CPU or available CPU Activation. For details, see "10.7   Setting Automatic Replacement of Failed CPU Cores."

E.5 Hypervisor Dump

Hypervisor may abort upon detecting an inconsistency in a physical partition. In this case, the firmware retains the contents of Hypervisor memory, and the system is rebooted in the factory-default configuration. For details, see "8.13 Collecting a Hypervisor Dump File."

E.6 Domain Console Logging Function

In a logical domain environment, the console output destination of the control domain is the XSCF. The console output destination of all the other domains is the service domain that started the virtual console terminal collection and distribution unit (vcc). In Oracle Solaris 11.1 and later, service domains support the console logging function of logical domains. For details, see "8.10 Domain Console Logging Function."

E.7 CPU Socket Restrictions

For the SPARC M12/M10 system with Oracle VM Server for SPARC 3.3 or later, the logical domain configuration can be managed based on the physical CPU socket. For details, see "8.14 Managing Logical Domain Resources Associated with CPU Sockets."

Appendix F

SAS2IRCU Utility Command Display Examples

This appendix contains display examples of typical SAS2IRCU utility commands for configuring and managing hardware RAID volumes of the SPARC M12/M10 system by using SAS-2 Integrated RAID Configuration Utility (SAS2IRCU) (referred to below as SAS2IRCU utility) version 14.00.00.00 or later from Broadcom Limited.

For details on the SAS2IRCU utility, see the Broadcom Limited website described in "14.2   Configuring Hardware RAID." For details on the SAS2IRCU utility and how to use it, see the *SAS-2 Integrated RAID Configuration Utility User Guide* on the same website.
SAS-2 Integrated RAID Configuration Utility (SAS2IRCU) is the copyrighted work of Broadcom Limited and its affiliated companies.

- Displaying a List of SAS Controllers Recognized by sas2ircu
- Displaying the Information of a Hardware RAID Volume
- Adding a Hardware RAID Volume
- Displaying the Configuration Status of a Hardware RAID Volume
- Creating a Hot Spare of a Hardware RAID Volume
- Deleting a Hot Spare of a Hardware RAID Volume
- Deleting a Hardware RAID Volume
- Identifying the Faulty Disk Drive of a Hardware RAID Volume

F.1   Displaying a List of SAS Controllers Recognized by sas2ircu

To display a list of SAS controllers recognized by sas2ircu, use the list command of sas2ircu.
The following example shows that Adapter Type = SAS2308_2 is an internal SAS controller.
Check the Index number displayed for the internal SAS controller.
The following shows an example of the SPARC M12-2.

```
# ./sas2ircu LIST
LSI Corporation SAS2 IR Configuration Utility.
Version 20.00.00.00 (2014.09.18)
Copyright (c) 2008-2014 LSI Corporation. All rights reserved.


        Adapter      Vendor  Device                        SubSys   SubSys
 Index    Type         ID      ID    Pci Address           Ven ID   Dev ID
 -----  -----------  ------  ------  ----------------      ------   ------
   0     SAS2308_2    1000h    87h   00h:03h:00h:00h       10cfh    187eh

        Adapter      Vendor  Device                        SubSys   SubSys
 Index    Type         ID      ID    Pci Address           Ven ID   Dev ID
 -----  -----------  ------  ------  ----------------      ------   ------
   1     SAS2308_2    1000h    87h   00h:03h:00h:00h       10cfh    187eh
```

F.2 Displaying the Information of a Hardware RAID Volume

To display the information of hardware RAID volumes and disk drives configured on the system, use the DISPLAY command of sas2ircu.

The following example shows the RAID 1 (Mirror) volume which is equipped with a disk drive in disk slot 0 as Primary and a disk drive in disk slot 1 as Secondary, and disk drives which do not make up the hardware RAID, in disk slots 2, 3, 4, and 5 for the SAS controller (*1) with Index=1.
*1 This can be checked by the list command of sas2ircu. See "F.1 Displaying a List of SAS Controllers Recognized by sas2ircu."

In the examples that follow, (1) to (4) indicate the following:
(1): SAS controller information
(2): RAID volume information
 (2-1): RAID volume 1 information
    You can obtain the following information (partial extract).
     - RAID volume ID is 286
     - RAID volume name is RAID1-SYS
     - RAID volume status is normal (Okay (OKY))
     - RAID level is RAID1 (Mirroring)
     - Disk (2:0) of SPARC M12/M10 internal disk slot 0 is mounted in PHY[0] (Primary)
     - Disk (2:1) of SPARC M12/M10 internal disk slot 1 is mounted in PHY[1]

(Secondary)
(3): Physical device information
 (3-1): Status of a disk drive (Drive Type=SAS_HDD) of SPARC M12/M10 internal
      disk slot 0 (Enclosure#:2,Slot#:0)
           It is optimized as a part of the RAID volumes. (State:Optimal (OPT))
 (3-2): Status of an enclosure services device (Device Type= Enclosure services
      device) of SPARC M12/M10 internal disk slot 0 (Enclosure#:2,Slot#:0)
           This represents a device other than hard disks. Although the Standby state
           is shown, this is a normal display. (State:Standby (SBY))
 (3-3): Status of a disk drive (Drive Type=SAS_HDD) of SPARC M12/M10 internal
      disk slot 2 (Enclosure#:2,Slot#:2)
           This represents a disk drive that is not in the RAID configuration. The
           status indicates that it can be incorporated into a RAID volume and a hot
           spare. (State:Ready (RDY))
(4): SPARC M12/M10 chassis information
(4-1): SAS address of the SAS controller

Note - You can find the device path and installation location of the SAS controller by checking the SAS address of the SAS controller on the OBP beforehand and comparing it to sas2ircu DISPLAY. For details on how to obtain SAS controller information on the OBP, see "14.2.4   Preparation Before Hardware RAID Operation."

```
root# ./sas2ircu 0 DISPLAY
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0
------------------------------------------------------------------------
Controller information <-- (1)
------------------------------------------------------------------------
Controller type                         : SAS2308_2
BIOS version                            : 0.00.00.00
Firmware version                        : 13.00.66.00
Channel description                     : 1 Serial Attached SCSI
Initiator ID                            : 0
Maximum physical devices                : 255
Concurrent commands supported           : 3072
Slot                                    : Unknown
Segment                                 : 0
Bus                                     : 3
Device                                  : 0
Function                                : 0
RAID Support                            : Yes


------------------------------------------------------------------------
IR Volume information <-- (2)
------------------------------------------------------------------------
IR volume 1 <-- (2-1)
Volume ID                               : 286
Volume Name                             : RAID1-SYS
Status of volume                        : Okay (OKY)
```

```
Volume wwid                           : 0aa6d102f1bf517a
RAID level                            : RAID1
Size (in MB)                          : 571250
Physical hard disks                   :
PHY[0] Enclosure#/Slot#               : 2:0
PHY[1] Enclosure#/Slot#               : 2:1


-----------------------------------------------------------------------
Physical device information <-- (3)
-----------------------------------------------------------------------
Initiator at ID #0

Device is a Hard disk <-- (3-1)
Enclosure #                           : 2
Slot #                                : 0
SAS Address                           : 5000039-4-281b-51e2
State                                 : Optimal (OPT)
Size (in MB)/(in sectors)             : 572325/1172123567
Manufacturer                          : TOSHIBA
Model Number                          : MBF2600RC
Firmware Revision                     : 3706
Serial No                             : EA25PC7007NC
GUID                                  : 50000394281b51e0
Protocol                              : SAS
Drive Type                            : SAS_HDD

Device is a Enclosure services device <-- (3-2)
Enclosure #                           : 2
Slot #                                : 0
SAS Address                           : 500000e-0-e049-073d
State                                 : Standby (SBY)
Manufacturer                          : FUJITSU
Model Number                          : NBBEXP
Firmware Revision                     : 0d32
Serial No                             : x3625413500
GUID                                  : N/A
Protocol                              : SAS
Device Type                           : Enclosure services device

Device is a Hard disk
Enclosure #                           : 2
Slot #                                : 1
SAS Address                           : 5000039-4-281b-549a
State                                 : Optimal (OPT)
Size (in MB)/(in sectors)             : 572325/1172123567
Manufacturer                          : TOSHIBA
Model Number                          : MBF2600RC
Firmware Revision                     : 3706
Serial No                             : EA25PC7007PT
GUID                                  : 50000394281b5498
Protocol                              : SAS
Drive Type                            : SAS_HDD

Device is a Hard disk <-- (3-3)
Enclosure #                           : 2
```

```
Slot #                          : 2
SAS Address                     : 5000039-4-281a-8ad2
State                           : Ready (RDY)
Size (in MB)/(in sectors)       : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                    : MBF2600RC
Firmware Revision               : 3706
Serial No                       : EA25PC7007G7
GUID                            : 50000394281a8ad0
Protocol                        : SAS
Drive Type                      : SAS_HDD

Device is a Hard disk
Enclosure #                     : 2
Slot #                          : 3
SAS Address                     : 5000039-4-281b-5dc2
State                           : Ready (RDY)
Size (in MB)/(in sectors)       : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                    : MBF2600RC
Firmware Revision               : 3706
Serial No                       : EA25PC7007T3
GUID                            : 50000394281b5dc0
Protocol                        : SAS
Drive Type                      : SAS_HDD

Device is a Hard disk
Enclosure #                     : 2
Slot #                          : 4
SAS Address                     : 5000039-4-281b-58b2
State                           : Ready (RDY)
Size (in MB)/(in sectors)       : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                    : MBF2600RC
Firmware Revision               : 3706
Serial No                       : EA25PC7007RA
GUID                            : 50000394281b58b0
Protocol                        : SAS
Drive Type                      : SAS_HDD

Device is a Hard disk
Enclosure #                     : 2
Slot #                          : 5
SAS Address                     : 5000039-4-281b-502e
State                           : Ready (RDY)
Size (in MB)/(in sectors)       : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                    : MBF2600RC
Firmware Revision               : 3706
Serial No                       : EA25PC7007LR
GUID                            : 50000394281b502c
Protocol                        : SAS
Drive Type                      : SAS_HDD

-------------------------------------------------------------------
```

```
Enclosure information <-- (4)
------------------------------------------------------------------------
Enclosure#                               : 1
Logical ID                               : 500000e0:e046ff10  <-- (4-1)
Numslots                                 : 8
StartSlot                                : 0
Enclosure#                               : 2
Logical ID                               : 500000e0:e049073f
Numslots                                 : 9
StartSlot                                : 0
------------------------------------------------------------------------
SAS2IRCU: Command DISPLAY Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

F.3   Adding a Hardware RAID Volume

Use the CREATE command of sas2ircu to add a hardware RAID volume to the system.

In the following example, a RAID1E (Mirroring Extended) volume named "RAID1E-VOL" is created for disk drives which are equipped with disk slots 2, 3, and 4 (entire areas of disks) of the SPARC M10-1.

```
root# ./sas2ircu 0 CREATE RAID1E MAX 2:2 2:3 2:4 RAID1E-VOL
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.
You are about to create an IR volume.
WARNING: Proceeding with this operation may cause data loss or data
        corruption. Are you sure you want to proceed (YES/NO)? YES
WARNING: This is your last chance to abort this operation. Do you wish
        to abort (YES/NO)? NO
Please wait, may take up to a minute...
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0         Volume 0 is now , enabled, inactive
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0         Volume 0 is now , enabled, active
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0         Volume 0 is now , enabled, active, data scrub
 in progress
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0         Volume 0 is now , enabled, active, background
 initialization in progress, data scrub in progress
Jan 20 16:20:15 1S-341-D0 scsi: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 16:20:15 1S-341-D0         Command failed to complete...Device is gone
SAS2IRCU: Volume created successfully.
SAS2IRCU: Command CREATE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

After adding a hardware RAID volume, check the hardware RAID volume and the disk drive information by executing the DISPLAY command of sas2ircu.
Check the following information.
(1): IR Volume information
  (1-1): Confirm that the new RAID volume (volume ID:285) is created as defined in the sas2ircu CREATE command, and the status of the RAID volume is "Okay (OKY)."
(2): Physical device information
  (2-1) (2-2) (2-3): Confirm that the status of the disk drives of disk slots 2, 3, and 4, which are newly incorporated into the RAID volume, is "Optimal (OPT)."

- Execution results of the DISPLAY command of sas2ircu (partial extract)

```
root# ./sas2ircu 0 DISPLAY
------------------------------------------------------------------------
IR Volume information   <-- (1)
------------------------------------------------------------------------
IR volume 1   <-- (1-1)
  Volume ID                             : 285
  Volume Name                           : RAID1E-VOL
  Status of volume                      : Okay (OKY)
  Volume wwid                           : 00c354402fc35418
  RAID level                            : RAID1E
  Size (in MB)                          : 856875
  Physical hard disks                   :
  PHY[0] Enclosure#/Slot#               : 2:2
  PHY[1] Enclosure#/Slot#               : 2:3
  PHY[2] Enclosure#/Slot#               : 2:4
IR volume 2
  Volume ID                             : 286
  Volume Name                           : RAID1-SYS
  Status of volume                      : Okay (OKY)
  Volume wwid                           : 0aa6d102f1bf517a
  RAID level                            : RAID1
  Size (in MB)                          : 571250
  Physical hard disks                   :
  PHY[0] Enclosure#/Slot#               : 2:0
  PHY[1] Enclosure#/Slot#               : 2:1
------------------------------------------------------------------------
Physical device information <-- (2)
------------------------------------------------------------------------
Device is a Hard disk   <-- (2-1)
  Enclosure #                           : 2
  Slot #                                : 2
  SAS Address                           : 5000039-4-281a-8ad2
  State                                 : Optimal (OPT)
  Size (in MB)/(in sectors)             : 572325/1172123567
  Manufacturer                          : TOSHIBA
  Model Number                          : MBF2600RC
  Firmware Revision                     : 3706
  Serial No                             : EA25PC7007G7
  GUID                                  : 50000394281a8ad0
  Protocol                              : SAS
```

```
   Drive Type                                 : SAS_HDD
Device is a Hard disk <-- (2-2)
  Enclosure #                                 : 2
  Slot #                                      : 3
  SAS Address                                 : 5000039-4-281b-5dc2
  State                                       : Optimal (OPT)
  Size (in MB)/(in sectors)                   : 572325/1172123567
  Manufacturer                                : TOSHIBA
  Model Number                                : MBF2600RC
  Firmware Revision                           : 3706
  Serial No                                   : EA25PC7007T3
  GUID                                        : 50000394281b5dc0
  Protocol                                    : SAS
  Drive Type                                  : SAS_HDD
Device is a Hard disk <-- (2-3)
  Enclosure #                                 : 2
  Slot #                                      : 4
  SAS Address                                 : 5000039-4-281b-58b2
  State                                       : Optimal (OPT)
  Size (in MB)/(in sectors)                   : 572325/1172123567
  Manufacturer                                : TOSHIBA
  Model Number                                : MBF2600RC
  Firmware Revision                           : 3706
  Serial No                                   : EA25PC7007RA
  GUID                                        : 50000394281b58b0
  Protocol                                    : SAS
  Drive Type                                  : SAS_HDD
```

F.4 Displaying the Configuration Status of a Hardware RAID Volume

Use the STATUS command of sas2ircu to display the configuration status of the created hardware RAID volume.

In the following examples, the configuration status of the newly created RAID volume (ID:285) is displayed. It indicates that the progress rate is 0.14% with the Background Init status.

Note - "Current Operation:Background Init" indicates that the RAID volume configuration is in process. When "Percentage complete" (progress rate) becomes 100%, it changes to "Current Operation:None," and the RAID volume can be used safely.

In the examples that follow, (1) to (2) indicate the following:
(1): RAID volume 1 information
   - RAID volume ID is 285
   - Current RAID operation is Background Init, and operation progress rate is 0.14%
   - RAID volume is enabled and optimized

(2): RAID volume 2 information
    - RAID volume ID is 286
    - No current RAID operation
    - RAID volume is enabled and optimized

```
root# ./sas2ircu 0 STATUS
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Background command progress status for controller 0...

IR Volume 1 <-- (1)
  Volume ID                             : 285
  Current operation                     : Background Init
  Volume status                         : Enabled
  Volume state                          : Optimal
  Volume wwid                           : 00c354402fc35418
  Physical disk I/Os                    : Not quiesced
  Volume size (in sectors)              : 1754880000
  Number of remaining sectors           : 1752440704
  Percentage complete                   : 0.14%

IR Volume 2 <-- (2)
  Volume ID                             : 286
  Current operation                     : None
  Volume status                         : Enabled
  Volume state                          : Optimal
  Volume wwid                           : 0aa6d102f1bf517a
  Physical disk I/Os                    : Not quiesced
SAS2IRCU: Command STATUS Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

F.5 Creating a Hot Spare of a Hardware RAID Volume

Use the HOTSPARE command of sas2ircu to create a hot spare of a hardware RAID volume.

In the following examples, a hot spare of a disk drive installed in disk slot 5 of SPARC M10-1 is created.

```
root# ./sas2ircu 0 HOTSPARE 2:5
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

WARNING: Proceeding with this operation may cause data loss or data
```

```
               corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
         to abort (YES/NO)? NO
Please wait, may take up to a minute...
SAS2IRCU: Hot Spare disk created successfully.
SAS2IRCU: Command HOTSPARE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

After creating a hot spare, check the following items by using the DISPLAY
command of sas2ircu.
(1) Physical device information
  (1-1) If the "State" of the disk drive of disk slot 5 is "HotSpare (HSP)"

- Execution results of the DISPLAY command of sas2ircu (partial extract)

```
root# ./sas2ircu 0 DISPLAY
------------------------------------------------------------------------
Physical device information <-- (1)
------------------------------------------------------------------------
Device is a Hard disk   <-- (1-1)
  Enclosure #                            : 2
  Slot #                                 : 5
  SAS Address                            : 5000039-4-281b-5022
  State                                  : Hot Spare (HSP)
  Size (in MB)/(in sectors)              : 572325/1172123567
  Manufacturer                           : TOSHIBA
  Model Number                           : MBF2600RC
  Firmware Revision                      : 3706
  Serial No                              : EA25PC7007LM
  GUID                                   : 50000394281b5020
  Protocol                               : SAS
  Drive Type                             : SAS_HDD
```

F.6   Deleting a Hot Spare of a Hardware RAID Volume

Use the HOTSPARE command of sas2ircu to delete a hot spare of a hardware RAID
volume.

In the following examples, a hot spare of a disk drive installed in disk slot 5 of
SPARC M10-1 is deleted.

```
root# ./sas2ircu 0 HOTSPARE DELETE 2:5
 LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.
```

```
WARNING: Proceeding with this operation may cause data loss or data
         corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
         to abort (YES/NO)? NO
SAS2IRCU: Hot Spare disk deleted successfully.
SAS2IRCU: Command HOTSPARE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

After deleting a hot spare, check the following items by using the DISPLAY command of sas2ircu.
(1) Physical device information
   (1-1) If the "State" of the disk drive of disk slot 5 is "Ready (RDY)"
   ▪ Execution results of the DISPLAY command of sas2ircu (partial extract)

```
root# ./sas2ircu 0 DISPLAY
------------------------------------------------------------------------
Physical device information <-- (1)
------------------------------------------------------------------------
Device is a Hard disk  <-- (1-1)
  Enclosure #                        : 2
  Slot #                             : 5
  SAS Address                        : 5000039-4-281b-5022
  State                              : Ready (RDY)
  Size (in MB)/(in sectors)          : 572325/1172123567
  Manufacturer                       : TOSHIBA
  Model Number                       : MBF2600RC
  Firmware Revision                  : 3706
  Serial No                          : EA25PC7007LM
  GUID                               : 50000394281b5020
  Protocol                           : SAS
  Drive Type                         : SAS_HDD
```

F.7   Deleting a Hardware RAID Volume

Use the DELETEVOLUME command of sas2ircu to delete a hardware RAID volume from the system.

The following example deletes the RAID volume with volume ID:285 on the SPARC M10.

```
root# ./sas2ircu 0 DELETEVOLUME 285
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

You are about to delete an existing RAID Volume on a controller. This command
will delete the specified RAID volume and associated HotSpare drive(s).
```

```
WARNING: Proceeding with this operation may cause data loss or data
         corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
         to abort (YES/NO)? NO
Please wait, may take up to a minute...
SAS2IRCU: Volume deleted successfully.
SAS2IRCU: Command DELETEVOLUME Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

After deleting a hardware RAID volume, check the hardware RAID volume and the disk drives items below by executing the DISPLAY command of sas2ircu.
(1) IR Volume information
  (1-1) If the RAID volume with volume ID:285 is deleted, and only volume ID:286 information exists
(2) Physical device information
  (2-1) (2-2) (2-3) If the "State" of the disk drives of disk slots 2, 3, and 4, which were incorporated as the RAID volume with deleted volume ID:285, is "Ready (RDY)"

- Execution results of the DISPLAY command of sas2ircu (partial extract)

```
root# ./sas2ircu 0 DISPLAY
------------------------------------------------------------------
IR Volume information  <-- (1)
------------------------------------------------------------------
IR volume 1   <-- (1-1)
  Volume ID                         : 286
  Volume Name                       : RAID1-SYS
  Status of volume                  : Okay (OKY)
  Volume wwid                       : 0aa6d102f1bf517a
  RAID level                        : RAID1
  Size (in MB)                      : 571250
  Physical hard disks               :
  PHY[0] Enclosure#/Slot#           : 2:0
  PHY[1] Enclosure#/Slot#           : 2:1
------------------------------------------------------------------
Physical device information  <-- (2)
------------------------------------------------------------------
Device is a Hard disk    <-- (2-1)
  Enclosure #                       : 2
  Slot #                            : 2
  SAS Address                       : 5000039-4-281a-8ad2
  State                             : Ready (RDY)
  Size (in MB)/(in sectors)         : 572325/1172123567
  Manufacturer                      : TOSHIBA
  Model Number                      : MBF2600RC
  Firmware Revision                 : 3706
  Serial No                         : EA25PC7007G7
  GUID                              : 50000394281a8ad0
  Protocol                          : SAS
  Drive Type                        : SAS_HDD
Device is a Hard disk  <-- (2-2)
```

```
   Enclosure #                            : 2
   Slot #                                 : 3
   SAS Address                            : 5000039-4-281b-5dc2
   State                                  : Ready (RDY)
   Size (in MB)/(in sectors)              : 572325/1172123567
   Manufacturer                           : TOSHIBA
   Model Number                           : MBF2600RC
   Firmware Revision                      : 3706
   Serial No                              : EA25PC7007T3
   GUID                                   : 50000394281b5dc0
   Protocol                               : SAS
   Drive Type                             : SAS_HDD
Device is a Hard disk  <-- (2-3)
   Enclosure #                            : 2
   Slot #                                 : 4
   SAS Address                            : 5000039-4-281b-58b2
   State                                  : Ready (RDY)
   Size (in MB)/(in sectors)              : 572325/1172123567
   Manufacturer                           : TOSHIBA
   Model Number                           : MBF2600RC
   Firmware Revision                      : 3706
   Serial No                              : EA25PC7007RA
   GUID                                   : 50000394281b58b0
   Protocol                               : SAS
   Drive Type                             : SAS_HDD
```

F.8   Identifying the Faulty Disk Drive of a Hardware RAID Volume

To identify the faulty hardware RAID volume and the faulty disk drive, use the DISPLAY command of sas2ircu.

In the following example, the disk drive of disk slot 1 of the SPARC M10-1 is faulty.

In the examples that follow, (1) to (2) indicate the following:
(1): RAID volume information
 (1-1): RAID volume 2 information
    You can obtain the following information (partial extract).
     - RAID volume ID is 286
     - RAID volume status is Degraded (Degraded (DGD))
     - RAID level is RAID1 (Mirroring)
     - Disk (2:0) of SPARC M12/M10 internal disk slot 0 is mounted in PHY[0] (Primary)
     - PHY[1] (Secondary) has no disk information (0:0)
(2): Physical device information
 (2-1): Status of disk drive (Drive Type=SAS_HDD) that has no information on
        installation location (Enclosure#:0,Slot#:0 = previously existed as Enclosure#:2,
        Slot#:1 but was not accessible when this command was executed)
            This indicates that the disk drive is out of order. (State:Failed (FLD))

```
root# ./sas2ircu 0 DISPLAY
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0
------------------------------------------------------------------------
Controller information
------------------------------------------------------------------------
  Controller type                        : SAS2308_2
  BIOS version                           : 0.00.00.00
  Firmware version                       : 13.00.66.00
  Channel description                    : 1 Serial Attached SCSI
  Initiator ID                           : 0
  Maximum physical devices               : 255
  Concurrent commands supported          : 3072
  Slot                                   : Unknown
  Segment                                : 0
  Bus                                    : 3
  Device                                 : 0
  Function                               : 0
  RAID Support                           : Yes

------------------------------------------------------------------------
IR Volume information <-- (1)
------------------------------------------------------------------------
IR volume 1
  Volume ID                              : 285
  Volume Name                            : RAID1E-VOL
  Status of volume                       : Okay (OKY)
  Volume wwid                            : 0fd4f41e8cd673de
  RAID level                             : RAID1E
  Size (in MB)                           : 856875
  Physical hard disks                    :
  PHY[0] Enclosure#/Slot#                : 2:2
  PHY[1] Enclosure#/Slot#                : 2:3
  PHY[2] Enclosure#/Slot#                : 2:4

IR volume 2 <-- (1-1)
  Volume ID                              : 286
  Volume Name                            : RAID1-SYS
  Status of volume                       : Degraded (DGD)
  Volume wwid                            : 0aa6d102f1bf517a
  RAID level                             : RAID1
  Size (in MB)                           : 571250
  Physical hard disks                    :
  PHY[0] Enclosure#/Slot#                : 2:0
  PHY[1] Enclosure#/Slot#                : 0:0

------------------------------------------------------------------------
Physical device information <-- (2)
------------------------------------------------------------------------
Initiator at ID #0

Device is a Hard disk <-- (2-1)
```

```
  Enclosure #                           : 0
  Slot #                                : 0
  SAS Address                           : 0000000-0-0000-0000
  State                                 : Failed (FLD)
  Manufacturer                          : TOSHIBA
  Model Number                          : MBF2600RC
  Firmware Revision                     : 3706
  Serial No                             : EA25PC700855
  GUID                                  : N/A
  Protocol                              : SAS
  Drive Type                            : SAS_HDD

Device is a Enclosure services device
  Enclosure #                           : 2
  Slot #                                : 0
  SAS Address                           : 500000e-0-e049-073d
  State                                 : Standby (SBY)
  Manufacturer                          : FUJITSU
  Model Number                          : NBBEXP
  Firmware Revision                     : 0d32
  Serial No                             : x3625413500
  GUID                                  : N/A
  Protocol                              : SAS
  Device Type                           : Enclosure services device

Device is a Hard disk
  Enclosure #                           : 2
  Slot #                                : 0
  SAS Address                           : 5000039-4-281b-6466
  State                                 : Optimal (OPT)
  Size (in MB)/(in sectors)             : 572325/1172123567
  Manufacturer                          : TOSHIBA
  Model Number                          : MBF2600RC
  Firmware Revision                     : 3706
  Serial No                             : EA25PC7007UE
  GUID                                  : 50000394281b6464
  Protocol                              : SAS
  Drive Type                            : SAS_HDD

Device is a Hard disk
  Enclosure #                           : 2
  Slot #                                : 2
  SAS Address                           : 5000039-4-281a-8ad2
  State                                 : Optimal (OPT)
  Size (in MB)/(in sectors)             : 572325/1172123567
  Manufacturer                          : TOSHIBA
  Model Number                          : MBF2600RC
  Firmware Revision                     : 3706
  Serial No                             : EA25PC7007G7
  GUID                                  : 50000394281a8ad0
  Protocol                              : SAS
  Drive Type                            : SAS_HDD

Device is a Hard disk
  Enclosure #                           : 2
```

```
   Slot #                                 : 3
   SAS Address                            : 5000039-4-281b-5dc2
   State                                  : Optimal (OPT)
   Size (in MB)/(in sectors)              : 572325/1172123567
   Manufacturer                           : TOSHIBA
   Model Number                           : MBF2600RC
   Firmware Revision                      : 3706
   Serial No                              : EA25PC7007T3
   GUID                                   : 50000394281b5dc0
   Protocol                               : SAS
   Drive Type                             : SAS_HDD

Device is a Hard disk
   Enclosure #                            : 2
   Slot #                                 : 4
   SAS Address                            : 5000039-4-281b-502e
   State                                  : Optimal (OPT)
   Size (in MB)/(in sectors)              : 572325/1172123567
   Manufacturer                           : TOSHIBA
   Model Number                           : MBF2600RC
   Firmware Revision                      : 3706
   Serial No                              : EA25PC7007LR
   GUID                                   : 50000394281b502c
   Protocol                               : SAS
   Drive Type                             : SAS_HDD
------------------------------------------------------------------------
Enclosure information
------------------------------------------------------------------------
   Enclosure#                             : 1
   Logical ID                             : 500000e0:e046ff10
   Numslots                               : 8
   StartSlot                              : 0
   Enclosure#                             : 2
   Logical ID                             : 500000e0:e049073f
   Numslots                               : 9
   StartSlot                              : 0
------------------------------------------------------------------------
SAS2IRCU: Command DISPLAY Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
root#
```

Note - The following message may be displayed on Oracle Solaris after operating a RAID volume to create or delete a RAID volume, delete a hot spare, etc. This indicates that there is no label information on the RAID volume or the disk drive. The RAID volume or the disk drive in this state cannot be used on Oracle Solaris. It will be usable on Oracle Solaris after executing the format command, selecting the appropriate RAID volume or disk drive, and labeling it.

- Example of output message

```
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0        Corrupt label; wrong magic number
```

■ Example of executing the format command

```
root@solaris:/root# format
Searching for disks...
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0        Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0        Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b58b0
(sd3):
Jan 20 15:55:07 1S-341-D0        Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b58b0
(sd3):
Jan 20 15:55:07 1S-341-D0        Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 15:55:07 1S-341-D0        Corrupt label; wrong magic number
Jan 20 15:55:08 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 15:55:08 1S-341-D0        Corrupt label; wrong magic number
done
c0t50000394281A8AD0d0: configured with capacity of 558.89GB
c0t50000394281B5DC0d0: configured with capacity of 558.89GB
c0t50000394281B58B0d0: configured with capacity of 558.89GB
AVAILABLE DISK SELECTIONS:
       0. c0t50000394281A8AD0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
          /scsi_vhci/disk@g50000394281a8ad0
          /dev/chassis/SYS/HDD02/disk
       1. c0t50000394281B5DC0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
          /scsi_vhci/disk@g50000394281b5dc0
          /dev/chassis/SYS/HDD03/disk
       2. c0t50000394281B58B0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
          /scsi_vhci/disk@g50000394281b58b0
          /dev/chassis/SYS/HDD04/disk
       3. c0t50000394281B5020d0 <LSI-Logical Volume-3000 cyl 24998 alt 2 hd 16
 sec 128>
          /scsi_vhci/disk@g50000394281b5020
          /dev/chassis/SYS/HDD05/disk
       4. c2t3AA6D102F1BF517Ad0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
 sec 557>
          /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3aa6d102f1bf517a,0
Specify disk (enter its number): 0
[disk formatted]
Disk not labeled.  Label it now? yes
```

Appendix G

SPARC M12-1/M10-1 XSCF Startup Mode Function

This appendix describes the XSCF startup mode function which can be used to reduce the startup time of SPARC M12-1/M10-1.

- Function Overview
- Restrictions and Notes
- Configuration Procedure

G.1 Function Overview

G.1.1 What is the XSCF Startup Mode Function?

The XSCF startup mode function has been introduced in XCP 2220 and later for SPARC M12-1/M10-1 systems.

The xscfstartupmode command is used to change the behavior of the XSCF at startup. The xscfstartupmode command allows the user to select "normal" (default) or "fast" mode.

The "fast" mode enables the SPARC M12-1/M10-1 system to automatically start the physical partition after the input power of the system is turned on (AC ON) and the XSCF has started. In "fast" mode, there is no need to enter the XSCF poweron command to start the physical partition.

For SPARC M12-1/M10-1 systems with XCP revisions prior to XCP 2220, or for SPARC M12-1/M10-1 systems with XCP 2220 or later and xscfstartupmode set to "normal" mode, the XSCF poweron command must be used to start the physical partition after the system is turned on (AC ON).

To start the physical partition automatically, set the startup mode to "fast", set the operation panel mode switch to "Locked" and turn on the input power of the system (AC ON). If the input power of the system is turned on (AC ON) when the operation panel mode switch is set to "Service", the startup mode reverts to "normal" and thus,

the physical partition is not automatically started.

To run in "normal" mode temporarily, set the operation panel mode switch to "Service" and turn on the input power (AC ON).

The XSCF startup mode function is specific to SPARC M12-1/M10-1 only and it is not supported on the M12-2/M12-2S/M10-4/M10-4S.

G.1.2 Conditions of Usage

The following conditions apply when using the XSCF startup mode function.

- If the startup mode is set to "fast" mode with the xscfstartupmode command, and the input power is turned on with the operation panel mode switch set to "Locked", the system will be started in the "fast" mode. However, even if the startup mode is changed to "fast", if the operation panel mode switch is changed from "Service" to "Locked" after the input power has been turned on, the system will be started in "normal" mode, not "fast" mode.

- When the startup mode is changed to "fast," a reboot of the XSCF does not cause the physical partition to start automatically. Automatic activation of the physical partition operates only when the input power is turned on.

- The startup mode of the system cannot be changed only by executing the rebootxscf command after changing the configuration of the startup mode. Turning off/on the input power is necessary to make the changed startup mode setting effective.

- The configuration of the startup mode is saved in the XSCF on the motherboard unit (MBU), but internal backup to the PSU backplane unit (PSUBP) is not performed. If the MBU is replaced, the startup mode may change to the default setting. After MBU replacement, make sure to check the startup mode and, if necessary, change the startup mode to the desired setting.

- When the system is started in the "fast" mode, do not change the configuration of XSCF or perform degradation/restoration, or configure the environment parameters of the OpenBoot PROM, or save the configuration information of logical domains. Perform these operations only in the "normal" mode. If you perform the above operations when the system had been started in the "fast" mode, the configurations and changes will be saved to the XSCF on the MBU, but internal backup to the PSUBP is not performed. If the MBU is replaced, the configuration information will not be recovered from the PSUBP internal backup, and the system may not be able to start.

In addition to the XSCF startup mode function "fast" setting, the time taken from applying input power to the system to the start of Oracle Solaris/Oracle VM Server for SPARC can be further reduced by:

- Using Solid State drive (SSD) internal storage as boot devices (rather than SAS disks)

- Setting the POST diagnosis level to off (from the default of min)

Note - When changing the POST diagnosis level, be sure to change the setting after confirming the contents of "G.2.2   Restrictions and Notes at the Time of System Operation."

G.2 Restrictions and Notes

G.2.1 Restrictions and Notes at the Time of System Installation

- System installation operations must be performed in XSCF startup mode "normal", and then the XSCF startup mode can be changed to "fast". The startup mode status can be referenced using the xscfstartupmode -d command described in "G.3 Configuration Procedure." The system hardware configuration information and XSCF configuration information are saved only to the XSCF (no internal back up is performed) when the XSCF startup mode is "fast". If there is a difference between the information stored inside the XSCF and the system hardware information, problems like XSCF process down and inability of the physical partitions to function properly may occur.

- If the system is configured to perform scheduled power operations using the setpowerschedule command, and the startup mode is set to "fast", the system will be started in the "fast" mode at the scheduled time.

- If power recovery is set to either "off" or "auto" with the setpowerschedule command, and the startup mode is set to "fast", the system will ignore the "off" or "auto" settings and will start in the "fast" mode when the input power is applied (AC ON).

G.2.2 Restrictions and Notes at the Time of System Operation

- In XSCF startup mode "fast", telnet/ssh user logins to XSCF are limited to a maximum of 10.

- The xscfstartupmode command itself will not be audited, but other auditing is not affected by the XSCF startup mode setting.

- When the physical partition is started in the "fast" mode, "power recover" is registered in the "Cause" field of the XSCF power log.

- If the POST diagnosis level is set to "off", CPU, memory, and I/O diagnosis by POST is not executed during physical partition power on. Therefore, except for the case where POST itself ceases to function, detection of abnormalities and consequent degradation of faulty components during POST diagnosis is not executed. Instead, "Hypervisor Abort" or "OS PANIC" may occur at the time the CPU, memory, or I/O abnormality is detected.

- If the POST diagnosis level is set to "min/max", CPU, memory, and I/O diagnosis is executed but the startup time increases in proportion to the time taken for the diagnosis operation.

- When changing the configuration information of XSCF, do so after starting XSCF in the "normal" startup mode. To run in "normal" mode temporarily, set the operation panel mode switch to "Service," turn off/on the input power to reboot XSCF and then change the configuration information of XSCF.

- When creating or changing the configuration information of logical domains, do so after starting XSCF in the "normal" startup mode. To run in "normal" mode temporarily, set the operation panel mode switch to "Service," turn off/on the input power to reboot XSCF and then create or change the configuration information of the logical domains while the physical partition is running, and make sure to execute the "ldm add-spconfig" command to save the logical domain configuration information to the XSCF.

G.2.3   Restrictions at the Time of Maintenance

- Hardware failures can be confirmed by the failure marks (denoted by "*") in the output produced by either the showhardconf or the showstatus XSCF commands. When the startup mode is set to "fast" and a hardware failure has been detected in the system, if the input power is turned off/on even once, all of the failure marks (denoted by "*") for the failed parts are cleared at the next system startup. Before replacing the failed parts, note the failure information with either the showhardconf or the showstatus XSCF commands. And then, refer to the FRU information in the error logs to replace the parts.

- When saving or restoring configuration information with the dumpconfig or the restoreconfig command, do so after starting XSCF in the "normal" mode. To run in "normal" mode temporarily, set the operation panel mode switch to "Service," turn off/on the input power to reboot XSCF and then execute these operations.

- The startup mode configuration setting is not included in the saved or restored information derived by using either the dumpconfig or the restoreconfig XSCF commands. Therefore, the startup mode should be reset after restoring the configuration information with the restoreconfig command following the replacement of the MBU. If the restoreconfig command is executed on a system on which the MBU had not been replaced, it does not remove the existing configuration information.

- Hardware cannot be replaced with the replacefru command when the system is started in "fast" mode. Replace hardware with the input power turned off. After that, set the operation panel mode switch to "Service" and turn on the input power and wait until XSCF has started. In this way the hardware configuration information and XSCF setup information is saved inside XSCF. After XSCF has started, turn off the input power and set the operation panel mode switch to "Locked". When the input power is then turned on, the system starts in "fast" mode.

- The startup mode is not initialized when the system is initialized to factory defaults using the restoredefaults XSCF command. Make sure to change the startup mode to "normal" and turn off/on the input power before executing the restoredefaults command.

- When updating XSCF firmware, do so after starting XSCF in "normal" mode.

G.3 Configuration Procedure

This section describes the flow to configure the XSCF startup mode function.

1. **Perform installation tasks like updating firmware, configuring XSCF network(s) and users, activating CPU cores, etc.**
   For details, see the latest *Product Notes* for your server.

Note - Do not set the startup mode to "fast" when performing system installation.

Note - XSCF startup mode is supported from XCP 2220 onwards. If the system firmware is older than XCP 2220, follow manuals or product notes to procure and update the system firmware.

---

2. **Turn on input power to the physical partition.**
   a. Confirm that the configuration information of the logical domains is "factory defaults" with the showdomainconfig command.
   b. Execute the poweron command to start the physical partition.

Note - Do not set the startup mode to "fast" when performing system installation.

---

3. **Install software like Oracle Solaris or Oracle VM Server for SPARC etc., and/or configure logical domains.**
   Regarding software installation, refer to "4.5 Connecting a DVD Drive." For details on how to configure logical domains, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide*.

Note - Do not set the startup mode to "fast" when performing system installation.

Note - If the configuration information of logical domains has been created, make sure to save this information to the XSCF by executing the "ldm add-spconfig" command.

---

4. **Use the poweroff command to power off the physical partition.**

5. **Set the XSCF startup mode to "fast" mode.**
   a. Login to XSCF with the "platadm" user privilege.
   b. Check the present value of the startup mode.
      For details on the xscfstartupmode(8) command, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

```
XSCF> xscfstartupmode -d
Setting Mode: normal
Current Mode: normal
```

   c. Set the startup mode to "fast".

```
XSCF> xscfstartupmode -m fast
```

    d. Confirm that the startup mode has been set to "fast".

```
XSCF> xscfstartupmode -d
Setting Mode: fast [need AC OFF/ON]
Current Mode: normal
```

6. **Set the POST diagnosis level to "OFF"** (when optionally electing to skip POST diagnosis during power on in order to further reduce the system startup time).
    a. Check the present POST diagnosis level.

```
XSCF> showpparmode -p 0
Host-ID                 :9007002b
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
Elastic Mode            :off
IOreconfigure           :false
CPU Mode                :auto
PPAR DR(Current)        :-
PPAR DR(Next)           :off
```

    b. Set the POST diagnosis level to "OFF".

```
XSCF> setpparmode -p 0 -m diag=off
```

    c. Confirm the state of POST diagnosis level.

```
XSCF> showpparmode -p 0
Host-ID                 :9007002b
Diagnostic Level        :off
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
Elastic Mode            :off
IOreconfigure           :false
CPU Mode                :auto
PPAR DR(Current)        :-
PPAR DR(Next)           :off
```

7. **Turn off the input power.**

8. **Set the operation panel mode switch to "Locked".**

9. **Turn on the input power to start the physical partition.**

10. **Confirm that the startup mode had been set to "fast".**
    For details on the xscfstartupmode(8) command, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

```
XSCF> xscfstartupmode -d
Setting Mode: fast
Current Mode: fast
```

Appendix H

OpenBoot PROM Environment Variables and Commands

This appendix describes OpenBoot PROM commands that are SPARC M12/M10 system-specific, OpenBoot PROM environment variables and commands that are not supported by the SPARC M12/M10 systems, and the behavior with the security mode enabled.

For details on matters not described in this appendix, see the eeprom command explanation in the reference manual of Oracle Solaris and the *OpenBoot 4.x Command Reference Manual* of Oracle Corporation.

- SCSI Device Display
- Unsupported OpenBoot PROM Environment Variables
- Unsupported OpenBoot PROM Commands
- Behavior With the Security Mode Enabled

H.1 SCSI Device Display

To display all devices on the SCSI bus, use the probe-scsi-all command.

```
{0} ok probe-scsi-all
```

H.2 Unsupported OpenBoot PROM Environment Variables

In the SPARC M12/M10 systems, the following OpenBoot PROM environment variables cannot be used.

- diag-device
- diag-file

- diag-level
- os-root-device

To set/display the Power-On Self-Test (POST) diagnosis level appropriate for diag-level, use the setpparmode command or showpparmode command of XSCF firmware.

H.3 Unsupported OpenBoot PROM Commands

In the SPARC M12/M10 systems, the following OpenBoot PROM commands cannot be used.

- cache-off
- cache-on
- callback
- clear-cache
- ecdata!
- ecdata@
- ectag!
- ectag@
- eject floppy
- firmware-version
- flush-cache
- help dump
- iomap?
- iomap-page
- iomap-pages
- iopgmap@
- iopgmap!
- map-region
- map-segments
- obdiag
- pgmap?
- rmap!
- rmap@
- sbus
- segmentsize
- smap!

- smap?
- smap@
- test-all
- .ver
- %f0 to %f31

H.4 Behavior With the Security Mode Enabled

When security-mode of the OpenBoot PROM environment variable is set to "command" or "full" and a displayable character string with one to eight characters is set as security-password, the security mode of OpenBoot PROM is enabled and the password is required for commands and operations.

(1) When security-mode is set to "command"

The boot command and the go command does not require the password but all other commands require the password. Note that the system boots automatically when "auto-boot? = true" is specified.

(2) When security-mode is set to "full"

Any actions including ordinary operations such as the boot command require password to be executed except the go command. The password is required at the start of booting even when "auto-boot? = true" is specified.

When the security mode is enabled, the prompt of OpenBoot PROM changes from "ok" to the security prompt mode with > triggered by either of the following and the password is required for the cases (1) and (2) above.

- The logout command is executed.
- The domain console is disconnected and reconnected while OpenBoot PROM is in operation (in XCP 2340 or later).
- A break signal is sent.
- The domain is restarted.
- An error occurred while an OpenBoot PROM command is running.

For details of security-mode of the OpenBoot PROM environment variable, see the manual from Oracle.

Appendix I

How to Specify the Boot Device

This appendix describes how to specify internal storage as the boot device on the OpenBoot PROM of a logical domain in the SPARC M12/M10 system.

- Device Path of the Internal Storage
- Method of Specification With a PHY Number
- Method of Specification With a Target ID
- Method of Specification With an SAS Address
- Method of Specification With a Volume Device Name

I.1   Device Path of the Internal Storage

To specify internal storage as the boot device, append information for identifying the disk to the end of the device path name of the internal storage. The device path of the internal storage varies depending on the model or the number of CPUs mounted. For details, see "Appendix A   Lists of SPARC M12/M10 System Device Paths."

There are four methods of identifying internal storage, that is, specifying internal storage as the boot device. Table I-1 describes these four methods. Note that the methods of specification that can be used differs between a standalone built-in hard disk and a built-in hardware RAID.

Table I-1   Methods of Specifying Storage as the Boot Device

Method of Specification	Summary	Applicable Internal Storage Type
With a PHY number	This specification method uses the PHY number corresponding to the disk slot where the built-in hard disk is installed. This method is also used as devalias on OpenBoot PROM.	Standalone hard disk
With a target ID	This specification method uses the target ID uniquely assigned to the built-in hard disk. The target ID may vary depending on the disk installation order.	Standalone hard disk
With an SAS address	This specification method uses the SAS address uniquely assigned to the built-in hard disk. The SAS address is changed when the disk is replaced.	Standalone hard disk
With a volume device name	This specification method uses the hardware RAID volume name.	Hardware RAID

I.2   Method of Specification With a PHY Number

This method uses the PHY number corresponding to the mounting slot of a built-in disk to identify the disk used as a boot device.

You can use this specification method when specifying a standalone built-in hard disk as a boot device. However, you cannot use it to specify a built-in hardware RAID.

Table I-2 lists the PHY numbers corresponding to disk slots.

Table I-2   PHY Numbers Corresponding to Disk Slots

Disk Slot	PHY Number
Built-in disk slot #0	100 or 0
Built-in disk slot #1	101 or 1
Built-in disk slot #2	102 or 2
Built-in disk slot #3	103 or 3
Built-in disk slot #4	104 or 4
Built-in disk slot #5	105 or 5
Built-in disk slot #6	106 or 6
Built-in disk slot #7	107 or 7

To find the PHY number of the boot disk, execute the probe-scsi-all command on

OpenBoot PROM, and check the PhyNum value.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
  Target a
  Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
  SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
                                                                    PHY number
  Target b
  Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
  SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
  Target e
  Unit 0 Encl Serv device FUJITSU BBEXP 0d32
  SASAddress 500000e0e06d233d PhyNum 14
```

Boot Device Notation

```
<Device path of the SAS controller>/disk@pX,Y:Z
```

Here, specify the PHY number corresponding to the mounting disk slot, for the X after "disk@p". Furthermore, specify the logical unit number (LUN) and slice number of the internal storage, for Y and Z, respectively.

Note - You can omit the logical unit number (LUN) and slice number. If omitted, LUN "0" and slice number "a" are assumed specified. If internal storage is used as the boot device, LUN "0" and slice number "a" are specified, so these numbers have the same values as when omitted. Therefore, in the use example, the notation is in a form that omits the LUN and slice number.

Use Example

Specify the following, where "0" is the PHY number of the boot disk.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0
```

I.3 Method of Specification With a Target ID

This method uses the target ID uniquely assigned to each disk to identify the disk used as a boot device.

You can use this specification method when specifying a standalone built-in hard

disk as a boot device. However, you cannot use it to similarly specify a built-in hardware RAID.

To find the target ID of the boot disk, execute the probe-scsi-all command on OpenBoot PROM, and check the Target value.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
  Target a
          Target ID
  Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
  SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
  Target b
  Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
  SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
  Target e
  Unit 0 Encl Serv device FUJITSU BBEXP 0d32
  SASAddress 500000e0e06d233d PhyNum 14
```

Boot Device Notation

```
<Device path of the SAS controller>/disk@X,Y:Z
```

Here, specify the target ID for the *X* after "disk@". Furthermore, specify the logical unit number (LUN) and slice number of the internal storage, for *Y* and *Z*, respectively.

Note - You can omit the logical unit number (LUN) and slice number. If omitted, LUN "0" and slice number "a" are assumed specified. If internal storage is used as the boot device, LUN "0" and slice number "a" are specified, so these numbers have the same values as when omitted. Therefore, in the use example, the notation is in a form that omits the LUN and slice number.

Use Example

Specify the following, where "a" is the target ID of the boot disk.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@a
```

I.4   Method of Specification With an SAS Address

This specification method uses the unique SAS address of a disk drive to specify the

boot device.

For internal storage, each disk drive has a uniquely assigned SAS address, with the SAS address changed when the disk is replaced. After disk replacement, the device name specified at the boot time changes as a result.

You can use this specification method when specifying a standalone built-in hard disk as a boot device. However, you cannot use it to similarly specify a built-in hardware RAID.

To find the SAS address of the boot disk, execute the probe-scsi-all command on OpenBoot PROM, and check the SASAddress value.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
  Target a
  Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
  SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
                                              SAS address
  Target b
  Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
  SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
  Target e
  Unit 0 Encl Serv device FUJITSU BBEXP 0d32
  SASAddress 500000e0e06d233d PhyNum 14
```

Boot Device Notation

```
<Device path of the SAS controller>/disk@wXXXXXXXX,Y:Z
```

Here, specify the SAS address for the *XXXXXXXX* after "disk@w". Furthermore, specify the logical unit number (LUN) and slice number of the internal storage, for *Y* and *Z*, respectively.

Note - You can omit the logical unit number (LUN) and slice number. If omitted, LUN "0" and slice number "a" are assumed specified. If internal storage is used as the boot device, LUN "0" and slice number "a" are specified, so these numbers have the same values as when omitted. Therefore, in the use example, the notation is in a form that omits the LUN and slice number.

Use Example

Specify the following, where "50000393d82891d2" is the SAS address of the boot disk.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@w50000393d82891d2
```

I.5   Method of Specification With a Volume Device Name

This specification method uses the volume device name of a built-in hardware RAID to specify the boot device. The volume device name is assigned to each volume configured in the RAID.

You can use this method when specifying a built-in hardware RAID as a boot device.

To find the volume device name of the boot disk, execute the probe-scsi-all command on OpenBoot PROM, and check the VolumeDeviceName value.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
  Target 11e Volume 0
  Unit 0 Disk LSI Logical Volume 3000 10485760 Blocks, 5368 MB
  VolumeDeviceName 3eb2fdbd4c32058f VolumeWWID 0eb2fdbd4c32058f
                   Volume device name
```

In XCP 2070 and earlier, VolumeDeviceName may not be output. In this case, execute the show-volumes command, which will output a volume WWID. Replace the first WWID character with "3" to get the volume device name.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
Name raid1-volume WWID 0eb2fdbd4c32058f
                       WWID of the RAID volume
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
Disk 1
  Primary Optimal
  Target a TOSHIBA MBF2300RC 3706
Disk 0
  Secondary Optimal
  Target b TOSHIBA MBF2300RC 3706
{0} ok
```

Boot Device Notation

```
<Device path of the SAS controller>/disk@wXXXXXXXX,Y:Z
```

Here, specify the volume device name for the *XXXXXXXX* after "disk@w". Furthermore, specify the logical unit number (LUN) and slice number of the built-in hardware RAID, for *Y* and *Z*, respectively.

> **Note -** You can omit the logical unit number (LUN) and slice number. If omitted, LUN "0" and slice number "a" are assumed specified. If a built-in hardware RAID is used as a boot device, LUN "0" and slice number "a" are specified, so these numbers have the same values as when omitted. Therefore, in the use example, the notation is in a form that omits the LUN and slice number.

Use Example

Specify the following, where "3eb2fdbd4c32058f" is the volume device name of the boot device.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@w3eb2fdbd4c32058f
```

Appendix J

Lists of DVD Drive Aliases

This appendix describes the aliases of DVD drives.

- External DVD Drive Aliases
- Remote Storage DVD Drive Aliases

J.1 External DVD Drive Aliases

This section lists the aliases of external DVD drives in SPARC M12/M10 systems.

J.1.1 SPARC M12-1 External DVD Drive Aliases

Table J-1   SPARC M12-1 External DVD Drive Aliases

Alias	Device Path
cdrom (front)	/pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk@0 (USB2.0/1.1)
cdrom0-30 (rear)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom0 (rear)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom1 (front)	/pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk@0 (USB2.0/1.1)

J.1.2　SPARC M12-2 External DVD Drive Aliases

For a 1-CPU (CMUL) or 2-CPU Configuration at Initial Installation

Table J-2　SPARC M12-2 External DVD Drive Aliases (Initial Installation Time: 1 CPU or 2 CPUs)

Alias	Device Path
cdrom (front)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom00-0-30 (rear)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom00-0 (rear)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom00-1 (front)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

J.1.3　SPARC M12-2S External DVD Drive Aliases

For a 1-CPU (CMUL) or 2-CPU Configuration at Initial Installation

Table J-3　SPARC M12-2S External DVD Drive Aliases (Initial Installation Time: 1 CPU or 2 CPUs)

Alias	Device Path
cdrom (front)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom00-0-30 (rear)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom00-0 (rear)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom00-1 (front)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom01-0-30 (rear)	/pci@8900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom01-0 (rear)	/pci@8900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom01-1 (front)	/pci@8900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom02-0-30 (rear)	/pci@9100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)

Alias	Device Path
cdrom02-0 (rear)	/pci@9100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom02-1 (front)	/pci@9100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom03-0-30 (rear)	/pci@9900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom03-0 (rear)	/pci@9900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom03-1 (front)	/pci@9900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom04-0-30 (rear)	/pci@a100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom04-0 (rear)	/pci@a100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom04-1 (front)	/pci@a100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom05-0-30 (rear)	/pci@a900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom05-0 (rear)	/pci@a900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom05-1 (front)	/pci@a900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom06-0-30 (rear)	/pci@b100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom06-0 (rear)	/pci@b100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom06-1 (front)	/pci@b100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom07-0-30 (rear)	/pci@b900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom07-0 (rear)	/pci@b900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom07-1 (front)	/pci@b900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom08-0-30 (rear)	/pci@c100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom08-0 (rear)	/pci@c100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom08-1 (front)	/pci@c100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

Table J-3   SPARC M12-2S External DVD Drive Aliases (Initial Installation Time: 1 CPU or 2 CPUs) *(continued)*

Alias	Device Path
cdrom09-0-30 (rear)	/pci@c900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom09-0 (rear)	/pci@c900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom09-1 (front)	/pci@c900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom10-0-30 (rear)	/pci@d100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom10-0 (rear)	/pci@d100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom10-1 (front)	/pci@d100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom11-0-30 (rear)	/pci@d900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom11-0 (rear)	/pci@d900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom11-1 (front)	/pci@d900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom12-0-30 (rear)	/pci@e100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom12-0 (rear)	/pci@e100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom12-1 (front)	/pci@e100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom13-0-30 (rear)	/pci@e900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom13-0 (rear)	/pci@e900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom13-1 (front)	/pci@e900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom14-0-30 (rear)	/pci@f100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom14-0 (rear)	/pci@f100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom14-1 (front)	/pci@f100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom15-0-30 (rear)	/pci@f900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom15-0 (rear)	/pci@f900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@6/disk@0 (USB2.0/1.1)

Alias	Device Path
cdrom15-1 (front)	/pci@f900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

J.1.4   SPARC M10-1 External DVD Drive Aliases

Table J-4   SPARC M10-1 External DVD Drive Aliases

Alias	Device Path
cdrom (front)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk@0
cdrom0 (rear)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk@0
cdrom1 (front)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk@0

J.1.5   SPARC M10-4 External DVD Drive Aliases

For a 2-CPU (CMUL) or 4-CPU Configuration at Initial Installation

Table J-5   SPARC M10-4 External DVD Drive Aliases (Initial Installation Time: 2 CPUs or 4 CPUs)

Alias	Device Path
cdrom (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom00-0 (rear)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom00-1 (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

J.1.6   SPARC M10-4S External DVD Drive Aliases

Table J-6 lists the aliases of the external DVD drives, where the logical system boards (LSBs) are numbered 0 to 15.

For a 2-CPU (CMUL) or 4-CPU Configuration at Initial Installation

Table J-6   SPARC M10-4S External DVD Drive Aliases (Initial Installation Time: 2 CPUs or 4 CPUs)

Alias	Device Path
cdrom (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

Table J-6   SPARC M10-4S External DVD Drive Aliases (Initial Installation Time: 2 CPUs or 4 CPUs) *(continued)*

Alias	Device Path
cdrom00-0 (rear)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom00-1 (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom01-0 (rear)	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom01-1 (front)	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom02-0 (rear)	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom02-1 (front)	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom03-0 (rear)	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom03-1 (front)	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom04-0 (rear)	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom04-1 (front)	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom05-0 (rear)	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom05-1 (front)	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom06-0 (rear)	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom06-1 (front)	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom07-0 (rear)	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom07-1 (front)	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom08-0 (rear)	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom08-1 (front)	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom09-0 (rear)	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom09-1 (front)	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom10-0 (rear)	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom10-1 (front)	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom11-0 (rear)	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom11-1 (front)	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom12-0 (rear)	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom12-1 (front)	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom13-0 (rear)	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom13-1 (front)	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom14-0 (rear)	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom14-1 (front)	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom15-0 (rear)	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom15-1 (front)	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

J.2 Remote Storage DVD Drive Aliases

This section lists the aliases of remote storage DVD drives in SPARC M12/M10 systems.

J.2.1 SPARC M12-1 Remote Storage DVD Drive Aliases

Table J-7   SPARC M12-1 Remote Storage DVD Drive Aliases

Alias	Device Path
rcdrom	/pci@8100/pci@4/pci@0/pci@8/usb@0/storage@7/disk@0

J.2.2 SPARC M12-2 Remote Storage DVD Drive Aliases

For a 1-CPU (CMUL) or 2-CPU Configuration at Initial Installation

Table J-8   SPARC M12-2 Remote Storage DVD Drive Aliases (Initial Installation Time: 1 CPU or 2 CPUs)

Alias	Device Path
rcdrom	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom00	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

J.2.3 SPARC M12-2S Remote Storage DVD Drive Aliases

For a 1-CPU (CMUL) or 2-CPU Configuration at Initial Installation

Table J-9   SPARC M12-2S Remote Storage DVD Drive Aliases (Initial Installation Time: 1 CPU or 2 CPUs)

Alias	Device Path
rcdrom	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom00	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom01	/pci@8900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom02	/pci@9100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

Table J-9   SPARC M12-2S Remote Storage DVD Drive Aliases (Initial Installation Time: 1 CPU or 2 CPUs)
(continued)

Alias	Device Path
rcdrom03	/pci@9900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom04	/pci@a100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom05	/pci@a900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom06	/pci@b100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom07	/pci@b900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom08	/pci@c100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom09	/pci@c900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom10	/pci@d100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom11	/pci@d900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom12	/pci@e100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom13	/pci@e900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom14	/pci@f100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom15	/pci@f900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

J.2.4   SPARC M10-1 Remote Storage DVD Drive Aliases

Table J-10   SPARC M10-1 Remote Storage DVD Drive Aliases

Alias	Device Path
rcdrom	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3/disk@0

J.2.5   SPARC M10-4 Remote Storage DVD Drive Aliases

For a 2-CPU (CMUL) or 4-CPU Configuration at Initial Installation

Table J-11   SPARC M10-4 Remote Storage DVD Drive Aliases (Initial Installation Time: 2 CPUs or 4 CPUs)

Alias	Device Path
rcdrom	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom00	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

J.2.6 SPARC M10-4S Remote Storage DVD Drive Aliases

Table J-12 lists the aliases of the DVD drives for remote storage, where the logical system boards (LSBs) are numbered 0 to 15.

For a 2-CPU (CMUL) or 4-CPU configuration at initial installation

Table J-12   SPARC M10-4S Remote Storage DVD Drive Aliases (Initial Installation Time: 2 CPUs or 4 CPUs)

Alias	Device Path
rcdrom	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom00	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom01	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom02	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom03	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom04	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom05	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom06	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom07	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom08	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom09	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom10	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom11	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom12	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom13	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom14	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom15	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

Appendix K

CPU Activation Interim Permit

This appendix describes the CPU Activation Interim Permit. The use of a CPU Activation Interim Permit allows, before adding and obtaining a sufficient number of CPU Activations, the use of additional CPU core resources.

- What is the CPU Activation Interim Permit?
- Terms of Use of the CPU Activation Interim Permit and Precautions
- Related Commands
- Flows and Procedures for Using a CPU Activation Interim Permit
- Event Notification of the CPU Activation Interim Permit
- Other Important Notes

K.1 What is the CPU Activation Interim Permit?

CPU Activation is a SPARC M12/M10 feature that allows you to optimize your operation.

By registering additional CPU Activation keys with your SPARC M12/M10, additional CPU cores can be added dynamically without interrupting your production workloads. This SPARC M12/M10 feature allows you to optimize your server investment.

But, the process to purchase a CPU Activation may take longer than one day, though you might need the additional CPU core resources now. The SPARC M12/M10 feature of CPU Activation Interim Permit solves this problem.

To enable a CPU Activation Interim Permit, you do not need to add a CPU Activation key. Once the CPU Activation Interim Permit is enabled, all available physical cores in the physical partition (PPAR) or the SPARC M12/M10 can be used for 30 days.

The CPU Activation Interim Permit enables you to immediately use required CPU core resources even when no additional purchased CPU Activation keys are at hand.

K.2 Terms of Use of the CPU Activation Interim Permit and Precautions

You can use a CPU Activation Interim Permit by executing the commands of the XSCF firmware. Table K-1 shows the required XCP firmware versions for each system to use a CPU Activation Interim Permit. The listed version of firmware in Table K-1 must be installed on your system to use a CPU Activation Interim Permit.

Table K-1   Supported Models for the CPU Activation Interim Permit

Model	XCP Version	Terms of Use
SPARC M10-1/M10-4 (*1)	XCP 232x	A CPU Activation Interim Permit can be used only once for the SPARC M10-1/M10-4. (*2)
	XCP 2330 or later	A CPU Activation Interim Permit can be used more than once, with certain conditions. (*3)
SPARC M12-1/M12-2/M12-2S/M10-4S	XCP 2330 or later	A CPU Activation Interim Permit can be used for each PPAR. A CPU Activation Interim Permit can be used more than once, with certain conditions. (*3)

*1 The SPARC M10-1 and SPARC M10-4 support a CPU Activation Interim Permit with XCP 2320 and later. However, we recommend using a CPU Activation Interim Permit with XCP 2330 or later, which allows you to re-enable a CPU Activation Interim Permit under the appropriate conditions.

*2 Once you have used the CPU Activation Interim Permit, you cannot use the function again, even after updating to XCP 2330 or later.

*3 To use the CPU Activation Interim Permit more than once, you must first register additional purchased CPU Activation keys and make settings to add purchased CPU Activations to the physical partition (for the SPARC M12-2S/M10-4S) or to the system (for the SPARC M12-1/M12-2/M10-1/M10-4). If the registration of additional purchased CPU Activations and the settings to assign additional CPU core resources to the physical partition (for the SPARC M12-2S/M10-4S) or to the system (for the SPARC M12-1/M12-2/M10-1/M10-4) have not been performed since the CPU Activation Interim Permit was last enabled, you cannot enable the CPU Activation Interim Permit again. For details, see "Enabling a CPU Activation Interim Permit More Than Once."

Precautions

- A CPU Activation Interim Permit can be used for 30 days. Make sure to add the already purchased CPU Activation key within this period. If the CPU Activation Interim Permit expires while the number of CPU cores used by Oracle VM Server for SPARC is equal to or greater than the quantity under the installed purchased CPU Activations, Oracle VM Server for SPARC deletes excess CPU cores automatically.

- When the CPU Activation Interim Permit is enabled, all the CPU cores in the system (a physical partition in the case of the SPARC M12-2S/M10-4S) are enabled. Therefore, the CPU automatic replacement function does not operate when a CPU core failure occurs.

- The license costs of some types of software vary depending on the number of CPU cores used. Confirm the license terms of the software when adding CPU cores through the use of a CPU Activation Interim Permit.

K.3   Related Commands

This section describes commands related to the CPU Activation Interim Permit.

K.3.1   Commands for Using a CPU Activation Interim Permit

Table K-2 lists XSCF commands for using a CPU Activation Interim Permit.

Table K-2   XSCF Commands for the CPU Activation Interim Permit

Use	Command
To enables/disable a CPU Activation Interim Permit	setinterimpermit(8)
To display the setting information/status of a CPU Activation Interim Permit	showinterimpermit(8)
CPU core usage of a CPU Activation Interim Permit	showinterimpermitusage(8) (*1)

*1 XCP 232x does not support the showinterimpermitusage(8) command.

For details on each command, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

K.3.2   Related Commands When Using a CPU Activation Interim Permit

The following commands are used to manage (register/delete) purchased CPU Activations or to display the status of CPU cores. They are also used as needed during the use of a CPU Activation Interim Permit.

- addcodactivation
- deletecodactivation
- showcodactivation
- setcod
- showcod
- showcodusage
- showcodactivationhistory

These commands do not display the settings of the CPU Activation Interim Permit and the usage status of temporary CPU core resources available when the CPU

Activation Interim Permit is enabled.

While CPU Activation Interim Permit is enabled, CPU Activation keys are not used for managing CPU core resources (checking whether a use violation occurs). Even in that case, however, you can change the number of CPU cores assigned to the system by adding or deleting CPU Activation keys in preparation for the expiration of the CPU Activation Interim Permit.

To check when a CPU Activation Interim Permit was enabled or disabled, check the XSCF event log by executing the showlogs event command of the XSCF.

K.4 Flows and Procedures for Using a CPU Activation Interim Permit

This section describes flows and procedures for using a CPU Activation Interim Permit. Before using a CPU Activation Interim Permit, carefully read the descriptions of the flows and procedures in this section.

This section also describes the case where the validity period elapses when CPU cores are used with the CPU Activation Interim Permit enabled and the case where the CPU Activation Interim Permit is disabled.

K.4.1 Flow and Procedure for XCP 2330 and Later

Operation Flow for XCP 2330 and Later

The operation flow is as follows.

1. **Confirm that additional CPU cores are required, and start the process of purchasing required CPU Activations.**
2. **Enable a CPU Activation Interim Permit.**
3. **Register the obtained CPU Activation keys with the system.**
4. **Disable the CPU Activation Interim Permit.**

Configuration Example

The description in "Operation Procedure for XCP 2330 and Later" uses the following configuration as an example.

- A single CPU socket SPARC M10-1 with 16 physical CPU cores is used.
- CPU Activations to activate 4 CPU cores have been purchased and registered in the system.
- The system consists of two logical domains and they are running.
  - Two CPU cores are assigned to the control domain (primary domain).

- Two CPU cores are assigned to the guest domain (dm0).

■ To respond to a load increase, the guest domain (dm0) requires six more CPU cores.

Figure K-1   Configuration Example for XCP 2330 or Later (SPARC M10-1)
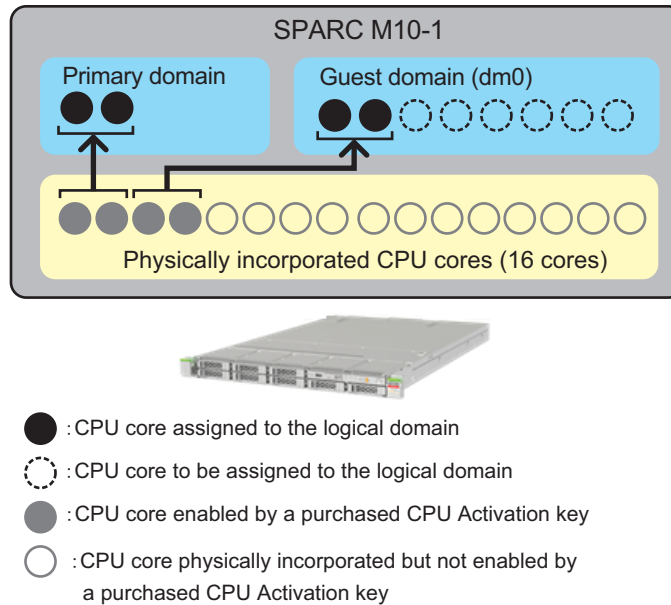
● : CPU core assigned to the logical domain

◌ : CPU core to be assigned to the logical domain

● : CPU core enabled by a purchased CPU Activation key

○ : CPU core physically incorporated but not enabled by
     a purchased CPU Activation key

Note - CPU Activation keys registered in the system enable a definite number of CPU cores. They do not enable CPU cores by specifying the CPU socket and physical location of each CPU core. For the purpose of easy understanding, specific CPU cores are enabled and assigned to the logical domains in Figure K-1.

Note - In a SPARC M12-2S/M10-4S system, a CPU Activation Interim Permit is enabled/disabled for each PPAR.

Operation Procedure for XCP 2330 and Later

The operation procedure is as follows.

1. **Confirm that additional CPU cores are required, and start the process of purchasing required CPU Activations.**
   Confirm the following before starting the purchase process.

   a. Determine whether additional CPU cores are required based on a load analysis or estimate that you perform for the entire system in the case of a SPARC M12-1/M12-2/M10-1/M10-4 system, or for the target physical partition (PPAR) in the case of a SPARC M12-2S/M10-4S system.

   b. A CPU Activation Interim Permit can be used for 30 days. We recommend confirming in advance how many days it will take for you to receive CPU

Activation keys in your region. For this information, contact your local sales representative.

2. **Enable a CPU Activation Interim Permit.**

   Perform the following.

   a. Execute the showinterimpermitusage command of the XSCF to check the current usage of the CPU cores of the system.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                       16
  Purchased Cores Assigned to PPAR:       4
  Cores In Use by Ldoms:                  4
  Interim Assignable Cores:               0
  In Use Interim Cores:                   0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

In the case of the SPARC M12-1/M12-2/M10-1/M10-4, only information for PPAR-ID 0 is displayed. In the case of SPARC M12-2S/M10-4S, information for all PPARs or a specified PPAR is displayed. Check the usage of CPU cores of the target PPAR for which the CPU Activation Interim Permit is used.

Table K-3 lists the meanings of values displayed by the showinterimpermitusage command.

Table K-3   Meanings of showinterimpermitusage

Column Display	Description	Meaning of Values of Command Example
Installed Cores	Number of physical CPU cores mounted on the system or PPAR	"16": The system has 16 physical CPU cores.
Purchased Cores Assigned to PPAR	Number of CPU Activations assigned to the PPAR	4: CPU Activations to activate 4 CPU cores are assigned to the system.
Cores In Use by Ldoms	Number of CPU core resources currently used in the logical domains	4: 4 CPU cores are currently used in the logical domains.
Interim Assignable Cores	Number of additional CPU cores made available when a CPU Activation Interim Permit is enabled	"0": No additional CPU cores have been made available yet. Reference - 12: 12 additional CPU cores have been made available.
In Use Interim Cores	Number of CPU cores currently used in the logical domains out of additional CPU cores made available when a CPU Activation Interim Permit is enabled	"0": No additional CPU cores made available are used in the logical domains.

If the number of "Purchased Cores Assigned to PPAR" is equal to or greater than that of "Installed Cores," then it indicates that CPU Activation keys for

all physically incorporated CPU cores have been registered. In this case, the CPU Activation Interim Permit is not required. Do not enable the function.

b. Execute the setinterimpermit command of the XSCF to enable the CPU Activation Interim Permit.
In the case of the SPARC M12-1/M12-2/M10-1/M10-4, the PPAR-ID specified by the setinterimpermit command is fixed at 0. All CPU cores in CPU chips mounted in the physical partition (fixed to PPAR 0) are made available by executing this command.
In the case of a SPARC M12-2S/M10-4S system, enable the CPU Activation Interim Permit by specifying a physical partition (PPAR). In this case, all CPU cores in all CPU chips mounted in each building block (SPARC M12-2S/M10-4S) composing the specified PPAR are made available.

```
XSCF> setinterimpermit -p 0 -c enable

Note:
 Please add CPU Activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue? [y|n] :y

Completed.
```

c. Execute the showinterimpermitusage command of the XSCF to check the number of additional CPU cores that are made available by the use of the CPU Activation Interim Permit.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                    16
  Purchased Cores Assigned to PPAR:    4
  Cores In Use by Ldoms:               4
  Interim Assignable Cores:           12
  In Use Interim Cores:                0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

This example shows that "Interim Assignable Cores" is "12", which means that 12 additional CPU cores have been made available by enabling the CPU Activation Interim Permit. In this case, up to 12 additional CPU cores can be used in the logical domains for 30 days.

Rather than using all the additional CPU cores that have been made available, only assign CPU cores corresponding to the number of CPU Activations you plan to purchase to logical domains.

For example, if you want to purchase and add two CPU cores, we strongly

recommend assigning only two additional CPU cores to logical domains. If you assign four CPU cores to logical domains and then purchase a CPU Activation to activate only two additional CPU cores, the total will be reduced by two CPU cores. This may cause a performance problem after you disable a CPU Activation Interim Permit.

d. If you execute the showcodusage command of the XSCF without options at this point, the following output appears.

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC           4        16            4 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
---------------- ------ --------- --------------
0  - PROC            4        16            4 cores
Unused - PROC        0         0            0 cores
```

Note that, if you execute the showcodusage command of the XSCF at this point, the display content does not change between before and after enabling the CPU Activation Interim Permit, even though the number of available CPU cores has increased through the use of the function.

Table K-4 lists the meanings of values displayed by the showcodusage command.

Table K-4   Meanings of showcodusage

Column Display	Description	Meaning of Values of Command Example
In Use	Number of CPU cores currently used in the logical domains of the entire system or each PPAR out of available CPU cores in the case where they are managed through the number of purchased CPU Activations	"4": 4 CPU cores are currently used in the logical domains of the entire system and PPAR 0.
Installed	Number of physical CPU cores mounted on the entire system or each PPAR	"16": 16 physical CPU cores are mounted on the entire system and PPAR 0.
CoD Permitted	Number of CPU Activations purchased and registered in the system	4: CPU Activations to activate 4 CPU cores are assigned to the system.
Status	Number of CPU Activations that are not currently used in the logical domains of the system (all PPARs) (difference between "CoD Permitted" and "In Use")	"OK": The value obtained by subtracting the value of "In Use" from the value of "CoD Permitted" is 0 or greater, which means no violation. Reference - "VIOLATION": The value obtained by subtracting the value of "In Use" from the value of "CoD Permitted" is less than 0, which means a violation.

Column Display	Description	Meaning of Values of Command Example
Unused- Assigned	Number of CPU Activations that are not currently used in the logical domains of the system (all PPARs). A negative value indicates that the number of CPU cores that are currently used in violation.	"0": CPU cores corresponding to the number of CPU Activations assigned to the system (all PPARs) are currently used. Reference - "-12": 12 more CPU cores than the number of assigned CPU Activations are currently used, which means a violation.

The showcodusage command is used to manage the number of CPU cores currently used in logical domains and the number of registered (purchased) CPU Activations. Therefore, the content displayed by the showcodusage command is not affected by whether a CPU Activation Interim Permit is enabled/disabled. The "CoD Permitted" field, which is for the number of purchased and registered CPU Activations, and "In Use," which is for the number of CPU cores used in logical domains, display the current values as they are.

In this example, no additional CPU cores have been assigned to the logical domains yet. The value of "CoD Permitted," which shows the number of CPU Activations registered in the system, is "4", and the value of "Installed," which shows the number of physical CPU cores, is "16". This means that there is a lack of CPU Activations for 12 physical CPU cores. However, the 12 CPU cores can be used for 30 days because the CPU Activation Interim Permit is enabled.

If, for example, you assign the 12 CPU cores to logical domains while the CPU Activation Interim Permit is enabled, "Status" displays "VIOLATION: 12 cores in excess." In this case, "VIOLATION" does not indicate urgency. It alerts that a CPU Activation violation will occur when the CPU Activation Interim Permit expires or is disabled.

In the Assigned field of the Unused row, you can confirm the number of CPU cores that have not yet been used in the logical domains of the system (all physical partitions (PPARs)) against the purchased CPU Activations. These unused CPU cores are used by the CPU automatic replacement function in the event of a failure of a CPU core in use.

e. Execute the showinterimpermit command of the XSCF to confirm the status of the CPU Activation Interim Permit.
The following example shows that the CPU Activation Interim Permit is enabled and there are 29 days left before the expiration.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: enabled [29 days remaining]
```

f. To start using additional CPU cores in one or more logical domains, execute the ldm add-core command from the control domain (primary domain). The following example shows that six CPU cores are added to the logical domain.

```
# ldm add-core 6 dm0
```

g. Execute the showcodusage command of the XSCF.
The following example shows that the value of "In Use" increased from "4" to "10" because six CPU cores were added and used in the logical domains. Since the difference between "In Use" and "CoD Permitted" is six, "VIOLATION: 6 cores in excess" is displayed, which means that six CPU cores are temporarily in violation. As mentioned above, this "VIOLATION" does not indicate urgency.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC        10        16             4 VIOLATION: 6 cores in excess
```

Note - It takes up to 20 minutes to reflect information on the CPU core usage of logical domains. Therefore, the showcodusage command may not display the change as a result of the use of the ldm command for up to 20 minutes.

---

h. If you want to confirm the number of CPU cores used in logical domains immediately after changing the assignment of CPU cores, execute the ldm list-permits command from the control domain.

```
# ldm list-permits CPU CORE
PERMITS (PERMANENT) IN USE REST
16      (16)         10     0
```

i. If the CPU Activation Interim Permit is enabled while all logical domains are powered off, the ldm command may not be required for adding CPU cores to the logical domains.
If executing the showdomainconfig command of the XSCF displays "factory-default" in "Booting config" as shown below, all available CPU cores will be automatically used in the control domain (primary domain) the next time the domain is powered on. This is because, in the case where the control domain is in factory default mode (shown as factory-default), all available hardware resources are assigned to the domain when the power is turned on.

```
XSCF> showdomainconfig -p 0
PPAR-ID     :0
Booting config
 (Current)   :factory-default
 (Next)      :factory-default
```

If "Booting config" is not "factory-default," execute the ldm command to assign additional CPU cores after the control domain is booted. After executing the ldm command, save the changed domain configuration information by using the "ldm add-spconfig" command. This ensures that the latest logical domain configuration information is used later when the domain

is rebooted.

We strongly recommend using a name different from the currently used one as the logical domain configuration name, as shown in the following example.

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
 (Current)   :before-IPermit
 (Next)      :IPermit-enabled
```

j. Execute the showinterimpermitusage command of the XSCF to check the current usage of CPU core resources.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                   16
  Purchased Cores Assigned to PPAR:   4
  Cores In Use by Ldoms:             10
  Interim Assignable Cores:          12
  In Use Interim Cores:               6

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

This example shows that "Cores In Use by Ldoms" displays "10", which means that the number of CPU cores currently used in the logical domains changed from 4 to 10. In addition, "In Use Interim Cores" displays "6", which means that 6 out of 12 available CPU cores in "Interim Assignable Cores" are additionally used in the logical domains at present.

3. **Register the obtained CPU Activation keys with the system.**
   Perform the following.

   a. After receiving newly purchased CPU Activation keys, register them with the system by using the addcodactivation command from the XSCF.

```
XSCF> addcodactivation
Product: SPARC M10-1 SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA........
Above Key will be added, Continue?[y|n]: y
XSCF>
```

   b. Set the number of CPU Activations for the physical partition by using the setcod command.

```
XSCF> setcod -p 0 -s cpu -c set 10
PROC Permits assigned for PPAR 1 : 4 -> 10

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

    c. Confirm the status of CPU cores by using the showcodusage command.

       The following example shows that ten CPU cores are available in total because six new CPU Activations are registered and added to four CPU Activations and settings are made for the physical partition.

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC        10        16               10 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
---------------- ------ --------- --------------
0  - PROC           10        16       10 cores
Unused - PROC        0         0        0 cores
```

    d. Execute the showinterimpermitusage command of the XSCF to check the current usage of CPU core resources.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                     16
  Purchased Cores Assigned to PPAR:    10
  Cores In Use by Ldoms:               10
  Interim Assignable Cores:             6
  In Use Interim Cores:                 0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

    You will disable the CPU Activation Interim Permit in step 4. Therefore, carefully confirm that "In Use Interim Cores" is "0", which means that the additional CPU core resources made available by the CPU Activation Interim Permit are not used in the logical domains.

    If the number displayed in the "Cores In Use by Ldoms" field is greater than that in the "Purchased Cores Assigned to PPAR" field, the system detects a CPU core violation. For details on system operation when a violation is detected after a CPU Activation Interim Permit expires or is disabled, see "K.4.3   Case Where the Function Has Expired or is Disabled."

  4. **Disable the CPU Activation Interim Permit.**

Perform the following.

    a. Execute the setinterimpermit command from the XSCF to disable the CPU Activation Interim Permit.

```
XSCF> setinterimpermit -p 0 -c disable
Interim permit will be disabled.
Continue?[y|n] :y

Completed.
```

    b. Execute the showcodusage command to check the current usage of CPU cores.

       Confirm that the Status field is OK, which means that all CPU cores in use are permitted to be used through the purchased CPU Activations.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC         10        16            10 OK: 0 cores available
```

    c. Execute the showinterimpermitusage command of the XSCF to check the current usage of CPU core resources.

       This example shows that "Interim Assignable Cores" is "0", which means that no additional CPU cores are made available by the CPU Activation Interim Permit.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                 16
  Purchased Cores Assigned to PPAR:  10
  Cores In Use by Ldoms:           10
  Interim Assignable Cores:         0
  In Use Interim Cores:             0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

Enabling a CPU Activation Interim Permit More Than Once

With XCP 2330 or later, a CPU Activation Interim Permit can be used more than once. To enable the CPU Activation Interim Permit more than once, however, all of the following conditions must be met.

Condition 1. Disable the CPU Activation Interim Permit even if it is enabled. (setinterimpermit(8))

Condition 2. Register an additionally purchased CPU Activation key with the system. (addcodactivation(8))

Condition 3. Assign the CPU core resources to be added to physical partition (PPAR). (setcod(8))

If the registration of the additional CPU Activations and the addition settings for the PPAR have not been performed since the last time the CPU Activation Interim Permit was enabled, you cannot enable the CPU Activation Interim Permit again.

Note - In addition, the validity period of 30 days will not be extended even when conditions 2 and 3 above are met. Disable the CPU Activation Interim Permit once here.

These conditions can be confirmed as follows by executing the showinterimpermit-v command.

(1) If the CPU Activation Interim Permit is currently enabled, it is necessary to execute setinterimpermit(8) to disable it for now. After the execution, the "Status" displayed by execution of show the interimpermit-v command will be changed to "Interim Permit cannot be enabled again (until more Purchased CPU Activations are installed and Purchased cores are assigned to the PPAR)".

(2) It is necessary that the number of purchased CPU Activation keys registered in the system has increased. It can be increased by executing addcodactivation(8). It is necessary that the value of "Registered CPU Activation Keys (in units of cores)" of "Current CPU Activation Information" displayed by executing the showinterimpermit-v command is greater than the value of "Registered CPU Activation Keys (in units of cores)" of "CPU Activation Information from the last time Interim Permit was enabled."

(3) The number of CPU core resources for the PPAR (for the SPARC M12-2S/M10-4S system) / the system (for the SPARC M12-1/M12-2/M10-1/M10-4 system) where you would like to re-enable the CPU Activation Interim Permit must be increased. It can be increased by executing setcod(8). It is necessary that the value of "Purchased Cores Assigned to PPAR" of "Current CPU Activation Information" displayed by executing the showinterimpermit-v command is greater than the value of "Purchased Cores Assigned to PPAR" of "CPU Activation Information from the last time the Interim Permit was enabled."

The following example shows that the value of "Registered CPU Activation Keys (in units of cores)" of "Current CPU Activation Information" increased by 16 and "Purchased Cores Assigned to PPAR" of "Current CPU Activation Information" by 8, and therefore, "can be enabled" is displayed. This means that the CPU Activation Interim Permit can be reused.

```
XSCF> showinterimpermit -v -p 0
PPAR-ID: 0
  Status: Interim Permit is disabled (can be enabled)

  CPU Activation Information from the last time Interim Permit was enabled:
    Registered CPU Activation Keys (in units of cores): 16
    Purchased Cores Assigned to PPAR:                    8

  Current CPU Activation Information:
```

```
Registered CPU Activation Keys (in units of cores): 32
Purchased Cores Assigned to PPAR:              16
```

To reuse the CPU Activation Interim Permit, register additional CPU Activations and add them to the PPAR by performing the same operation described in step 3 in Operation Procedure for XCP 2330 and Later.

Then, perform the same operation described in step 2 in "Operation Procedure for XCP 2330 and Later" to enable the CPU Activation Interim Permit.

K.4.2 Flow and Procedure for XCP 232*x*

With XCP 232*x*, a CPU Activation Interim Permit can be used only for a SPARC M10-1/M10-4 system.

Operation flow for XCP 232x

The operation flow is as follows.
1. **Realize that additional CPU cores are required, and start the process of purchasing required CPU Activation keys.**
2. **Enable a CPU Activation Interim Permit.**
3. **Register the obtained CPU Activation keys with the system.**
4. **Disable the CPU Activation Interim Permit.**

Configuration Example

The description in "Operation Procedure for XCP 232x" uses the following configuration as an example.
- Single CPU socket SPARC M10-1 with 16 physical CPU cores is used.
- CPU Activations to activate 4 CPU cores have been purchased and registered in the system.
- The system consists of two logical domains and they are running.
    - Two CPU cores are assigned to the control domain (primary domain).
    - Two CPU cores are assigned to the guest domain (dm0).
    - To respond to a load increase, the guest domain (dm0) requires six more CPU cores.

Figure K-2   Configuration Example for XCP 232x (SPARC M10-1)
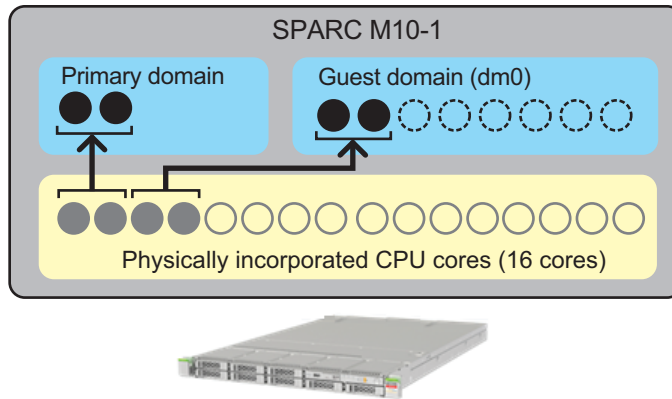
● : CPU core assigned to the logical domain

◌ : CPU core to be assigned to the logical domain

⬤ : CPU core enabled by a purchased CPU Activation key

○ : CPU core physically incorporated but not enabled by
     a purchased CPU Activation key

Note - CPU Activation keys registered in the system enable a definite number of CPU cores. They do not enable CPU cores by specifying the CPU socket and physical location of each CPU core. For the purpose of easy understanding, specific CPU cores are enabled and assigned to the logical domains in Figure K-2.

Operation Procedure for XCP 232x

The operation procedure is as follows.

1. **Confirm that additional CPU cores are required, and start the process of purchasing required CPU Activation keys.**
   Confirm the following before starting the purchase process.

   a. Determine whether additional CPU cores are required based on a load analysis or estimate that you perform for the system.

   b. A CPU Activation Interim Permit can be used for 30 days. We recommend confirming in advance how many days it will take for you to receive CPU Activation keys in your region. For this information, contact your local sales representative.

2. **Enable a CPU Activation Interim Permit.**
   Perform the following.

   a. Execute the showcodusage command of the XSCF to check the current usage of the CPU cores of the system.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC          4        16             4 OK: 0 cores available
```

Table K-5 lists the meanings of values displayed by the showcodusage command.

Table K-5   Meanings of showcodusage

Column Display	Description	Meaning of Values of Command Example
In Use	Number of CPU cores currently used in the logical domains of the entire system out of available CPU cores in the case where they are managed through the number of purchased CPU Activations	"4": 4 CPU cores are currently used in the logical domains of the entire system.
Installed	Number of physical CPU cores mounted on the entire system	"16": 16 physical CPU cores are mounted on the entire system.
CoD Permitted	Number of CPU Activations purchased and registered in the system	4: CPU Activations to activate 4 CPU cores are assigned to the system.
Status	Number of CPU Activations that are not currently used in the logical domains of the system (difference between "CoD Permitted" and "In Use")	"OK": The value obtained by subtracting the value of "In Use" from the value of "CoD Permitted" is 0 or greater, which means no violation. **Reference -** "VIOLATION": The value obtained by subtracting the value of "In Use" from the value of "CoD Permitted" is less than 0, which means a violation.
Unused- Assigned	Number of CPU Activations that are not currently used in the logical domains of the system. A negative value indicates that the number of CPU cores that are currently used in violation.	"0": CPU cores corresponding to the number of CPU Activations assigned to the system are currently used. **Reference -** "-12": 12 more CPU cores than the number of assigned CPU Activations are currently used, which means a violation.

If the value of "Installed" is equal to that of "CoD Permitted," then it indicates that CPU Activation keys for all physically incorporated CPU cores have been registered. In this case, the CPU Activation Interim Permit is not required. Do not enable the function.

b. Execute the setinterimpermit command of the XSCF to enable the CPU Activation Interim Permit. All CPU cores in CPU chips mounted on the system are made available by executing this command.

```
XSCF> setinterimpermit -p 0 -c enable
Note:
  Interim Permit can be used only once.
  Please add CPU activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue?[y|n] :y

Completed.
```

c. Execute the showcodusage command of the XSCF to check the number of additional CPU cores that are made available.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC          4        16             4 OK: 0 cores available
```

This example shows that "Installed" is "16". The value did not change between before and after the CPU Activation Interim Permit was enabled. However, it shows that 12 additional CPU cores have been made available by enabling the CPU Activation Interim Permit. In this case, up to 12 additional CPU cores can be used in the logical domain (dm0) for 30 days.

Rather than using all the additional CPU cores that have been made available, only assign CPU cores corresponding to the number of CPU Activations you plan to purchase to logical domains.

For example, if you want to purchase and add two CPU cores, we strongly recommend assigning only two additional CPU cores to logical domains. If you assign four CPU cores to logical domains and then purchase a CPU Activation to activate only two additional CPU cores, the total will be reduced by two CPU cores. This may cause a performance problem after you disable a CPU Activation Interim Permit.

d. If you execute the showcodusage command of the XSCF without options at this point, the following output appears.

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC          4        16             4 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
---------------- ------ --------- --------------
0  - PROC             4        16        4 cores
Unused - PROC         0         0        0 cores
```

Note that, if you execute the showdusage command of the XSCF at this point, the display content does not change between before and after enabling the CPU Activation Interim Permit, even though the number of available CPU cores has increased through the use of the function.

The showcodusage command is used to manage the number of CPU cores

currently used in logical domains and the number of registered (purchased) CPU Activations. Therefore, the content displayed by the showcodusage command is not affected by whether a CPU Activation Interim Permit is enabled/disabled. The "CoD Permitted" field, which is for the number of purchased and registered CPU Activations, and "In Use," which is for the number of CPU cores used in logical domains, display the current values as they are.

In this example, no additional CPU cores have been assigned to the logical domains yet. The value of "CoD Permitted," which shows the number of CPU Activations registered in the system, is "4" and the value of "Installed," which shows the number of physical CPU cores, is "16". This means that there is a lack of CPU Activations for 12 physical CPU cores. However, the 12 CPU cores can be used for 30 days because CPU Activation Interim Permit is enabled.

If, for example, you assign the 12 CPU cores to logical domains while the CPU Activation Interim Permit is enabled, "Status" displays "VIOLATION: 12 cores in excess." In this case, "VIOLATION" does not indicate urgency. It alerts that a CPU Activation violation will occur when the CPU Activation Interim Permit expires or is disabled.

In the "Assigned" field of the "Unused" row, you can confirm the number of CPU cores that have not yet been used in the logical domains of the system against the purchased CPU Activations. These unused CPU cores are used by the CPU automatic replacement function in the event of a failure of a CPU core in use.

e. Execute the showinterimpermit command of the XSCF to confirm the status of the CPU Activation Interim Permit. The following example shows that the CPU Activation Interim Permit is enabled and there are 29 days left before the expiration.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: enabled [29 days remaining]
```

f. To start using additional CPU cores in one or more logical domains, execute the ldm add-core command from the control domain (primary domain). The following example shows that six CPU cores are added to the logical domain.

```
# ldm add-core 6 dm0
```

g. Execute the showcodusage command of the XSCF.
The following example shows that the value of "In Use" increased from "4" to "10" because six CPU cores were added and used in the logical domains. Since the difference between "In Use" and "CoD Permitted" is six, "VIOLATION: 6 cores in excess" is displayed, which means that six CPU cores are temporarily in violation. As mentioned above, this "VIOLATION" does not indicate urgency.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC       10       16               4 VIOLATION: 6 cores in excess
```

> **Note -** It takes up to 20 minutes to reflect information on the CPU core usage of logical domains. Therefore, the showcodusage command may not display the change as a result of the use of the ldm command for up to 20 minutes.

h. If you want to confirm the number of CPU cores used in logical domains immediately after changing the assignment of CPU cores, execute the ldm list-permits command from the control domain.

```
# ldm list-permits
```

i. If the CPU Activation Interim Permit is enabled while all logical domains are powered off, the ldm command may not be required for adding CPU cores to the logical domains.

   If executing the showdomainconfig command of the XSCF displays "factory-default" in "Booting config" as shown below, all available CPU cores will be automatically used in the control domain (primary domain) the next time the domain is powered on. This is because, in the case of the control domain ("factory-default"), all available hardware resources are assigned to the domain when the power is turned on.

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
 (Current)   :factory-default
 (Next)      :factory-default
```

   If "Booting config" is not "factory-default", execute the ldm command to assign additional CPU cores after the control domain is booted. After executing the ldm command, save the changed domain configuration information by using the "ldm add-spconfig" command. This ensures that the latest logical domain configuration information is used later when the domain is rebooted.

   We strongly recommend using a name different from the currently used one as the logical domain configuration name, as shown in the following example.

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
 (Current)   :before-IPermit
 (Next)      :IPermit-enabled
```

3. **Register the obtained CPU Activation keys with the system.**

Perform the following.

a. After receiving newly purchased CPU Activations, register them with the system by using the addcodactivation command from the XSCF.

```
XSCF> addcodactivation
Product: SPARC M10-1 SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA........
Above Key will be added, Continue?[y|n]: y
XSCF>
```

b. Set the number of CPU Activations for the physical partition by using the setcod command.

```
XSCF> setcod -p 0 -s cpu -c set 10
PROC Permits assigned for PPAR 1 : 4 -> 10

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

c. Confirm the status of CPU cores by using the showcodusage command.

The following example shows that ten CPU cores are available in total because six new CPU Activations are registered and added to four CPU Activations and settings are made for the physical partition.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC        10        16            10 OK:  0 cores available
```

d. You will disable the CPU Activation Interim Permit in step 4. Therefore, carefully check that the required number of CPU cores is displayed in "CoD Permitted." The number displayed in the "In Use" field must be equal to or less than that in the "CoD Permitted" field while the domain is running. If the number displayed in the "In Use" field is greater than that in the "CoD Permitted" field, the system detects a CPU core violation. For details on system operation when a violation is detected after the CPU Activation Interim Permit expires or is disabled, see "K.4.3 Case Where the Function Has Expired or is Disabled."

4. **Disable the CPU Activation Interim Permit.**
   Perform the following.

a. Execute the setinterimpermit command from the XSCF to disable the CPU Activation Interim Permit.

```
XSCF> setinterimpermit -p 0 -c disable
Interim permit will be disabled.
Continue?[y|n] :y

Completed.
```

b. Execute the showcodusage command to check the current usage of CPU cores.

Confirm that the Status field is OK, which means that all CPU cores in use are permitted to be used through the purchased CPU Activations.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC        10        16            10 OK: 0 cores available
```

K.4.3 Case Where the Function Has Expired or is Disabled

This section describes system operation and action to be performed when a CPU Activation Interim Permit expires or is disabled.

Configuration Example

The description here uses the following configuration as an example.

- Single CPU socket SPARC M10-1 with 16 physical CPU cores is used.

- CPU Activations to activate 4 CPU cores have been purchased and registered in the system.

- The system consists of two logical domains and they are running.
  - Two CPU cores are assigned to the control domain (primary domain).
  - Two CPU cores are assigned to the guest domain (dm0).

- To respond to a load increase, the guest domain (dm0) requires six more CPU cores.

- A CPU Activation Interim Permit is enabled, and six additional CPU cores have been assigned to the guest domain (dm0) as a temporary action.

Figure K-3   Configuration Example for the Case Where the Function Has Expired or is Disabled (SPARC M10-1)
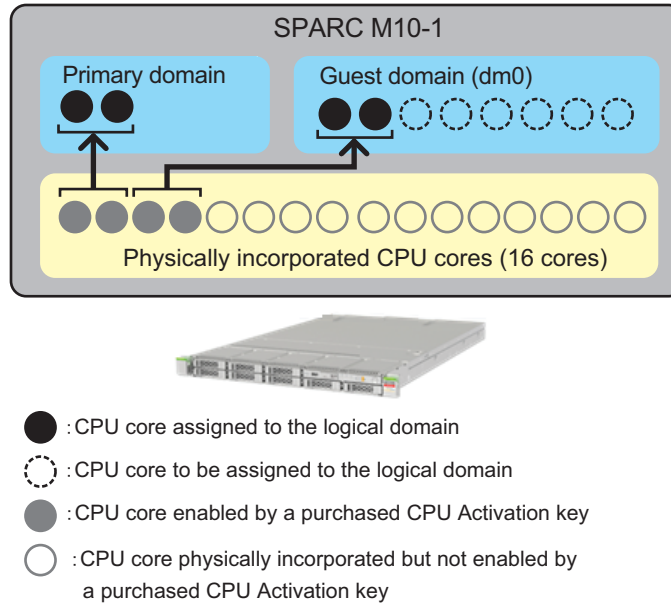
Note - CPU Activation keys registered in the system enable a definite number of CPU cores. They do not enable CPU cores by specifying the CPU socket and physical location of each CPU core. For the purpose of easy understanding, specific CPU cores are enabled and assigned to the logical domains in Figure K-3.

System Operation and Action

The CPU Activation Interim Permit expires 30 days later regardless of whether additional CPU Activation keys are registered in the system. In addition, a CPU Activation Interim Permit may be disabled inadvertently by the setinterimpermit command of the XSCF. Once the CPU Activation Interim Permit is disabled, it cannot be enabled again with XCP 232*x*. Even with XCP 2330 and later, the function cannot be enabled again instantly then and there.

If the CPU Activation Interim Permit expires or is disabled when any CPU cores are in the use violation state "VIOLATION," the system operates in the following way.

a.   When 30 minutes elapse after the violation, a notification is sent to the system, which tries to delete excessive CPU cores from logical domains.

b.   When 60 minutes elapse after the violation, the system tries to shut down the control domain.

c.   When 90 minutes elapse after the violation, the system tries to shut down all domains.

If you perform either of the following operations within 30 minutes after the violation is detected, the system does not perform operations a. to c. above.

- Reducing the number of CPU cores currently used in logical domains
- Register additional purchased CPU Activation keys by using the addcodactivation command of the XSCF, and then adding the number of CPU Activations to the physical partition by using the setcod command.

If the CPU Activation Interim Permit expires and you execute the showinterimpermit command of the XSCF, "expired" will be displayed as shown in the following example.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: expired
```

If the CPU Activation Interim Permit expires or is disabled and you execute the showcodusage command of the XSCF, the usage of CPU cores will be displayed as shown in the following example.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC        10       16               4 VIOLATION: 6 cores in excess
```

In this case, "VIOLATION" is displayed in the "Status" field because the CPU Activation Interim Permit has expired. The example shows that six CPU cores are used in violation, which actually warns the system of urgency. In the case of this example, you must immediately delete six CPU cores in total from logical domains.

After detecting a violation, the system tries to delete CPU cores from logical domains until the number of CPU cores in use matches the number of purchased and registered CPU Activation keys. Six CPU cores will be deleted in this example.

The system deletes CPU cores starting with the one with the highest CPUID (CID) value. The system may not be able to delete CPU cores for some reasons, such as that a vcpu belonging to the CPU core is associated with a specific process by pbind. In that case, the CPU core with the second highest CID value will be deleted.

You can check the CID value by using the ldm command from Oracle Solaris, as shown below.

```
# ldm list-domain -o core
NAME
primary
CORE
    CID    CPUSET
    0      (0, 1)
    4      (8, 9)
-----------------------------------------------------------
NAME
dm0
CORE
    CID    CPUSET
    8      (16, 17)
    12     (24, 25)
    <Omitted>
```

After the number of CPU cores becomes equal to or less than the number of CPU cores whose use is permitted by purchased CPU Activation keys, the above action is not performed.

As mentioned above, deletion of CPU cores may fail. A failure of the deletion occurs when a vcpu is associated with a specific process by pbind or other means or when the CPU core to be deleted is the last one in a logical domain. If the system cannot delete enough CPU cores (six CPU cores in this case), the control domain will be shut down.

To recover from the above situation, perform either of the following operations.

- Delete enough CPU cores from logical domains by using the ldm command, or stop one or more logical domains.

- Register a sufficient number of purchased CPU Activation keys by using the addcodactivation command of the XSCF, and then add the number of CPU Activations to the physical partition by using the setcod command.

If enough CPU cores cannot be deleted due to shut down of the control domain, all logical domains will be shut down.

If all logical domains are shut down, possible recovery methods are as follows.

a. Select the configuration information file of the logical domains that is saved before the CPU Activation Interim Permit is enabled.
Select the old configuration information file of the logical domains by using the setdomainconfig command of the XSCF, as shown below. Then, boot the system.

```
XSCF> setdomainconfig -p 0
PPAR-ID        :0
Booting config
(Current)    :IPermit-enabled
(Next)       :IPermit-enabled
-------------------------------------------------------------
Index        :1
config_name :factory-default
domains      :1
date_created:-
-------------------------------------------------------------
Index        :2
config_name :before-IPermit
domains      :2
date_created:"2015-03-24 19:21:30"
-------------------------------------------------------------
Index        :3
config_name :IPermit-enabled
domains      :2
date_created:"2016-06-16 12:00:30"
Select Index of Using config_name : 2
PPAR-ID of PPARs that will be affected :00
Logical domain config_name will be set to "before-IPermit".
Continue?[y|n] :y
```

b. If your purpose is to recover the control domain, start only the control domain,

and then delete the necessary amount of CPU core resources from the control domain.

Note - Even if the number of CPU cores used in the control domain is greater than the number of CPU cores permitted for use by purchased CPU Activation keys, the control domain is always booted normally. The same applies even if the CPU Activation Interim Permit has expired or is disabled. However, if enough CPU cores cannot be deleted within 30 minutes after the detection of the violation, the system starts automatic deletion of CPU cores again according to the above procedure. After successful deletion of CPU core resources, save the corrected logical domain configuration information by using the ldm add-spconfig command so that it can be used in the future when the control domain is rebooted.

---

    c.   If your purpose is to recover a specific guest domain, perform the following procedure.
           1. Boot only the control domain.

           2. Delete CPU cores assigned to the guest domain from the control domain, and save the corrected logical domain configuration information by using the ldm add-spconfig command.

           3. Boot the guest domain.

    d.   Register additional purchased CPU Activation keys by using the addcodactiovation command of the XSCF, and add the number of CPU Activations to the physical partition by using the setcod command.

If you need to recover both the control domain and guest domain without using the old configuration information file of logical domains, both of the above operations b. and c. may be required.

K.5 Event Notification of the CPU Activation Interim Permit

This section describes notification of events related to a CPU Activation Interim Permit.

K.5.1 Types of Notification

The following are the four types of event notification to be made in connection with a CPU Activation Interim Permit.

    a.   XSCF event log
        An event log that can be referenced by using the showlogs event command of the XSCF

    b.   Messages of domain console (in the case of XCP 2330 or later)
        Messages that are registered in syslog and displayed on the primary domain console

c. E-mail
   E-mail sent if the e-mail notification function of the XSCF is enabled (See "10.2 Receiving Notification by E-mail When a Failure Occurs.")

d. SNMP trap
   An SNMP trap received if the system is monitored by the SNMP agent function of the XSCF (See "10.3   Monitoring/Managing the System Status With the SNMP Agent.")

K.5.2   Notification Examples

Starting 14 days prior to CPU Activation Interim Permit expiration, notifications are sent every 4 hours until the CPU Activation Interim Permit is disabled or expires. Notifications of each event are in this format: PPAR-ID 0: Interim Permit due to expire in 14 days.

As soon as the CPU Activation Interim Permit has expired, notifications are sent. Notifications of each event are in this format: PPAR-ID 0: Interim Permit has expired.

When a CPU core use violation occurs after the CPU Activation Interim Permit expires or is disabled, a notification will be sent. Notifications of each event are in this format: PPAR-ID 0: CoD PROC violation occurred.

Also when the CPU core use violation is resolved, a notification will be sent. Notifications of each event are in this format: PPAR-ID 0: CoD PROC violation resolved.

The following provides examples of notification of events.

The description here uses examples of events 14 days before the CPU Activation Interim Permit expires.

Example 1. XSCF event log

```
XSCF> showlogs event
May 23 18:11:51 JST 2016        PPAR-ID 0: Interim Permit due to expire in 14
days
```

Example 2. syslog message on the primary domain console (for XCP 2330 and later)
- Message example

```
 PPAR-ID 0: Interim Permit due to expire in 14 days
```

- syslog log example

```
 Jul 22 01:10:45 4S-441-D0 SC Alert: [ID 695932 daemon.notice]
 PPAR-ID 0: Interim Permit due to expire in 14 days
```

Example 3. E-mail

```
From no-reply@xxxx Mon May 23 18:11:51 2016
Date: Mon, 23 May 2016 18:11:51 +0900
From: no-reply@xxxx
Message-Id: <1463994711.2429@xxxx>
To: administrator@m10.org
Subject:  Event: M10-1: M10-1: serial# TZ01111111, PPAR-ID 0: Interim Permit
due to expire in 14 days
Content-Length: 200

TYPE: Event, VER: XCP-2320
MODE-SWITCH: Service
SEVERITY: Event
EVENT-TIME: 05-23-2016 18:11:51 JST
CSN: TZ01111111
SERVER-ID: xxxx
FRU: -
DIAGCODE: -
MSG: PPAR-ID 0: Interim Permit due to expire in 14 days
```

Example 4. SNMP trap

The SNMP trap OID 1.3.6.1.4.1.211.1.15.4.1.2.0.5 is sent. This trap contains .1.3.6.1.4.1.211.1.15.4.1.2.1.1.0 (scfTrapEventType.0), which is an object with a value indicating the type of the event.

For details on the OID, see the *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists*.

K.6 Other Important Notes

This section describes notes on using a CPU Activation Interim Permit.

K.6.1 PPAR DR and CPU Activation Interim Permit

A CPU Activation Interim Permit can be used simultaneously with physical partition dynamic reconfiguration (PPAR DR).

Note - While PPAR DR is being executed by the addboard or deleteboard command, at that moment, changing the mode of a CPU Activation Interim Permit will fail. In other words, a conflict between the setinterimpermit command and the addboard/deleteboard command will result in failure of either command.

For example, suppose that you are going to use PPAR DR to add BB#4 to a PPAR for which a CPU Activation Interim Permit is enabled. In this case, all CPU cores in all CPU chips mounted on BB#4 are made available when the addition process of PPAR DR is completed.

However, if the logical domain configuration of this PPAR is "not" factory-default,

you need to use the ldm command of Oracle Solaris to incorporate the added CPU cores into logical domains.

Conversely, suppose that you are going to use PPAR DR to delete BB#4 from the PPAR for which a CPU Activation Interim Permit is enabled. In this case, all CPU cores in all CPU chips mounted on BB#4 are automatically deleted from the PPAR as part of the deletion process of PPAR DR. Therefore, you must delete CPU core resources from logical domains in advance before deleting them from the PPAR.

K.6.2 When Attempting to Use a CPU Activation Interim Permit Again (for XCP 232*x* Only)

If you try to enable a CPU Activation Interim Permit again for a system for which the function has already been used, by using the setinterimpermit command of the XSCF, the command will fail.

The following example shows a case where the command fails.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: disabled
XSCF> setinterimpermit -p 0 -c enable
Note:
  Interim Permit can be used only once.
  Please add CPU activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue?[y|n] :y

The Interim Permit cannot be enabled because it has already been used once.
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: disabled
```

If XCP 232*x* is used, this is not a defect because a CPU Activation Interim Permit can be enabled only once for each system.

If all of the following items apply to you, contact your local sales representative.

- You used a CPU Activation Interim Permit for a system on which XCP 232*x* was installed.
- Then, you updated the firmware to XCP 2330 or later.
- You purchased additional CPU Activation keys, registered them with the system, and assigned CPU core resources to the PPAR.
- You want to use a CPU Activation Interim Permit again.

K.6.3 Moving CPU Activation Keys (Deleting/Moving)

Moving (deleting and moving) one or more purchased CPU Activation keys from one SPARC M12/M10 to another when the CPU Activation Interim Permit is enabled

does not affect the move process.

Use the deletecodactivation command of the XSCF for deleting and the addcodactivation command for adding.

Before deleting a CPU Activation key from a SPARC M12/M10 by using the deletecodactivation command, be sure to externally save the CPU Activation key as a text file, etc. by using the showcodactivation command.

The saved CPU Activation key can be added to another SPARC M12/M10 by using the addcodactivation command.

The CPU Activation Interim Permit is not affected by the CPU Activation move process. Note that, however, the number of CPU cores in use must not exceed the number of purchased CPU Activations after the move process in a system for which the CPU Activation Interim Permit is not enabled.

While the CPU Activation Interim Permit is enabled, all purchased CPU Activation keys can be deleted from the system, and the system continues operating even after the deletion. However, once the CPU Activation Interim Permit is disabled or expires, the system does not operate until a purchased CPU Activation key is registered in the system.

K.6.4 Output of the ldm Command

If you use the ldm command of Oracle Solaris when a CPU Activation Interim Permit is enabled, "PERMANENT" is displayed for additional available CPU cores, even though they are not actually permanent.

As an example, suppose that there are four CPU cores in the primary domain of a SPARC M12/M10 and the use of them is permitted by purchased CPU Activation keys. Executing "ldm list-domain -l" when a CPU Activation Interim Permit is enabled displays the following information.

```
# ldm list-domain -l
NAME                STATE       FLAGS    CONS    VCPU   MEMORY   UTIL   NORM   UPTIME
primary             active      -n-c--   UART     8     63744M   0.0%   0.0%   16d 21h
 6m
<Omitted>
CPU CORE
PERMITS (PERMANENT)    IN USE      REST
16      (16)           16          0
<Omitted>
```

Actually, only four CPU cores are permanently available (that is, made available by purchased CPU Activation keys). However, all of the 16 CPU cores incorporated physically are displayed as permanent ones in the output of the command when the CPU Activation Interim Permit is enabled.

Index