FUJITSU

SPARC Enterprise™ M3000 Server Product Notes

For XCP Version 1093

Manual Code C120-E629-01EN
Part No. 875-4659-10
July 2010, Revision A

Please
Recycle

Contents

Preface

These product notes contain late-breaking information about the SPARC Enterprise M3000 server hardware, software, or documentation that became known after the documentation set was published.

Note – Once an XCP version newer than the XCP version supported by this manual is released, only the manuals related to the new XCP version are subsequently updated.
You must therefore check the manuals for the latest XCP version in addition to those related to the XCP version you are using.

Global Site
http://www.fujitsu.com/sparcenterprise/manual/
Japanese Site
http://primeserver.fujitsu.com/sparcenterprise/manual/
North American Site
https://download.computers.us.fujitsu.com/

Technical Support

If you have technical questions or issues that are not addressed in the SPARC Enterprise M3000 server documentation, contact a sales representative or a certified service engineer.

Software Resources

The Solaris Operating System and Sun Java Enterprise System software are preinstalled on your SPARC Enterprise M3000 server.

Contact a sales representative or a certified service engineer for software resources for your SPARC Enterprise M3000 server.

Note – For latest patch information go to:

Global Site
http://www.fujitsu.com/global/support/software/security/products-s/patch-info/
Japanese Site
https://software.fujitsu.com/jp/security/products-others/unix/
North American Site
https://download.computers.us.fujitsu.com/

Installation information and README files are included in the patch download.

Accessing Documentation

Note – Information in these product notes supersedes the information in the SPARC Enterprise M3000 server documentation set.

Instructions for installing, administering, and using your SPARC Enterprise M3000 server is provided in the SPARC Enterprise M3000 server documentation set. The documentation set is available for download from the following website:

Global Site
http://www.fujitsu.com/sparcenterprise/manual/

Japanese Site
http://primeserver.fujitsu.com/sparcenterprise/manual/

North American Site
https://download.computers.us.fujitsu.com/

Sun Oracle Software (for Oracle Solaris OS, and so on) Related Manuals
http://docs.sun.com

Fujitsu Welcomes Your Comments

If you have any comments or requests regarding this document, or if you find any unclear statements in the document, please state your points specifically on the form at the following URL.

For Users in U.S.A., Canada, and Mexico:

http://www.computers.us.fujitsu.com/www/support_servers.shtml?support/servers

For Users in Other Countries:
SPARC Enterprise contact

http://www.fujitsu.com/global/contact/computing/sparce_index.html

General Information About XCP 1093

This section describes the general information about XCP 1093.

Supported Firmware and Software

The following firmware and operating system (OS) are supported depending on the processors being installed on the SPARC Enterprise M3000 server..

TABLE 1 Supported Firmware and Operating System Versions

Installed Processors	XCP Version	Operating System Version
SPARC64 VII processors		
2.52GHz	XCP 1080 or later	Solaris 10 5/08 or later, with required patches
2.75GHz	XCP 1091 or later	Solaris 10 10/08 or later

Note – XCP 1080 is the first XCP release for the SPARC Enterprise M3000 server.

Note – 8GB DIMM is supported in XCP 1081 or later.

For XCP, you can download the latest files of firmware at the following websites.

Global Site:
https://updatesite.jp.fujitsu.com/unix/en/download/firmware/

Japanese Site:
https://updatesite.jp.fujitsu.com/unix/jp/download/firmware/

Many web browsers support the XSCF Web. The browsers in TABLE 2 have demonstrated compatibility with the XSCF Web through testing. For other information about XSCF Web, see "Notes on XSCF Web" on page 6.

TABLE 2 Tested Web Browser Versions

Web Browser Application	Version
Microsoft Internet Explorer	6.0, 7.0, or 8.0
Firefox (Solaris 10)	2.0 or 3.5.9

Solaris OS Patch Information

Patches are not required for servers running Solaris 10 10/08 OS or later.

Patches for Solaris 10 5/08

The following patches are required for Solaris 10 5/08 OS only on servers containing SPARC64 VII 2.52GHz processors:

- 119254-59
- 138866-01
- 137137-09

For additional Solaris Operating System information, see "Solaris OS Issues and Workarounds" on page 24.

Note – See "Software Resources" on page viii for information on how to find the latest patches. Installation information and README files are included in the patch download.

Patches for Emulex PCI Express (PCIe) Cards

The following Emulex cards require drivers supplied in patch 120222-26:

- XSEFC402AF Sun StorageTek Enterprise Class 4Gb Dual-Port Fibre Channel PCI-E HBA
- XSEFC401AF Sun StorageTek Enterprise Class 4Gb Single-Port Fibre Channel PCI-E HBA

Updating to XCP 1093

To update your XCP to XCP 1093, refer to the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide* for instructions.

Resetting the XSCF Firmware

After updating the XCP firmware to 1093, do not fail to reset the XSCF by using the `rebootxscf`(8) command.

Functionality Issues and Limitations

This section describes the known issues and limitations at the time of this release.

Notes on Active Directory

- While Active Directory is enabled, when you attempt to login to XSCF via the telnet, you might fail to login due to timeout of the query to secondary alternated server or later.
- If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail. In such case, specify larger value for the timeout and then try again.

Notes on LDAP/SSL

If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail. In such case, specify larger value for the timeout and try again.

Notes on Power Consumption Monitoring Function and Airflow Indicator

- The amount of power consumption and exhaust air might not be indicated correctly in the MIB information, in the `showenvironment power` and the `showenvironment air` command output, and on the XSCF Web in the following cases; and you should wait for one minute and check the value again.
  - During the server powering on or powering off, or for a while after the power-on or power-off complete
  - During the active replacement of power supply unit, or for a while after the active replacement complete
- The figures on the power consumption monitoring function and airflow indicator respectively represent the dissipation power and volume of air exhausted from the server. The figures of peripheral devices are not included.

Notes on NTP Server

- We recommend the domain to use the XSCF Unit as NTP server. In this case, pay attention to the following points:
  - XSCF must be connected to an external NTP server
  - When you connect one or more NTP servers in addition to XSCF, connect the same NTP server as XSCF is using

  For details on NTP server, contact a service engineer. For details on NTP settings, refer to the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

Notes on the NTP Server Referring to the Local Clock

When the NTP server which XSCF refers to is referring to the server's own system time (local clock), and when the address of "127.127.1.0" is set to that local clock, time synchronization in XSCF might fail.

The address of the XSCF's own local clock is fixed to "127.127.1.0." On the other hand, when the address of the local clock of the NTP server which XSCF refers to is set to "127.127.1.0," the address of the clock source (refid) has the same value as the address of the XSCF's own local clock. An NTP server like this is excluded from the target of XSCF time synchronization.

You can execute the `showntp -l` command to refer to the address of the NTP server's own clock source which is set in XSCF and the address of the XSCF's own local clock.

```
XSCF> shownntp -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 server outputs, the upper (192.168.1.2) indicates the NTP server which is set by using the `setntp`(8) command. The refid is `LOCAL(0)`, which means that the local clock which has the address of "127.127.1.0" is set to the clock source of this NTP server. On the other hand, the lower indicates the XSCF's own local clock. The address of the XSCF's own local clock is fixed to "127.127.1.0." Due to this, the NTP server (192.168.1.2) is excluded from the target of XSCF time synchronization; which results in the XSCF synchronizes with its own local clock.

With any of the following measures to avoid the trouble, time can be correctly synchronized with the NTP server which is set by using the `setntp`(8) command.

- **Change the clock source that the NTP server being set in XSCF refers to**

  Use the `shownntp -l` command and check the clock source of the NTP server which is set in XSCF. An NTP server which indicates the refid of `LOCAL(0)` in the output is referring to the local clock which has the address of "127.127.1.0," and you should change it to refer to another clock source.

  When you change the clock source of an NTP server, make sure in advance that it has no impact on other NTP clients.

- **Change the address of the local clock of the NTP server**

  Of the NTP server which XSCF refers to, change the address of the local clock to "127.127.1.1," "127.127.1.2," or "127.127.1.3." Change `/etc/inet/ntp.conf` of Solaris OS. To enable the change, restart of the NTP daemon is required.

  When you change the address of the local clock of an NTP server, make sure in advance that it has no impact on other NTP clients.

- **Change the stratum value of the NTP server**

  Of the NTP server which XSCF refers to, change the stratum value to "1." An NTP server which has the stratum value of "1" becomes the most significant clock source and has no refid. Therefore, there is no chance that it will have the same address as the XSCF's own local clock.

  When you change the stratum value of an NTP server, make sure in advance that it has no impact on other NTP clients.

- **Change the address of the XSCF's own local clock**

  By using the `setntp -m localaddr=`*value* command, change the address of the XSCF's own local clock. In *value*, specify the least significant byte of the clock address of the local clock 127.127.1.*x* for *value*. A numeric from 0 to 3 can be

specified. By specifying either from 1 to 3, the address of an NTP server which is referring to the local clock does not correspond to the address of the XSCF internal local clock anymore, and a server which is referring to the local clock can also be set as the NTP server of XSCF.

Notes on XSCF Web

- Under the Windows 7 and Internet Explorer 8.0 environment, XSCF Web does not support the use through the built-in Administrator account.
- On Internet Explorer 8.0, when you move the on-screen horizontal frame up or down to change the frame height and use the [Monitor Msg Show/Hide] button, the screen background color may turn black. In this case, click Refresh on the View menu or press F5 key to refresh the display, to go back to the screen right after the login.

  When you moved the on-screen horizontal frame up or down to change the frame height, do not use the [Monitor Msg Show/Hide] button.
- To use XSCF Web on the SPARC Enterprise M3000 server which is installed the XCP 1080, disable the cache function of your browser. If you leave the browser cache function enabled, the old cached data might be displayed. To disable the cache function:
  - Internet Explorer 6 and 7

    [Tools] -> [Internet Options...] -> [Advanced] tab and check the "Do not save encrypted pages to disk" box.
  - Netscape 7.1 or later

    [Edit] -> [Preferences] -> [Advanced] -> [Cache] -> [Compare the page in the cache to the page on the network] setting and select the "Every time I view the page" radio button.
  - Firefox 2

    Type "`about:config`" in address box, then type "`cache`" in filter box. Change the "browser.cache.check_doc_frequency" settings value to "`1`."
- Using the XSCF Web, when you import XCP or update the firmware, Session ID error may be displayed on the web browser. And in the Autologout setting, when you specify the timeout period as over 30 minutes, Internal Server Error might be displayed when you perform the firmware update. Please close the current browser and open the new browser to reconnect to XSCF Web.
- When you use the XSCF Web under the Internet Explorer 6 or 7, or Firefox 2 environment, if a plug-in such as the search tool installed with the browser, remove the plug-in or disable the pop-up blocking.

When you use the XSCF Web under the Internet Explorer 8 or Firefox 3 environment, if a plug-in such as the search tool installed with the browser, disable the pop-up blocking.

- When you use XSCF Web under the Firefox 3 environment and attempt to log in to XSCF, you may be prompted by the browser to save the login ID/password. In this case, do not save the login ID/password. If you save the login ID/password, the stored data can be displayed unexpectedly on the LDAP, SMTP and REMCS web pages.

  Use one of two settings described below, to disable the browser's ID/password remember function:

  - Disable the entire browser ID/password remember function

    Click on the [Tools] menu, and select [Preferences]. On the [Security] panel, see [Passwords] and uncheck the "Remember passwords for sites" checkbox.

  - Designate the XSCF Web address as an exception to the ID/password save operation

    Click on the [Tools] menu, and select [Preferences]. On the [Security] panel, see [Passwords] and check the "Remember passwords for sites" checkbox. Then, on the dialog for the ID/password saving which appears in the login attempt to XSCF, click the "Never for This Site" button. As a result, the XSCF Web address will be registered in the "Exceptions" list to the ID/password save operation, and the dialog to prompt the ID/password saving will no longer be displayed in the subsequent login attempts to XSCF.

General Functionality Issues and Limitations

- The log archive feature by the `setarchiving`(8) and the `showarchiving`(8) commands, and the Log Archives menu of XSCF Web is not supported.
- When you use the external power control interface of the external power controller, the following notification signals are not supported:
  - The OS panic or the server hardware error signal (*CPUN/RTNU)
  - The server hardware error signal (power fail, temperature error, and fan error) (*ALARM)
- You cannot use the following user account names, as they are reserved for system use: `root`, `bin`, `daemon`, `adm`, `operator`, `nobody`, `sshd`, `rpc`, `rpcuser`, `ldap`, `apache`, `ntp`, `admin`, `proxyuser`, and `default`.
- XSCF-LAN is compliant with auto-negotiation. When you connect XSCF-LAN and the network device which has been fixed to the full-duplex mode, according to the IEEE 802.3 rule, XSCF-LAN communicates in the half-duplex mode. Due to this, network communication speed may slow down or communication error may occur. Do not fail to set the network device which connects with XSCF-LAN to the auto-negotiation mode.

- At this time the `restoredefaults`(8) command is not supported.
- At this time the `-e`, `-l`, `-P` options of the `snapshot`(8) command are not supported.

Information About Hardware

This section describes the special instructions and the issues about the SPARC Enterprise M3000 server hardware.

Notes on the Use of 200V Power Supply

For the servers that have the B-type plug, confirm that a 15A overcurrent protection device is available outside the server. If not, prepare an external 15A overcurrent protection that can be achieved by means of no-fuse breakers (NFBs) or fuses. The B-type plug refers to plugs other than grounding-type ones with two parallel blades, such as the NEMA L6-30, L6-20, L6-15, and L5-15.

Notes on DVD Drive and Discs

See the "*Notes on DVD Drives and Discs in SPARC Enterprise*" on the website below before using the CD/DVD discs in the standard DVD drive mounted in this server.

URL:
`http://primeserver.fujitsu.com/sparcenterprise/manual/`

CD-RW/DVD-RW Drive Unit

Two types of CD-RW/DVD-RW drive units are supported, slot-in type (FIGURE 1-11) and tray type (FIGURE 1-12).

FIGURE 1-11 Slot-in Type

FIGURE 1-12 Tray Type

Note – The locations of LED and button may vary depending on the servers.

Note – When you use the medium on the tray type CD-RW/DVD-RW drive unit, make sure that the center of the medium is secured to the clamp of the tray, and then push the tray into the drive.

Notes on the Use of USB Memory

To execute the `dumpconfig`(8), `restoreconfig`(8) or `snapshot`(8) command, if you specify USB memory as the destination to store data, prepare the USB memory as a medium in advance.
The data stored will include the information about the system. To use USB memory, you need to pay attention to the management of the USB memory in which the data stored, from the data security viewpoint.

We do not provide guarantees to every USB memory from any manufacturers that currently on the market against its connectivity to XSCF and proper operation. Depending on the USB memory in use, defects such as the XSCF firmware error or reset may occur. In case such defects occurred, stop the use of USB memory immediately.

To connect the USB memory to the USB port for XSCF, connect the USB memory directly to the USB port. If connected via USB hub or USB extension cables, it may cause errors.

Power Control and Operator Panel Mode Switch

You can use the mode switch on the operator panel to switch between system power-on/off when you use the remote power control utilizing the RCI function or the automatic power control system (APCS).

For details, see the "Limitations and Cautions" in "Preface" of the *SPARC Enterprise M3000 Server Service Manual*.

Hardware Documentation Updates

This section contains late-breaking hardware information that became known after the documentation set was published and corrections in the SPARC Enterprise M3000 server hardware documentation.

TABLE 3 lists known documentation updates.

TABLE 3 Hardware Documentation Updates

Title	Page Number	Update
SPARC Enterprise M3000 Server Site Planning Guide	2-4, 2-5	The height of container box indicated in TABLE 2-2 "Physical Specifications" and FIGURE 2-3 "Server Container Box" will be corrected. The correct value is 289 mm/11.4 in..
	3-6	The rush current and leakage current values will be added to TABLE 3-3 "Electrical Specifications". See “Electrical Specifications” on page 13 for detail.
SPARC Enterprise M3000 Server Overview Guide	1-24	Section 1.4.5.2, "CD-RW/DVD-RW Drive Unit" will be changed. See “CD-RW/DVD-RW Drive Unit” on page 10 for detail.
	1-25	1.4.6.2 "SAS Port" The article on "SAS Port" will be replaced by the following. The SAS port connects the server to an external device, such as a tape drive, which has an SAS interface. For information on which devices can be connected, contact a service engineer. Note that the transfer rate of this port is up to 600MB/s (3Gbps x 2wide).
SPARC Enterprise M4000/M5000 Servers Service Manual	11-1	"Accessing the CD-RW/DVD-RW Drive Unit," in Section 11.1, will be added the explanation of the type of the drive unit and the identifying the drive unit. See “CD-RW/DVD-RW Drive Unit” on page 10 for detail.

Updates of the SPARC Enterprise M3000 Server Site Planning Guide

The following information supersedes the information in the *SPARC Enterprise M3000 Server Site Planning Guide*.

Electrical Specifications

This section explains the electrical specifications of the M3000 server.

Note – The electrical power values in TABLE 3-3 are the maximum values based on the fully configured server. The actual values may differ from these values, depending on the server configuration.

TABLE 3-3 Electrical Specifications

	Specification			
Item	**CPU: 2.52 GHz**		**CPU: 2.75 GHz**	
Input voltage	100 to 120 VAC	200 to 240 VAC	100 to 120 VAC	200 to 240 VAC
Number of power cords	2 (1 cord for each power supply unit)		2 (1 cord for each power supply unit)	
Power cord length	3 m/9.84 ft		3 m/9.84 ft	
Redundancy	1 + 1 redundant configuration		1 + 1 redundant configuration	
Rated current*	4.80 A	2.59 A	5.15 A	2.81 A
Frequency	50/60 Hz		50/60 Hz	
Maximum power consumption	470 W	460 W	505 W	500 W
Apparent power	480 VA	517 VA	515 VA	562 VA
Heat dissipation	1,603.7 BTU/hr (1,692 kJ/hr)	1,569.6 BTU/hr (1,656 kJ/hr)	1,723.1 BTU/hr (1,818 kJ/hr)	1,707.9 BTU/hr (1,802 kJ/hr)
Power factor	0.98	0.89	0.98	0.89
Rush current†	25 A or less	25 A or less	25 A or less	25 A or less
Leakage current†	1.75 mA or less	1.75 mA or less	1.75 mA or less	1.75 mA or less

*. In a redundant configuration, the rated current per cord is half the value shown in TABLE 3-3.

†. This value represents the current for each power cord.

Information About Software

This section describes the special instructions and the issues about the SPARC Enterprise M3000 server software.

Active Directory and LDAP/SSL

The XCP 1091 release introduces support for the Active Directory and LDAP/SSL features.

- Active Directory is a distributed directory service from Microsoft Corporation. Like an LDAP directory service, it is used to authenticate users.
- LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. It uses LDAP directory service to authenticate users.

Note – For security reasons, XSCF uses only LDAP over SSL protocol (LDAPS) to communicate with an Active Directory server or an LDAP/SSL server.

Active Directory and LDAP/SSL each provides both authentication of user credentials and authorization of the user access level to networked resources. They use authentication to verify the identity of users before they can access system resources, and to grant specific access privileges to users in order to control their rights to access networked resources.

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

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

- In the simplest case, user's privileges are determined directly through the Active Directory or LDAP/SSL configuration on the XSCF. There is a defaultrole parameter for both Active Directory and LDAP/SSL. If this parameter is configured or set, all users authenticated via Active Directory or LDAP/SSL are assigned privileges set in this parameter. Setting up users in an Active Directory or LDAP/SSL server requires only a password with no regard to group membership.
- If the defaultrole parameter is not configured or set, user privileges are learned from the Active Directory or LDAP/SSL server based on the user's group membership. On XSCF, the group parameter must be configured with the corresponding group name from the Active Directory or LDAP/SSL server. Each group has privileges associated with it which are configured on the XSCF. A user's group membership is used to determine the user's privileges once authenticated.

Three types of groups can be configured: administrator, operator, and custom. To configure an administrator or operator group, only group name is required.

An administrator group has `platadm`, `useradm`, and `auditadm` privileges associated with it. An operator group has `platop`, and `auditop` privileges associated with it. To configure a custom group, both group name and privileges are required. For each type of group, up to five groups can be configured. A user assigned to more than one group receives the sum of all privileges associated with those groups.

To support these new features, two new configuration screens (`Active Directory` and `LDAP/SSL`) have been added to the `Settings` menu of the XSCF Web. Remote users can log in and use the XCSF Web once they have been authenticated by Active Directory or LDAP/SSL.

Note – If you are an Active Directory or LDAP/SSL user, do not upload a public key. If one has already been uploaded, use the following command to delete it:
`XSCF>` **`setssh -c delpubkey -a -u proxyuser`**
If you are an Active Directory or LDAP/SSL user, be sure to log in to the XSCF network through the SSH service by the authentication not with the user public key but with the password.

Configuring XSCF for Active Directory Support

The commands setad(8) and showad(8) let you set and view the Active Directory configuration from the command line.

By default, Active Directory support is disabled. To enable Active Directory support, use the following command:

```
XSCF> setad enable
```

To disable Active Directory support, use the following command:

```
XSCF> setad disable
```

To show if Active Directory support is enabled or disabled, enter:

```
XSCF> showad
```

Use the setad(8) command with its various parameters to configure Active Directory. For example, you can use it to set up one primary and five alternate Active Directory servers, assign group names and privileges, configure a particular user domain, control logging of diagnostic messages, and more. User domain can be configured explicitly through the setad userdomain command on XSCF, or entered at login prompt using the form, user@domain.

See the setad(8) and showad(8) man pages, and the note about these commands in TABLE 11.

Configuring XSCF for LDAP/SSL Support

The commands setldapssl(8) and showldapssl(8) let you set and view LDAP/SSL configuration from the command line. These commands do for LDAP/SSL what the setad(8) and showad(8) commands do for Active Directory, and support many of the same parameters.

For more information, see the setldapssl(8) and showldapssl(8) man pages.

Notes on User Account Name and UID

If the Service Processor is configured to use Lightweight Directory Access Protocol (LDAP), Active Directory, or LDAP/SSL for user account data, the user name and UID (if specified) must not already be in use locally or in LDAP, Active Directory, or LDAP/SSL.

New `proxyuser` System Account

To support Active Directory and LDAP/SSL, this release features a new system account named `proxyuser`. Verify that no user account of that name already exists. If one does, use the `deleteuser`(8) command to remove it, then reset XSCF before using the Active Directory or LDAP/SSL feature.

XCP Issues and Workarounds

This section contains information about XCP issues. TABLE 4, TABLE 5, and TABLE 6 list issues you might encounter, depending upon which XCP release you are using.

Known Issues and Workarounds in XCP 1093

TABLE 4 lists known XCP issues and possible workarounds in XCP 1093.

TABLE 4 Known Issues and Workarounds in XCP 1093

ID	Description	Workaround
RTIF1-080725-001	In `setsnmp addv3traphost`, when the authentication failed due to the reasons such as the trap host not working, or the wrong user name or password, the subsequent SNMP traps will not be notified.	No workaround is available. Confirm that the SNMP trap host is working and re-execute the `setsnmp`(8) command using the correct user name.
RTIF1-080725-002	When the SNMPv3 trap has been set, after the watchdog timeout occurred in XSCF and XSCF reset, the subsequent SNMP traps will not be notified.	Reset the XSCF.
RTIF1-081016-002	When FRUs are cold-replaced (with the system off), (after `poweron`) the monitor process might not generate entries in the monitor message log identifying the replacement operation that has occurred.	No workaround is available.
RTIF1-081225-001	In the `settimezone -c adddst` command, when you set eight or more letters to the abbreviation of time zone and the name of Daylight Saving Time, execution of the `showlogs` command induces a segmentation fault and results in an error.	Specify the abbreviation of time zone and the name of Daylight Saving Time in seven letters or less.

TABLE 4 Known Issues and Workarounds in XCP 1093 *(Continued)*

ID	Description	Workaround
RTIF1-090108-003	Date and time of the Last Update which displayed on the XSCF Web may not be updated.	Please refresh the display.
RTIF1-090427-005	When you use the `setpasswordpolicy`(8) command and set "`9999999999`" (10 digits) in Different Characters, the `showpasswordpolicy`(8) command displays "`-1`."	No workaround is available. Use XSCF Web.
RTIF1-100331-001	When you use the `sethttps`(8) command to create the self CA (Certificate Authority) or a CSR with specifying only spaces (for example, " ") in the *e-mail* operand, the HTTPS function might be disabled after XSCF reset.	When you create the self CA or a CSR, do not specify only spaces in the *e-mail* operand.
RTIF1-100331-002	When you start up a domain from a disk that is connected to the 8Gbps fibre channel card (SE0X7F21F, SE0X7F22F) and if it is unable to start the domain due to causes such as disk failure, an error log of "`FRU: /UNSPECIFIED`" might be registered.	No workaround is available.

XCP Issues Fixed in XCP 1093

TABLE 5 lists XCP issues fixed in XCP 1093.

TABLE 5 XCP Issues Fixed in XCP 1093

ID	Description	Workaround
RTIF1-100713-001	While the Solaris 10 OS is running, if the occurrence of RED State Exception or watchdog reset or the execution of the `reset xir` command lead to the domain CPU reset, the following message might be displayed on the console and the domain might hang up. `Failed to complete trap processing. mid=0xXX`	No workaround is available. When this problem occurred, turn off the domain power and then turn on.

XCP Issues Fixed in Releases Earlier Than XCP 1093

TABLE 6 lists XCP issues that have been fixed in releases earlier than XCP 1093.

TABLE 6 XCP Issues Fixed in Releases Earlier Than XCP 1093

ID	Description	Workaround
RTIF1-070418-009	While XSCF is running, a process may go down, a watchdog timeout may occur, or a hang-up may occur. After this, XSCF may reset.	Check that XSCF is started. If not started, stop the domain and then execute the system power off/on (AC OFF/ON). To turn on the system power that you turned off, wait at least 30 seconds before power-on.
RTIF1-070528-002	While XSCF is running, watchdog timeout may occur and XSCF may reboot.	Check that XSCF is started. If not started, stop the domain and then execute the system power off/on (AC OFF/ON). To turn on the system power that you turned off, wait at least 30 seconds before power-on.
RTIF1-070824-001	When remote power control mode of interlocking mechanism for power supply to domain, is enabled, after the motherboard unit is replaced, the interlocking for power supply by RCI cannot work.	After the motherboard unit is replaced, configures the RCI again and sets the remote power control mode.
RTIF1-071102-002	The snmp daemon might quit.	To restart the snmp daemon, issue the command `setsnmp enable`.
RTIF1-080725-004	After set the Daylight Saving Time by using the XSCF shell, XSCF Web does not show the correct time in the Logs menu.	No workaround is available. Use the `showlogs`(8) command of the XSCF shell.
RTIF1-081006-001	The error log "`XSCF FMEM write error`" recorded and the firmware update might fail.	Power off (AC OFF) the system, and power on (AC ON) again. Then, re-execute the firmware update.
RTIF1-081006-002	In the `setemailreport`(8) command, when you specified over 255 characters in the SMTP address, an error results.	Do not specify over 255 characters in the SMTP address.
RTIF1-081006-003	During the domain operation, after the XSCF reset due to the XSCF unit failure, the hardware status shows `Deconfigure` in the status of CPU and memory.	Replace the motherboard unit only. When no failure found on the memory, you do not need to replace the memory.
RTIF1-081006-004	During the firmware update, there might be the following output message and a XSCF panic might occur. `kernel BUG in jffs2_do_read_inode at fs/jffs2/readinode.c:XXX!`	Reset XSCF and use the `flashupdate`(8) command to retry the firmware update.

TABLE 6 XCP Issues Fixed in Releases Earlier Than XCP 1093 *(Continued)*

ID	Description	Workaround
RTIF1-081006-005	The network configuration on the XSCF Web does not support the function equivalent to the `setnetwork -r` command. And when you specified localhost or localdomain to the host name or the domain name, the error message "`SessionID has expired`" appears.	Use the `setnetwork -r` command on the XSCF shell.
RTIF1-081006-006	The panic log on the XSCF Web might not be displayed from the top of the message.	When the output is insufficient, execute the `showlogs panic` command on the XSCF shell.
RTIF1-081006-007	The `password`(8) command indicates that the [*user*] operand is optional but will fail if a [*user*] operand is not included when other options are specified.	No workaround is available. Specify the *user* operand to execute the `password`(8) command when you specify other options.
RTIF1-081006-011	SNMP trap host configuration changes are not valid until `setsnmp disable` and `setsnmp enable`.	Modify the SNMP setting: XSCF> `setsnmp disable` XSCF> `setsnmp enable`
RTIF1-081016-001	Power failure at the commercial AC supply connector to the UPS does not send notification/send trap.	No workaround is available.

RTIF1-081016-003	In Internet Explorer 6 or 7, clicking on the [Reset] button then the [OK] button from the Settings->Audit->Add Policy poupup screen will log the user out with message:
	`Error`
	`Session Error`
	`Session ID has been expired`
		Log back into the browser interface and use the `backspace` key to clear text in the 'User' text box of the popup screen instead of using the Reset button.

RTIF1-081030-002	When the timezone other than three characters has been set, the error logs cannot be displayed on XSCF Web "Error Log" page. In addition, XSCF Web "Panic Log" and "IPL Message Log" pages display the date on the table with "---".	Use the `showlogs`(8) command on the XSCF shell.
RTIF1-081104-001	The monitor message log might not be registered when a PCI slot error detected.	No workaround is available. Use the `showlogs error` command or the `fmdump` command to check the fault information of PCI slot.
RTIF1-090108-001	The domain console may display this message: `ipsec_check_inbound_policy: Policy Failure for the incoming packet (not secure)`	This message can be safely ignored.

TABLE 6 XCP Issues Fixed in Releases Earlier Than XCP 1093 *(Continued)*

ID	Description	Workaround
RTIF1-090108-002	In the dual power feed system, when the power failure and the power recovery occurred repeatedly on one line, all domains will be forcibly powered off. And in the power recovery from the forced power-off, a PSU illegal configuration might be registered in the error log and the power recovery might not be started.	You need to remove and insert the power cable.
RTIF1-090115-001	When you execute the `settelnet -c disable` command, the Telnet service will be stopped immediately. However, unless you reset XSCF by using the `rebootxscf`(8) command, you might fail in the subsequent restart of the Telnet service.	After you stopped the Telnet service, execute the `rebootxscf`(8) command to reset XSCF.
RTIF1-090122-001	"`Power recovery`" message is output before a PSU has recovered.	After the "`Power recovery`" message is output, wait 60 seconds before removing power from another PSU.
RTIF1-090220-001	In a system connecting multiple hosts and one or more I/O units with RCI, the power-on operation to one of those RCI hosts may not power on any of the RCI I/O units.	All the RCI hosts shall be powered on.
RTIF1-090220-002	After replaced the motherboard unit, the RCI power interlocking setting restores to its default value.	If you have set the power interlocking to a value other than the default, replace the motherboard unit and then use the `setpwrmode`(1M) command to set the power interlocking setting again.
RTIF1-090427-001	Despite the normal status of ppp network interface for the XSCF-to-Solaris OS communication, SNMP MIB notifies abnormal (down) status.	No workaround is available.
RTIF1-090427-002	After the XSCF reset or switching, you cannot login to XSCF using the LDAP server.	No workaround is available. Log in to active XSCF with initial account and execute the following command to re-import the certificate chain. '`setldap -c` <*remote file*>'
RTIF1-090427-004	In the setting of the LDAP server, the number of characters which can be specified differs between XSCF Web and XSCF Shell. On XSCF Web, you can enter up to 128 characters.	To set 129 characters or more, use XSCF Shell.
RTIF1-090430-001	After you set https (using the self certificate authority) by XSCF and created a web server certificate, https is not enabled.	To set the self certificate authority, do not specify a blank character.

TABLE 6 XCP Issues Fixed in Releases Earlier Than XCP 1093 *(Continued)*

ID	Description	Workaround
RTIF1-090508-001	In a domain mounted with the 10 Gigabit Ethernet card (SE0X7HE1F), when you set the OpenBoot PROM environmental variable `diag-switch?` to `true`, the following warning message appears on the console; and at the same time, "`Msg: Device error (FCode informed error)`" is recorded in the error log. `WARNING: /pci@7,700000: FCODE map-in doesn't match decoded register type;` And when you execute the `showstatus`(8) command, "`Degraded`" might be indicated to the FRU which has installed the relevant card.	The entire output can be safely ignored. To avoid these outputs, execute the following command at the ok prompt and set the OpenBoot PROM environmental variable `diag-switch?` to `false`. `setenv diag-switch? false`
RTIF1-090729-001	When you use the `sethttps`(8) command to create a self-signed web server certificate, if the number of characters specified in a parameter exceeds 100, it might result in an internal error and you might fail to create the certificate.	Specify up to 100 characters in the parameter and execute the `sethttps`(8) command again.
RTIF1-090824-001	The XSCF might go down and require a reboot, or you might see console error messages and a core dump (`ereport.chassis.software.core`) when one of these conditions occurs: • A local account has been created with a user ID explicitly assigned to a value larger than 65536 (`adduser -u` *uid*). • An LDAP account has been used that has a UID value larger than 65536.	Use only user accounts with a user ID (UID) value between 100 and 60000. This is the range of auto-assigned UIDs for the XSCF command `adduser`(8).
RTIF1-091021-001	While Active Directory is enabled, if you log in to XSCF using the user name that registered in the Active Directory server, the `showconsolepath`(8) command displays not the log-in user name but "`proxyuser`."	No workaround is available.
RTIF1-091105-001	The `loadcert console` operand is missing in the usage of the `setad`(8) command and the `setldapssl`(8) command.	For how to use the `loadcert console` operand of the `setad`(8) command and the `setldapssl`(8) command, see the man page.
RTIF1-091109-001	Once domain detected a failure related to DIMM or PCI, the error log about this detected failure is registered every time you reset XSCF.	This error log can be safely ignored.

TABLE 6 XCP Issues Fixed in Releases Earlier Than XCP 1093 *(Continued)*

ID	Description	Workaround
RTIF1-091109-002	In XSCF, a host route cannot be set. When you use the `setroute`(8) command and set the netmask to 255.255.255.255, it returns an `invalid parameter`.	To set a host route, do not specify the netmask (`-m` option).
RTIF1-091109-003	When you use the `setnameserver`(8) command or the DNS setting of XSCF Web to register the DNS server or the search path, you can specify two or more same IP address values or domain names. However, when you specify two or more same IP address values or domain names to delete all the DNS servers or the search paths which are same, it returns an `invalid parameter`.	To delete all the DNS servers or the search paths which are same, specify just one corresponding address or domain name. In doing so, all the DNS servers or the search paths which are same will be deleted. Register the data again as needed.
RTIF1-091109-004	When you start up a domain from a disk connected to the 8-Gbps fibre channel card (SE0X7F21F, SE0X7F22F), if you fail to specify the correct device path, an error log with no message might be registered. In the same way, when you start up a domain from a disk connected to the 8-Gbps fibre channel card (SE0X7F21F, SE0X7F22F), even if the domain cannot be started due to reasons such as disk failure, the error log might not be registered.	No workaround is available.

Solaris OS Issues and Workarounds

This section contains information about Solaris OS issues. TABLE 7, TABLE 8, TABLE 9 and TABLE 10 list issues you might encounter, depending upon which Solaris OS release you are using.

Solaris OS Issues and Workarounds for All Supported Releases

TABLE 7 lists Solaris OS issues that you might encounter in any supported release of Solaris OS.

TABLE 7 Solaris OS Issues and Workarounds for All Supported Releases

CR ID	Description	Workaround
6481002	Installing the Solaris OS from the network using certain PCI-Express cards may cause a panic.	If you are using a Sun PCI-E Dual Gigabit Ethernet Adapter MMF card or a Sun PCI-E Dual Gigabit Ethernet Adapter UTP card, do not install the Solaris using either of these cards. Instead, use other network devices, such as the onboard Gigabit Ethernet or another network device.
6519290	Large amounts of I/O on swap devices can cause the system to appear hung by overwhelming the I/O system. The amount of I/O required can be generated through a number of ways, eg memory shortage, heavy use of `/tmp` etc.	Set the following to `/etc/system` and then reboot the domain: `set maxfastscan=0x2000`
6531036	The error message `network initialization failed` appears repeatedly after a boot net installation.	No workaround is available. This message can be safely ignored.

6532215	volfs or dscp service may fail when domain is booted.
	
	`svc:/platform/sun4u/dscp:default: Method "/lib/svc/method/svc-dscp start" failed with exit status 95.`
	
	`svc:/system/filesystem/volfs:default: Method or service exit timed out. Killing contract 59.`
		Restart the service if the failure is observed. To avoid the problem, issue the following commands.
		
		`# svccfg -s dscp setprop start/timeout_seconds=count: 300`
		`# svccfg -s volfs setprop start/timeout_seconds=count: 300`
		`# svcadm refresh dscp`
		`# svcadm refresh volfs`

TABLE 7 Solaris OS Issues and Workarounds for All Supported Releases *(Continued)*

CR ID	Description	Workaround
6537511	Bluetooth partner is hung during security tests execution.	Restart application server.

6660168	If a `ubc.piowbeue-cpu error` occurs on a domain, the Solaris Fault Management cpumem-diagnosis module might fail, causing an interruption in FMA service.
	If this happens, you will see the following output in the console log:
	`SUNW-MSG-ID: FMD-8000-2K, TYPE: Defect, VER: 1, SEVERITY: Minor`
	`EVENT-TIME: Fri Apr 4 21:41:57 PDT 2008`
	`PLATFORM: SUNW,SPARC-Enterprise, CSN: 2020642002, HOSTNAME: <hostname>`
	`SOURCE: fmd-self-diagnosis, REV: 1.0`
	`EVENT-ID: 6b2e15d7-aa65-6bcc-bcb1-cb03a7dd77e3`
	`DESC: A Solaris Fault Manager component has experienced an error that required the module to be disabled. Refer to http://sun.com/msg/FMD-8000-2K for more information.`
	`AUTO-RESPONSE: The module has been disabled. Events destined for the module will be saved for manual diagnosis.`
	`IMPACT: Automated diagnosis and response for subsequent events associated with this module will not occur.`
	`REC-ACTION: Use fmdump -v -u <EVENT-ID> to locate the module. Use fmadm reset <module> to reset the module.`
		If FMA service fails, issue the following command on the domain to recover:
		`# svcadm clear fmd`
		
		Then restart cpumem-diagnosis:
		`# fmadm restart cpumem-diagnosis`

6668237	After DIMMs are replaced the corresponding DIMM faults are not cleared on the domain.	This has been fixed in patch 143527-01. [*Workaround*] Use the following commands: `# fmadm repair` *fmri*|*uuid* `# fmadm rotate`

TABLE 7 Solaris OS Issues and Workarounds for All Supported Releases *(Continued)*

CR ID	Description	Workaround
6723202	The `raidctl` command cannot be used to create a hardware RAID using the onboard SAS/LSI controller on the SPARC Enterprise M3000 server. The `raidctl` command can be used to view disk/controller status, and can be used on any PCI Host Bus Adapter (HBA) installed in the system.	No workaround is available. This issue will not be fixed.
6745410	Boot program ignores the Kadb option which causes the system not to boot.	Use kmdb instead of kadb.
6765239	If a SAS device containing multiple SAS targets is connected to the onboard external SAS interface, it will not work properly. The enumeration of target IDs within the device may change across reboots.	Use a FUJITSU SAS card (SE0X7SA1F/SE0X7SA1X). Alternatively, check for the availability of a patch for this defect.
6872501	If 139555-08 has been applied to the domain, cores are not offlined when requested by the XSCF. This CR effects only Solaris 10 5/09, Solaris 10 10/09, and an earlier version of Solaris OS with patch 139555-08.	This has been fixed in patch 143359-02. [*Workaround*] Use `fmdump`(8) with its `-v` option on the Service Processor to identify the faulty core. Once identified, use `psradm`(1M) on the domain to offline the core.
6888928	IPMP interface fails since probe packets are not sent through that interface. Problem occurs with M3000/M4000/M5000/M8000/M9000 servers running any Solaris release running IPMP with patch 141444-09 installed.	This has been fixed in patch 142900-02. [*Workaround*] Disable probe-based failure detection.

Solaris OS Issues Fixed in Solaris 10 10/09

TABLE 8 lists issues that have been fixed in Solaris 10 10/09 OS. You might encounter them in supported releases earlier than Solaris 10 10/09.

TABLE 8 Solaris OS Issues Fixed in Solaris 10 10/09

CR ID	Description	Workaround
6572827	The `prtdiag -v` command reports PCI bus types incorrectly. It reports "PCI" for PCI-X leaf devices and "UNKN" for legacy PCI devices.	This has been fixed in patch 141444-09. [*Workaround*] No workaround is available.
6800734	The `deleteboard`(8) command hang in a domain.	This has been fixed in patch 141444-09. No workaround is available.
6827340	DR and Memory patrol might fail due to command error.	This has been fixed in patch 142344-01. No workaround is available.

Solaris OS Issues Fixed in Solaris 10 5/09

TABLE 9 lists issues that have been fixed in Solaris 10 5/09 OS. You might encounter them in supported releases earlier than Solaris 10 5/09.

TABLE 9 Solaris OS Issues Fixed in Solaris 10 5/09

CR ID	Description	Workaround
6588555	XSCF reset during DR operation to the permanent memory might cause domain panic.	This has been fixed in patch 139555-08. [*Workaround*] Do not start an XSCF reset while a DR operation is running. Wait for a DR operation to finish before starting the reset.
6623226	The Solaris command `lockstat`(1M) or the dtrace lockstat provider might cause a system panic.	This has been fixed in patch 140336-01. [*Workaround*] Do not use the Solaris `lockstat`(1M) command or the dtrace lockstat provider.

TABLE 9 Solaris OS Issues Fixed in Solaris 10 5/09 *(Continued)*

CR ID	Description	Workaround
6680733	Sun Quad-port Gigabit Ethernet Adapter UTP (QGC) & Sun Dual 10 GigE Fiber XFP Low Profile Adapter (XGF) NICs might panic under high load conditions.	This has been fixed in patch 139570-01. [*Workaround*] If possible, use the card in x8 slot. Otherwise, there is no workaround.
6689757	Sun Dual 10 GigE Fiber XFP Low Profile Adapter (XGF) with a single or improperly installed XFP optical transceivers might cause the following error to show on the console: `The XFP optical transceiver is broken or missing.`	This has been fixed in patch 139570-01. [*Workaround*] Check and make sure that both XFP optical transceivers are firmly seated in the housing. Do not mix INTEL and Sun XFP optical transceivers in the same Adapter. Do NOT plumb a port with the ifconfig command if the port does not contain an XFP optical transceiver or it contains one but the transceiver is not in use.
6725885	`cfgadm` will display non-existent SPARC Enterprise M3000 system boards (SB1 to SB15).	This has been fixed in patch 140401-01. The `cfgadm` output for SB1-SB15 can be ignored.

Solaris Issues Fixed in Solaris 10 10/08

TABLE 10 lists issues that have been fixed in Solaris 10 10/08 OS. You might encounter them in supported releases earlier than Solaris 10 10/08.

TABLE 10 Solaris OS Issues Fixed in Solaris 10 10/08

CR ID	Description	Workaround
6608404	Hot-plug of the X4447A-Z, PCI-e Quad-port Gigabit Ethernet Adapter UTP card might cause other network devices to fail.	To avoid the defect, do not install this card.

TABLE 10 Solaris OS Issues Fixed in Solaris 10 10/08 *(Continued)*

CR ID	Description	Workaround

6679370	The following message may be output on the console during the system booting.
	
	`SUNW-MSG-ID: SUN4-8000-75, TYPE: Fault, VER: 1, SEVERITY: Critical`
	`...`
	`DESC:`
	`A problem was detected in the PCI-Express subsystem.`
	`Refer to http://sun.com/msg/SUN4-8000-75 for more information.`
	`...`
		This has been fixed in patch 137137-09.
		Note - Before adapting the patch, delete the following setting from `/etc/system`:
		`set pcie_expected_ce_mask = 0x2001`
		
		[*Workaround*]
		Add the following to `/etc/system` and then reboot the domain.
		
		`set pcie_expected_ce_mask = 0x2001`

6720261	If your domain is running Solaris 10 5/08 OS, the system might panic/trap during normal operation:	This has been fixed in patch 137137-09. [*Workaround*] Set the following parameter in the system specification file (`/etc/system`): `set heaplp_use_stlb=0` Then reboot the domain.

Software Documentation Updates

This section contains late-breaking software information that became known after the documentation set was published and corrections in the SPARC Enterprise M3000 server software documentation.

The corrections for *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF Reference Manual*, if not otherwise specified, also apply to the man pages which XSCF provides. These corrections supersede the information on the man pages.

TABLE 11 lists known documentation updates.

TABLE 11 Software Documentation Updates

Title	Page Number	Update
SPARC Enterprise M3000/M4000/M5000/ M8000/M9000 Servers XSCF User's Guide		The description of this feature, described in "Active Directory and LDAP/SSL" on page 14, has not yet been added.
	8-19	8.1.10, two sections, "Confirming That the XSCF Firmware Is Updated When the XSCF Unit Is Replaced (in a System With a Single XSCF Unit or Both Replacement in a System With Redundant XSCF Units)" and "Confirming That the XSCF Firmware Is Updated When the MBU Is Replaced (in the M3000 server) ", the step2 and step3 will be changed as below: 2. If the replacement unit and the replaced unit have different versions, a message is displayed. In this case, the firmware is not updated automatically. The operator must match the number of the firmware versions. 3. When you update, follow the procedure in "Updating XCP From External Media" or "Updating XCP From the Network" to update XCP, and confirm the version.

Identifying Degraded Memory in a System

1. **Log in to XSCF.**
2. **Type the following command:**

```
XSCF> showstatus
```

The following example identifies that DIMM number 0A on the Motherboard unit has degraded memory..

```
XSCF> showstatus
    MBU_A Status:Normal;
*     MEM#0A Status:Degraded;
```