System Release 7.17.2
ASTRO® 25
INTEGRATED VOICE AND DATA

Generic Application Server
Feature Guide

NOVEMBER 2017

MN004334A01-A

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN004334A01-A	Original release of the *Generic Application Server Feature Guide*.	November 2017

This page intentionally left blank.

Contents

List of Figures

This page intentionally left blank.

List of Tables

List of Procedures

This page intentionally left blank.

List of Processes

This page intentionally left blank.

About Generic Application Server Feature Guide

This manual provides an introduction to the Generic Application Server (GAS). Included are detailed procedures for installation, configuration, operation, and maintenance. This manual is intended to be used by field service managers and field service technicians after they have attended the Motorola Solutions formal training.

NOTICE: Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

What Is Covered in this Manual?

This manual contains the following chapters:

- Generic Application Server Description on page 27, provides a high-level description of the server hardware, the Generic Application Server, and its functions.
- Generic Application Server Theory of Operation on page 39, provides additional explanation of the functions of the Generic Application Server.
- Generic Application Server Installation on page 43, details installation procedures for the Generic Application Server.
- Generic Application Server Configuration on page 61, details configuration procedures relating to the Generic Application Server.
- Generic Application Server Operation on page 77, details the tasks that you perform once the Generic Application Server is installed and operational.
- Generic Application Server Maintenance on page 93, provides maintenance information relating to the Generic Application Server.
- Generic Application Server Troubleshooting on page 99, provides fault management and troubleshooting information relating to the server hardware and the Generic Application Server.
- Generic Application Server FRU/FRE Procedures on page 119, lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs), and includes replacement procedures applicable to the server hardware.
- Generic Application Server Reference on page 141, contains supplemental reference information relating to the server hardware and the Generic Application Server.
- Disaster Recovery on page 149, provides disaster recovery procedures pertaining to the Generic Application Server.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Refer to the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as the R56 manual. This document may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation Reference Guide	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
ISSI.1 Network Gateway Feature Guide	Includes information required to understand, install, manage, and troubleshoot an ISSI.1 Network Gateway Site, an interconnectivity solution for P25 ISSI.1 compatible systems.

Chapter 1

Generic Application Server Description

This chapter provides a high-level description of the Generic Application Server and the function it serves in your system.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

1.1 Generic Application Server Overview

The Generic Application Server is a software installed on each server, along with the embedded Oracle® Solaris operating system.

The Generic Application Server supports the virtualization of applications. Virtualization supports multiple applications residing on a reduced number of hardware platforms. The Generic Application Server uses Solaris Containers to permit multiple server applications to run as virtual servers on the same physical hardware.

The Generic Application Server performs the following functions:

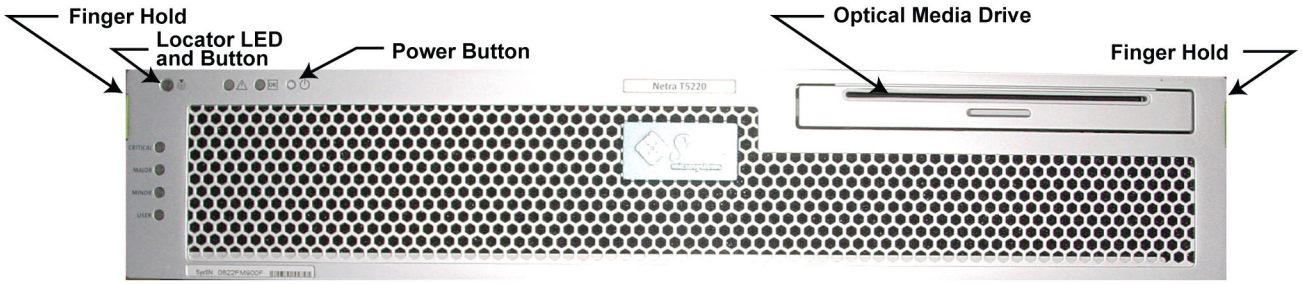
- Isolates applications from hardware by providing a generic interface to any hardware-specific functionality.
- Supports the virtualization of applications, enabling the applications to use containers and to share common platform resources.
- Assigns and controls access to platform resources. Ensures that no single application can reserve or use resources to the extent that other applications are unable to execute.
- Sends environment-related traps (temperature, voltage, current, and so on) to the Unified Event Manager (UEM).
- Provides capability to start up and shut down the entire physical server.

1.2 Generic Application Server Components

Depending on a system configuration, the Generic Application Server resides on the Sun Netra T5220 server or the Netra SPARC T4-1 server, or, for the PTT Gateway, the Sun Netra X4270 with Solaris 10 operating system. For more information about the PTT Gateway hardware and applications, see the Public Safety LTE *Push-To-Talk (PTT) Gateway* manual.

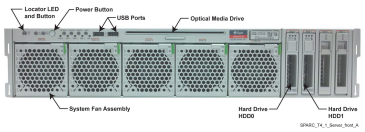
The T5220 server runs on the Sun Solaris 2.10 operating system and the T4-1 server on the Oracle® Solaris 11 or Oracle® Solaris 10 operating system.

Figure 1: T5220 Server Front Panel Components



Netra_T5220_Server_front1

Figure 2: T4-1 Server Front Panel Components



1.2.1
T5220 Server Components

This section describes the Sun Netra T5220 server.

1.2.1.1
T5220 Server Front Panel Components

Front panel components include:

- Bezel assembly and finger holds to open the bezel
- Locator LED and button
- Power button
- DVD-RW optical media drive

Locator LED and Button

The Locator LED and button enable you to identify a particular server in a rack. The LED and button are physically colocated. You can remotely turn on the Locator LED from the Sun Integrated Lights Out Manager (ILOM). Use the lighted LED to identify the server, and then, on the server, press the Locator button to toggle off the Locator LED.

NOTICE: There are two Locator LEDs and buttons: one on the front, and the other on the rear of the server.

Power Controls

The power cables control power supply to the server. As soon as power cables are connected, standby power is applied.

CAUTION: Do **not** use the recessed Power button on the front of the server, to power off the server. Using this button could produce an undesired server state. The preferred way to power off the server is from the ILOM.

Optical Media

The DVD-RW optical media drive is used to load and install the Generic Application Server software, other applications, and patches on the hard drive.

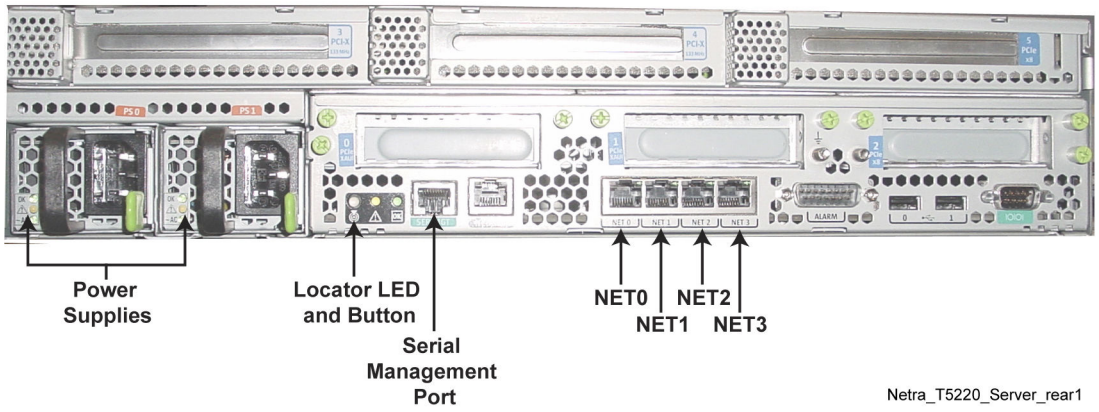
1.2.1.2

T5220 Server Rear Panel Components

Rear panel components include:

- Power supplies
- Ports
- Locator LED and button

Figure 3: T5220 Server Rear Panel Components



1.2.1.2.1

T5220 Server Ports

Table 1: Ports on the Server – T5220 Server on page 29 describes the ports on the rear of the server, as shown in Figure 3: T5220 Server Rear Panel Components on page 29. The front of the server has no ports.

Table 1: Ports on the Server – T5220 Server

Port	Description
Power supplies (PS1, PS0)	The rear panel has two 650 W power supplies. The redundant 650 W power supplies provide power to the server subcomponents. One power supply can be hot-swapped while the other is still running, without having to power off the server.
SER MGT	RJ-45 serial connector to the terminal server for managing the Generic Application Server; it can be used to access the ILOM and the server console through the ILOM.
NET MGT	One 10/100 Mbps Ethernet network management port (not used)
Ethernet 0 (NET0)	100 Mbps full duplex, RJ-45 connector for Ethernet connection; used in all configurations.
Ethernet 1 (NET1)	100 Mbps full duplex, RJ-45 connector for Ethernet connection
Ethernet 2 (NET2)	100 Mbps full duplex, RJ-45 connector for Ethernet connection
Ethernet 3 (NET3)	100 Mbps full duplex, RJ-45 connector for Ethernet connection

Table continued…

Port	Description
Alarm	DB-15 connector to the central office alarm system (not used)
USB ports	USB ports (from left to right): USB0, USB1 (not used)
IOIOI	DB-9 connector for general purpose serial data transfers (not used)

1.2.1.3

T5220 Server Front LEDs

Figure 4: T5220 Server Front Showing LEDs

Netra_T5220_Server_front_LEDs

1.2.1.3.1

T5220 Server System Status Indicators

The server has system status indicators that are on the front of the server.

Table 2: Server System Status Indicators

LED	Color	Description
Locator	White	Enables you to identify a particular server. Press the button to toggle the indicator on or off. You can turn on the Locator LED from the ILOM. This LED provides the following indications: • Off - Normal operating state. • Fast blink - The server received a signal as a result of one of the ILOM commands.
Service Required	Amber	Provides a fault detection indicator. This LED provides the following indications: • Off - Normal operating state. • On - Indicates that service is required. The `show faulty` command provides details about any faults that cause this indicator to illuminate.
Activity	Green	Provides the power and operating system indicator. This LED provides the following indications: • On - Drives are receiving power. Solidly lit if the drive is idle. • Flashing - Drives are processing a command. • Off - Power is off.

1.2.1.3.2

T5220 Server Alarm Status Indicators

The alarm status indicators are located vertically on the bezel of the server. Only the Critical LED is used.

NOTICE: Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

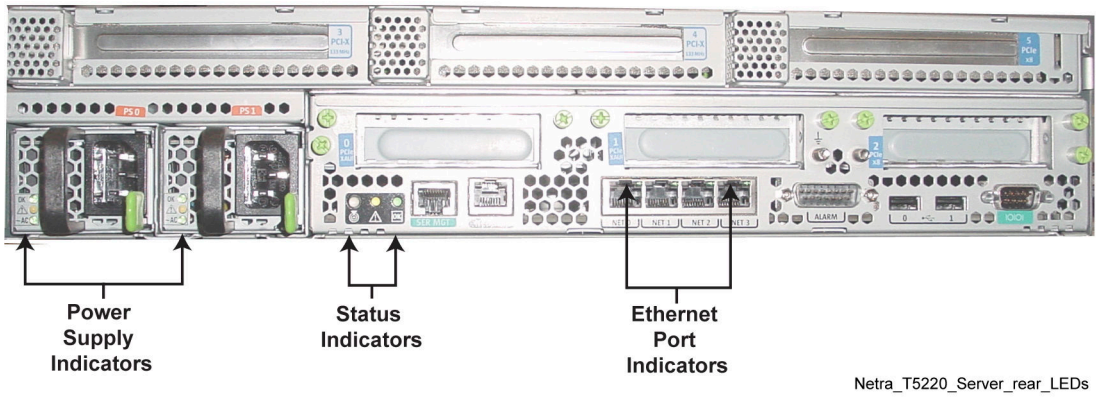
Table 3: T5220 Server Alarm Status Indicators

LED	Color	Description
Critical	Red	Indicates a critical alarm.
Major	Red	Not used, as alarms are reported to the UEM.
Minor	Amber	Not used, as alarms are reported to the UEM.
User	Amber	Not used, as alarms are reported to the UEM.

1.2.1.4

T5220 Server Rear LEDs

Figure 5: T5220 Server Rear Showing LEDs



1.2.1.4.1

T5220 Server Power Supply Unit Indicators

The Power Supply Unit (PSU) LEDs are on the rear of each power supply on the left side. This table describes the PSU status indicators, in order, from top to bottom.

Table 4: T5220 Server Power Supply Indicators

LED	Color	Description
Power OK	Green	• On - Normal operation. • Off - Power is off.

Table continued…

LED	Color	Description
Fault	Amber	• On - Power supply has detected a failure. • Off - Normal operation.
Input OK	Green	• On - Normal operation. Input power is within normal limits. • Off - No input voltage, or input voltage is below limits.

1.2.1.4.2

T5220 Server System Status Indicators

The server has system status indicators that are on the rear of the server.

Table 5: T5220 Server System Status Indicators

LED	Color	Description
Locator	White	Enables you to identify a particular server. Press the button to toggle the indicator on or off. You can turn on the Locator LED from the ILOM. This LED provides the following indications: • Off - Normal operating state. • Fast blink - The server received a signal as a result of one of the ILOM commands.
Service Required	Amber	Provides a fault detection indicator. This LED provides the following indications: • Off - Normal operating state. • On - Indicates that service is required. The `show faulty` command provides details about any faults that cause this indicator to illuminate.
Power OK	Green	Provides the power and operating system indicator. This LED provides the following indications: • Off - The system is unavailable. Either the system has no power or the ILOM is not running. • Steady on - Indicates that the system is powered on and is running in its normal operating state. • Standby blink - Indicates that the service processor is running while the system is running at a minimum level in Standby mode, and is ready to be returned to its normal operating state. • Slow blink - Indicates that normal transitory activity is taking place. The system diagnostics might be running, or the system might be booting.

1.2.1.4.3

T5220 Server Network Link and Speed Indicators

The network link indicator LED is at the upper left of each Ethernet connector, labeled 0-3.

The network speed indicator LED is at the upper right of each Ethernet connector, labeled 0-3.

Table 6: T5220 Server Network Link and Speed Indicators

LED	Color	Description
Network Link Indicator (left side)	Green	Network link status • Steady On - A link is established. • Blinking - Activity has been detected on this port. • Off - No link is established.
Network Speed Indicator (right side)	Amber or Green	Network speed status • Amber On - The link is operating as a Gigabit connection (1000 Mbps). • Green On - The link is operating as a 100-Mbps connection. • Off - The link is operating as a 10/100-Mbps connection.

1.2.1.5

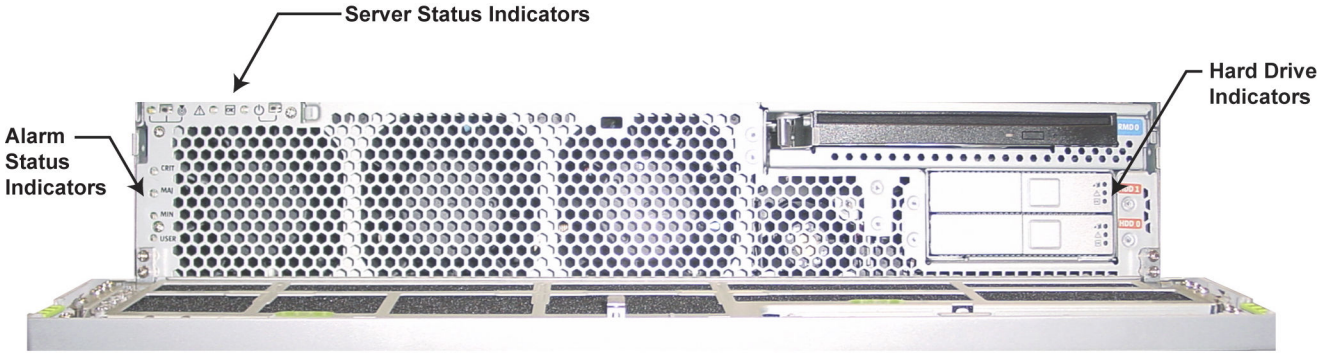
T5220 Server Open Bezel LEDs

This section describes the LEDs on the front of the open bezel, which include the following:

- System status indicators
- Alarm status indicators
- Hard drive indicators

NOTICE: The system status indicators and alarm status indicators are identical to the front of the server, so only the hard drive indicators are described in detail in this section.

Figure 6: T5220 Server Open Bezel Showing LEDs



Netra_T5220_Server_front_wo_cover_LEDs

1.2.1.5.1

T5220 Server Hard Drive Indicators

The hard drive indicator LEDs are located to the right of each hard drive installed in the server chassis. The bezel must be open to view the hard drive indicators, as shown in Figure 6: T5220 Server Open Bezel Showing LEDs on page 33. For more information, see T5220 Server Internal Components on page 121.

1.2.2
T4-1 Server Components

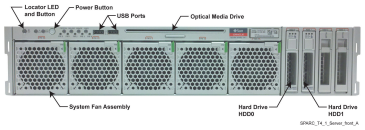
This section describes front and rear panel components of the Netra SPARC T4-1 server.

1.2.2.1
T4-1 Server Front Panel Components

The front panel components include:

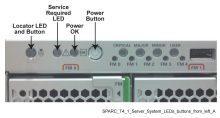
- Locator LED and button
- Power button
- USB ports
- Hard Drives
- Fan assembly
- DVD-RUSB optical media drive

Figure 7: T4-1 Server Front Panel Components



1.2.2.2
T4-1 Server Front LEDs and Buttons

Figure 8: T4-1 Server Front Showing LEDs and Power Buttons



Alarm lights on the front panel of the T4-1 server are not in use.

Table 7: T4-1 Server Front Panel System LEDs and Buttons

LED/Button	Color	Description
Locator LED and button	White	The Locator LED can be turned on to identify a particular system. When on, it blinks rabidly. There are two methods for turning a Locator LED on: • Issuing the Oracle ILOM command set /SYS/LOCATE value=Fast_Blink • Pressing the Locator button.
Service Required LED	Amber	Steady on light – a fault has been detected in the system and that service is required.
Power OK LED	Green	• Off – System is not running in its normal state. System power might be off. The SP might be running. • Steady on – System is powered on and is running in its normal operating state. No service actions are required.

Table continued…

LED/Button	Color	Description
		• Blink – System is running in standby mode and can be quickly returned to full operation. • Slow blink – A transitional activity is taking place. • Fast blink – SP is booting.
Power button	N/A	The recessed Power button toggles the system on or off. • Press and release to turn on the system. • Press and release to shut down the system in a normal manner. • Press and hold for more than 5 seconds to perform an emergency shutdown.

1.2.2.3

T4-1 Server Rear Panel Components

Figure 9: T4-1 Server Rear Panel Components

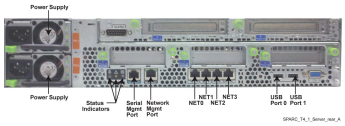


Table 8: Ports on the T4-1 Server Rear

Port	Description
Power supplies (PS1), (PS0)	The rear panel has two 650 W power supplies. The redundant 650 W power supplies provide power to the server subcomponents. One power supply can be hot–swapped while the other is still running, without having to power off the server.
SER MGT port	RJ-45 serial connector to the terminal server for managing the server; it can be used to access ILOM and the server console through ILOM.
NET MGT port	One 10/100 Mbps Ethernet network management port (not used).
Ethernet port 0 (NET0)	100 Mbps full duplex, RJ-45 connector for Ethernet connection. Used in all configurations.
Ethernet port 1 (NET1)	10 Mbps half duplex, RJ-45 connector for Ethernet connection.
Ethernet port 2 (NET2)	10 Mbps half duplex, RJ-45 connector for Ethernet connection.
Ethernet port 3 (NET3)	Autonegotiating, RJ-45 connector for Ethernet connection.
USB ports (0, 1)	USB ports left to right: USB0, USB1 (not used).
VGA video port (IOIOI)	Connector for general purpose serial data transfers (not used).

1.2.2.4
T4-1 Server Rear Power LEDs

The Power Supply Unit (PSU) LEDs are on the rear of each power supply on the left side.

Figure 10: T4-1 Server Power Supply LEDs

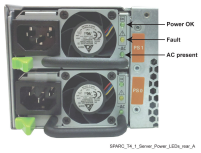


Table 9: T4-1 Server Power Supply Indicators

LED	Color	Description
Power OK	Green	• On Normal operation. • Off Power is off.
Fault	Amber	• On Power supply has detected a failure. • Off Normal operation. **NOTICE:** The front and rear panel Service Required LEDs are also lit when the system detects a power supply fault.
AC Present	Green	This LED turns on when AC voltage is applied to the power supply. **NOTICE:** For DC models, the DC input OK LED. It turns on when the input DC power is present.

1.2.2.5
T4-1 Server Hard Drive Indicators

Figure 11: T4-1 Server Rear Showing Status Indicators

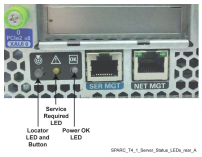


Table 10: T4-1 Server Rear Panel System Indicators

LED/Button	Color	Description
Locator LED and button	White	The Locator LED can be turned on to identify a particular system. When on, it blinks rabidly. There are two methods for turning a Locator LED on: • Issuing the Oracle ILOM command set /SYS/LOCATE value=Fast_Blink • Pressing the Locator button.
Service Required LED	Amber	Steady on light – a fault has been detected in the system and that service is required.

Table continued…

LED/Button	Color	Description
Power OK LED	Green	• Off – System is not running in its normal state. System power might be off. The SP might be running. • Steady on – System is powered on and is running in its normal operating state. No service actions are required. • Blink – System is running in standby mode and can be quickly returned to full operation. • Slow blink – A transitional activity is taking place. • Fast blink – SP is booting.

1.3
Generic Application Server in the System

The Generic Application Server (GAS) provides scalability and allows one or multiple applications to run on a single server. Software applications can be consolidated, while providing your organization with the full operational benefits and functionality of ASTRO® 25 systems.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

1.3.1
Application Containers on Generic Application Servers

The Generic Application Server (GAS) is based on the Solaris operating system and automates the creation of logical servers, called containers, to host ASTRO® 25 system applications.

GAS has the following functionality:

- Supports multiple application containers on a single physical server.
- Assigns and controls access to server resources.
- Ensures that no single application can reserve or use resources to the extent that other applications are unable to execute.

1.3.2
Server Applications on Generic Application Servers

Your ASTRO® 25 system can include Generic Application Servers (GAS) to host the ISSI.1 Network Gateway.

NOTICE:
For the current ASTRO® 25 system release, the ISSI.1 Network Gateway is supported on a T5520 or T4.

Table 11: ISSI.1 Network Gateway Configuration on Generic Application Servers

The following table lists the server applications installed on a GAS-based ISSI.1 Network Gateway.

Resident Applications	GAS ID Number	Application Name
Up to three pairs of ISSI applications (one pair consists of an ISSI.1 Gateway Module and a Site Link Relay Module).	1	z00XsYYYgas01.zoneX

For more information on the ISSI.1 Network Gateway, see the *ISSI1. Network Gateway Feature Guide*.

1.4 Level of the Access

You enters your personal domain account credentials (user name and password) to access a Generic Application Server. The access privileges of a user account are based on the roles assigned to the user. Functions and tasks you must perform on an ASTRO® 25 system are grouped into logical roles. Each role equates to a domain group maintained in the Active Directory. A user account can be a member of one or many domain groups. Group membership is assigned to a user, based on the performed tasks.

However, the root account is the only account that can be used to access the Generic Application Server locally – the Active Directory maintains the root account (a local account).

The Integrated Lights Out Manager (ILOM) accounts are used to monitor and manage the system platform. The ILOM account passwords are set during the installation. ILOM accounts are not domain controlled.

All passwords can be changed as necessary after installation.

Table 12: ILOM User Accounts

User	Level of the Access
ILOM root account	System-level maintenance account. This account can only log on using the system console. Connecting at this level through Secure Shell (SSH) protocol is not allowed. This account can perform any ILOM command.
ILOM service account	Operator account. This account is for nondestructive actions, such as power on/off, status check, and switch to the console.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see Appendix B in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

The only local account on the GAS is root. All other accounts are domain controlled. Everyone uses their personal account. Access to the GAS and command execution privileges on the GAS are based on the ASTRO® 25 system authorization roles assigned to a personal account. A domain group equates to an ASTRO® 25 system authorization role. The domain group membership of the user's account determine the access and command execution privileges.

Chapter 2

Generic Application Server Theory of Operation

The Generic Application Server is based on the Solaris operating system and automates the creation of logical servers, called containers, to host ASTRO® 25 system applications. The Generic Application Server is used to automate the installation and configuration process (including Solaris installation and configuration, security tools configuration, and supplemental configuration). It is also used for SNMP fault management.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

2.1 Managing Resources

The Generic Application Server functions as the primary container (in Solaris terminology, as a global zone). Application containers reside within the Generic Application Server environment.

- The Generic Application Server is always present, and serves as the default Solaris environment. Unlike the containers, the Generic Application Server is bootable from the physical hardware.
- Each container contains a virtual Generic Application Server environment. The privileges of a container are always a subset of the privileges assigned to the Generic Application Server. Containers allow the consolidation of several applications onto one hardware platform. Containers provide virtual mapping from an application to the platform resources.

The Generic Application Server manages resources, such as LAN ports, in the same way, regardless of whether a single or multiple application is installed. The Generic Application Server sets limits on the resources that an application can request. For example, for the LAN ports, the Generic Application Server uses physical LAN ports and creates virtual LAN ports that are available for each application. Only the Generic Application Server has access to the physical resources of the server.

2.2 Resource Balancing

Resource balancing is important for the installation and operation of multiple applications. Resource balancing is the feature on the Generic Application Server that guarantees a minimum amount of resources for the containers. Depending on the configuration, it allows the containers to use all available resources. By default, this feature is disabled and must be enabled from the Generic Application Server administration menu. When the feature is enabled, unreserved SWAP and RAM are redistributed among the installed applications.

The resources that can be balanced are limited to RAM and SWAP. The CPU is always balanced by the operating system, using the fair share scheduling algorithm, regardless of the state of resource balancing.

The containers should have sufficient resources. A non-configurable setting within the application determines whether the application supports resource balancing. Resource balancing should be enabled after the container application installation is complete.

2.3 POST

The power-on self test (POST) runs various system checks before bringing the system up to normal operation, as follows:

```
0:0:0>POST enabling CMP 0 threads: 00000000.ffffffff
0:0:0>VBSC mode is: 00000000.00000001
0:0:0>VBSC level is: 00000000.00000001
0:0:0>VBSC selecting Normal mode, MAX Testing.
0:0:0>VBSC setting verbosity level 2
0:0:0>Basic Memory Tests....Done
0:0:0>Test Memory....Done
0:0:0>Setup POST Mailbox ....Done
0:0:0>Master CPU Tests Basic....Done
0:0:0>Init MMU.....
0:0:0>NCU Setup and PIU link train....Done
0:0:0>L2 Tests....Done
0:0:0>Extended CPU Tests....Done
0:0:0>Scrub Memory....Done
0:0:0>SPU CWQ Tests...Done
0:0:0>MAU Tests...Done
0:0:0>Network Interface Unit Tests....Done
0:0:0>Functional CPU Tests....Done
0:0:0>Extended Memory Tests....Done
```

2.4 Integrated Lights Out Manager

The Sun Integrated Lights Out Manager (ILOM) is a system controller that enables you to remotely manage and administer the server. The server is shipped with ILOM installed. The ILOM provides advanced service processor hardware and software that you can use to manage and monitor the server. It also provides access to the Solaris console.

The ILOM allows you to actively manage and monitor the server, independent of the state of the operating system. You can see hardware faults, control the power state of the server, view the status of sensors, view the buffered console history, and determine hardware configuration. The ILOM runs an embedded operating system and has its own serial management port used to connect to the ILOM.

By default, the system console is directed to ILOM and is configured to show server console information as soon as you install and power on the server. The ILOM enables you to monitor and control your server from the serial management port, using a connection from the system terminal server. ILOM provides a command-line interface used to administer remote servers.

Table 13: Components Monitored by the ILOM

Component Monitored	Information Revealed
Voltage	Status and thresholds
System enclosure temperature	Ambient temperature and any thermal warning or failure conditions
CPU	Presence, temperature, and any thermal warning or failure conditions
Power supplies	Presence and status
Hard drive	Presence and status

Table continued…

Component Monitored	Information Revealed
Front and rear fans	Speed in revolutions per minute (rpm) and status
Server front and rear	LED status

2.5 Software Components

Virtualization

Server virtualization is done through the creation of containers, as the applications are installed. It enables the applications to share common platform resources. Virtualization of applications means that multiple applications reside on the same physical platform, and all applications see the multiprocessor as a single CPU.

Containers

Solaris Containers is an operating system-level virtualization technology built into the Generic Application Server. It uses software-defined boundaries to isolate software applications and services, allowing multiple environments to be created within a single instance of the Generic Application Server. Each environment has its own identity.

The Generic Application Server uses Solaris Containers to permit multiple server applications to run as virtual servers on the same physical hardware. A container is Oracle implementation of virtualization. The Generic Application Server builds the containers automatically during the installation of ASTRO® 25 system applications.

2.6 Backup and Recovery Overview

The backup administrator can perform backups but is not authenticated to perform restore operations. A user that belongs to the secadm group can restore ssh keys only, and an install admin can restore all.

Table 14: Backup and Recovery Overview

Generic Application Server Level	Application Level
Persistent Storage backup: • Backs up critical data locally. • See Backing Up the Generic Application Server to Persistent Storage on page 95.	Back up data on the server applications separately.
Restore: • Restores critical data. • The Restore procedure is the same for all backups. • See Restoring the Generic Application Server from Persistent Storage on page 96.	Restore data on the server applications separately.

2.7

Managing the Generic Application Server and Its Applications

Administrative Menu Structure for the Generic Application Server on page 146 shows the menu structure for the Generic Application Server and clarifies the purpose for its options. Executing a Menu Option from the Administrative Menu on page 145 explains how to execute any of the menu options.

Chapter 3

Generic Application Server Installation

This chapter details installation procedures relating to the Generic Application Server.

3.1 Installing the Generic Application Server Overview

Process:

1. Install the physical hardware. See Hardware Installation and Parts Overview on page 43.
2. Connect the cables. See Cable Connections on page 46.
3. If the server is not powered on, see Powering On the Server on page 77.
4. Perform one of the following actions:
   - If a server with Solaris is already installed, perform Preparing to Reinstall a Generic Application Server on page 116.
   - If you perform a server out-of-the-box installation, perform Preparing for the Generic Application Server Installation on page 47.
   - If you Install the firmware (if necessary), perform Installing the System Firmware on page 49.
5. Install the Generic Application Server on all the servers, see Installing the Generic Application Server on page 52.
6. Set up the time zone and local date and time. See Configuring the Time Zone on page 74 and Setting the Local Date and Time on page 74.
7. Load the applications, see Loading the Applications on page 56.
8. Install the applications, see Installing the Applications on page 57.
9. Ensure that the UEM manages Generic Application Servers. See Discovering Generic Application Servers in Unified Event Manager on page 59.

3.2 Hardware Installation and Parts Overview

For installation procedures, see Installing a T5220 Server in a Rack on page 44 or Installing a T4-1 Server in a Rack on page 45.

T5220 Server Rack Mount Installation

The servers ship with either a 19-inch, 4-post rack mount or a cabinet. The rack kit consists of:

- Two mounting brackets
- Two rear mount support brackets
- Two rear mount flanges
- Bag of screws (see the following table)

In the rest of this manual, the term rack means either an open rack or a closed cabinet.

Table 15: 19–Inch Rack Mount Screw Kit Contents – T5220 Server

Amount	Description	How Used
10	M5 x 4.5 mm Phillips flathead screws	8 for mounting brackets, 2 extra
10	M4 x 0.5 mm x 5 mm Phillips panhead screws	4-6 for rear mount brackets, 6-4 extra
10	M5 x 12.7 mm screws	10 for rack (if needed)
10	M6 x 13 mm screws	10 for rack (if needed)
9	M6 square clip nuts	9 for rack (if needed)
12	10-32 x 0.5 in. combo head screws	12 for rack (if needed)
12	12-24 x 0.5 in. combo head screws	12 for rack (if needed)

T4-1 Server Rack Mount Installation

When you receive your server, place it in the environment where you plan to install it. Leave it in a shipping crate at its final destination for 24 hours. This resting period prevents thermal shock and condensation.

Verify that you have received all components that ship with your server. The servers ship with a 4-post rack (mounting at both front and rear). The rack kit consists of:

- SPARC T4-1 server
- 2 AC power cords
- RJ-45 to DB-9 crossover adapter for the SER MGT port
- Antistatic wrist strap
- Rack mount kit
- Cable management arm (if ordered)
- “SPARC T4-1 Server Getting Started Guide” with license and safety documents
- Optional components (for example, PCIe cards) that are packaged separately from the other items

Ensure that:

- Distance between front and rear mounting planes are minimum 622 mm and maximum 895 mm (24.5 inches to 35.25 inches).
- Distance to a front cabinet door is at least 27 mm (1.06 inch).
- Distance to a rear cabinet door is at least 900 mm (35.5 inches) with the cable management arm, or 770 mm (30.4 inches) without the cable management arm.
- Distance between structural supports and cable troughs is at least 456 mm (18 inches).

For details, see “SPARC T4-1 Server Getting Started Guide”.

3.2.1
Installing a T5220 Server in a Rack

Prerequisites: Ensure that the front and rear clearance of the server allow a minimum of 5 mm (0.2 in.) at the front of the server and 80 mm (3.15 in.) at the rear of the server, when mounted. The front-to-back rail spacing must be at least 460 mm (18.11 inches) and not more than 715 mm (28.15 inches) from the outside face of the front rail to the outside face of the back rail.

WARNING: The equipment may be damaged if wrong screws are used to install a server in a rack.

NOTICE: When installing servers, Motorola Solutions recommends mounting the first device in the lowest position in the rack, allowing for ventilation, and then continuing to build towards the top with additional servers.

Procedure:

1. Install the mounting brackets. Using eight of the supplied M5 x 4.5 mm flathead Phillips screws (four screws for each bracket), secure the mounting brackets to the sides of the server. Ensure that the handles are facing the front of the server.
2. Measure and record the depth of the rack.
3. Install the rear mount support brackets. Using two to three of the supplied M4 x 0.5 x 5 mm panhead Phillips screws for each bracket, install the rear mount support brackets on the sides of the server towards the rear. Extend the rear mount support brackets to the measured depth of the rack. If the rack is especially deep, you may only be able to secure the rear mount support brackets using two screws per side.
4. Lift the server to the desired location in the rack.

   WARNING: Including the brackets, the server weighs approximately 40 pounds. Use caution when lifting.
5. Using two screws per side, secure the front of the mounting brackets attached to the sides of the server to the front of the rack.
6. Using two screws for each rear mount support bracket, secure the rear mount support brackets to the rear of the rack.
7. Attach one end of the dedicated green ground cable to the grounding stud on the back of the server. Attach the other end of the ground cable to the rack grounding BUS bar attached to the rack.

   NOTICE: While the AC power cords do provide ground to the AC power supplies of the server, the whole server system is grounded through the dedicated green ground cable.
8. Connect the cables to the server, as described in Cable Connections on page 46.

3.2.2
Installing a T4-1 Server in a Rack

CAUTION:
The weight of the servers on extended slide rails can be enough to overturn an equipment rack.

The server weighs approximately 60 lb (25 kg). Two people are required to lift and mount the server into a rack enclosure.

Procedure:

1. Ensure that the rack is compatible with the server installation requirements.
2. To stabilize the rack, perform the following actions:
   - **a** Open and remove the front and rear doors from the rack cabinet.
   - **b** Use all anti-tilt mechanism provided.
   - **c** Extend leveling feet fully downward to the floor.
   - **d** Extend all anti-tilt devices before installing the server.
3. Install Slide Rails. For detailed procedure, see “SPARC T4-1 Server Getting Started Guide”.
4. If the rack is equipped with an antitilt bar, verify that it has been deployed and, if not, deploy it.

5 Insert the ends of the mounting brackets into the sliding rails.

6 While pressing the two green slide rail release buttons, push the server into the rack until the slide rail locks on the front of the mounting brackets engage the slide rail assemblies until you hear a click at that point.

7 Install the CMA. For detailed procedure, see “Install the CMA” in “SPARC T4-1 Server Getting Started Guide”.

8 Connect cables. See Cable Connections on page 46.

3.3 Cable Connections

Before installing software, ensure that all required hardware connections are established.

For more detailed information on specific connections, see the following guides:

- *Master Site Infrastructure Reference Guide*
- *ISSI.1 Network Gateway Feature Guide*

Table 16: Server Cable Connections

Server Port	Connects to	Using	Purpose
SER MGT	Terminal server	Shielded Category 5 Ethernet cable with RJ-45 connectors	Provides console management capability for the server; it can be used to access both the Sun Integrated Lights Out Manager (ILOM) console and the server console. When connecting either a DB-9 or a DB-25 cable, use an adapter to perform the crossovers given for each connector.
Ethernet 0 (NET0)	Ethernet LAN switch	Shielded Category 5 Ethernet cable with RJ-45 connectors	Supports various types of traffic flow, such as fault, configuration, accounting, and performance traffic.
Ethernet 1 (NET1)	Ethernet LAN switch	Shielded Category 5 Ethernet cable with RJ-45 connectors	Supports an Ethernet connection.
Ethernet 2 (NET2)	Ethernet LAN switch	Shielded Category 5 Ethernet cable with RJ-45 connectors	Supports an Ethernet connection.
Ethernet 3 (NET3)	Ethernet LAN switch	Shielded Category 5 Ethernet cable with RJ-45 connectors	Supports an Ethernet connection.
Power Supply	Power source	Standard AC power cord	Provides AC power to the server. Power cords are plugged into the internal power strips installed on the rack.

3.3.1
Cabling Generic Application Servers

Procedure:

1. Connect the SER MGT port on the back of the Netra T5220/T4-1 server to the terminal server, using a shielded Ethernet cable with RJ-45 connectors. The port on the terminal server varies depending on the server and your setup.
2. Depending on the applications installed on this server, connect the Ethernet 0, Ethernet 1, and Ethernet 2 ports, using an Ethernet cable with RJ-45 connectors. The port connections vary, depending on the server and your setup.
3. Attach the socket end of the AC power cable to the power supply connector on the back of the server. Attach the plug end of the power cable to the power source. To ensure redundant operation of the power supplies, connect the two power cords to separate circuits.

   NOTICE: Do not attach power cables to the power supplies until you have finished connecting the data cables and have connected the server to a terminal server. The server goes into Standby mode and the ILOM system controller initializes as soon as the input power cables are connected to the power source. System messages might be lost if the server is not connected to a terminal server at this time.
4. Verify that the server is operational:
   - Review system messages on the terminal server.
   - Ping the router and other servers to verify connectivity.

3.4
Preparing for the Generic Application Server Installation

Follow this procedure to install an out-of-the-box server that was not installed with a previous version of Solaris. This procedure verifies the firmware version and configures the server to boot to the `OK` prompt.

During the install process, you are prompted to set the ILOM password. See ILOM Passwords on page 89.

Prerequisites: Ensure that the networking connections from the server to the Ethernet LAN switch and the terminal server are functioning.

Procedure:

1. Establish a serial connection to the server through the SER MGT port at the back of the server.
2. If not connected already, connect the power cords to the power supplies. Plug the power cords into the power source which applies power to the ILOM only.

   Once connected, the server automatically goes into Standby power mode. The ILOM boots and displays its power-on self-test messages. Though the system power is still off, the ILOM is already monitoring the system, regardless of the system power state. After the ILOM is finished starting up, you will see the ILOM login prompt.
3. Wait for the ILOM login prompt to appear as follows.

   ```
   SUNSPXXXXXXXXXXXX login:
   ```

   The ILOM login prompt starts with **SUNSP**. Service Processor (SP) is the generic name for the ILOM.
4. Perform one of the following actions:

If…	Then…
If the T5220 server is used in your system,	Enter: `root` as a login name and its corresponding password. **Result:** Version information and password set to default messages appear.
If the T4–1 server is used in your system,	Enter: `root` as the ORACLESP-1244BD0C3C login and corresponding password. **Result:** Version information and password set to default messages appear.

5 Enter: `set /SP reset_to_defaults=all`

The ILOM is set to the factory default settings.

6 Enter: `reset /SP`

A restart is initiated. The following confirmation message appears:

```
Are you sure you want to reset /SP (y/n)?
```

Enter: **y**

7 As a login name and its corresponding password, enter: `root`

The following messages appear:

```
SUNSPXXXXXXXXXXX login:
 Password:
 Waiting for daemons to initialize...
 Daemons ready
 Sun(TM) Integrated Lights Out Manager Version
 Version 2.0.4.26
 Copyright 2008 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
 Warning: password is set to factory default.
 ->
```

8 At the ILOM prompt, enter: `show /HOST sysfw_version`

Write down the information obtained. You will need it later. If the version of the Sun System Firmware installed is older than the one on the disk, install the system firmware. See Installing the System Firmware on page 49 after this procedure is complete.

The firmware version appears, as follows:

```
/HOST
 Properties:
 sysfw_version = Sun System Firmware #.#.# YYYY/MM/DD HH:MM
```

9 Configure the server to boot to the `OK` prompt, enter each command. Press ENTER after each entry, as follows:

```
set /HOST/bootmode state=reset_nvramset /HOST/bootmode script='setenv
auto-boot? false'set /SP/policy HOST_AUTO_POWER_ON=enabled
```

10 To power on the server, enter: `start /SYS`

The following prompt appears:

```
Are you sure you want to start /SYS (y/n)?
```

11 Enter: **y**

The `Starting /SYS` message appears.

12 To switch to the host console, enter: `start /SP/console`

The following prompt appears:

```
Are you sure you want to start /SP/console (y/n)?
```

13 Enter: **y**

The system startup messages are printed to the screen; startup may take up to 5 minutes. You may need to press ENTER to see the `OK` prompt.

3.5 Installing the System Firmware

Prerequisites: The system must be powered on at this time. Disks cannot be inserted into the DVD drive unless the system is powered on.

When and where to use: Use this procedure if the version of the Sun System Firmware installed is older than the one on the disk. Otherwise, go to Installing the Generic Application Server on page 52.

Procedure:

1 Insert the *Generic Application Server system Firmware* disk into the DVD drive.

2 At the `OK` prompt, configure the system to stop after the installation of firmware, by entering: `setenv auto-boot? false`

3 Boot the system off the installation media. At the `OK` prompt, enter: `boot cdrom - install`

The system is booted from the Firmware disk and the following message appears:

```
Run Factory Tests? (y/n):
```

4 Enter: **y**

A message appears, containing a summary of factory tests and information on firmware versions. Then the confirmation message appears:

```
Do you wish to install the available firmware? (y/n):
```

5 Depending on the factory test results, perform one of the following actions:

If…	Then…
If all tests passed,	enter: `n` **Step result:** The procedure is now complete. Skip to the last step.
If either the OBP Version and/or LOM Version tests failed,	enter: `y` Go to the next step.
If any tests other than the OBP Version and/or LOM Version tests failed,	the GAS cannot be installed. The service team must investigate. Go to the last step.

6 The firmware disk downloads the firmware image to the ILOM, powers off the host, flashes the firmware, resets the ILOM, and powers on the host.

NOTICE: This process may take up to 20 minutes.

7 Wait for the ILOM login prompt to appear:

```
SUNSPXXXXXXXXXXX login:
```

8 Enter: `root` as a login name and its corresponding password.

The following messages appear:

```
SUNSPXXXXXXXXXXX login:
 Password:
 Waiting for daemons to initialize...
 Daemons ready
 Sun(TM) Integrated Lights Out Manager Version
 Version 2.0.4.26
 Copyright 2008 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
 Warning: password is set to factory default.
 ->
```

9 Verify that the version of the system firmware installed is correct. At the ILOM prompt, enter: `show /HOST sysfw_version`

The version appears as follows:

```
/HOST
 Properties:
 sysfw_version = Sun System Firmware #.#.#.# YYYY/MM/DD HH:MM
```

10 To power on the server, enter: `start /SYS`

The following message appears:

```
Are you sure you want to start /SYS (y/n)?
```

11 Enter: **y**

The system returns one of the following messages:

```
Starting /SYS
 start: Target already started
```

12 To switch to the host console, enter: `start /SP/console`

The following prompt appears:

```
Are you sure you want to start /SP/console (y/n)?
```

13 Enter: **y**

To see the `OK` prompt, you may need to press ENTER.

The system startup messages are printed to the screen; startup may take up to 5 minutes. When startup is complete, the `OK` prompt appears. **Example:**

```
Sun Netra T5220, No Keyboard
 Copyright 2008 Sun Microsystems, Inc. All rights reserved.
 OpenBoot 4.29.0, 32640 MB memory available, Serial #82574156.
 Ethernet address 0:14:4f:eb:fb:4c, Host ID: 84ebfb4c.
 {0} ok
```

14 Push the eject button on the DVD drive to manually eject the media and remove the *Generic Application Server System Firmware* disk from the DVD drive.

3.6

Installing the Firmware in Systems being Upgraded

Procedure:

1. Display the Firmware version and view the current settings. At the Oracle ILOM prompt, enter: `-> show /HOST sysfw_version`
2. Perform the following actions:
   a. Make sure that the Oracle ILOM SP network managements port is configured.
   b. Open an SSH session and connect to the SP: `% ssh root@xxx.xxx.xxx.xxx`

      To continue connecting, enter `yes`

      Wait for Daemons to initialize and a version to display. **Result:** You have logged in to the Oracle ILOM.
   c. To power off the host, enter: `-> stop /SYS`
   d. To set the keyswitch_state parameter to normal, enter: `-> set /SYS keyswitch_state=normal`
   e. Enter `load` with the path to the new flash image. The `load` command updates the SP flash image and the host firmware. This command requires the following information:

- IP address of a TFTP server on the network that can access the flash image
- Full path name to the flash image that the IP address can access.

The command usage is as follows: `load [-script] -source tftp://xxx.xxx.xx.xxx/pathname` where:

`-script` – Does not prompt for confirmation and acts as if yes was specified.

`-source` – Specifies the IP address and full path name (URL) to the flash image.

Step example:
Enter: `-> load -source tftp://129.99.99.99/pathname`

The following appears:

```
NOTE: A firmware upgrade will cause the server and ILOM to be reset.
It is recommended that a clean shutdown of the server be done prior
to the
upgrade procedure.
An upgrade takes about 6 minutes to complete. ILOM will enter a
special mode
to load new firmware.
No other tasks can be performed in ILOM until the firmware upgrade is
complete
and ILOM is reset.
Are you sure you want to load the specified file (y/n)?
```

Enter: `y`

```
Do you want to preserve the configuration (y/n)?
```

Enter: `y`

```
Firmware update is complete.
ILOM will now be restarted with the new firmware.
Update Complete. Reset device to use new image.
->
```

After the flash image has been updated, the server automatically resets, runs diagnostics, and returns to the login prompt on the serial console.

```
U-Boot 1.x.x
Custom AST2100 U-Boot 3.0 (Aug 21 2010 - 10:46:54) r58174
```

```
***
Net:   faradaynic#0, faradaynic#1
Enter Diagnostics Mode ['q'uick/'n'ormal(default)/
e'x'tended(manufacturing mode)] .....   0
Diagnostics Mode - NORMAL
 DIAGS> Memory Data Bus Test ... PASSED
DIAGS> Memory Address Bus Test ... PASSED
I2C Probe Test - SP
Bus     Device                          Address Result
===     ============================    ======= ======
6                  SP FRUID (U1101)     0xA0    PASSED
6               DS1338(RTC) (U1102)     0xD0    PASSED
DIAGS> PHY #0 R/W Test ... PASSED
DIAGS> PHY #0 Link Status ... PASSED
DIAGS> ETHERNET PHY #0, Internal Loopback Test ... PASSED
## Booting image at 110a2000 ... ***

Mounting local filesystems...
Mounted all disk partitions.
Configuring network interfaces...FTGMAC100: eth0:ftgmac100_open
Starting system log daemon: syslogd and klogd.
Starting capidirect daemon: capidirectd . Done
Starting Event Manager: eventmgr  . Done
Starting ipmi log manager daemon: logmgr . Done
Starting IPMI Stack: . Done
Starting sshd.
Starting SP fishwrap cache daemon: fishwrapd . Done
Starting Host deamon: hostd . Done
Starting Network Controller Sideband Interface Daemon: ncsid . Done
Starting Platform Obfuscation Daemon: pod . Done
Starting lu main daemon: lumain . Done
Starting Detection/Diagnosis After System Boot: dasboot  Done
Starting Servicetags discoverer: stdiscoverer.
Starting Servicetags listener: stlistener.
Starting Dynamic FRUID Daemon: dynafrud  Done

hostname login:
```

3. To display the OpenBoot version, enter: `> show /HOST obp_version`
4. To display POST Version, enter: `> show /HOST post_version`

3.7 Installing the Generic Application Server

Prerequisites: If you are installing the server currently running on the Generic Application Server, shut down the server before the installation. See Powering Off the Server on page 89.

When and where to use:
The Generic Application Server can be installed at the Zone Core, or at a site as an ISSI.1 Network Gateway. The installation of Generic Application Server requires the *GAS Application Installation Disk*, which installs both the embedded Solaris operating system and the Generic Application Server software to prepare for installation of other applications.

Procedure:

1. Insert the *GAS Application Installation Disk* into the DVD drive.
2. At the `OK` prompt, enter: `boot cdrom - install nowin`

   The system boots off the installation media and installs the GAS application. The installation is complete when the following prompt appears:

```
gashost console login:
```

3 Enter: `root`

The `#` prompt appears.

4 Enter: `epasswd`

The password prompt appears.

5 Enter a desired password. Press ENTER. Enter the password again to verify it. Press ENTER.

The gashost command-line prompt appears and the password is set.

6 Enter: `admin_menu`

The Generic Administration Server administrative menu appears.

7 Enter the corresponding number for **Software Administration**. Press ENTER.

8 Enter the corresponding number for **Eject CD/DVD**. Press ENTER.

The DVD drive ejects.

9 Enter: **q**

The gashost command-line prompt appears.

Postrequisites:

If a new version of system firmware was installed, perform Configuring System Firmware on page 53.

If the system firmware was not updated, perform Setting GAS Identity Common Starting Steps on page 54.

3.7.1
Configuring System Firmware

Procedure:

1 If needed, log on to the server using the root account credentials.

The gashost command-line prompt appears.

2 Enter: `/cdrom/cdrom0/.install_config/configure_system_fw`

The following confirmation prompt is displayed:

```
Do you wish to configure the firmware and LOM (y/n):
```

3 Enter: **y**

IMPORTANT: Review the output of the configuration during the configuration. If an error condition occurs, the event is displayed on the screen.

When ILOM configuration is complete, the ILOM restarts and the ILOM login prompt appears.

4 Enter: `start /SP/console`

The following confirmation prompt appears:

```
Are you sure you want to start /SP/console (y/n)?
```

5 Enter: **y**

The system switches to the gashost console.

Postrequisites: Continue with Setting GAS Identity Common Starting Steps on page 54.

3.7.2
Generic Application Server Identity

The information entered to answer the prompts in the Set Identity process specifies the GAS identity. The intended purpose of the server determines the answers to the prompts.

3.7.2.1
Setting GAS Identity Common Starting Steps

Procedure:

1. If needed, log on to the server using the root account credentials. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **OS Administration**. Press ENTER.
3. Enter the corresponding number for **Manage Platform Configuration**. Press ENTER.
4. Enter the corresponding number for **Set Identity**. Press ENTER.

   The following prompt appears:

   ```
   Enter the GAS Identity Type (0=Astro, 1=Custom):
   ```

3.7.2.2
Setting GAS Identity in the ASTRO Site

Prerequisites: Setting GAS Identity Common Starting Steps on page 54

Procedure:

1. Enter: **0**

   The following prompt appears:

   ```
   Enter Generic Application Server location (1=Zone Core, 2=Site):
   ```

2. Enter: **2**

   The following prompt appears:

   ```
   Enter Zone ID (1-7):
   ```

3. Enter the appropriate value. Press ENTER.

   The following prompt appears:

   ```
   Enter Site ID (1-100):
   ```

4. Enter the appropriate value. Press ENTER.

   The following prompt appears:

   ```
   Enter GAS ID (1-9):
   ```

5. Enter the appropriate value. Press ENTER.

   The Time Zone Selection prompt appears:

   ```
   TIME ZONE SELECTION
   ------------------
   <Primary Time Zone List>
    Please select a zone (#-#, r - relist):
   ```

Postrequisites: Setting GAS Identity Common Ending Steps on page 55

3.7.2.3

Setting GAS Identity Common Ending Steps

Prerequisites: Setting GAS Identity Common Starting Steps on page 54

Procedure:

1. Enter the number for the primary time zone from the list. Press ENTER.

   The secondary Time Zone Selection prompt appears:

   ```
   TIME ZONE SELECTION
   ------------------
   <Secondary Time Zone List>
   Please select a zone (#-#, r - relist):
   ```

2. Enter the number for the secondary time zone from the list. Press ENTER.

   The following prompt appears:

   ```
   Enter the Centralized Syslog Server(s) for this GAS
   (colon separated list):
   ```

3. Enter the fully qualified domain name (hostname.domainname) for each syslog server.

   For multiple entries, separate each syslog server with a colon (:). Enter nothing if there are no syslog servers for this GAS.

   The following prompt appears:

   ```
   Preserve existing application data? (y/n):
   ```

4. Enter: **n**

   If new installation, there is no data to preserve.
   Issues to consider concerning preserving existing application data:

   - When reinstalling a server, if the GAS ID and/or the ZONE ID for this server were changed, then answer N to this prompt.
   - When reinstalling a server, and the GAS ID and the ZONE ID for this server were not changed, then determine if the data existing on the server should be preserved after the identity is set and answer this prompt accordingly.
   - When installing a new, fresh out of the box server, answer **n** to this prompt.

   The prompting sequence for this identity process is complete. A summary of the entered data appears for confirmation.

   ```
   GAS IDENTITY SUMMARY
   ------------------------------------
   <List of identity parameters and entered values>
   ------------------------------------
   Are these settings correct? (y, n, q - quit):
   ```

5. Review the summary from the previous step and ensure that all identity parameters are correct.

   IMPORTANT: Ensure that the data displayed in the summary is correct before setting the identity of the GAS. Once the identity of the GAS has been set it can only be changed by reinstalling the GAS from the installation media.

If…	Then…
If all identity parameters are correct and the server is ready to have its identity set,	enter: **y** **Step result:** The process updates the identity parameters of the GAS and then server reboots. When finished, the login prompt reflects the hostname of the new identity.
If any of the identity parameters is incorrect,	enter: **n** **Step result:** The Set Identity process goes back to the beginning of the prompting sequence.
If you want to stop the Set Identity process without saving changes to the server,	enter: **q** **Step result:** The Set Identity process exits and the Manage Platform Configuration menu appears.

3.8 Loading the Applications

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

Your system configuration determines which applications to load. The applications can be loaded and installed in any order.

Prerequisites:

- Configure time zone and local date and time. See Configuring the Time Zone on page 74 and Setting the Local Date and Time on page 74. Installing an application without the correct settings for time zone and local date/time might cause errors.
- Join the Generic Application Server to the Domain. See Active Directory Domain on page 66.

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Application Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Load Container Server Software**. Press ENTER.

   The following prompt appears:

   ```
   Please insert application media and press <ENTER>
   ```
4. Insert the optical media of the application to load, depending on your system configuration. Press ENTER. Wait until the drive LED stops blinking before proceeding to the next step.

   The installation file is loaded from the application optical media to the installation depot on the Generic Application Server. The following status message appears:

   ```
   Searching for media...found
   Loading MOTdepot-(app-name)...done
   ```
5. Enter the corresponding number for **Eject CD/DVD**. Press ENTER.

NOTICE: If no media exists in the CD/DVD drive, the following status message appears, followed by the Application Administration menu:

The **Application Administration** menu appears.

6 Repeat step 3 to step 5 for each application being installed on a given Generic Application Server.

7 Log off from the server. See Logging Off the Terminal Server on page 84.

3.9 Installing the Applications

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

CAUTION: A system can become unusable if incorrect applications are installed on the server.

For detailed procedures, see the *ISSI.1 Network Gateway Feature Guide*.

Prerequisites:

- Perform Loading the Applications on page 56
- Join the Generic Application Server to the active directory domain before loading applications.

Procedure:

1 Log on to the Generic Application Server's Main Menu. See Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Application Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Install Containers**. Press ENTER.

- If the `Select a single application` sub-menu appears, continue to step 4.
- If that sub-menu does not appear, continue to step 5.

Depending on which Generic Application Server you are installing, different server applications are ready to be installed. The following prompt appears:

```
Available applications to install are:
<list of applications>
Install <applicationX> (y/n)[y]:
```

4 If a sub-menu appears, enter the corresponding number for the desired application.

The sub-menu appears as follows:

```
Select a single application
<1. application 1>
<2. application 2>
...
<X. application X>
<n. none >
(1-X,n)[1]:
```

5 At the `Install <applicationX>(y/n)[y]:` prompts, enter: `y` for each application you want to install. Press ENTER. At the `Install <instance number>` prompts, enter the number corresponding to the application. Press ENTER.

A series of prompts that follows either asks for an application to be installed and prompts (y/n) to install the application, or asks for the instance number of the application to be installed, and prompts (1-***<x>***, n), where ***<x>*** is the maximum number of instances of the application.

The following message appears:

```
 Confirm installation of <list of applications chosen to install>? (y/
n):
```

6 Enter: `y`

7 Perform one the following actions:

If…	Then…
If the application to be installed can be associated with an existing persistent storage,	the progress message appears. To proceed, enter: `y`
If the application to be installed cannot be associated with an existing persistent storage,	the following message appears: `Application <application name> requires a persistent storage to install. Proceed to create persistent storage? (y, a=abort):` Go to step 9.

8 Enter the number of the persistent storage to be associated with the application that is currently being installed. Press ENTER.

The following message appears:

```
 Application <application name> will be associated with <persistent
storage>.
 Proceed? (y/n):
```

9 Enter: `y`

If multiple applications have been loaded onto the GAS, repeat step 6 and step 8.

The message similar to the following appears, depending on the applications installed:

```
Resource Balancing Status: <current state of resource balancing>
Resources will be allocated as displayed

             Supports   Requested  Requested  Allocated  Allocated
Application  Balancing  RAM (MB)   SWAP (MB)  RAM (MB)   SWAP (MB)
-------------------------------------------------------------------
global zone     No          512      1024        512       1024
zc01.zone1      Yes        1536      3072       1536       3072
zds01.zone1     Yes        1280      2560       1280       2560
atr01.zone1     Yes        1280      2560       1280       2560
===================================================================
Unreserved                                    28032      56064

Are you sure you want to continue? (y/n): y
```

10 Enter: `y`

All the application software begins to install. No other user interaction is required for the installation.

If necessary, you can exit the **Install Containers** menu without interrupting the installation. Exiting is useful for an unattended install. Also, an automatic timeout occurs after 15 minutes; if you are automatically logged out, you can log back on and check the installation status. See Viewing the Installation Status on page 91. If a message appears, indicating that the installation was not completed successfully, then examine the installation logs. See Viewing the Installation Log on page 117.

When the installation is complete, a status message appears, displaying the results of each application installation, along with the following message:

```
Press 'q' to return to menu
```

11 When the installation is marked complete on the status screen, perform resource balancing. See Running Resource Balancing on page 90.

Postrequisites: Exit to the command prompt or log off. See Logging Off the Terminal Server on page 84.

3.10 Discovering Generic Application Servers in Unified Event Manager

Unified Event Manager (UEM) application discovers a Generic Application Server after the GAS software, the applications, and UEM are installed. UEM uses the discovery process to find devices that are managed in the system. For details, see the “UEM Description” and “UEM Operation” chapters of the *Unified Event Manager User Guide*.

In UEM, check the condition of the Generic Application Server and its links to verify that the Generic Application Server is operational.

This page intentionally left blank.

Chapter 4

Generic Application Server Configuration

This chapter details configuration procedures relating to the Generic Application Server.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

4.1 T4-1 Server RAID Configuration Commands

This section lists the command-line-driven SAS-2 Integrated RAID configuration utility and explains how to use them.

Prerequisites:

- Windows®: x86, x64 (AMD64)
- Linux: x86, x86_64 (supported with x86 build), PPC64
- UEFI: EFI Byte Code (EBC)
- Solaris: x86 (or compatible), SPARC

FreeBSD: x86 (or i386), AMD64 (or compatible) SAS2IRCU operates with storage devices that are compliant with existing SCSI standards.

SAS2IRCU requires PCI 2.x or PCI 3.0 firmware and MPI v2.0. SAS2IRCU supports the following operating systems.

Table 17: SASIRCU Commands

SAS2IRCU Commands	Description
CREATE	This command creates Integrated RAID columns on LSI SAS-2 controllers. Command-line: `sas2ircu <controller_#> create <volumen_type><size> {<Enclosure:Bay>} {VolumeName} [nonprompt]` Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<volume_type>*** is a volume type for the new volume. Valid values are RAID0, RAID1, RAID10, or RAID1E. • ***<size>*** of the RAID volume in MB, or *MAX* for the maximum size available. • ***<Enclosure:BAY>*** is the value of the disk drive for the new RAID volume. Determining these values from the output of the DISPLAY command. • ***<[VolumeName]>*** is a user-specified string to identify the volume. • *[nonprompt]* is an optional parameter that prevents warning and prompts from appearing while the command is running.

Table continued…

SAS2IRCU Commands	Description
	Program Return Values: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter.
DELETE	Command-line: `sas2ircu <controller_#> delete [nonprompt]` Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • *[nonprompt]* is an optional parameter that prevents warning and prompts from appearing while the command is running. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter.
DELETEVO-LUME	This command deletes a specific RAID volume and the associated hot spare drives ion the specified controller. Command-line: `sas2ircu <controller_#> deletevolume volumeID [nonprompt]` Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<volumeID>*** is an ID of the specific IR volume that you want to delete. • *[nonprompt]* is an optional parameter that prevents warning and prompts from appearing while the command is running. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter.
DISPLAY	This command displays information about LSISAS-2 controller configurations, including controller type, firmware version, BIOS version, volume information, physical drive information, and enclosure. Command line: `sas2ircu <controller_#> display [filename]` Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • *[filename]* is an optional valid filename to store the command output to a file. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter.

Table continued…

SAS2IRCU Commands	Description
HOTSPARE	This command adds a hot spare drive to spare pool 0 or deletes a hot spare drive. The capacity of the hot spare drive must be greater that or equal to the capacity of the smallest drive in the RAID volume. Determine if this is true using the DISPLAY command on the drive. **Command line:** `sas2ircu <controller_#> hotspare [delete] <Enclusure:Bay>` Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<Enclosure:Bay>*** is the value of the disk drive for the new RAID volume. Determining these values from the output of the DISPLAY command. • *[delete]* command deletes the hot spare disk at *Enclosure:Bay*. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter.
STATUS	This command displays the status of any existing Integrated RAID volumes and the status of any operation currently in progress on the selected controller. If no operation is in progress, SAS2IRCU prints a message indicating this condition before it exits. Command-line: `sas2ircu <controller_#> status` Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
LIST	This command displays a list of all controllers in the system, along with each corresponding controller index. You need the controller index as an input parameter for other SAS2IRCU commands. Command line: `sas2ircu list` No parameters. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find specified adapter
CONSTCHK	This command requests the Integrated RAID firmware to start a consistency check operation on the specified volume. Command-line: `sas2ircu <controller_#> constchk <volumeID> [nonprompt]`

Table continued…

SAS2IRCU Commands	Description
	Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<volumeID>*** is an ID of the specific IR volume that you want to delete. • *[nonprompt]* is an optional parameter that prevents warning and prompts from appearing while the command is running. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
ACTIVATE	This command activates an inactive Integrated RAID volume. Command-line: `sas2ircu` ***<controller_#>*** `activate` ***<volumeID>*** Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<volumeID>*** is an ID of the specific IR volume that you want to delete. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
LOCATE	This command locates a specific drive in a volume by turning on its location indicator and flashing its LED. The command works only for drives installed in a disk enclosure. It does not work for drives attached directly to the enclosure. Command line: `sas2ircu` ***<controlelr_#>***`locate` ***<Enclosure:Bay><action>*** Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<Enclosure:Bay>*** is the value of the disk drive for the new RAID volume. Determining these values from the output of the DISPLAY command. • ***<action>***: - **ON** – Turn on the location indicator of the drive - **OFF** – Turn off the location indictor of the drive. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
LOGIR	This command uploads or clears the Integrated RAID log information. Command-line: `sas2ircu controller_#> logir` ***<action>***`[filename] [nonpormpt]`

Table continued…

SAS2IRCU Commands	Description
	Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<action>***: - **UPLOAD** – Upload the controller logs to a file - **CLEAR** – Clear the controller logs. • *[filename]* specifies the name of the file to which the logs must be uploaded. The default filename is LOGIR.LOG. • *[nonprompt]* – prevents warning and prompts from appearing while the command is running. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
BOOTIR	This command selects an existing RAID volume as the primary boot device. If an IR volume is selected as the boot device, the DISPLAY command displays this information in the IR Volume information section, if the selected IR boot volume is available to the controller. If you attempt to set a failed RAID volume as the primary boot device, the command fails with a warning message. For example, if volume 322 is in the failed state and you attempt to set it as the primary boot device, SAS2IRCU displays the following error message: `SAS2IRCU: Volume specified by 322 is in Failed state!` Command line: `sas2ircu` ***<controller_#>*** `bootir` ***<volumeID>*** Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<volumeID>*** is an ID of the specific IR volume that you want to delete. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
BOOTENCL	This command selects a specific enclosure/slot as the primary boot device. If an enclosure/slot is selected as the boot location, the DISPLAY command displays this information in the Enclosure information section. Command line: `sas2ircu` ***<controller_#>*** `bootencl` ***<Enclosure:Bay>*** Parameters: • ***<controller_#>*** is the index of the controller for the newly created volume. • ***<Enclosure:Bay>*** is the value of the disk drive for the new RAID volume. Determining these values from the output of the DISPLAY command. **Program Return Values**:

Table continued…

SAS2IRCU Commands	Description
	0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure. 0x02 ADAPTER_NOT_FOUND: Cannot find a specified adapter
HELP	This command displays usage information for the command specified in the input parameter. Command-line: `sas2ircu help <commandname>` Parameters: • ***<commandname>*** is a name of a supposed SAS2IRCU command. **Program Return Values**: 0x00 — SUCCESS: Command completed successfully. 0x01 — FAILURE: Bad command-line arguments or operational failure.

4.2 Information Assurance Configuration

This section explains configuring information assurance. The following procedures are performed on the Generic Application Server, regardless of which applications are loaded on the server.

- Enabling Centralized Authentication, which involves Active Directory Domain on page 66
- Enabling Centralized Event Logging on page 69
- SNMP Credentials on page 71

For more information on these features, see the *Information Assurance Reference Guide*.

4.2.1 Active Directory Domain

Join the Generic Application Server to the Active Directory domain to centralize passwords at the domain server.

You can either join only the Generic Application Server to the domain or to join the Generic Application Server and all the applications to the domain. It is highly recommended that you join the GAS to the domain immediately after GAS installation, and then select the **join all** option, after all the containers have been installed. Joining all rejoins the GAS to the domain, while joining all the Applications to the domain. If the applications have been joined to the domain from the GAS, they do not have to join to the domain individually.

4.2.1.1 Joining the Generic Application Server to the Domain

Prerequisites:

- The Network Time Protocol (NTP) servers, Domain Name Services (DNS) servers, and domain controllers must be operating before you proceed with the joining procedure.
- Validate the time between the Generic Application Server and the domain controller. The time must be synchronous within 2 minutes before you proceed with the joining operation.
- Contact your system administrator for the domain administrator account name and password that are needed for this procedure.

Procedure:

1 Log on to the server using the root account credentials. See Logging On to the Generic Application Server on page 85.

IMPORTANT: To perform this procedure, log on as a root. Only the root account can join the GAS and applications to the Active Directory Domain. Root is the only interactive account available to access the GAS before joining the GAS to the domain.

2 Enter the corresponding number for **Services Administration**. Press ENTER.

3 Enter the corresponding number for **Manage AAA Client Configuration**. Press ENTER.

4 To join the GAS to the domain, enter the corresponding number for **Join Domain**. Press ENTER.

5 Perform one of the following actions:

If…	Then…

If a GAS currently joined to a domain,	the following message appears:
	`Currently joined to the Domain: [DOMAIN_NAME]`
	`To join another domain, first un-join this domain.`
	`Unjoin from this domain (y/n):`
	Enter **y** and provide the domain administrator account and password to unjoin.
	The GAS is unjoined from the domain.

If a GAS did not join to a domain,	no additional messages appear.

The list of available Active Directory Domains is displayed, similar to the following:

```
1. [domain]
Select a domain to join (1, q):
```

6 Enter the corresponding number of the domain to be joined. Enter the domain admin account and its corresponding password to authorize the join process.

The following message appears, followed by the Manage AAA Client Configuration menu, when finished:

```
Using short domain name -- [SHORT_DOMAIN_NAME]
Joined '[GAS_HOSTNAME]' to realm '[DOMAIN_NAME]'
Processing...Join is OK
```

7 Log off the server. See Logging Off the Terminal Server on page 84.

4.2.1.2

Joining the Generic Application Server and All Installed Applications to the Domain

Prerequisites:

- The Network Time Protocol (NTP) servers, Domain Name Services (DNS) servers, and domain controllers must be operating before you proceed with the joining procedure.
- Validate the time between the Generic Application Server and the domain controller. The time must be synchronous within 2 minutes before you proceed with the joining operation.
- Contact your system administrator for the domain administrator account name and password that are needed for this procedure.

IMPORTANT: Only the root account can join the GAS and Applications to the Active Directory Domain. Root is the only interactive account available to access the GAS before joining the GAS to the domain. To perform this procedure, log on as a root.

Procedure:

1. Log on to the server using the root account credentials. See Logging On to the Generic Application Server on page 85.
2. Type the corresponding number for **Services Administration**. Press ENTER.
3. Type the corresponding number for **Join All to the Domain**. Press ENTER.
4. Select **Join All to a Domain**. Press ENTER.

   A list of all installed applications, including the GAS with the current domain status, is displayed, followed by a list of available domains. **Example:**

```
ApplicationDomainMembership Status
----------------------------------------------------------
z001gas03.zone1[domain]Joined
z001zc02.zone1<NONE>Not Joined

Active Directory Domains
-----------------------------------
1. [domain]
Select a domain to join (1, q):
```

5. Enter the number of the domain to be joined, and provide the domain administrator account and password.

   A message similr to the following one appears:

```
All applications will be joined to:
AD Domain: [domain]
AD Username: [domain administrator]
Proceed with Join All operation (y/n):
```

6. Enter: **y**

   A message similar to the following one appears, followed by the **Manage AAA Client Configuration** menu:

```
Joining: z00Xgas0Y.zoneX
Using short domain name -- [domain]
Joined 'Z00XGAS0Y' to realm '[domain]'
Processing...Join is OK

Joining: z00X[appname].zoneX
Using short domain name -- A79
Joined 'Z001[APNAME]' to realm '[domain]'
Processing...Join is OK

Join All successful
```

7. Log-off the server. See Logging Off the Terminal Server on page 84.

4.2.2
Displaying Domain Membership Status

Procedure:

1. Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Services Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Manage AAA Client Configuration**. Press ENTER.

4 Enter the corresponding number for **Display Domain Membership Status**. Press ENTER.

A list of applications currently installed on the GAS server is displayed, together with their domain status.

4.2.3
Enabling Centralized Event Logging

This procedure enables the Centralized Event Logging feature for the Generic Application Server and all installed application containers. This is done with the use of the logging server's Fully Qualified Domain Name (FQDN) or IP address. Adding the first logging server enables the centralized logging feature. When enabled, operating system events, which are normally captured and written to log files within the Generic Application Server and the application containers, are also forwarded to the Centralized Event Logging server. Centralized Event Logging for an individual application container may also be enabled through menus in that application container.

For details on this feature, see the *Centralized Event Logging Feature Guide*.

Use to enable Centralized Event logging on an ISSI.1 Network Gateway. Before enabling the Centralized Event Logging server from the Generic Application Server menu, install all server applications for that Generic Application Server. If you add an ISSI container to this Generic Application Server later, disable Centralized Event Logging before adding the new server application, then re-enable Centralized Event Logging once the server application has been added. This is the only way to successfully enable Centralized Event Logging on an ISSI server application added later.

Prerequisites:

- See “DNS Dependencies” section in the *Centralized Event Logging Feature Guide*. This section lists DNS dependencies that you must consider before enabling centralized logging.
- See the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator for information about setting up Active Directory users so that they can perform specific administration menu procedures.

Procedure:

1 Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Services Administration**. Press ENTER.

3 Enter the corresponding number for **Manage Syslog Client Configuration**. Press ENTER.

4 Enter the corresponding number for **Add Centralized Logging Server**. Press ENTER.

The following message appears:

```
Enter centralized syslog server to add (q=quit):
```

5 Enter either the Fully Qualified Domain Name (FQDN) or the IP Address of a Centralized Logging Server (see Event Logging Client Configuration on page 70) in the current system configuration. Press ENTER.

NOTICE: An FQDN is in the [hostname].[domainname] form. The FQDNs for the Centralized Logging Servers are listed in Event Logging Client Configuration tables, in the *Centralized Event Logging Feature Guide*.

Messages report that Centralized Logging has been enabled for this Generic Application Server and that the "loghost" server you specified has been added to the configuration for this Generic Application Server.

NOTICE: Repeat step 4 and step 5 for any additional Centralized Event Logging servers.

6 To verify the status of Centralized Event Logging, enter the corresponding number for **Display Centralized Logging Status**. Press ENTER.

The system reports whether centralized logging is enabled or disabled, and displays a list of configured logging servers.

Postrequisites: Log off from the server. See Logging Off the Terminal Server on page 84.

4.2.3.1
Event Logging Client Configuration

Event messages are forwarded to a Centralized Event Logging Server, depending on the location of the client. For configuration details in both DSR and non-DSR systems, see the "Event Logging Client Configuration" section in the *Centralized Event Logging Feature Guide*.

4.2.4
Disabling Centralized Event Logging

This procedure removes a Centralized Event Logging server for the Generic Application Server and all installed application containers. Removing all logging servers disables the Centralized Event Logging feature. When the Centralized Event Logging feature is disabled, operating system events are written only to log files within the Generic Application Server and the application containers. Centralized Event Logging for an individual application container may also be disabled through menus in that application container.

For details on this feature, see the *Centralized Event Logging Feature Guide*.

Prerequisites: For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

Procedure:

1 Log on to the **Generic Application Server Main Menu**. Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Services Administration**. Press ENTER.

3 Enter the corresponding number for **Manage Syslog Client Configuration**. Press ENTER.

4 Enter the corresponding number for **Remove Centralized Logging Server**. Press ENTER.

The following message appears:

```
Current centralized logging servers:
[Numbered List of Current Logging Servers]
Which centralized logging server would you like to remove?
(1-[#], a=all, q=quit):
```

5 Perform one of the following actions:

- If you want to remove selected logging, enter the number of a Centralized Logging Server in the list of the logging servers you want to remove.
- If you want to remove all logging servers, enter: `a`

NOTICE: Removing all logging servers in the list disables the Centralized Event Logging feature.

Press ENTER.

6 Perform one of the following actions:

If…	Then…
If you are removing one of the logging servers present in the list,	the following message appears: `[LOGGING SERVER FQDN or IP] removed from centralized logging servers for [GAS SERVER].` Go to step 8.
If you are removing the last one of the logging servers present in the list,	the following message appears: `Removal of remaining centralized logging servers will disable centralized logging. Would you like to continue? (y/n):`

7 Enter: `y`

The following message appears: `[LOGGING SERVER FQDN or IP] removed from centralized logging servers for [GAS SERVER].`

8 To verify the status of Centralized Event Logging, type the corresponding number for **Display Centralized Logging Status**. Press ENTER.

The system reports whether centralized logging is enabled or disabled, and displays a list of configured logging servers.

Postrequisites: Log off from the server. If needed, see Logging Off the Terminal Server on page 84.

4.2.5
SNMP Credentials

For information and procedure on configuring SNMP credentials, see the *SMNPv3 Feature Guide*.

4.3
Network Time Protocol Configuration

The Network Time Protocol (NTP) is a service used to provide time and date information to devices in the network. It is used in the system to synchronize all devices to the same time and date and allow those devices to include time stamps in error logs and SNMP fault information.

A TRAK device is the preferred NTP source for most of the system configurations. Secondary sources may vary depending on your specific configuration and purchased features.

NOTICE: If the TRAK devices is not included in your system, no manual configuration is required to set up a Generic Application Server as an NTP source. This is done during the installation process, based on the Generic Application Server ID that was entered. If the TRAK device is included in your system, manually configure each of the TRAK devices in the system on each of the Generic Application Servers set up as an NTP source.

Adding a Remote NTP Time Source on page 72 and Removing a Remote NTP Time Source on page 72 list the steps to take when adding and removing a remote NTP time source on a Generic

Application Server. Details on enabling and disabling the secondary NTP source on a Generic Application Server can be found in Enabling Hosting of Secondary Local NTP Source on page 73 and Disabling Hosting of Secondary Local NTP Source on page 73, respectively.

For details regarding the NTP Server, as well as the primary and secondary NTP source for devices in your system, see the *Network Time Protocol Server Feature Guide*.

4.3.1
Adding a Remote NTP Time Source

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Services Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Manage NTP Client Configuration**. Press ENTER.
4. Enter the corresponding number for **Add External NTP Time Source**. Press ENTER.

   The following message appears:

   ```
   Please enter IP address of external NTP time source (q=quit):
   ```
5. Enter the IP address of the remote time source. Press ENTER.

   The following message appears:

   ```
   <IP address> added as external NTP time source
   ```

Postrequisites: Log off the server. See Logging Off the Terminal Server on page 84.

4.3.2
Removing a Remote NTP Time Source

Procedure:

1. Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Services Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Manage NTP Client Configuration**. Press ENTER.
4. Enter the corresponding number for **Remove External NTP Time Source** from the menu. Press ENTER.

   A list of current external NTP sources is displayed, followed by this message:

   ```
   Which external NTP time source would you like to remove?
   ```
5. Enter the number of the time source to be removed. Press ENTER.

   The following message appears:

   ```
   External NTP time source [EXT_NTP_IP_ADDRESS] removed.
   ```

Postrequisites: Log off the server. See Logging Off the Terminal Server on page 84.

4.3.3
Enabling Hosting of Secondary Local NTP Source

If a GAS is not configured to host a secondary NTP server, the following message appears when you attempt to access this function:

```
This GAS does not host secondary NTP servers.
```

IMPORTANT: Secondary local NTP sources can only be enabled and disabled in certain system configurations.

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Services Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Manage NTP Server Configuration**. Press ENTER.
4. Enter the corresponding number for **Enable Hosting of NTP**. Press ENTER.

   NOTICE: Depending on the configuration, ntp0X stands for either ntp03 or ntp06.

   The following message appears:

   ```
   Enabled hosting of <ntp0X>
   ```

Postrequisites: Log off the server. See Logging Off the Terminal Server on page 84.

4.3.4
Disabling Hosting of Secondary Local NTP Source

If a GAS is not configured to host a secondary NTP server, the following message appears when you attempt to access this function:

```
This GAS does not host secondary NTP servers.
```

IMPORTANT: Secondary local NTP sources can only be enabled and disabled in certain system configurations.

Procedure:

1. Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Services Administration**. Press ENTER.
3. Enter the corresponding number for **Manage NTP Server Configuration**. Press ENTER.
4. Enter the corresponding number for **Disable Hosting of NTP**. Press ENTER.

   NOTICE: Depending on the configuration, ntp0X stands for either ntp03 or ntp06.

   The following message appears:

   ```
   Disabled hosting of <ntp0X>
   ```

Postrequisites: Log off the server. See Logging Off the Terminal Server on page 84.

4.4 Configuring the Time Zone

CAUTION: The Generic Application Servers default to the UTC time zone and must be set to a local time zone for the proper operation of the ASTRO® 25 system.

Prerequisites:

- Your account must be a member of the Platform Administrator or Installation Administrator role. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
- Set the Generic Application Server to local time, as by default, it installs with Coordinated Universal Time (UTC).

Procedure:

1. Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **OS Administration**. Press ENTER.
3. Enter the corresponding number for **Manage Platform Configuration**. Press ENTER.
4. Enter the corresponding number for **Set Time Zone**. Press ENTER.
5. Enter the corresponding number for country. Press ENTER.

   A list of time zones for the selected country appears.
6. If applicable for the selected country, type the corresponding number for a desired time zone. Press ENTER.

   A confirmation message appears:

   ```
   Selected Time Zone: US/Central
   Is this correct (y/n):
   ```
7. Enter: Y

   The final confirmation message appears:

   ```
   NOTICE: Changing the time zone will require a reboot of the
   Generic Application Server from the main menu in order to take effect.
   Are you sure you want to continue (y/n):
   ```
8. Enter: Y

   NOTICE: The output appears only when changing time zones on a Generic Application Server with applications installed. If no applications are currently installed, the change only affects the Generic Application Server.

   A list of installed containers with the result of the time change for that container appears. The application in the container specifies whether the time zone is changed.
9. Reboot the server. See Rebooting the Server on page 87.

4.5 Setting the Local Date and Time

Prerequisites: Your account must be a member of the Platform Administrator or Installation Administrator role. For information about setting up Active Directory users so that they can perform

specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

CAUTION: The time and date settings on the Generic Application Servers must be set as close as possible to local time, for proper time synchronization of the system. Due to the critical nature of this setting, it is best to set it after changing the time zone and before installing the application. Changing the time after installing the application may adversely affect its proper configuration and operation, and, in the worst case, lead to the loss of both Wide Area Trunking and High Availability, especially when setting the time backwards.

When and where to use:
After the installation is complete, set the local date and time on the Generic Application Server. Perform this procedure, regardless of whether your system does or does not use a TRAK 9100.

If your system uses a TRAK 9100, the Generic Application Server date and time must be close to the TRAK 9100 date and time. If the date and time do not match closely, synchronization takes too long or may fail.

NOTICE: All listed Generic Application Server names refer to servers located in zone cores. Generic Application Servers located outside zone cores cannot serve as NTP sources.

For details regarding the Network Time Protocol (NTP) Server, as well as the primary and secondary NTP source for devices in your system, see the *Network Time Protocol Server Feature Guide*. The NTP Administration option in the GAS server OS Administration menu allows you to configure the NTP.

Procedure:

1. Log on to the GAS. Stay at the `#` prompt. See Logging On to the Generic Application Server on page 85 and do not perform step 5.
2. Enter: `date`

   The current date and time displays.
3. Enter: `date mmddHHMMyy`

   Where:

   - mm – 2-digit month
   - dd – 2-digit day of the month
   - HH – hour in the 24 hour time format
   - MM – minute
   - yy – year

   Time change is immediate and does not require a reboot. A time change affects the screen lock timer. A screen lock occurring shortly after changing the time is normal.
4. At the `#` prompt, enter: `exit`

   The console login prompt appears.

This page intentionally left blank.

Chapter 5

Generic Application Server Operation

This chapter details the tasks that you perform once the Generic Application Server is installed and operational on your system.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

5.1 Powering On the Server

As soon as the power cords are connected, standby power is applied.

Procedure:

1. To power on the server, plug in both power supply cords and connect the server to a power source.

   The server enters the On state. Once connected, the server automatically goes into Standby power mode.
   When the input power cables are connected to the system, the Sun Integrated Lights Out Manager (ILOM) boots and displays its power-on self-test messages. Though the system power is still off, the ILOM is already monitoring the system, regardless of the system power state. The startup messages from the ILOM appear. After the ILOM is finished starting up, the following ILOM login prompt appears:

   ```
   SUNSPXXXXXXXXXXXX login:
   ```

2. Enter `root` or `service` as the logon name. Press ENTER. Enter the corresponding password when prompted. Press ENTER.

   The ILOM prompt appears.

3. Establish a connection to the system console. At the ILOM prompt, enter: `start /SYS`

   The following prompt appears:

   ```
   Are you sure you want to start /SYS (y/n)?
   ```

4. Enter: **y**

   The following message appears:

   ```
   Starting /SYS
   ```

The server is started.

5.2

Using PuTTY to Access an SSH Server from a Windows-Based Device

NOTICE:
A Motorola Solutions-customized version of PuTTY is available for installation from the ASTRO® 25 system *Windows Supplemental* media. See: Installing Motorola Solutions PuTTY on Windows-Based Devices on page 79

The Motorola Solutions customization is for PuTTY key generation. Command syntax and details are included in a “Motorola Changes” topic in the *PuTTY User Manual* included in the PuTTY installed files. Motorola Solutions does not customize `PuTTY.exe` and other PuTTY tools used for SSH, SCP (pscp), and SFTP (psftp) sessions (for instructions on these other tools, see their topics in the *PuTTY User Manual*).

In ASTRO® 25 systems, generally the Windows-based device used for this procedure would be a Network Management (NM) Client, but in a K core configuration, other Windows-based service devices are provided instead of the NM Client.

The devices you can access are limited by Router Access Control Lists (ACLs), configuration files, firewall rules, and user permissions. For details, contact your system administrator and see the configuration files for your network transport devices. For general information, see the *Information Assurance Reference Guide*.

Procedure:

1. Log on to the Windows-based device using the domain user account.

   The desktop appears.

2. If the version of PuTTY on this Windows-based device was installed from the ASTRO® 25 system *Windows Supplemental* media, launch the PuTTY application:
   - **For Windows 7 and Windows Server 2008:** From **Start**, select **Programs** → **Motorola** → **Motorola PuTTY** → **PuTTY**.
   - **For Windows 10 and Windows Server 2012:** In the Windows search field, type in: `putty`. In the list of results, click **PuTTY**.
3. In the **PuTTY Configuration** window, perform the following actions:
   a. As the **Connection type**, select **SSH**.
   b. In the **Port** field, leave **22**.

   For an SSH session with a Solaris-based server, make sure that the PuTTY application is configured as follows:
   a. From the **Category** pane on the left, select **Terminal** → **Keyboard**. Under **The Backspace key**, select **Control-H**.
   b. From the **Category** pane on the left, select **Window** → **Selection**. Under **Control use of mouse**, select **Compromise**.

   It is important that the default settings are used for **Attempt “keyboard-interactive” auth [SSH-2]**. That check box should remain selected on the settings screen accessed from **Connection, SSH, Auth** in the **Category** pane. If this check box is not selected, the SSH session disconnects before you can log on to the SSH server device.
4. Specify a user name and an SSH server in the **Host Name (or IP address)** field, in the following format:

   <User name>@<SSH server host name or IP address>

Other methods for specifying a user name for interactive sessions are available. For example, if you navigate to **Connection** then **Data** in PuTTY and select **Prompt**, then, when you do not provide a user name in the command above, you will be prompted for a user name after you click **Open** in the next step. For additional information, see PuTTY online help.

If you want to save these settings for future use, enter a name for the session in the **Saved Sessions** field on the main Session window in PuTTY and click **Save**. The session name that you entered appears in the list below the **Saved Sessions** field.

> **CAUTION:** Do not save a session with the name “Default Settings”. Saving a host in a session called “Default Settings” may cause SSH connection failure for non-interactive and command-line functions.

5 Click **Open**.

The **PuTTY Configuration** window closes, and if you established the first connection to the SSH server or if the SSH servers key has changed, a window appears displaying the server’s SSH fingerprint.

6 Perform one of the following actions:

a Click **Cancel** if the fingerprint does not match the fingerprint of the host key generated most recently on the SSH server device, so that the interactive session is not established, then skip the rest of this procedure so that you can investigate the reason for the mismatch.

b Click **Yes** after verifying the fingerprint, if you want to accept the SSH server device into the known hosts list on the SSH client device where PuTTY is installed.

If you click **Yes** when there are still default SSH server keys on the SSH server device, then entries for the default keys are added to a known hosts list on the SSH client device where PuTTY is installed. These entries are not automatically overwritten during the key rotation procedures for the supported non-interactive ASTRO® 25 system SSH interfaces. Perform additional procedure to remove them. See: Removing Interactive Entries from the Known Hosts List on an NM Client on page 81

The interactive session is established. Proceed to step 7.

c Click **No** to establish the interactive session, **without** accepting the SSH server device into the known hosts list on the SSH client device where PuTTY is installed. Then proceed to step 7.

It is recommended that you click **No** if your organizations policies require key rotation to replace default SSH keys, and the default SSH server keys from initial installation were not yet replaced by generating new SSH server keys on the device you are connecting to.

For verifying the fingerprint of an SSH server (host), it is recommended that you refer to the fingerprint recorded when generating the keys on the SSH server. For additional information on verifying fingerprints for Solaris-based and Linux-based SSH servers, see: Fingerprint Verification in SSH Session Warning Banner on page 82

7 Perform one of the following actions:

- If you launched the SSH session only for testing secure mode and adding the SSH server to the known hosts list on the Windows device, you can close the SSH window.
- If you launched the SSH sessions for additional reasons, proceed with the interactive session. Log in to the SSH server device, if prompted.

5.2.1
Installing Motorola Solutions PuTTY on Windows-Based Devices

PuTTY is, by default, automatically installed on an NM Client. However, if it is not installed, use this procedure to install it.

When and where to use:
For Windows-based devices that do not already have PuTTY installed, the application can be installed as needed.

NOTICE:
This procedure installs a version of PuTTY customized by Motorola Solutions.

The Motorola Solutions customization adds a version of PuTTYgen that is modified for the Microsoft Windows operating systems used in ASTRO® 25 systems. Command syntax and details are included in a “Motorola Changes” topic in the *PuTTY User Manual* included in the PuTTY installed files. `PuTTY.exe` and other PuTTY tools that are installed in this procedure have not been customized by Motorola Solutions. See the *PuTTY User Manual* for instructions on these other tools.

Procedure:

1 Insert the *Windows Supplemental* media into the drive of the Windows-based device.

IMPORTANT: If you are installing to a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* media for this procedure. See the *Virtual Management Server Software User Guide* for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

2 Log on to the Windows-based device with administrator privileges.

3 To uninstall a previous version of PuTTY on Windows 7 and Windows 10:

a From **Start**, open **Control Panel**.

b Click **Programs** → **Programs and Features** → **Uninstall a program**

c From the list of programs, select **Motorola PuTTY**. Click **Uninstall** above the list.

4 Open the command prompt window.

5 Navigate to the `\WIF` directory on the CD/DVD drive.

6 Enter: `WindowsInstallFramework.exe /e /i` ***<feature.xml>***

Where ***<feature.xml>*** is `"Motorola PuTTY.xml"`

To install other features at the same time, you can add more ***<feature.xml>*** parameters, depending on whether the following features are implemented in your ASTRO® 25 system:

- `"Motorola WinSCP.xml"` installs the WinSCP utility.

  For information, see http://www.winscp.net.

- `"Motorola Windows Bar Client.xml"` installs the Backup and Restore (BAR) client application.

  This applies only to domain controllers and Authentication Center servers, unless you have implemented the backup feature for all Windows-based BAR clients in your system.

  For details, see the *Backup and Restore Services Feature Guide*.

- `"Motorola Windows Logging Client.xml"`
  installs the Event Logging client application, if you have implemented the Centralized Event Logging feature in your system.

  For details, see the *Centralized Event Logging Feature Guide*.

7 Click **Finish**.

The **PuTTY** utility and the *PuTTY User Manual* are available by navigating to the list of programs on your computer, and selecting:

- For Windows 7: **Motorola** → **Motorola PuTTY**

- For Windows 10: **Motorola**

8 Remove the media from the drive.

9 Optional: Create a shortcut on the desktop to the PuTTY application, which is located at:

`<systemdrive>:\Program Files (x86)\Motorola\Motorola PuTTY\bin\PuTTY.exe`

This is recommended if you need to use the application to initiate multiple sessions because the PuTTY application window automatically closes each time it initiates a session.

Related Links

Using PuTTY to Access an SSH Server from a Windows-Based Device on page 78

5.2.2

Removing Interactive Entries from the Known Hosts List on an NM Client

Perform the following procedure to detect and remove default SSH keys from the known hosts list for an interactive user on a Network Management (NM) Client.

IMPORTANT: Repeat this procedure, including the step for logging on to the NM Client, for each interactive user that may have added default SSH keys to the known hosts list on this NM Client.

When and where to use: If a user who is logged into a Network Management (NM) Client initiates an SSH session with an SSH server device before an SSH key rotation, and selects **Yes** at the fingerprint prompt, this creates entries in an NM Client known hosts list. These *interactive* account entries are not addressed in the key rotation procedures for the supported ASTRO® 25 system *non-interactive* SSH interfaces.

Procedure:

1 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See: Logon to Network Management Clients SSH Configuration on page 82

The desktop appears.

2 From **Start**, select **All apps** → **Motorola** → **puttyDefaultKeyDetector**.

NOTICE: If you are logging with an Administrator account, right-click **puttyDefaultKeyDetector** and select **Run As Administrator**.

The following columns of information display in the **puttyDefaultKeyDetector** window:

- **Key Type** will always display `Default PuTTY SSH Host Key`.
- **Key Name** is a combination of Host IP and actual key type (dsa or rsa2).
- **Windows Account** shows the user for which the keys are detected and can be removed (this is the account used to log on to the NM Client in step 1)

3 Based on the results in the **Key Name** column, select the rows for the keys you want to delete:

- To select more than one consecutive entry, press the SHIFT key then click the entries you want to delete.
- To select more than one non-consecutive entry, press the CTRL key then click the entries you want to delete.
- To select one entry, click one row and proceed to the next step.

4 Click **Remove Selected**.

You are prompted to confirm you want to remove the selected key(s).

5 On the confirmation window, click **OK**.

A message reports that the deletion was successful.

6 On the success message window, click **OK**.

The list of keys automatically refreshes, and the key(s) you had selected for deletion no longer display in the list.

7 Click **Exit** to close the window.

The **puttyDefaultKeyDetector** window closes. The desktop appears.

Related Links

Using PuTTY to Access an SSH Server from a Windows-Based Device on page 78

5.2.2.1

Logon to Network Management Clients SSH Configuration

For SSH configuration procedures performed on Network Management (NM) Clients, you need to log on either as the local Windows administrator, or using your Active Directory account that is a member of the “secadm” user group.

NOTICE: It is recommended that you log on with the Active Directory account. To log on using an Active Directory account, the domain controller must be available on the network, and the NM Client must be joined to the domain.

When logging on to an NM Client, be sure to enter the Active Directory domain before your Active Directory username, in the following format: ***<domain>\<username>***.

For general use of PuTTY to initiate sessions with other devices from an NM Client, you can log on to the NM Client using any valid local account, or using your Active Directory account that is a member of a group with authority to log on to NM Clients (for example, the “nm_client-login” user group).

For information on Active Directory user groups in ASTRO® 25 systems, see the *Authentication Services Feature Guide*.

The following extra steps are required when configuring SSH:

When using the command prompt window to generate SSH keys on the NM Client, you need to access the command prompt window by right-clicking the Command Prompt option on the Accessories menu, and choosing to Run as administrator. If a **User Account Control** window displays, enter your password and click **Continue**, or click **Allow**.

For procedures that require logging on to the NM Client as the local Windows administrator, ask your system administrator for the username and password required. The local Windows administrator account set up by Motorola Solutions on NM Clients is "secmoto".

Related Links

Removing Interactive Entries from the Known Hosts List on an NM Client on page 81

5.2.3

Fingerprint Verification in SSH Session Warning Banner

SSH session fingerprint verification (and accepting the host into the known hosts list) is performed for each device as part of the ASTRO® 25 system SSH configuration process, so that each device is ready for interactive sessions without requiring a service user to verify fingerprints.

If the warning banner displays for you when initiating an SSH session, fingerprint verification is recommended before accepting the host into the known hosts list.

It is recommended that you refer to the fingerprint recorded when generating the keys on the SSH server. Contact your system administrator for this information if needed.

For Solaris-based and Linux-based SSH servers, the root user can execute the following command to view the SSH key fingerprint on the device: `ssh-keygen -lf /etc/ssh/ssh_host_rsa_key`

IMPORTANT: This command should only be executed when you are connected to the console of the SSH server device. Performing this command when connected to a device over the network (for example, in a PuTTY session) is not a reliable method.
See the instructions for connecting to an SSH server in Accessing the Root Command Prompt on Devices Using Default Keys on page 83.

Related Links

Using PuTTY to Access an SSH Server from a Windows-Based Device on page 78

5.2.3.1

Accessing the Root Command Prompt on Devices Using Default Keys

Prerequisites: For information on Active Directory user groups in ASTRO® 25 systems, see the *Authentication Services Feature Guide*.

Procedure:

For command-line procedures that need to be performed as the root user, access the root user prompt for the device by performing one of the following:

- Use an SSH session to connect to the device:
  1. Establish an SSH session using your Active Directory account that is a member of a user group authorized to access this device.

     For example, the user group ucs-login is authorized to log on to the UCS.
  2. Enter: `su -`
  3. Enter the root account password to access the root command prompt.
- Use a console connection to access the server and log on with the root account. For details, see the appropriate device manual:
  - *ISSI.1 Network Gateway Feature Guide*
  - *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide*
  - *Packet Data Gateways Feature Guide*
  - *Virtual Management Server Software User Guide*

Related Links

Fingerprint Verification in SSH Session Warning Banner on page 82

5.3

Logging On Through a Terminal Server

You can have up to eight terminal server telnet sessions running simultaneously. For security reasons, Motorola Solutions recommends that you use the Windows `cmd.exe` window to telnet into the terminal server. The `cmd.exe` window does not leave a trail, whereas using the **Run** dialog box allows anyone to see and reuse the most recent IP addresses and commands entered in this window. The preferred way to connect is through PuTTY, except when you must access the ILOM prompt or during the installation process.

Procedure:

1. Click **Start** in the lower-left corner of the screen.

   The Windows **Start** menu appears.

2. Access the command window.

   Step example: To open the **Run** dialog box, press the WINDOWS ICON KEY + R. Enter: **cmd**
   The advantage of this window is security; it leaves no IP address trail for others to follow.

   The command prompt window appears, allowing your input.

3. Enter: `telnet` ***<TERMINAL_SERVER_IP_ADDR>***

   Do not press ENTER multiple times or you may be automatically logged out.

   The `Login:` prompt appears.

4. Enter the user name that identifies this session with the terminal server, such as `user1`. Press ENTER.

   The `Password:` prompt appears.

5. Enter the ***<login password>***. Press ENTER.

   The **Main Menu** appears.

6. Enter the corresponding number for **ZC/Unix Server Menu** associated with the Generic Application Server to which you want to log on. Press ENTER.

   The Generic Application Servers are listed.

7. Enter the corresponding number for the server. Press ENTER.

   The console `Login:` prompt appears.

Postrequisites: For further steps, see Logging On to the Generic Application Server on page 85.

5.4 Logging Off the Terminal Server

If you did not log off before disconnecting a terminal session, the next time you connect using the terminal server, you are still logged on.

Procedure:

1. To get to an administrative menu, at the prompt enter: **q**

   The `#` prompt appears.

2. Enter: **exit**

   The console `login:` prompt appears.

3. To exit the terminal server, at the console login prompt, press CTRL + Z.

   The `Console escape` message appears.

4. To exit, enter: **e**

   The **ZC/Unix Server Menu** appears.

5 To quit, enter: **q**.

The `Connection to host lost` message appears.

5.5 Logging On to the Generic Application Server

Once you have established an administrative session with the server through either the terminal server or PuTTY, you can log on to the Generic Application Server. To log on, you must be at the login prompt for the server you are attempting to log on to.

WARNING: When multiple users are logged on to a server, any system configuration changes performed during the active sessions may conflict and leave the server in an undesirable state. Verify with the other users that the work you want to perform does not cause conflict.

Prerequisites:
A login ID and a password for the server. Keep the administrator password secret and change it frequently.

Procedure:

1 Connect to the Generic Application Server, using the terminal server or PuTTY.

- Logging On Through a Terminal Server on page 83
- Using PuTTY to Access an SSH Server from a Windows-Based Device on page 78
- Changing Domain Account Passwords on page 88

If you do not log off before disconnecting a terminal session, the next time you connect using the terminal server, you are still logged on. Follow Logging Off the Terminal Server on page 84 to log off the terminal server after each session.

2 Perform the following actions:

If…	Then…
If the `z00Xgas0Y console login:` prompt appears,	go to step 4.
If the `SUNSPXXXXXXXXX log-in:` ILOM prompt appears,	perform the following actions: **a** As the login name and its corresponding password, enter: `root` **b** To switch to the host console, enter `start /SP/console` **c** At the `Are you sure, you want to start /SP/console (y/n)?` prompt, enter: **y**

3 After switching to the host console, to refresh the screen, press ENTER.

If…	Then…
If the console login prompt appears,	go to the next step.
If the console screen is locked and the user who was previously logged on is reconnecting to the console,	the user who was previously logged on unlocks the screen and returns to the active session. For details, see Unlocking a Screen on page 86. Go to the next step.

If…	Then…
If the console screen is locked and a user (either root or an account with platform administrator privileges) other than the user who was previously logged on is connecting to the console,	the new user terminates the active session to unlock the screen and return to the GAS login prompt. For details, see Unlocking a Screen on page 86. Go to the next step.
If the # prompt is displayed,	go to the last step.

4 Perform the following actions:

If…	Then…
If the GAS or server application you are logging on to is joined to an Active Directory domain, and a domain controller is available to the server on the network,	log on to the server using your Active Directory account credentials.
If the GAS or server application you are logging on to is not joined to an Active Directory domain, or a domain controller is not available to the server on the network,	use a console connection to access the server, and log on with the root account.

The # prompt appears.

5 Enter: `admin_menu`

The server administration menu and the menu prompt appear.
There may be a slight delay while the system inserts asterisks on the menu options that your account does not have privileges to perform.

5.6 Unlocking a Screen

Only the user who is logged on can unlock the screen and return to the current session. A user account that has Platform Administrator privileges or the root account can unlock the screen, but the session terminates.

Procedure:

1 Connect to the Generic Application Server, using the terminal server.

The message similar to the following appears:

```
Screen used by [USER ACCOUNT NAME] on hostname: z00XgasY.
```

2 To unlock the screen, enter the user name and password.

If your Active Directory account does not have Platform Administrator privileges, then the screen does not unlock.

- If you are currently logged on unlocks the screen, the current session returns.

- If user logon or password were incorrect, the console `login:` prompt appears.
- If the screen is unlocked with a user account with Platform Administrator privileges or with the root account, the following message appears:

```
Your session is being terminated for security reasons.
```

5.7 Enabling the Applications

Applications must be enabled after they are installed, or when the Generic Application Server starts or is rebooted. Critical applications start automatically.

See Chapter 6 in the *ISSI.1 Network Gateway Feature Guide*.

5.8 Disabling the Applications

Before shutting down the Generic Application Server, disable all server application containers first. Applications are disabled from their respective administration menus. Disabling an application container stops all the core processes. Disable an application before powering down the server for maintenance, repair, or troubleshooting.

CAUTION: Rebooting the Generic Application Server while the applications installed in containers on the server are enabled may corrupt the databases of those applications. Ensure that all installed applications are disabled before rebooting the Generic Application Server.

5.9 Rebooting the Server

The Generic Application Server Main Menu of each server provides a selection for rebooting the server. This selection reboots the server back to the login prompt. For example, you may need to reboot the server if the Generic Application Server is running in Coordinated Universal Time (UTC), and you want to set it to a local time zone. After changing the time zone, you reboot the server.

CAUTION:
Rebooting a server can seriously disrupt system functionality. Do not attempt to reboot a server unless you are aware of all the consequences of bringing down the server. Rebooting from the Generic Application Server Main Menu ensures that all containers are shut down properly. Only reboot the server from the **Generic Application Server Main Menu**.

Rebooting the applications in an enabled state may corrupt the system. If you reboot the server, disable the applications first.

Prerequisites: To perform a system reboot, a Unix account must have either installation administrator or platform administrator privileges.

Procedure:

1. Disable the applications. See Disabling the Applications on page 87 for details.
2. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85
3. Enter the corresponding number for **OS Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

4 Enter the corresponding number for **Reboot Server**. Press ENTER.

A message appears, listing the applications to disable before rebooting.

```
The following applications must be disabled before proceeding: (for
example)
 app01
 app02
 Failure to do so may result in corruption requiring a system
reinstall.
 Have the applications been disabled? (y/n):
```

5 To confirm that you have disabled the applications, enter: **y**

If you answer No (N), the `Operation aborted` message appears.

The following prompt appears:

```
Are you sure you want to continue? (y/n):
```

6 Enter: **y**

If you answer No (N), the `Operation aborted` message appears.

The server reboots back to the login prompt.

5.10 Changing Domain Account Passwords

All personal user accounts in the ASTRO® 25 system are managed on the active directory domain. The root account is the only local interactive account available on the Generic Application Server. Everybody can change their own domain account password from the Generic Application Server command prompt. Change only your own password. Each account has permissions to change its own password.

Procedure:

1 Log on to the GAS. Perform steps 1 through 4 of Logging On to the Generic Application Server on page 85.

2 At the `#` prompt, enter: `epasswd`

The `epasswd` command changes the personal domain account passwords, as well as the GAS server root account password.

The change password prompt appears.

3 Enter the existing login password. Press ENTER.

The following prompts appear:

```
  New password:
New password (again):
```

4 Enter the new password. Re-type the new password when prompted. Press ENTER.

The following confirmation message appears:

```
Kerberos password changed.
```

The password is changed. For security conscious organizations, see the *Unix Supplemental Configuration Setup Guide* (for example, changing the EEPROM password).

5.11 ILOM Passwords

This section explains how to change the password for the ILOM root account and for the ILOM Service account.

5.11.1 Changing the Password for the ILOM Root Account

The passwords for ILOM accounts are not configured as part of the Generic Application Server installation. Perform the following procedure manually, after the server is installed and configured.

Procedure:

1. Log on to the ILOM, using the root or service account.
2. Execute the following command: `set /SP/users/root password`

   The following message and prompt display:

   ```
   Enter new password:
   Enter new password again:
   ```

3. Enter the new password twice.

   The ILOM prompt (`->`) appears.

5.11.2 Changing the Password for the ILOM Service Account

The passwords for ILOM accounts are not configured as part of the Generic Application Server installation. Perform the following procedure manually, after the server is installed and configured.

Procedure:

1. Log on to the ILOM, using the service account.
2. Execute the following command: `set /SP/users/service password`

   The following message and prompt display:

   ```
   Enter current password:
   ```

3. Enter the current password for the ILOM service account.

   The following prompt displays:

   ```
   Enter new password:
   Enter new password again:
   ```

4. Enter the new password twice.

   The ILOM prompt (`->`) appears.

5.12 Powering Off the Server

Performing a graceful shutdown makes sure all your data is saved and the system is ready for a restart.

CAUTION: Applications running on the Solaris platform can be adversely affected by a poorly executed system shutdown. Ensure that you disable all applications. Shut down the operating system, as described in this section, before powering off the system. Powering off the server can seriously disrupt system functionality. Do not attempt to power off a server unless you are aware of all the consequences of bringing down the server. Shutting down from the Generic Application Server Main Menu ensures that all containers are shut down properly. Only shut down the server from the Generic Application Server Main Menu.

NOTICE: To perform a shutdown, your user account must have the Installation Administrator or Platform Administrator privileges.

Procedure:

1. Notify all users of the system power down.
2. Disable the applications. See Disabling the Applications on page 87.

   CAUTION: Powering off the applications in an enabled state may corrupt the system. If you must power off the server, disable the applications first.
3. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
4. Enter the corresponding number for **OS Administration**. Press ENTER.
5. Enter the corresponding number for **Shutdown**. Press ENTER.

   The following message appears

   ```
   The following applications must be disabled before proceeding:
    <list of applications>
    Failure to do so may result in corruption requiring a system
   reinstall.
    Have the applications been disabled? (y/n):
   ```
6. Enter: **y**

   The `Are you sure you want to continue? (y/n):` prompt appears.
7. Enter: **y**

   The `OK` prompt appears.
8. Enter: `#.`

   The ILOM prompt (`->`) appears.
9. Enter: `stop /SYS`

   The following prompt appears:

   ```
   Are you sure you want to stop /SYS (y/n)?
   ```
10. Enter: **y**

    The following message, followed by ILOM prompt (`->`), appears:

    ```
    Stopping /SYS
    ```

5.13 Running Resource Balancing

Resource balancing is the feature on the Generic Application Server that guarantees a minimum amount of resources for the containers and, depending on the configuration, allows containers to use

all available resources. When this feature is performed from the Generic Application Server Administration menu, unreserved SWAP and RAM are redistributed among the installed applications.

Prerequisites: Perform resource balancing after the application installation is complete.

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85
2. Enter the corresponding number for **Application Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Manage Scalable Resources**. Press ENTER.
4. Enter the corresponding number for **Balance Resources**. Press ENTER.

   A warning message appears.
5. When prompted for confirmation, enter: `y`

   IMPORTANT: Before balancing resources, ensure that all the application installs planned for the Generic Application Server have been completed. Balancing resources distributes unused system resources to all installed container applications and reversing this process would require uninstalling/reinstalling of all the applications residing on the server.

   The following message appears:

   ```
   Balancing resources...done
   ```
6. To quit, enter: `q`

Postrequisites: Exit to the command prompt or log off. See Logging Off the Terminal Server on page 84.

5.14 Viewing the Installation Status

You can view the installation status during the installation process. For detailed information, see “Installing the Applications”.

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Application Administration**. Press ENTER.
3. Enter the corresponding number for **Display Container Status**. Press ENTER.

   A message appears, indicating the installation status.
4. To return to the `#` prompt, enter: **q**

This page intentionally left blank.

Chapter 6

Generic Application Server Maintenance

This chapter describes periodic maintenance procedures relating to the Generic Application Server.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

6.1 Software Patch Installation

If you have a *MOTOPATCH for Solaris 10 CD* with a `readme.txt` file containing MOTOPATCH installation instructions, refer instead to one of the following for MOTOPATCH installation instructions for devices running Solaris 10:

- PTSS/SUS Extranet Site: https://sites.google.com/a/motorolasolutions.com/sus-motopatch/

Information on Loading OS patches is listed in the Loading OS Patches on page 93. For information on Installing OS patches on a Generic Application Server, see Installing OS Patches on page 94.

6.1.1 Loading OS Patches

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Software Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Load Software**. Press ENTER.
4. Enter the corresponding number for **Load OS Patches**. Press ENTER.

   The following message appears:

   ```
   Would you like to load the Patch Disk? (y/n):
   ```
5. Enter: **y**

   The following message is displayed:

   ```
   Please insert the Patch media and press <Enter>
   ```
6. Press ENTER.

   The following message is displayed:

   ```
   Searching for media...found
   Loading Patch Disk
   ```

   When the load is complete, the following message is displayed, followed by the **Load Software** menu.

```
Patch Disk loaded successfully
```

7 Enter: **q**

The **Software Administration** menu is displayed.

8 Enter the corresponding number for **Eject CD/DVD**. Press ENTER.

9 To exit the menu, enter: **q**

6.1.2 Installing OS Patches

Procedure:

1 Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Software Administration**. Press ENTER.

NOTICE: For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Install Software**. Press ENTER.

4 Enter the corresponding number for **Install OS Patches**. Press ENTER.

The OS Patch is installed and the **Install Software** menu is displayed.

5 To exit to the command prompt, enter: **q**

6.2 FRU/FRE Components

Periodic testing of stored components is necessary for the battery only.

You can query the clock battery sensor from the Sun Integrated Lights Out Manager (ILOM):

T5220 server:

```
show /SYS/MB/V_VBAT
```

The lower threshold is 2.69V.

The lithium battery is a standard 3 V CR 2032. The expected battery life ranges from 5 to 15 years, depending on usage variables.

See Replacing Batteries T5220 Servers on page 137.

T4-1 server:

```
-> show /SYS/MB/V_BAT  /SYS/MB/V_BAT
```

Targets:

Properties:

type = Voltage

pmi_name = MB/V_BAT

class = Threshold Sensor

value = 3.200 Volts

upper_nonrecov_threshold = N/A

upper_critical_threshold = N/A

upper_noncritical_threshold = N/A

lower_noncritical_threshold = 2.560 Volts

lower_critical_threshold = N/A

lower_nonrecov_threshold = N/A

alarm_status = cleared

Threshold is reported as 2.560 Volts.

See Replacing Batteries in T4-1 Servers on page 138.

6.3 Ejecting CD and DVD

Procedure:

1. Log on to the Generic Application Server Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Software Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Eject CD/DVD**. Press ENTER.
4. To exit to the command prompt, enter: **q**

6.4 Backing Up the Generic Application Server to Persistent Storage

This procedure explains how to back up the Generic Application Server data to persistent storage. The backed up data is stored locally in persistent storage on the Netra server. Persistent storage is a location on the server that remains unchanged during the installation of the Generic Application Server.

The persistent storage backup includes critical data, the information used to restore the Generic Application Server during the recovery process. Critical data includes files containing application software version information, Secure Shell (SSH) configuration, SNMP configuration, NTP configuration, Centralized Logging status, and configured servers, as well as key information. Only critical data is restored during a recovery.

To back up application data, see the specific backup procedure in the *ISSI.1 Network Gateway Feature Guide*. This backup does not back up any data from the container applications.

Use this procedure, for example, to back up data if the Generic Application Server is reinstalled.

Procedure:

1. Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Backup and Restore Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Backup Administration**. Press ENTER.

4 Enter the corresponding number for **Backup All Critical Data** or the **Backup Data to Persistent Storage**. Press ENTER.

The following message appears:

```
Backup GAS
-----------------------------------
A GAS backup will overwrite any existing backup data in persistent
storage.
Do you wish to proceed with GAS backup? (y/n):
```

5 Enter: `y`

The following message appears, followed by the Backup Administration menu:

```
Backing up GAS ...
```

Postrequisites: Log off the server. If needed, see Logging Off the Terminal Server on page 84.

6.5 Restoring the Generic Application Server from Persistent Storage

This procedure explains Restoring the Generic Application Server data. This procedure restores critical data, such as files containing application software version information and SSH configuration and key information. The Restore procedure is the same for all backups, including Backup and Restore (BAR). Restoring from persistent storage restores the last backup placed there (either from a persistent storage backup or BAR, when the BAR backs up data to the server).

When and where to use:
For the full recovery process, which includes replacing the server hardware, refer to Disaster Recovery on page 149.

The restored data includes the most recently backed up information assurance settings. If you have changed the configuration since the last backup, see Information Assurance Configuration on page 66 to reconfigure. You must enable Centralized Event Logging; see Enabling Centralized Event Logging on page 69.

Procedure:

1 Log on to the Generic Application Server's Main Menu. Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Backup and Restore Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Restore Administration**. Press ENTER.

4 Enter the corresponding number for the type of restore that is to be performed. Press ENTER.

The following message appears:

```
GAS Restore
-----------------------------------
A GAS restore may overwrite existing configurations.
Do not perform any operations during a GAS restore.
Do you wish to proceed with GAS restore? (y/n):
```

5 Enter: `y`

A message appears, listing the status of the restore operation, together with the status for the Backup and Restore Agent and centralized logging.

Postrequisites: Log off from the server. See Logging Off the Terminal Server on page 84.

6.6 Loading the Persistent Storage from Network

Procedure:

1 Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Software Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Manage Persistent Storage**. Press ENTER.

4 Enter the corresponding number for **Load Persistent Storage from Network**. Press ENTER.

The following message appears:

```
Load From Network
-----------------------------------
Please enter hostname/IP address to load data from, or 'q' to quit:
```

5 Enter the hostname or IP address. Press ENTER.

In turn, each server with data asks for a confirmation to transfer.

The following message is displayed:

```
Testing <IP Address> connection...
The following application data is available for transfer:
<List of data>
Load <hostname>.<domainname> data (y/n)[y]:
```

6 For each set of data you want to transfer, enter: `Y`

The following message is displayed for each set of data you want to transfer:

```
Confirm loading data for <hostname>.<domainname>? (y/n):
```

7 For each set of data you want to transfer, enter: `Y`

The following messages are displayed for each set of data, followed by the Manage Persistent Storage menu.

```
Transfer in progress
Transferring <hostname>.<domainname> data...
```

8 To exit to the command prompt, enter: `q`

6.7 Removing the Persistent Storage

Procedure:

1 Log on to the Generic Application Server Main Menu. Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Software Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Manage Persistent Storage**. Press ENTER.

4 Enter the corresponding number for **Persistent Storage Removal**. Press ENTER.

The following message appears:

```
Remove Persistent Storage
-------------------------------------
1. <hostname>.<domainname>
Please select a persistent storage file system to remove (1-1, q):
```

5 Enter the number of the Persistent Storage you want to remove. Press ENTER.

A confirmation message appears, followed by the **Manage Persistent Storage** menu.

6 To exit to the command prompt, enter: `q`

Chapter 7

Generic Application Server Troubleshooting

This chapter provides fault management and troubleshooting information relating to the Generic Application Server and server hardware.

7.1 General Troubleshooting for Servers

The following list describes troubleshooting steps for general server problems:

1. In the Unified Event Manager (UEM) application, check the condition of the server and the links to it.
2. In the server administration environment, check the functionality of server components. See Basic ILOM Commands on page 100 for details. Replace the server components if necessary.
3. See Basic Container Functions on page 105 for other commands that are useful for the Generic Application Server administrator, for example, to display running services or to enable/disable a service.
4. If there is a problem with the hard drive, DVD-RW optical media drive, fans, power supply, or the tape drive, see Troubleshooting Application Failures on page 111 for details.
5. Check the physical condition of the server chassis. Check the LEDs and verify that power is being supplied to the components. See Server LEDs for Troubleshooting on page 112 for details about LEDs.
6. View the installation log. See Viewing the Installation Log on page 117 for details.
7. Check for any sharp bends or kinks in cabling. Test any suspected cabling for noise, continuity, attenuation, and crosstalk. Replace the cabling if necessary.
8. Run `ping`, `pathping`, and other network administration commands to identify any link or intermediate devices (switch or routers) with high latency or connection problems to the server.
9. Reboot the server through the server administration environment.
10. Reinstall the operating software and application software on the server, if necessary.

7.2 ILOM Access

You can access ILOM from the Serial Management port (SER MGT) on the back of the server. By default, ILOM uses the SER MGT port to communicate with the console through an external terminal server. This connection provides console management capability for the server; it can be used to access both the ILOM console and the server console.

7.2.1 Switching Between the System Console and the ILOM

This procedure allows you to switch from the ILOM prompt (`->`) to the Solaris console (`#`) prompt.

Procedure:

1. At the -> prompt, enter: `start /SP/console`

   The following prompt appears:

   ```
   Are you sure you want to start /SP/console (y/n)?
   ```

2. Enter: **y**

   The following message appears:

   ```
   Serial console started. To stop, type #.
   ```

3. Press ENTER.

   The `User Name:` prompt appears.

4. Log on.

   The # prompt appears.

5. To switch from the Solaris console (# prompt) to the ILOM prompt (->), enter: **#.** (pound period).

7.2.2
Logging on to the ILOM

When you connect to the ILOM for the first time, you are automatically connected as the admin account. The next time you log on, however, specify the password; see "Changing ILOM Passwords".

Procedure:

1. Ensure that the console is connected to the ILOM. To escape from the console, at the console login prompt, type **#.**. Press ENTER.

   The `SUNSPXXXXXXXXXXXX login:` prompt appears. The ILOM login prompt starts with **SUNSP**.

2. Enter the login name for your ILOM root account. Press ENTER.

   The Password prompt appears.

3. Enter the password for your ILOM root account. Press ENTER.

   The ILOM (->) prompt appears. You can now use ILOM commands or switch back to the system console.

7.3
Basic ILOM Commands

This section covers the basic ILOM commands supported by Motorola Solutions.. The Generic Application Server has two accounts for the ILOM.

The following ILOM commands are described in the following section: starting the console, viewing the console history, viewing events, viewing the locator LED state, viewing the environmental status, viewing fault status, viewing the server ID and status, viewing network configuration, and logging out.

Table 18: Supported ILOM Commands and ALOM Equivalents

Supported ILOM Commands	ALOM Equivalent
start /SP/console	console

Table continued…

Supported ILOM Commands	ALOM Equivalent
show /SP/console/history	consolehistory
show /SP/logs/event/list	showlogs
show /SYS/LOCATE	showlocator
show -o table -l 2 /SYS	showenvironment
show faulty	showfru
show /HOST	showplatform
show /SP/network	shownetwork
exit	logout

7.3.1
Starting the Console

Procedure:

1. At the `->` prompt, enter: `start /SP/console`

   Multiple users can connect to the system console from the ILOM, but only one user at a time has write access to the console. Any input from other users is ignored.

   The following message appears:

   ```
   Are you sure you want to start /SP/console (y/n)?
   ```

2. Enter: **y**

   The following message appears:

   ```
   Serial console started. To stop, type #.
   ```

3. Press ENTER.

   The `User Name:` prompt appears.

4. Log on.

   The `#` prompt appears.

7.3.2
Viewing the Console History

Procedure:

1. At the ILOM prompt (`->`), enter:
   `set /SP/console line_count=<number of lines to view> start_from=<starting point>`

   Step example: ***<number of lines to view>*** is a number from 0 to 2048. If you enter `0`, you obtain the whole available console history. ***<starting point>*** stands for either `beginning` or `end`. If you type `beginning`, you obtain the number of lines from the first entry in console history. If you type `end`, you obtain the number of lines from the last entry in console history.
   The new console history limits appear.

2 Enter: `show /SP/console/history`

The console history is displayed, based on the limits set in the previous step.

Example:
Use the `show /SP/console/history` command to display system console messages logged in ILOM buffers. The ILOM records messages written to the console. Messages include output from POST, PROM, Solaris boot messages, and the Solaris console.

To see the last (most recent) 1000 lines in the buffer:

```
set /SP/console line_count=1000 start_from=end
 Set 'line_count' to '1000'
 Set 'start_from' to 'end'
  show /SP/console/history
```

To see the first 500 lines in the buffer:

```
set /SP/console line_count=500 start_from=beginning
 Set 'line_count' to '500'
 Set 'start_from' to 'beginning'
  show /SP/console/history
```

To see the entire buffer:

```
set /SP/console line_count="" start_from=beginning
 Set 'line_count' to ''
 Set 'start_from' to 'beginning'
  show /SP/console/history
```

7.3.3
Viewing Events

Use the `show /SP/logs/event/list` command to display all the events logged in the ILOM event buffer. Events include server reset events and all ILOM commands that change the state of the system (such as power on).

At the ILOM prompt (->), enter: `show /SP/logs/event/list`

The following is an example of a log containing the events logged in the ILOM event buffer:

```
ID      Date/Time                  Class     Type      Severity
 -----  -------------------------  --------  --------  --------
 5268   Tue Mar 24 18:21:14 2009  Audit     Log       minor
        root : Open Session : object = /session/type : value = shell :
success
 5267   Tue Mar 24 18:20:39 2009  Audit     Log       minor
        root : Close Session : object = /session/type : value = shell :
success
 5266   Tue Mar 24 18:04:46 2009  Audit     Log       minor
        root : Set : object = /users/service/password : value = ***** :
success
 5265   Tue Mar 24 18:04:15 2009  Audit     Log       minor
        root : Set : object = /users/root/password : value = ***** : success
 5264   Mon Mar 16 23:06:39 2009  Chassis   Log       critical
        CRITICAL ALARM is set
 5263   Mon Mar 16 23:06:12 2009  Chassis   Log       critical
        CRITICAL ALARM is set
 5262   Mon Mar 16 23:06:12 2009  Chassis   Log       minor
        CRITICAL ALARM is cleared
 5261   Mon Mar 16 23:06:06 2009  Chassis   Log       minor
        CRITICAL ALARM is cleared
 5260   Mon Mar 16 23:05:50 2009  Chassis   Log       minor
        CRITICAL ALARM is cleared
```

```
5259   Mon Mar 16 23:04:04 2009  Chassis   Log       minor
       CRITICAL ALARM is cleared
```

7.3.4
Viewing the Locator LED State

A white Locator LED is in the front upper left corner of the server bezel. A smaller Locator LED is also on the back of the server. The Locator LED is used to identify the server from others in a rack. Use the `show /SYS/LOCATE` command to view the state of the Locator LED (on or off):

At the -> prompt, type `show /SYS/LOCATE`. An example message showing the state of the locator LED is shown below:

```
Properties:
type = Indicator
ipmi_name = LOCATE
value = Off
```

7.3.4.1
Toggling the Locator LED

Use the `set /SYS/LOCATE` command to turn on and off the Locator LED.

- To turn on the Locator LED, enter:`set /SYS/LOCATE value=fast_blink` , where you set the value to **fast_blink**.
- To turn off the Locator LED, enter: `set /SYS/LOCATE value=off`, where you set the value to **off**.

7.3.5
Viewing the Environmental Status

To display the environmental status of the server (l is short for level), enter: `show -o table -l 2 /SYS`. This information includes:

- system temperatures
- power supply status
- front panel LED status
- hard disk drive status
- fan status
- voltage sensor status
- current sensor status

At the -> prompt, enter: `show -o table -l 2 /SYS`

Table 19: Environmental Status Example

Target	Property	Value
/SYS	type	Host System
/SYS	ipmi_name	/SYS

Table continued…

/SYS	keyswitch_state	Normal
/SYS	fault_state	Faulted
/SYS	power_state	On
/SYS/SERVICE	type	Indicator
/SYS/SERVICE	ipmi_name	SERVICE
/SYS/SERVICE	value	On
/SYS/LOCATE	type	Indicator
/SYS/LOCATE	ipmi_name	LOCATE
/SYS/LOCATE	value	Off

7.3.6
Viewing Fault Status

Use the `show faulty` command to view fault status from the ILOM. This command displays any currently faulted item on the server.

At the ILOM prompt (->), enter: `show faulty`

Table 20: Fault Status Example

Target	Property	Value
/SP/faultmgmt/0	fru	/SYS/PS1
/SP/faultmgmt/0/	timestamp	Mar 11 07:13:27
faults/0		
/SP/faultmgmt/0/	sp_detected_fault	Generic Powersupply fault at
faults/0		PS1 asserted
/SP/faultmgmt/0/	timestamp	Mar 11 07:13:19
faults/1		
/SP/faultmgmt/0/	sp_detected_fault	Input power unavailable for PSU
faults/1		at PS1

7.3.7
Viewing the Server ID and Status

Use the `show /HOST` command to display the server's platform ID and status.

At the -> prompt, enter: `show /HOST`

The platform ID and status appear. The following is an example of the `show /HOST` output:

```
Targets:
```

```
bootmode
diag
domain
Properties:
 autorestart = reset
 autorunonerror = true
 bootfailrecovery = none
 bootrestart = none
 boottimeout = 0
 hypervisor_version = Hypervisor 1.7.1 2009/01/22 06:50
 macaddress = 00:14:4f:ec:0f:56
 maxbootfail = 10
 obp_version = OBP 4.30.1 2009/01/17 05:30
 post_version = POST 4.30.1 2009/01/17 05:59
 send_break_action = (none)
 status = Solaris running
 sysfw_version = Sun System Firmware #.#.# YYYY/MM/DD HH:MM
```

7.3.8
Viewing Network Configuration

Use the `show /SP/network` command to display the current network configuration information.

At the -> prompt, enter: `show /SP/network`

The network configuration information appears; for example:

```
Properties:
 commitpending = (Cannot show property)
 dhcp_server_ip = none
 ipaddress = <IP address>
 ipdiscovery = static
 ipgateway = <IP address>
 ipnetmask = <IP address>
 macaddress = ##:##:##:##:##:##
 pendingipaddress = <IP address>
 pendingipdiscovery = static
 pendingipgateway = <IP address>
 pendingipnetmask = <IP address>
 state = enabled
```

(where ## represents a hex number)

7.3.9
Logging Out

Use the `exit` command to log out of an ILOM session.

At the -> prompt, enter: `exit`

You are logged out of ILOM and a prompt similar to the following appears:

```
SUNSPXXXXXXXXXXX login:
```

7.4
Basic Container Functions

This section contains commands that are useful for the Generic Application Server administrator.

7.4.1
Displaying Running Services

Use the `svcs` command to display information about the services that are running on a Generic Application Server.

7.4.1.1
Displaying All Services

At the `#` prompt, to display all the services running on the Generic Application Server, enter: `svcs -a`

The following information appears; for example:

```
# svcs -a
```

Table 21: All Services

STATE	STIME	FMRI
legacy_run	Mar_26	lrc:/etc/rc2_d/S00set-tmp-permissions
legacy_run	Mar_26	lrc:/etc/rc2_d/S07set-tmp-permissions
legacy_run	Mar_26	lrc:/etc/rc2_d/S10lu
disabled	Mar_26	svc:/network/nis/client:default
disabled	Mar_26	svc:/network/ldap/client:default
online	Mar_26	svc:/site/create-zoneszpool:default
online	Mar_26	svc:/system/zones:default
online	Mar_26	svc:/application/zc01-zone3:default

7.4.1.2
Displaying States of Services

At the `#` prompt, to display an explanation for service state, enter: `svcs -x (service name)`

- `svcs -x` without a service name shows any services that are failed.
- The `-x` option explains the states of services that are enabled, but are not running or are preventing another enabled service from running.

The following information appears; for example:

```
# svcs -x /system/console-login:default
svc:/system/console-login:default (Console login)
State: online since March 27, 2009  9:27:22 AM UTC
See: ttymon(1M)
See: /var/svc/log/system-console-login:default.log
Impact: None.
```

7.4.1.3
Displaying All Available Information About the Service

At the `#` prompt, to display all available information about the selected services and service instances, with one service attribute displayed for each line, enter: `svcs -l <service name>`

The following information appears; for example:

```
# svcs -l /system/console-login:default
```

```
fmri         svc:/system/console-login:default
name         Console login
enabled      true
state        online
next_state   none
state_time   March 27, 2009  9:27:22 AM UTC
logfile      /var/svc/log/system-console-login:default.log
restarter    svc:/system/svc/restarter:default
contract_id  8425
dependency   optional_all/none svc:/application/ghscommon-svcs (online)
dependency   require_all/none svc:/system/filesystem/minimal (online)
```

7.4.2
Enabling or Disabling a Service

Use the `svcadm` command to enable or disable a service when needed.

CAUTION: When the system is functioning normally, there should be no need to enable or disable a service. Performing this operation could put the system in an unusable state.

NOTICE: Only the root can enable/disable a service.

7.4.2.1
Enabling a Service

To enable a service, at the `#` prompt, enter: `svcadm enable -s [service name]`

NOTICE:
Since the `svcadm` command does not accept periods ("."), you must replace them with dashes ("-"). For example, "zc01.zone1" would have to be replaced with "zc01-zone1".

Use the `-s` option with the `svcadm` command. The `-s` option prevents the `#` prompt from returning until the enable/disable has completed. Otherwise, it is possible to try to run a command on the container while the previous command is still in process.

7.4.2.2
Disabling a Service

To disable a service, at the `#` prompt, enter: `svcadm disable -s [service name]`

NOTICE: Since the `svcadm` command does not accept periods ("."), you must replace them with dashes ("-"). For example, "zc01.zone1" would have to be replaced with "zc01-zone1". Use the `-s` option with the `svcadm` command. The `-s` option prevents the `#` prompt from returning until the enable/disable has completed. Otherwise, it is possible to try to run a command on the container while the previous command is still in process.

7.4.3
Administering System Application Containers

Use the `zoneadm` command to administer application containers. Under normal operation, the application containers do not need to be enabled or disabled.

7.4.3.1
Displaying Application Container Status

To display a list of installed containers and their current status, at the `#` prompt, enter: `zoneadm list -cv`

The following information appears; for example:

```
# zoneadm list -cv
```

Table 22: Application Container Status

ID	NAME	STATUS	PATH	BRAND	IP
0	global	running	/	native	shared
5	zc01.zone3	running	/opt/zones/zc01.zone3	native	shared
6	zds01.zone3	running	/opt/zones/zds01.zone3	native	shared
9	atr01.zone3	running	/opt/zones/atr01.zone3	native	shared

Containers that are functioning correctly have a status of **running** and are considered powered on. Containers that have a status of **installed** are not in a functioning state and are considered powered off.

7.4.3.2
Enabling a Container

To enable a container that is not in the running state, at the # prompt, enter: `svcadm enable -s [container name]`

NOTICE: Since the `svcadm` command does not accept periods ("."), you must replace them with dashes ("-").

Repeat the `zoneadm list -cv` command to verify that the container was enabled.

7.4.3.3
Disabling a Container

CAUTION: If a container must be disabled, it is important to disable the application first. Disabling an application container can seriously disrupt system functionality. Do not attempt to disable an application container unless you are aware of all the system impacts. See Disabling the Applications on page 87.

A container is a running service on the GAS. To disable a container, see Disabling a Service on page 107 using the container name for the service name.

NOTICE: Since the `svcadm` command does not accept periods ("."), you must replace them with dashes ("-").

Repeat the `zoneadm list -cv` command to verify that the container was disabled.

7.4.3.4
Uninstalling a Container Application

Procedure:

1. Log on to the Generic Application Server's Main Menu. See Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **Application Administration**. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Type the corresponding number for **Uninstall Container**. Press ENTER.

The following message is displayed:

```
Enter application name to un-install, or 'q' to quit:
```

4 From the list above the prompt, enter an application name. Press ENTER.

The following message is displayed:

```
Confirm un-install of <nnnn.zonex> (y/n):
```

5 Enter: **y**

The View uninstallation status screen is displayed.

6 When the row corresponding to the application being uninstalled is removed from the list, type `q`.

The **Application Administration** menu appears.

7 Enter: **q**

The Solaris prompt appears.

8 Enter: `exit`

The login prompt appears.

7.4.4
Viewing Log Files

Procedure:

1 Log on to the Generic Application Server's Main Menu. See Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **OS Administration** menu. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Display Logs**. Press ENTER.

4 Enter the corresponding number for the log file type to view.

A list of available logs appears.

5 Select the log file to view.

The logfile appears.

6 Enter: **q**

The list of log files appears.

7 Enter: **q**

The Solaris prompt appears.

7.4.5
Getting Log Files

Procedure:

1. Log on to the Generic Application Server's Main Menu. Logging On to the Generic Application Server on page 85.
2. Enter the corresponding number for **OS Administration** menu. Press ENTER.

   For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.
3. Enter the corresponding number for **Get Log Files**. Press ENTER.
4. Select the log file type to get.

   A message similar to the one below is displayed, followed by the **Get Log Files** menu:

   ```
   Getting kernel files, this may take a while...
    Created /var/getlogs/kernel-20100314211948.tar.gz
   ```
5. Enter: **q**

   The Solaris prompt is displayed.

7.4.6
Viewing the Status of the Hard Drives

Use the `raidctl` command to view the status of the hard drives.

7.4.6.1
Viewing the Controller, Volume, and Current Hard Drives

To list the controller, volume, and current hard drives, at the `#` prompt, enter: `raidctl`

The following information appears; for example:

```
# raidctl
Controller: 1
 Volume:c1t0d0
 Disk: 0.0.0
 Disk: 0.1.0
```

The output format is as follows:

```
Controller: [controller number]
 Volume: [volume name]
 Disk: [hard drive name]
 Disk: [hard drive name]
```

7.4.6.2
Viewing the Hard Drive Status and Specifications

To view a table with the status and specification information about the hard drives, at the `#` prompt, enter: `raidctl -l [volume name]`. Press ENTER.

Use the [volume name] from the `raidctl` command output.

For example, the following information appears:

p

Table 23: Hard Drive Status and Specifications

Volume	Sub Disk	Size	Stripe Size	Status	Cache	RAID Level
c1t0d0		279.3G	N/A	OPTI-MAL	OFF	RAID1
	0.0.0	279.3G		GOOD		
	0.1.0	279.3G		GOOD		

NOTICE: Size is the actual size of the drives in the system and may be different from the one shown in the example. The GOOD status means that hard drives are synchronized.

7.4.6.3

Viewing the Hard Drive Status

To list the status of the hard drives and volume, at the # prompt, enter: raidctl -S .

Current status of the disks is important to verify that the disks are synchronized

The following information appears; for example:

```
raidctl -S
1 "LSI_1068E"
c1t0d0 2 0.0.0 0.1.0 1 OPTIMAL
0.0.0 GOOD
0.1.0 GOOD
```

NOTICE: A GOOD status means that the hard drives are synchronized.

The output format is as follows:

```
 [controller ID number] "[controller type]"
 [RAID volume name] [number of disks] [Disk ID] [RAID Level] [Current
Status]
 [Disk ID] [Current Status]
 [Disk ID] [Current Status]
```

7.5

Troubleshooting Application Failures

This section describes how the server isolates failed applications from the others that still operate normally.

Use the Unified Event Manager (UEM) to view status and alarm messages for the server and its components, including the following FRU-related state changes:

- Temperature
- Hard drives
- Power supplies
- Fans

The UEM provides fault management functions for the Generic Application Server, including:

- Discovering devices
- Handling faults
- Detecting and reporting the loss of communication and synchronization

The UEM processes fault notifications (SNMPv3 traps) from the Generic Application Server, and reports any loss of communication. If a fault occurs, the Generic Application Server can generate a GAS LED alarm in the UEM.

The UEM also provides management functions such as the ability to troubleshoot faults and send commands to the Generic Application Server.

The UEM uses "maps" to provide a quick summary of the status of physical devices and their links. Each icon represents a subnet or a group of subnets that contain the devices and links managed by the UEM. There are two views of the Zone Physical map:

- Summary View: displays smaller icons and a larger number of subnets on the screen
- Detail View: displays a distinctive icon for each individual subnet type and displays the subnet name

For more information on using the UEM, see the “UEM Operation” chapter of the *Unified Event Manager User Guide*.

7.6 Server LEDs for Troubleshooting

This section describes how the LEDs appear if there is a problem with the server.

7.6.1 Server Status Indicators

The server has system status indicators that are located on the front and back of the server.

Table 24: Server System Status Indicators

LED	Description	If there is a problem with the server...
Locator	Enables you to identify a particular server.	White light on is the only way to locate the server.
Service Required	Provides a fault detection indicator.	Amber light on indicates that the server has detected a problem and requires the attention of service personnel.
Activity	Provides the power and operating system indicator.	Green light off indicates that either power is not present or the Solaris operating system is not running.

7.6.2
Alarm Status Indicators

The alarm status indicators are located vertically on the bezel of the server.

Table 25: Alarm Status Indicators

LED	Description	If there is a problem with the server...
Critical	Indicates a critical alarm.	For example, Red light on indicates call processing-related issues.
Major	Not used, as alarms are reported to the UEM.	Not used
Minor	Not used, as alarms are reported to the UEM.	Not used
User	Not used, as alarms are reported to the UEM.	Not used

7.6.3
Hard Drive Indicators

The hard drive indicator LEDs are located to the right of each hard drive that is installed in the server chassis. The bezel must be open to view the hard drive indicators.

Table 26: Hard Drive Indicators

LED	Description	If there is a problem with hard drives ...
OK to Remove	Hard drive removal indicator	Not used
Fault	Fault indicator	Amber light on indicates that the drive has a fault and requires attention.
Activity	Activity indicator	Green light off indicates no activity.

7.6.4
Power Supply Unit Indicators

The Power Supply Unit (PSU) LEDs are located on the rear of each power supply, on the left side.

Table 27: Power Supply Indicators

LED	Description	If there is a problem with the power supplies ...
Power OK	Activity indicator	Green light off indicates that either power is not present, or the PSU has shut down due to an internal protection event.
Fault	Fault detection indicator	Amber light on indicates that the power supply has detected a failure.
T5220 Server: Input OK T4–1 server:	Input power indicator	Green light off indicates no input voltage, or input voltage below limits.

LED	Description	If there is a problem with the power supplies ...
AC present		

7.6.5
Network Link and Speed Indicators

The network link and speed indicators are located above the Ethernet connectors, on the rear of the server.

Table 28: Network Link and Speed Indicators

LED	Description	If there is a problem with the server...
Network Link Indicator (left side)	Network link status	Green light off indicates that the link is not established.
Network Speed Indicator (right side)	Network speed status	Green light off indicates: • If the network link indicator is on, the network link is established but not running at its maximum supported speed. • If the network link indicator is off, the network link is not established.

7.7
Troubleshooting Hardware Problems

This section provides tips/procedures for troubleshooting FRUs, including the hard drive, the DVD-RW drive, fans, and power supplies.

The hard drive stores critical information for call processing, resource management, and mobility management. The hard drive includes all the basic software and routines necessary for successful operation of the Generic Application Server and includes databases containing information about radios, sites, and other equipment. Having a connection problem or corruption within any of these devices causes problems in several other devices.

Table 29: Troubleshooting the Hard Drive

Problem	Troubleshooting
The hard drive is not operating properly.	Perform the following actions: • Execute the `show faulty` ILOM command. • Verify that the power connection to the hard drive is secured and in good condition. • Reboot the server to re-initialize all processes. See Rebooting the Server on page 87. • Replace the hard drive and cabling, if necessary.
Necessary data on the hard drive is corrupt or lost.	Perform the following actions: • Ensure that you have the latest infrastructure database. Check the time and date of the last backup in the Backup and Restore Server.

Problem	Troubleshooting
	• Replace the hard drive or cabling, as necessary.

Table 30: Troubleshooting the DVD-RW Drive

Problem	Troubleshooting
The DVD-RW drive is not operating properly.	Perform the following actions: • Verify that the CD or DVD being used is clean and in good condition. • Verify that the DVD-RW drive is seated properly. • Verify that the power connection to the drive is secured and in good condition. • Replace the DVD-RW drive and cabling, if necessary.

The server must be kept within a certain temperature range. To do this, the server uses fans to cool the drives and modules.

Table 31: Troubleshooting the Fans

Problem	Troubleshooting
The fans are not operating properly.	Perform the following actions: • Visually inspect the fans (front and rear) for any loose parts or physical damage. • Check the power connections. • Replace the fans, as necessary.

Dual redundant 650 W power supplies, located in the rear of the server, provide highly available power to the server subcomponents.

Table 32: Troubleshooting the Power Supply

Problem	Troubleshooting
Voltage fault	Perform the following actions: • Check the component status for the power supplies. Execute the `show -o table -l 2 /SYS` command through the ILOM to view the environment. • Check the power supplies and incoming power for any problems. • Replace the power supplies, correct the incoming power problem, as necessary.
The LED on the power supply is not illuminated.	Perform the following actions: • Check the power connection and the incoming power for any problems. Verify that the incoming power is within the guidelines specified for the server.

Problem	Troubleshooting
	• Check the component status for the power supply. Execute the `show -o table -l 2 /SYS` command through the ILOM to view the environment. • Verify that the power supply is fully inserted and secured in the chassis. • Replace the power supply, as required.

7.8

Preparing to Reinstall a Generic Application Server

This procedure applies to a server already installed and configured with the Generic Application Server software. This procedure powers down the server properly, so that you can continue with the installation.

When and where to use: Perform this procedure as the first step to recover from a catastrophic failure of the server, for example, when both hard drives in a mirrored configuration are not functioning.

Procedure:

1. Establish a serial connection to the server through the SER MGMT port on the back of the server.
2. If you are in the host console (either logged on, or at the login prompt), switch to the ILOM. Enter: `#`

   The message similar to the following appears:

   ```
   Serial console stopped.
    ->
   ```

3. If you are already logged on the ILOM, log off. Enter: `exit`
4. Perform one of the following steps:

If…	Then…

If the T5220 server is used in your system,	at the `SUNSPXXXXXXXXXXXX login:` prompt, log on using the login and password of the ILOM root account.
	Result: The following messages appear on the screen:
	`Waiting for daemons to initialize...`
	`Daemons ready`
	`Sun(TM) Integrated Lights Out Manager Version`
	`Version 2.0.4.26`
	`Copyright 2008 Sun Microsystems, Inc. All rights reserved.`
	`Use is subject to license terms.`
	`Warning: password is set to factory default.`
	`->`

If T4-1 server is used in your system,	open an SSH session and connect to the SP: % ssh `root@xxx.xxx.xxx.xxx`
	`Are your sure you want to continue connecting (yes/no)?`
	`yes`

If…	Then…
	Password: password (nothing displayed) Waiting for daemons to initialize... Daemons ready Integrated Lights Out Manager Version 3.x.x.x Copyright 2010 Oracle and/or its affiliates. All rights reserved. Use is subject to license terms. ->

5 To power the system off, enter: `stop /SYS`

The following prompt appears:

```
Are you sure you want to stop /SYS (y/n)?
```

6 Enter: **y**

The following prompt appears:

```
Stopping /SYS
```

7 To log off the ILOM, enter: `exit`

The login prompt appears.

8 Disconnect the server power cords from the power supplies.

The server is powered down.

Postrequisites: Perform Preparing for the Generic Application Server Installation on page 47

7.9 Viewing the Installation Log

To view the installation logs on the server, browse to this location: `/var/sadm/install/logs`

7.10 Viewing the NTP Status

Procedure:

1 Log on to the Generic Application Server's Main Menu. See Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Software Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Display NTP Status**. Press ENTER.

A list of NTP aliases and a list of NTP sources similar to the one below is displayed, followed by the **Manage NTP Server Configuration** menu.

```
Hosted NTP aliases:
<List of NTP Aliases>
```

```
Remote NTP time sources:
<List of NTP Sources>
```

4 Exit to the command prompt or log off. See Logging Off the Terminal Server on page 84.

7.11 Viewing the Application Data Summary

Procedure:

1 Log on to the Generic Application Server's Main Menu. Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Application Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Display Application Data Summary**. Press ENTER.

The View Application Data Summary table appears, followed by the following prompt:

```
Enter q to quit:
```

4 Enter: `q`

The Manage Persistent Storage menu is displayed.

7.12 Viewing Resource Summary

Procedure:

1 Log on to the Generic Application Server's Main Menu. See Logging On to the Generic Application Server on page 85.

2 Enter the corresponding number for **Application Administration**. Press ENTER.

For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

3 Enter the corresponding number for **Manage Scalable Resources**. Press ENTER.

4 Enter the corresponding number for **Display Resources Summary**. Press ENTER.

The current resource balancing status and a table with the current resource allocation are displayed, followed by the **Manage Scalable Resources** menu.

5 Exit to the command prompt or log off. See Logging Off the Terminal Server on page 84.

Chapter 8

Generic Application Server FRU/FRE Procedures

A Field Replaceable Unit (FRU) is the lowest repair level for a device that can be replaced in the field. The server FRU hardware comprises of self-contained modules. When determined to be faulty, they are quickly and easily replaced with a known good module, to bring the equipment back to normal operation. The faulty module must be shipped to the Motorola Solutions Infrastructure Depot Operations (IDO) for further troubleshooting and repair. See T5220 Server FRU/FRE Part List on page 120 for a list of FRUs.

A Field Replaceable Entity (FRE) is a device that does not include any field replaceable subcomponents or subassemblies. FRE replacement involves the replacement of the entire assembly. The server FRE hardware does not contain any replaceable modules. When FRE hardware is determined to be faulty, the entire unit is replaced. The faulty hardware must also be shipped to the Motorola Solutions IDO for further troubleshooting and repair.

If you are replacing a server, the software is not installed and a full installation of the Generic Application Server is required.

In addition to FRUs and FREs, some components are available as replacement parts from the North America Parts Organization. These components are disposable or irreparable and cannot be shipped to the Motorola Solutions IDO for repair.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

8.1 Motorola Solution Support Center Contact Information

The Motorola Solution Support Center (SSC) provides technical support, Return Material Authorization (RMA) numbers for FRUs and FREs, and confirmations for troubleshooting results. Call the Motorola System Support Center for information about returning faulty equipment or ordering advance exchanges.

International: 302-444-9800

8.2 North America Parts Organization Contact Information

The North America Parts Organization provides FRUs and FREs (without advance exchanges or for spares), and other replacement parts.

International (non-FAX): 302-444-9842

8.3 Original Settings

Always use the switch, jumper, and software configuration settings specified by Motorola Solutions. If other settings are necessary for proper system operation, consult the Motorola Solution Support Center (SSC). Deviating from the original configuration set up by Motorola Solutions may result in damage to equipment or loss of service.

8.4
Required Tools and Equipment

Take the following items to the replacement site when replacing equipment in the server:

- Electrostatic Discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent)
- Antistatic mat
- Cross tip screwdriver

8.5
T5220 Server FRU/FRE Part List

This section lists the available FRU/FREs for the server, along with the part numbers, and refers to the appropriate procedure for replacing the item. Use the part number for the item when ordering replacements.

Table 33: T5220 Server FRE List

Component Type	Part Number	Replacement Procedure
Sun Netra T5220 Server without software	DLN6699A	Replacing a Server on page 139

Table 34: T5220 Server FRU List

Component Type	Part Number	Replacement Procedure
Hard Drive, 300 GB	DLN6700A	Replacing Hard Drives in T5220 Servers on page 125
DVD-RW Drive, 8X	• (If PATA): DLN6698A • (If SATA): DLN6726A	Replacing Optical Media Drives in T5220 Servers on page 126
Power Supply (PS), 650 W	DLN6697A	Replacing Power Supply Units in T5220 Servers on page 127

The following are the replacement parts orderable from the North America Parts Organization only.

Table 35: T5220 Server Replacement Part List

Component Type	Part Number	Replacement Procedure
FB-DIMM memory, 4 GB (2 x 2 GB)	SYLN8958	Replacing FB-DIMM Memory Modules in T5220 Servers on page 129
Air filters, ten-pack	3571852H01	Replacing Air Filters in T5220 Servers on page 131
System Fan Assembly	5900925801	Replacing the System Fan Assembly in T5220 Servers on page 134
FB-DIMM Fan	5900925601	Replacing FB-DIMM Fans in T5220 Servers on page 135

Table continued…

Component Type	Part Number	Replacement Procedure
Hard drive fan assembly	590092570001	Replacing the Hard Drive Fan Assembly in T5220 Servers on page 136

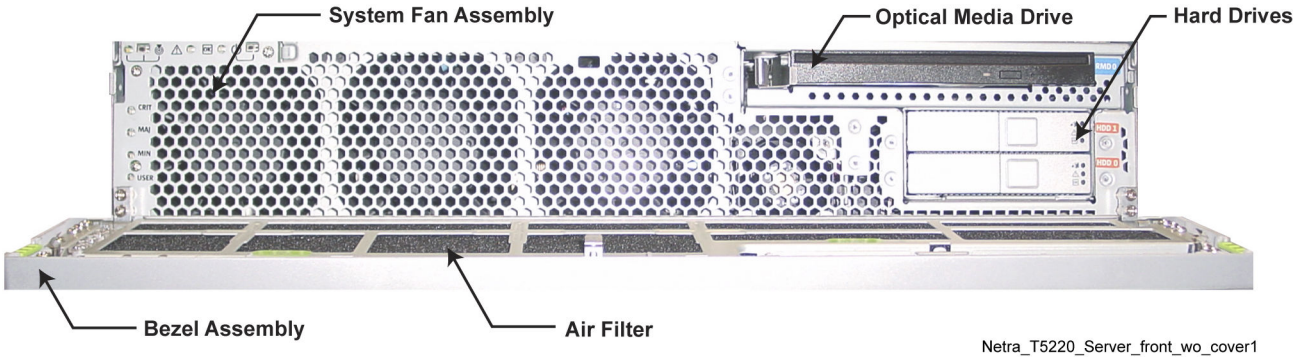
The Netra T5220 documentation set from Oracle also includes comprehensive replacement procedures.

8.5.1
T5220 Server Open Bezel

The open bezel, as shown below, reveals the following components:

- Bezel assembly
- System fan assembly
- Air filter
- Optical media drive
- Hard drives

Figure 12: T5220 Server Open Bezel

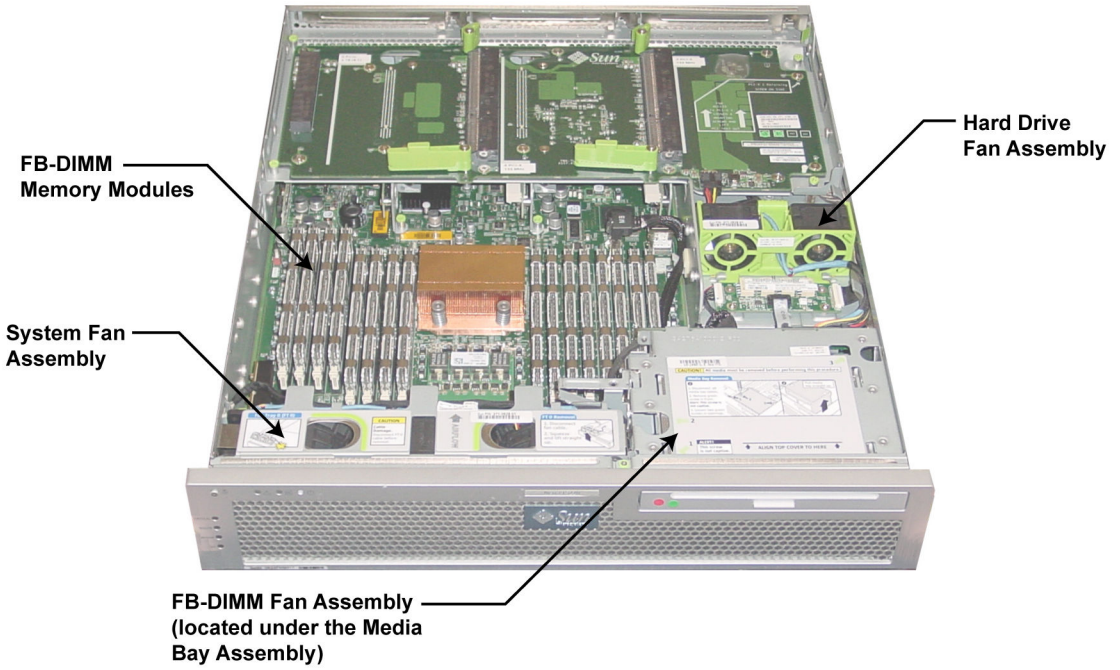


8.5.2
T5220 Server Internal Components

The internal components are located in the main part of the chassis and include:

- Fully Buffered DIMMs (FB-DIMMs) memory modules
- System fan assembly
- FB-DIMM fan assembly
- Hard drive fan assembly

Figure 13: T5220 Server Internal FRU



8.5.2.1

FB-DIMM Memory Modules

In the server memory, 16 slots hold DDR-2 memory FB-DIMMs in the following configurations:

- 4 FB-DIMMs (Group 1)
- 8 FB-DIMMs (Groups 1 and 2)
- 16 FB-DIMMs (Groups 1, 2, and 3)

8.5.2.2

System Fan Assembly

The System Fan Assembly contains three fans for cooling the motherboard assembly. The system fan assembly is labeled FT0.

8.5.2.3

FB-DIMM Fan

The FB-DIMM fan is a single fan for cooling FB-DIMMs. The FB-DIMM fan assembly is labeled FT2. The fan is located under the media bay assembly.

8.5.2.4

Hard Drive Fan Assembly

The Hard Drive Fan Assembly includes fans that provide supplemental cooling of the hard drives and the optical media drive. The hard drive fan assembly is labeled FT1.

8.6
FRU/FRE Parts List for the T4-1 Server

Table 36: FRE for the T4-1 Server

Component Type	Part Number
Netra SPARC T4-1 server	DLN6927A

Table 37: FRU for the T4-1 Server

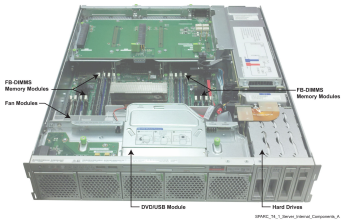
Component Type	Part Number
1200W AC PSU 12V	DLN6930A
300 GB SAS-2 Hard Drive	DLN6929A
Netra Gen2 DVD Drive	DLN6928A

Table 38: Replacement Parts List for T4-1 Server

Component Type	Part Number
Air Filter (pack of 10)	35009380001
DIMM	01009712001
Fan Module	59009278001
Hard Drive Fan	59009279001

8.6.1
Server Internal Components for the T4-1 Server

Figure 14: T4-1 Server Internal Components



The following are motherboard components:

- PCIe/XAUI risers
- DIMMS
- Motherboard assembly
- Service Processor
- SCC module
- Battery
- Removable back panel cross beam

The following are I/O components:

- Top cover
- Hard drive backplane

- Hard drive cage
- Right control panel light pipe assembly
- DVD/USB module
- Hard drives
- Left control panel light pipe assembly

The following are power distribution/fan module components:

- Fan modules
- Fan power board
- Air duct
- Power supplies
- Power supply backplane
- Power distribution board/bus bar
- Connector board

8.7 Preparing a Server for Service

If a FRU/FRE has been determined as the cause of failure, this is a high-level process necessary to place the server back in operation.

NOTICE: To minimize alarms in the UEM, you can unmanage the devices in the UEM before beginning this process. The UEM re-discovers the devices without intervention, after receiving a status change when the server and applications are back online.

Process:

1. Before powering off, disable all application containers first. See Disabling the Applications on page 87.
2. Power down the server. See Powering Off the Server on page 89.
3. Replace the defective parts, as documented in the current section.
4. Power up the server. See Powering On the Server on page 77.
5. Install the software if necessary. See the following sections:
   - Generic Application Server Installation on page 43
   - Loading the Applications on page 56
   - Installing the Applications on page 57
6. Restore the databases. See Restoring the Generic Application Server from Persistent Storage on page 96 to restore the databases.
7. Bring the Generic Application Server on-line with minimal system disruption. See Enabling the Applications on page 87.

8.7.1 Avoiding Electrostatic Discharge

Use an antistatic wrist strap to avoid electrostatic discharge.

Procedure:

1. Power off the server, as described in Powering Off the Server on page 89.

2 Prepare an antistatic surface on which to set parts during removal and installation. Place ESD-sensitive components such as printed circuit boards on an antistatic mat.

3 When servicing or removing server components, attach an antistatic strap to your wrist and then to any clean metal area on the chassis. Then, disconnect the power cords from the server.

4 Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.

   All field replaceable units (FRUs) that are not hot swappable require the removal of the top cover of the server.

5 To remove antistatic measures when you are finished, perform the following steps:

   a Remove any antistatic straps or conductors from the server chassis.

   b Take off the antistatic wrist strap.

8.8 Replacing Hard Drives in T5220 Servers

The hard drive stores the Generic Application Server software. The server uses two 300 GB hard drives. They are not hot swappable. Swapping in a preloaded hard drive is not supported.

Prerequisites: Replacing a hard drive does not require removing the server from a rack.

Procedure:

1 Power off the server, as described in Powering Off the Server on page 89.

2 Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.

3 Press the green finger holds on either side of the bezel, and then pull forward and down to the open position.

4 Identify the location of the hard drive that you want to remove.

5 On the drive you plan to remove, push the latch release button.

   CAUTION: The latch is not an ejector. Do not bend it too far to the left. Doing so can damage the latch.

   The latch opens.

6 Grasp the latch and pull the drive out of the drive slot. Continue to the next step to install the new hard drive.

   Do not remove the drive unless the hard drive status is `GOOD` . See Viewing the Status of the Hard Drives on page 110 to verify that the drives are synchronized before swapping.

7 Remove the replacement hard drive from its packaging and place it on an antistatic mat.

8 Align the replacement drive with the drive slot.

   The hard drive is physically addressed in line with the slot in which it is installed. It is important to install a replacement drive in the same slot as the drive that was removed.

9 Slide the drive into the bay until it is fully seated.

10 Close the latch to lock the drive in place and then close the bezel.

11 Power on the server, as described in Powering On the Server on page 77. The server recognizes the new hard drive once it has booted up.

12 Proceed to Installing the Generic Application Server on page 52. You must reload the Generic Application Server software.

13 Restore the server. See Restoring the Generic Application Server from Persistent Storage on page 96.

8.9 Replacing Hard Drives in T4-1 Servers

Procedure:

1 Perform one of the following actions:
   - If you cannot take the hard drive offline without shutting down the OS, power off the server, then go to step 3.
   - If you can take offline the drive without shutting down the OS, go to step 2 .

2 Perform the following actions:
   a To list all drives in the device tree, including drives that are not configured, at the Oracle Solaris prompt, enter: `cfgadm -al`
   b To unconfigure any drive whose status is listed as configured, enter: `cfgadm -c unconfigure`
   c Verify that the drive's blue Ready-to-Remove LED is lit blue.

```
# cfgadm —c unconfigure c0: :dsk/c1td0
```

3 Press the drive release button to unlock the drive and pull on the latch to remove the drive. Leave the latch open.

4 Install the replacement drive or a filler tray. Perform the following actions:
   a Insert the drive into the drive bay and slide it forward until it is seated.
   b Close the latch to lock the drive in place.
   c Bring the drive online.
   d Configure the drive. Enter: `cfgadm -c configure`
   e Verify the functionality of the hard drive. For details, see the Oracle documentation.

8.10 Replacing Optical Media Drives in T5220 Servers

The DVD-RW drive is used to load and install the application software and patches on the hard drive. The location of the DVD-RW drive.

WARNING: The DVD-RW drive contains a laser device. To avoid the risk of radiation exposure, do not attempt to open the DVD-RW drive enclosure or remove a DVD-RW drive using any procedures other than the procedures contained in this section.

Procedure:

1 Power off the server, as described in Powering Off the Server on page 89.

2 Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.

3 Press the green finger holds on either side of the bezel, and then pull forward and down to the open position.

4 Push the release tab to the left and pull the probe forward, freeing the optical media drive.

5 Remove the optical media drive from the media bay assembly and set it aside on an antistatic mat. Continue to the next step to install the new optical media drive.

6 Remove the replacement optical media drive from its packaging and place it on an antistatic mat.

7 Hold the tab to the left and insert the optical media drive into the media bay assembly.

8 Press the optical media drive in until it seats, and then release the tab.

9 Close the bezel, and remove the electrostatic discharge measures.

10 Power on the server, as described in Powering On the Server on page 77.

8.11 Replacing the DVD or USB Assembly in T4-1 Servers

Procedure:

1 Power off the server. See Powering Off the Server on page 89.

2 Perform the following actions:

- Remove any optical disks from the DVD module.
- Unplug any USB cables from the USB port.

3 Bring the server to the standby mode. With a pointed object, for example a stylus or pen, momentarily press the recessed Power button on the server.

4 Disconnect the power cord.

5 Attach an antistatic wrist strap.

6 If the lower right hard drive bay contains an HDD or SDD module, remove it.

7 Reach in under the DVD/USB module and pull the release tab out.

Use the finger indentation in the hard drive bay below the DVD/USB module to extend the release tab.

8 Slide the DVD/USB module out of the hard drive cage.

9 Place the module on an antistatic mat.

10 Ensure that the DVD module you want to install is of the serial SATA type.

11 Slide the DVD/USB module into the front of the chassis until it seats.

12 Slide the release tab back into the system.

13 If you removed a hard drive from the lower right drive bay, reinstall it.

14 Reconnect the power cords to the power supplies.

Depending on how the firmware is configured, the system might boot as soon as the power cords are connected and standby power is applied.

15 Power on the system. See Powering On the Server on page 77.

8.12 Replacing Power Supply Units in T5220 Servers

The server has dual redundant 650 W Power Supply Units (PSUs) to provide power to the server components. One PSU can be hot swapped while the other is still running, without having to power off the server.

CAUTION: When opening and closing the levers on power supply units, keep hands and fingers away from the base and sides of the levers, as the levers can pinch.

Procedure:

1. Identify which power supply requires replacement. The UEM identifies a faulty power supply. You can also use the `show faulty` command at the Sun Integrated Lights Out Manager (ILOM) prompt (`->`).
2. At the ILOM (`->`) prompt, enter: `set /SYS/PSn prepare_to_remove_action=true`

   `n` is the power supply number.

   If the command is successful, the following prompt appears:

   ```
   Set 'prepare_to_remove_action' to 'true'
   ```

   If the command is not successful, the following prompt appears:

   ```
   set: Operation not allowed on identified device
   ```

   NOTICE: The `set /SYS/PSn` command indicates if it is OK to perform a hot swap of a power supply. This command does not perform any action, but it provides a warning if the power supply should not be removed because the other power supply is not providing power to the server.

3. To list all the properties of the power supply, enter: `show /SYS/PSn`

   `n` is the power supply number.

   One of the following prompts appears:

   ```
   prepare_to_remove_status = Ready
    prepare_to_remove_status = NotReady
   ```

   If the property is set to Ready, the power supply is safe to remove, continue to the next step. If it is not allowed to remove the power supply, the property is set to NotReady, which is the default setting.

4. Disconnect the power cord from the PSU being replaced.

   CAUTION: Do not remove the power input cable from the remaining PSU or the system will go through an immediate ungraceful shutdown.

5. Grasp the power supply handle and push the power supply latch to the right.
6. Pull the power supply out of the chassis. Continue to the next step to install the new power supply.
7. Remove the replacement power supply from its packaging and place it on an antistatic mat.
8. Align the replacement power supply with the empty power supply bay.
9. Slide the power supply into the bay until it is fully seated.
10. Reconnect the power cord to the power supply.
11. Verify that the amber LED on the replaced power supply and the service required LEDs are not lit.
12. Verify the status of the power supplies. At the ILOM (`->`) prompt, enter: `show -o table -l 2 /SYS`

8.13

Replacing Power Supply Units in T4-1 Servers

The two power supply units enable you to hot-swap a power supply.

Procedure:

1. Ensure that you have a replacement.
2. Identify which power supply requires replacement.

   You can hot-swap the faulty power supply without shutting down the server.
3. Disconnect the power cord from the PSU being replaced.
4. Grasp the power supply handle, press the release latch and pull the power supply out of the server.
5. Remove the replacement power supply from its packaging and place it on an antistatic mat.
6. If the power supply bay contains a power supply filter panel, remove it.
7. Align the replacement power supply with the empty power supply bay.
8. Slide the power supply into the bay until it locks into place.
9. Reconnect the power cord to the power supply.
10. Verify that the power supply **Power OK** and **AC present** LEDs are lit, and that the Fault LED is not lit.
11. Verify that the amber LED on the replaced power supply and the service required LEDs are not lit.
12. Perform one of the following actions:
    - If the previous steps did not remove the fault, see “Diagnostic Process” in “SPARC T4-1 Server Getting Started Guide”.
    - If step 10 and step 11 show no faults, return the server to operation.

8.14

Replacing FB-DIMM Memory Modules in T5220 Servers

The location of the memory modules is shown in the "Server – Internal Components" section. The memory modules are shown in the "Server – Internal Components" figure.

Prerequisites: Ensure that all power is removed from the server before removing or installing FB-DIMMs or damage to the FB-DIMMs might occur.

CAUTION: Disconnect the power cables from the system before performing this procedure.

Procedure:

1. Prepare the server for FB-DIMM removal:
   a. Power off the server, see Powering Off the Server on page 89.
   b. Make a note of the location of the cables and power cords, and then unplug all connections.
   c. Remove the server from the rack.
   d. Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.
2. Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.

3 To remove the PCI mezzanine, perform the following actions:
   a Disconnect any I/0 cables from the rear of the PCI mezzanine.
   b Disconnect the PCI mezzanine cable.
   c Use a cross tip screwdriver to loosen the four green captive screws securing the PCI mezzanine.
   d Lift the PCI mezzanine up and out.
   e Lift the PCI mezzanine away from the chassis and place it on an antistatic mat.
4 Remove the FB-DIMM/CPU duct. See Replacing Air Ducts in T5220 Servers on page 132.
5 If you are replacing a faulty FB-DIMM, locate the FB-DIMMs that you want to replace. Press the DB-DIMM DIAG button on the motherboard to activate the DB-DIMM status LEDs. Any faulty FB-DIMMs are indicated with a corresponding amber fault LED on the motherboard.

   Make a note of the faulty FB-DIMM location so that you can install the replacement in the same location.
6 Push down on the ejector tabs on each side of the FB-DIMM until the FB-DIMM is released.
7 Grasp the top corners of the faulty FB-DIMM and remove it from the server.
8 Place the FB-DIMM on an antistatic mat. Repeat step 6 through step 8 to remove any additional FB-DIMMs. Continue to the next step to install the new FB-DIMMs.
9 Unpack the replacement FB-DIMMs and place them on an antistatic mat.
10 Ensure that the ejector tabs are in the open position.
11 Line up the replacement FB-DIMM with the connector. Align the FB-DIMM notch with the key in the connector. This action ensures that the FB-DIMM is oriented correctly.
12 Push the FB-DIMM into the connector until the ejector tabs lock the FB-DIMM in place. If the FB-DIMM does not easily seat into the connector, verify that the orientation of the FB-DIMM is correct. If the orientation is reversed, damage to the FB-DIMM might occur.
13 Repeat step 10 through step 12 until all replacement FB-DIMMs are installed.
14 Install the air duct. See Replacing Air Ducts in T5220 Servers on page 132.
15 To install the PCI mezzanine, perform the following actions:
   a Position the PCI mezzanine onto the chassis.
   b Lower the PCI mezzanine and slide it towards the front of the server.
   c Use a cross tip screwdriver to tighten the four green captive screws securing the PCI mezzanine.
   d Reconnect the PCI mezzanine cable.
16 Install the top cover of the server:
   a Place the top cover on the chassis. Set the cover down so that it hangs over the rear of the server by about an inch (25 mm).
   b Carefully align the front of the top cover with the black line (with arrows) printed on top of the media bay assembly.
   c Slide the cover forward until it latches into place.
17 To bring the server back online, perform the following actions:
   a Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.
   b Reinstall the server in the rack.
   c Connect the cables and power cords.

d Power on the server. See Powering On the Server on page 77

8.15

Replacing FB-DIMM Memory Modules in T4-1 Servers

Prerequisites:
Familiarize yourself with DIMM population rules and prepare the server for service. For details, see the Oracle documentation.

Procedure:

1. Identify faulty DIMMS. Perform one of the following actions:
   - **a** Use **DIMM Fault Remind**. Go to step step 2.
   - **b** At the Oracle ILOM promptenter: `show faulty` and go to step 6.
2. Swing the air duct up and forward to the fully open position.
3. Press **DIMM Remind**.

   An amber LED associated with the faulty DIMM lights for a few minutes.
4. Note the DIMM next to the illuminated LED.
5. Ensure that all other DIMMs are seated correctly in their slots.
6. If you haven't already done so, swing the air duct up and forward to the fully open position.
7. Push down on the ejector tabs on each side of the DIMM until the DIMM is released.
8. Grasp the top corners of the faulty DIMM and lift it out of its slot.
9. Place the DIMM on an antistatic mat.
10. Repeat step 7 through step 9 for any other DIMMs you intend to remove.
11. Perform one of the following actions:
    - If you do not plan to install replacement DIMMs at this time, install filler panels in the empty slots.
    - If you have dual-ranked x4 (2Rx4) DIMMs with System Firmware 8.2.1.b or later, install new DIMM. Go to step 12.
12. If you haven't done so already, swing the air duct up and forward to the fully open position.
13. Prepare the replacement DIMMs and place them on an antistatic mat.
14. Ensure that the ejector tabs on the connector that will receive the DIMM are in the open position.
15. Align the DIMM notch with the key in the connector.
16. Push the DIMM into the connector until the ejector tabs lock the DIMM in place.

    If the DIMM does not easily seat into the connector, check the DIMM's orientation.
17. Repeat step 14 through step 16 to install all new DIMMs.
18. Return the air duct to the closed position.
19. Returning the server to operation and verify DIMM functionality.

8.16

Replacing Air Filters in T5220 Servers

The air filter ensures the supply of clean air to the front fan assembly and is fitted inside the bezel.

Procedure:

1. Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.
2. Press the green finger holds on both sides of the bezel, and then pull forward and down to the open position.
3. Grasp the finger holds and lift the air filter from the bezel.

   Do not operate the server without an air filter.
4. To install the new air filter, perform the following actions:
   a. Remove the replacement air filter from its packaging.
   b. Insert the air filter into the bezel and close the bezel.

8.17 Replacing Air Filters in T4-1 Servers

You don't need to power off the server before you remove the air filter.

Prerequisites:

- Review safety and handling information.
- Gather the tools for service.
- Consider filler panel options.
- Find the server serial number.
- Identify the server to be serviced.
- Locate the component service information.
- For cold-service operations, shut down the OS and move the server out of the rack.
- Gain access to internal components.

Procedure:

1. Grasp the left and right sides of the filter tray and pull it straight off.
2. Flip the filter tray over to access the air filter.
3. Carefully compress the air filter and feed it out from the restraining hooks of the filter tray.
4. Set the air filter aside.
5. Feed the edges of the air filter under the restraining hooks of the filter tray.
6. Massage the filter in the filter tray so that there are no folds or wrinkles, and so that the air filter lies flat against the filter tray.
7. Install the filter tray to the server, with the indicators in the upper left corner.

   The bezel snaps into place.

8.18 Replacing Air Ducts in T5220 Servers

The air duct aids cooling of the FB-DIMMs and the CPU.

Procedure:

1. To prepare the server for air duct removal, perform the following actions:
   a. Power off the server, see Powering Off the Server on page 89.

b Make a note of the location of the cables and power cords, and then unplug all connections.

c Remove the server from the rack.

d Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.

2 Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.

3 To remove the PCI mezzanine, perform the following actions:

a Disconnect any I/0 cables from the rear of the PCI mezzanine.

b Disconnect the PCI mezzanine cable.

c Use a cross tip screwdriver to loosen the four green captive screws securing the PCI mezzanine.

d Lift the PCI mezzanine up and out.

e Lift the PCI mezzanine away from the chassis and place it on an antistatic mat.

4 Facing the server, release the tab on the right of the air duct and pull upward.

5 Lift the duct out of the chassis, releasing it from the pins on the left side of the chassis, and set it aside on an antistatic mat.

6 Perform one of the following actions:

- If you removed the air duct as part of a different procedure, return to that procedure
- If you have not removed the air duct as part of a different procedure, continue to the next step to install the new air duct.

7 Remove the replacement air duct from its packaging.

8 With the duct at a 45 degree angle, position the pin holes in the duct to align them with the pins of the chassis.

9 Lower the duct to the horizontal position until the tab is secured in place.

10 To install the PCI mezzanine, perform the following actions:

a Position the PCI mezzanine onto the chassis.

b Lower the PCI mezzanine and slide it towards the front of the server.

c Use a cross tip screwdriver to tighten the four green captive screws securing the PCI mezzanine.

d Reconnect the PCI mezzanine cable.

11 To install the top cover of the server, perform the following actions:

a Place the top cover on the chassis. Set the cover down so that it hangs over the rear of the server by about an inch (25 mm).

b Carefully align the front of the top cover with the black line (with arrows) printed on top of the media bay assembly.

c Slide the cover forward until it latches into place.

12 If you installed the air duct as part of a different procedure, return to that procedure. Otherwise, perform the following tasks to bring the server back online:

a Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.

b Reinstall the server in the rack.

c Connect the cables and power cords.

d Power on the server. See Powering On the Server on page 77.

8.19

Replacing the System Fan Assembly in T5220 Servers

The system fan assembly contains three fans for cooling the motherboard assembly. The system fan assembly is labeled FT0.

Procedure:

1. To prepare the server for fan assembly removal, perform the following steps:
   - **a** Power off the server, see Powering Off the Server on page 89.
   - **b** Make a note of the location of the cables and power cords, and then unplug all connections.
   - **c** Remove the server from the rack.
   - **d** Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.
2. Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.
3. Disconnect the fan assembly cable from the power board.
4. Remove the fan assembly cable from the cable guides.
5. Insert your forefinger and thumb into the holes at the top of the fan assembly, squeeze them together, and lift the fan assembly from the chassis.
6. Set the fan assembly aside on an antistatic mat.
7. If you removed the fan assembly as part of a different procedure, return to that procedure. Otherwise, continue to the next step to install the new system fan assembly.
8. Remove the replacement fan assembly from its packaging and place it on an antistatic mat.
9. Insert your forefinger and thumb into the holes at the top of the fan assembly, squeeze them together, and lower the fan assembly into the chassis.
10. Reconnect the fan assembly cable to the power board.
11. Route the fan assembly cable back into the cable guides.
12. Install the top cover of the server:
    - **a** Place the top cover on the chassis. Set the cover down so that it hangs over the rear of the server by about an inch (25 mm).
    - **b** Carefully align the front of the top cover with the black line (with arrows) printed on top of the media bay assembly.
    - **c** Slide the cover forward until it latches into place.
13. If you installed the fan assembly as part of a different procedure, return to that procedure. Otherwise, perform the following tasks to bring the server back online:
    - **a** Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.
    - **b** Reinstall the server in the rack.
    - **c** Connect the cables and power cords.
    - **d** Power on the server. See Powering On the Server on page 77

8.20

Replacing Fan Modules in T4-1 Servers

CAUTION: You will perform actions in an area that contains live voltages. Avoid contact with cable terminals or other electrified surfaces.

Procedure:

1. Check the front or rear panel System Fault LED.

   A fan fault will cause the System Fault LED (on front and rear of server) as well as a Fan Fault LED in the array of fan status LEDs to be lighted.

2. Extend the server to the maintenance position. Perform the following actions:
   a. Optional: Use the `set /SYS/LOCATE` command from the -> prompt to locate the system that requires maintenance.
   b. Make sure that no cables will be damaged or will interfere when the server is extended.
   c. From the front of the server, release the two slide release latches.
   d. While squeezing the slide release latches, slowly pull the server forward until the slide rails latch.
3. Release the two fan compartment door latches and swing the door open.
4. Check which fan module or modules have an amber LED, as they need to be replaced.
5. To remove a fan module, grasp the pull tab, pull the module toward the front of the system, and then lift it up and out of the fan module compartment.
6. Check to be certain adjacent fan modules are still fully seated pressing down on the top of the neighboring fan modules.
7. Align the connector pins on the base of the new fan module with the connector on the fan module board and lower the module straight down into the slot.
8. Press down on the top of the module until it is fully seated.
9. Verify that the new fan is functioning. Check status LEDs.
10. Return the server to its operational position in the rack.

8.21

Replacing FB-DIMM Fans in T5220 Servers

The FB-DIMM fan is a single fan for cooling FB-DIMMs. The FB-DIMM fan assembly is labeled FT2.

Procedure:

1. To prepare the server for FB-DIMM fan removal, perform the following actions:
   a. Power off the server, see Powering Off the Server on page 89.
   b. Make a note of the location of the cables and power cords, and then unplug all connections.
   c. Remove the server from the rack.
   d. Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.
2. Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.
3. Pull the tag labeled FT2 and remove the FB-DIMM fan assembly.
4. Set the FB-DIMM fan assembly aside on an antistatic mat.

5 If you removed the fan assembly as part of a different procedure, return to that procedure. Otherwise, continue to the next step to install the new FB-DIMM fan.

6 Remove the replacement FB-DIMM fan assembly from its packaging and place it on an antistatic mat.

7 Reinsert the FB-DIMM fan assembly in the slot with the airflow direction arrow facing the rear of the server.

8 Slide the FB-DIMM fan assembly in the slot until fully seated.

9 To install the top cover of the server, perform the following actions::

   a Place the top cover on the chassis. Set the cover down so that it hangs over the rear of the server by about an inch (25 mm).

   b Carefully align the front of the top cover with the black line (with arrows) printed on top of the media bay assembly.

   c Slide the cover forward until it latches into place.

10 If you installed the fan assembly as part of a different procedure, return to that procedure. Otherwise, perform the following tasks to bring the server back online:

   a Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.

   b Reinstall the server in the rack.

   c Connect the cables and power cords.

   d Power on the server. See Powering On the Server on page 77.

8.22 Replacing the Hard Drive Fan Assembly in T5220 Servers

The Hard Drive Fan Assembly provides supplemental cooling of the hard drives and the optical media drive. The hard drive fan assembly is labeled FT1.

Procedure:

1 To prepare the server for hard drive fan removal, perform the following actions:

   a Power off the server, see Powering Off the Server on page 89.

   b Make a note of the location of the cables and power cords, and then unplug all connections.

   c Remove the server from the rack.

   d Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.

2 Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.

3 Disconnect the hard drive fan assembly cable from the power board connector.

4 Carefully lift the hard drive fan assembly cable from the cable guides.

5 Push the release button on the hard drive fan bracket, and pivot the bracket backwards.

6 Slide the bracket forward and lift out the hard drive fan assembly.

7 Set the hard drive fan assembly aside on an antistatic mat. Continue to the next step to install the new hard drive fan assembly.

8 Remove the replacement hard drive fan assembly from its packaging and place it on an antistatic mat.

9 Lower the hard drive fan assembly, and slide the hard drive fan bracket back so that the tabs enter the slots.

10 Pivot the hard drive fan bracket towards the rear of the server until it clicks.

11 Connect the hard drive fan assembly cable to the power board.

12 Route the hard drive fan assembly cable back into the cable guides.

13 To install the top cover of the server, perform the following actions:

- **a** Place the top cover on the chassis. Set the cover down so that it hangs over the rear of the server by about an inch (25 mm).
- **b** Carefully align the front of the top cover with the black line (with arrows) printed on top of the media bay assembly.
- **c** Slide the cover forward until it latches into place.

14 To bring the server back online, perform the following actions:

- **a** Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.
- **b** Reinstall the server in the rack.
- **c** Connect the cables and power cords.
- **d** Power on the server. See Powering On the Server on page 77.

8.23 Replacing Batteries T5220 Servers

The server uses one lithium battery, which is installed in the Service Processor Board.

Procedure:

1 To prepare the server for battery removal, perform the following actions:

- **a** Power off the server, see Powering Off the Server on page 89.
- **b** Make a note of the location of the cables and power cords, and then unplug all connections.
- **c** Remove the server from the rack.
- **a** Ensure that the server is properly grounded, as described in Avoiding Electrostatic Discharge on page 124.

2 Remove the server cover, using a cross tip screwdriver to press the top cover release button located near the front of the cover. Slide the cover towards the rear of the server. Lift the cover off the chassis and set it aside.

3 To remove the PCI mezzanine, perform the following actions:

- **a** Disconnect any I/0 cables from the rear of the PCI mezzanine.
- **b** Disconnect the PCI mezzanine cable.
- **c** Use a cross tip screwdriver to loosen the four green captive screws securing the PCI mezzanine.
- **d** Lift the PCI mezzanine up and out.
- **e** Lift the PCI mezzanine away from the chassis and place it on an antistatic mat.

4 Pry the battery out of the service processor board, using a small flat-blade screwdriver.

5 Set the battery aside on an antistatic mat. Continue to the next step to install the new battery.

6 Remove the replacement battery from its packaging.

7 Press the new battery in with the "+" side facing up.

8 To install the PCI mezzanine, perform the following actions:
   a Position the PCI mezzanine onto the chassis.
   b Lower the PCI mezzanine and slide it toward the front of the server.
   c Use a cross tip screwdriver to tighten the four green captive screws securing the PCI mezzanine.
   d Reconnect the PCI mezzanine cable.
9 To install the top cover of the server, perform the following actions:
   a Place the top cover on the chassis. Set the cover down so that it hangs over the rear of the server by about an inch (25 mm).
   b Carefully align the front of the top cover with the black line (with arrows) printed on top of the media bay assembly.
   c Slide the cover forward until it latches into place.
10 To bring the server back online, perform the following actions:
   a Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.
   b Reinstall the server in the rack.
   c Connect the cables and power cords.
   d Power on the server. See Powering On the Server on page 77.

8.24
Replacing Batteries in T4-1 Servers

CAUTION: This procedure exposes sensitive components to electrostatic discharge.

Procedure:

1 To prepare the server for battery removal, perform the following actions:
   a Power off the server, see Powering Off the Server on page 89.
   b Make a note of the location of the cables and power cords, and then unplug all connections.
   c Remove the server from the rack.
   d Ensure that the server is properly grounded as described in Avoiding Electrostatic Discharge on page 124.
2 Remove the top cover.
3 Remove riser 0 leftmost riser as viewed from the rear of the server).
4 Push the top edge of the battery against the spring and lift it out of the carrier.
5 Insert the new battery into the battery carrier with the negative side (-) facing out.
6 Replace the top cover.
7 To bring back the server online, perform the following actions:
   a Remove the antistatic measures. See Avoiding Electrostatic Discharge on page 124.
   b Reinstall the server in the rack.
   c Connect the cables and power cords.
   d Power on the server. See Powering On the Server on page 77.
8 To set the day and time using the Oracle ILOM, enter: `clock`
9 To check the status of the system battery, enter: `show /SYS/MB/BAT`

```
fault_state = OK
```

8.25 Replacing a Server

When and where to use: Replace the server if it is not serviceable by FRUs or replacement parts.

Procedure:

1. Power off the server, as described in Powering Off the Server on page 89. Make a note of the location of the cables and power cords, and then unplug all connections.
2. Remove the server from the rack.
3. Unpack the replacement server, and then inspect it to ensure that it is in good condition.
4. Replace the server in the rack.
5. Replace the cables and power cords.
6. Power on the server, as described in Powering On the Server on page 77.
7. If a full installation of the Generic Application Server is required, see Preparing a Server for Service on page 124 for the process.

8.26 Hardware Disposal

When equipment, batteries, or scrap materials are no longer needed, secure the items in a cool, dry place, or dispose of the items according to your company standards and local ordinances.

This page intentionally left blank.

Chapter 9

Generic Application Server Reference

This chapter contains supplemental reference information relating to the server hardware and the Generic Application Server.

Only the ISSI.1 Network Gateway is certified for the Solaris/GAS server platform, while other server applications, such as the ZC, UCS/PM, FMS, PDG, AuC, BAR, vCenter Appliance, SSS, ATR, ZSS, Syslog, GMC, InfoVista, CSMS, are commonly hosted on Virtual Management Servers.

9.1 T5220 Server Specifications

The Sun Netra T5220 server is the physical hardware where the Generic Application Server software resides.

Table 39: Server General Specifications – T5220 Server

Component	Specification
CPUs and Memory	One UltraSPARC T2 multicore processor, two 300 GB hard drives, 32 GB RAM, Processor: 1 CPU, four cores per CPU, eight threads per core, 1.2 GB speed.
Operating System	Solaris 2.10
Input Power Requirements	AC: 100 VAC to 240 VAC single phase, 47-63 Hz
Physical Characteristics	• Height: 87.4 mm (3.44 in.), two rack unit (RU) • Width: 425.5 mm (16.75 in.) excluding bezel, 442 mm (17.4 in.) including bezel • Depth: 502 mm (20 in.) to rear connectors; 525 mm (20.67 in.) overall maximum depth (including power supply)
Enclosure	Fits into a standard 19-in. wide rack (19-in. 4-post rack kit is included) or a cabinet.
Operating Temperature	5 °C (41 °F) to 40 °C (104 °F)
Non-operating Temperature	-40 °C (-40 °F) to 70 °C (158 °F)
Operating Altitude	Up to 3000 m (9840 ft)
Non-operating Altitude	Up to 12,000 m (39,370 ft)
Operating Humidity	10% to 90% relative humidity, non-condensing
Non-operating Humidity	Up to 93% relative humidity, non-condensing, 38 °C (100.4 °F) maximum wet bulb
Operating and Idling Acoustic Noise	7.7 B (LWAd (1 B=10 dB)) operating and 7.2 B idling, in accordance with ISO 9296 standards
Weight	15.81 kg (34.78 lbs) for two HDD configuration

Table continued…

Component	Specification
Standards	FCC and CE

9.2 T4-1 Server Specifications

The Oracle SPARC T4-1 server is the physical hardware where the Generic Application Server software resides.

Table 40: T4-1 Server General Specifications

Component	Specification
CPUs and Memory	One T4 2.85 Ghz multicore processor Sixteen DDR3 DIMM memory slots supporting 4, 8, or 16 GB modules
Operating System	Oracle® Solaris 10
Input Power Requirements Two hot-swappable power supplies	Power Supply Unit 1: 100 to 120 VAC, 50/60 Hz Power Supply Unit 2: 200 to 240 VAC, 50–60 Hz
Physical Characteristics	• Height: 88.6 mm (3.49 in.) two rack units • Width: 425.5 mm (16.75 in.) • Depth: 714.5 mm (28.13 in.) • Weight: 27.2 kg (60 lb), with two power supplies and 8 HDDs, but without PCI cards and rackmount hardware
Enclosure	4-post rack (mountinf at both front and rear). 2-post racks are not compatible.
Operating Temperature	5 °C (41 °F) to 35 °C (95 °F)
Non-operating Temperature	-40 °C (-40 °F) to 65 °C (149 °F)
Operating Altitude	Up to 3 000 m (9840 ft.)
Non-operating Altitude	Up to 12 000 m (40 000 ft.)
Operating vibration	5.15 G (vertical), 0.10 G (horizontal), 5 – 500 Hz, swept-sine
Non-operating vibration	0.5 G (vertical), 0.25 G (horizontal), 5 – 500 Hz, swept-sine
Operating shock	3.0 G, 11 ms, half-sine
Non-operating shock	• Roll-off: 1-inch roll-off free fall, front to back rolling directions • Threshold: 25 mm threshold height at 0.75 m/s impact velocity
Standards	ANSI/EIA 310-D-1992 or IEC 60927

9.3 Server Connector Pinouts

This section provides pinout information for the following ports on the server:

- Ethernet ports
- Serial management port

The Network Management, USB, Alarm, and Serial (IOIOI) ports are not used and pinouts are not included.

9.3.1
Ethernet Port – Pinouts

The server has four Ethernet system domain ports. All four Ethernet ports use a standard RJ-45 connector.

Table 41: Ethernet Connection Transfer Rates

Connection Type	IEEE Terminology	Transfer Rate
Ethernet	10BASE-T	10 Mbps
Fast Ethernet	100BASE-TX	100 Mbps
Gigabit Ethernet	1000BASE-T	1000 Mbps

The pin numbering of each of the ports is 1-8, from the rightmost pin to the left.

Table 42: Gigabit Ethernet Port Pin Signals

Pin	Signal Description
1	Transmit/Receive Data 0+
2	Transmit/Receive Data 0–
3	Transmit/Receive Data 1+
4	Transmit/Receive Data 2+
5	Transmit/Receive Data 2–
6	Transmit/Receive Data 1–
7	Transmit/Receive Data 3+
8	Transmit/Receive Data 3–

9.3.2
Serial Management Port – Pinouts

The serial management connector (labeled SER MGT) is an RJ-45 connector accessible from the rear panel. This port is the default connection to the system and should be used only for server management. The pin numbering of the port is one to eight (1-8), from the leftmost pin to the right. The default serial connection settings for this port are:

- Rate: 9600 baud
- Parity: none
- Stop bits: 1 (one)

- Data bits: 8 (eight)

Table 43: Serial Management Port Pin Signals

Pin	Signal Description
1	Request to Send (RTS)
2	Data Terminal Ready (DTR)
3	Transmit Data (TXD)
4	Ground
5	Ground
6	Receive Data (RXD)
7	Data Set Ready (DSR)
8	Clear to Send (CTS)

If you require connecting to the SER MGT port using a cable with either a DB-9 or a DB-25 connector, you can use an RJ45 to DB-9 adapter or RJ45 to DB-25 adapter to perform the crossovers given for each connector. Tables below describe how the adapters are wired.

Table 44: RJ45 to DB-9 Adapter Crossovers

Serial Port (RJ45 Connector)		DB-9 Adapter	
Pin	Signal Description	Pin	Signal Description
1	RTS	8	CTS
2	DTR	6	DSR
3	TXD	2	RXD
4	Signal Ground	5	Signal Ground
5	Signal Ground	5	Signal Ground
6	RXD	3	TXD
7	DSR	4	DTR
8	CTS	7	RTS

Table 45: RJ45 to DB-25 Adapter Crossovers

Serial Port (RJ45 Connector)		DB-9 Adapter	
Pin	Signal Description	Pin	Signal Description
1	RTS	5	CTS
2	DTR	6	DSR
3	TXD	3	RXD
4	Signal Ground	7	Signal Ground
5	Signal Ground	7	Signal Ground
6	RXD	2	TXD
7	DSR	20	DTR

Table continued…

Serial Port (RJ45 Connector)		DB-9 Adapter	
Pin	Signal Description	Pin	Signal Description
8	CTS	4	RTS

9.4 Administration Menus and Submenus

Generic Application Server functions are accessed from its administration menu. This section contains the complete menu hierarchy. The administration menu is accessed using the Generic Application Server administrator or manager accounts.

9.4.1 Executing a Menu Option from the Administrative Menu

The menu options you can execute are based on the specific role that you have been assigned in the system. If some of the options do not match your role, they are marked with an asterisk (*).

Prerequisites: For information about setting up Active Directory users so that they can perform specific administration menu procedures, see the Appendix in the *Authentication Services Feature Guide*, and contact your Active Directory administrator.

Procedure:

1. Choose a desired option to execute from Table 46: Administrative Menu Structure — Generic Application Server on page 146, and then, going up towards the entry in Menu column, identify the submenus names in all applicable submenu **(level 5)**, **(level 4)**, **(level 3)**, **(level 2)**, and **Menu** columns.

   An asterisk (*) in front of a corresponding number for ***<DESIRED MENU OPTION>*** indicates insufficient permissions.

2. Log on to a server with the available option to execute, using your Active Directory account. See Logging On to the Generic Application Server on page 85.

3. Type the corresponding number for ***<DESIRED MENU OPTION>*** in the **Menu** column, as identified in the first step. Press ENTER.

If…	Then…
If *<DESIRED MENU OPTION>* is a command identified to execute in the first step,	the ***<DESIRED MENU OPTION>*** is executed. Go to the next step.
If *<DESIRED MENU OPTION>* is a submenu,	the ***<DESIRED MENU OPTION>*** menu appears. Repeat the current steps for the **(level 2)** submenu, and thereafter for all subsequent lower-level submenus, as noted in the first step.
If the user does not have sufficient permissions,	the following message appears: `Insufficient Privileges for: <DESIRED MENU OPTION>.` Log off, contact your Network Administrator for required permissions, and start again from the first step.

4. Continue with another procedure that requires the same credentials or log off from the server application. If needed, see Logging Off the Terminal Server on page 84.

9.4.2
Administrative Menu Structure for the Generic Application Server

To invoke the menu, enter: `admin_menu`

Table 46: Administrative Menu Structure — Generic Application Server

Menu	(level 2)	(level 3)	(level 4)	(level 5)	Submenus and Options
Software Administration					
	Load Software				
		Load OS Patches			
	Install Software				
		Install OS Patches Patches must have already been loaded.			
	Eject CD/DVD				
	Reboot Server				
OS Administration					
	Manage Platform Configuration				
		Set Time Zone Only the GAS can change the time zone.			
	Security Provisioning				
		Manage SNMP Passphrases			
			Configure Agent SNMPv3		
		Manage SSH Keys			
			Verify SSH Connectivity		
			Detect Default SSH Key Usage		
	Get Log Files Gather up log files into a single zipped archive and put it in the /var/getlogs directory.				
		Get Server Log Files			
		Get Kernel Audit Files			
		Get Core Files			
		Get All Files			
	Display Logs (View Logs after selecting) Generates selectable lists of available logfiles to view.				
		Authentication Log Files			
		Cron Log Files			
		Device Messages Log Files			
		Install Log Files			
		Login Log Files			

Table continued…

Menu	(level 2)	(level 3)	(level 4)	(level 5)	Submenus and Options
		Patching Log Files			
		SNMP Log Files			
		System Log Files			
		Services: Application Log Files			
		Services: Network Log Files			
		Services: Site Log Files			
		Services: System [A-L] Log Files			
		Services: System [M-Z] Log Files			
		Services: Other Log Files			
	Reboot Server				
	Shutdown				
Services Administration					
	Manage AAA Client Configuration				
		Join Domain			
		Join All to Domain			
		Display Domain Membership Status			
	Manage BAR Client Configuration				
		Register Client			
		Get Host & User Keys			
		Verify SSH Keys			
		Reset BAR Client			
	Manage Syslog Client Configuration				
		Add Centralized Logging Server			
		Remove Centralized Logging Server			
		Display Centralized Logging Status			
	Manage NTP Server Configuration				
		Enable Hosting of NTP			
		Disable Hosting of NTP			
		Display NTP Status			
	Manage NTP Client Configuration				
		Add External NTP Time Source			
		Remove External NTP Time Source			
		Display NTP Status			
Backup and Restore Administration					

Table continued…

Menu	(level 2)	(level 3)	(level 4)	(level 5)	Submenus and Options
	Backup Administration				
		Backup All Critical Data			
		Backup Data to Persistent Storage			
	Restore Administration				
		Restore All Critical Data			
		Restore All Critical Data Except SSH			
		Restore SSH Keys and Configuration			
Application Administration					
	Load Container Server Software				
	Install Container				
	Uninstall Container				
	Display Container Status				
	Manage Persistent Storage				
		Load Persistent Storage from Network			
		Persistent Storage Removal			
		Display Application Data Summary			
	Manage Scalable Resources Manage the system resources on the GAS for the server application containers.				
		Balance Resources			
		Display Resources Summary			
	Eject CD/DVD				

Chapter 10

Disaster Recovery

This chapter provides references and information enabling you to recover a Generic Application Server in the event of a failure.

10.1 Recovering Solaris Servers

Process:

1. Recover the Solaris Servers. See Recovering Solaris Servers on page 149.
2. Complete the recovery of the Solaris Servers. See Completing the Recovery of the Solaris Servers on page 150.

10.1.1 Recovering the Solaris Server Hardware

Process:

1. Check the label on the front of the server to identify which Solaris server failed and the application software required.
2. If MAC Port Lockdown is enabled, unlock the HP Switch Port corresponding to the failed server. See “Unlocking/Locking HP Switch Ports When Replacing Connected Devices” in the *MAC Port Lockdown Feature Guide*. Complete the steps related to disabling the MAC Port Lockdown.
3. Install the server hardware and cables.

   See the following in the *Generic Application Server Feature Guide*:

   - “Hardware Installation and Parts Overview”
   - “Cable Connections”
4. Install the Generic Application Server Firmware and Software. See the following procedures in the *Generic Application Server Feature Guide*:

   - “Preparing for the Generic Application Server Installation”
   - “Installing the System Firmware”
   - “Installing the Generic Application Server”
   - “Configuring the Time Zone”
   - “Setting the Local Date and Time”
5. Delete the GAS and all ASTRO® 25 system applications that were installed on the GAS from the Domain Controller. See “Deleting a Computer Object from an Active Directory Domain” in the *Authentication Services Feature Guide*.
6. Join the GAS to the Active Directory Domain. See “Joining the Generic Application Server to the Domain” in the *Generic Application Server Feature Guide*.
7. Even if you have a *MOTOPATCH for Solaris 10 CD* with a `readme.txt` file containing MOTOPATCH installation instructions, refer instead to one of the following for MOTOPATCH installation instructions for devices running Solaris 10:

   - PTSS/SUS Extranet Site: https://compass.motorolasolutions.com/cgi/go/363341193

- Compass PatchTrack (Internal Motorola) http://compass.mot-solutions.com/go/354101592

8 Change the root default password. See “Changing the Root Account Password for a Solaris-Based Device” in the *Unix Supplemental Configuration Setup Guide*.

9 Change the ILOM password. See “Changing the Password for the ILOM Root Account” in the *Generic Application Server Feature Guide*.

10 Register the Backup/Recovery client on the Generic Application Server. See “Registering BAR Clients After SSH Configuration” in the *Backup and Restore Services Feature Guide*.

11 Restore backed-up data to the Generic Application Server. See Restoring the Generic Application Server from Persistent Storage on page 96.

12 After recovering necessary applications, continue with the Solaris Server Recovery. See Completing the Recovery of the Solaris Servers on page 150.

10.1.2
Completing the Recovery of the Solaris Servers

Process:

1 Join the Generic Application Server and all applications to the domain. See “Joining the Generic Application Server and All Installed Applications to the Domain” in the *Generic Application Server Feature Guide*.

2 Enable resource balancing on the Generic Application Server to distribute the remaining RAM and SWAP. See “Running Resource Balancing“ in the *Generic Application Server Feature Guide*.

3 **For systems with Centralized Event Logging:** Enable Centralized Event Logging for all applications and the Generic Application Server. See “Enabling Centralized Event Logging” in the *Generic Application Server Feature Guide*.

4 If required by your organization, perform supplemental configuration of the operating system. See Performing Supplemental Configuration of the Operating System on page 150.

5 If MAC Port Lockdown was enabled at the beginning of the device recovery, follow Verifying the New MAC Address Has Been Learned by the HP Switch and Re-Enabling the MAC Port Lockdown on page 151.

6 **For DSR systems only:** Ensure that the UNC in the primary core are enabled, and the backup UNC are disabled. For details on desired states in server applications, see the *Dynamic System Resilience Feature Guide*.

10.1.2.1
Performing Supplemental Configuration of the Operating System

This process is recommended only for maximum security organizations and is not the recommended configuration.

Process:

1 Set the EEPROM security mode and password. See “Changing EEPROM Security Mode Setting” in the *Unix Supplemental Configuration Setup Guide*.

2 Configure the EEPROM Banner. See “Setting or Change the EEPROM Banner on a Generic Application Server” in the *Unix Supplemental Configuration Setup Guide*.

3 Configure the login banner. See “Managing Banners on a Solaris-Based Device” section in the *Unix Supplemental Configuration Setup Guide*.

10.1.2.2

Verifying the New MAC Address Has Been Learned by the HP Switch and Re-Enabling the MAC Port Lockdown

Process:

1. Obtain the MAC address of the recovered Solaris server. It will be needed to verify that the HP Switch has learned the new MAC address before locking down the port again.
   a. Log on to the Generic Application Server as root. Stay at the # prompt and run the following command: `ifconfig -a`

      If needed, see "Logging On to the Generic Application Server" in the *Generic Application Server Feature Guide*.

   b. Locate the MAC address in the **ether** field that corresponds to e1000g0.
2. Enable MAC Port Lockdown. See "Unlocking/Locking HP Switch Ports When Replacing Connected Devices" in the *MAC Port Lockdown Feature Guide*. Complete the portion of the procedure to enable MAC Port Lockdown and validate that the MAC address on the switch port matches the MAC address from the previous step.

This page intentionally left blank.