Notice

The information contained in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF STRATUS TECHNOLOGIES, STRATUS MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE. Stratus Technologies assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document.

Software described in Stratus documents (a) is the property of Stratus Technologies Bermuda, Ltd. or the third party, (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

Stratus documentation describes all supported features of the user interfaces and the application programming interfaces (API) developed by Stratus. Any undocumented features of these interfaces are intended solely for use by Stratus personnel and are subject to change without warning.

This document is protected by copyright. All rights are reserved. No part of this document may be copied, reproduced, or translated, either mechanically or electronically, without the prior written consent of Stratus Technologies.

Stratus, the Stratus logo, ftServer, Continuum, Continuous Processing, StrataLINK, and StrataNET are registered trademarks of Stratus Technologies Bermuda, Ltd.


The registered trademark Linux is used pursuant to a sublicense from the Linux Mark Institute, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Red Hat, Red Hat Linux, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the United States and other countries. UNIX is a registered trademark of X/Open Company, Ltd., in the U.S.A. and other countries.

All other trademarks are the property of their respective owners.

Manual Name: Stratus ftServer System Administrator’s Guide for the Linux Operating System
Part Number: R003L
Revision Number: 09
Software Release Number: ftServer System Software for the Linux Operating System, Release 7.0.4
Publication Date: December 2009

Stratus Technologies, Inc.
111 Powdermill Road
Maynard, Massachusetts 01754-3409

© 2009 Stratus Technologies Bermuda, Ltd. All rights reserved.
## Contents

### Preface

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>xi</td>
</tr>
</tbody>
</table>

### 1. Introduction to ftServer System Administration

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of System and Network Administration</td>
<td>1-2</td>
</tr>
<tr>
<td>ftServer System Terminology</td>
<td>1-2</td>
</tr>
<tr>
<td>Managing Data Storage Devices</td>
<td>1-2</td>
</tr>
<tr>
<td>Using Stratus Fault-Tolerant Tools and Software</td>
<td>1-3</td>
</tr>
<tr>
<td>Managing the System With SNMP</td>
<td>1-3</td>
</tr>
<tr>
<td>Managing Virtual Technician Modules (VTMs)</td>
<td>1-3</td>
</tr>
<tr>
<td>Troubleshooting ftServer Systems</td>
<td>1-4</td>
</tr>
<tr>
<td>Unsupported Linux Tools</td>
<td>1-4</td>
</tr>
<tr>
<td>System Documentation</td>
<td>1-4</td>
</tr>
<tr>
<td>Additional Documentation and Resources</td>
<td>1-5</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>1-5</td>
</tr>
<tr>
<td>Stratus ftServer System Documentation</td>
<td>1-5</td>
</tr>
<tr>
<td>Acronyms and Terms</td>
<td>1-5</td>
</tr>
</tbody>
</table>

### 2. Configuring the ftServer System

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Internal Disk Storage</td>
<td>2-1</td>
</tr>
<tr>
<td>Internal Disk Naming</td>
<td>2-2</td>
</tr>
<tr>
<td>Internal Disk Storage Restrictions</td>
<td>2-4</td>
</tr>
<tr>
<td>The Console Log and the <code>/var/log/messages</code> File</td>
<td>2-4</td>
</tr>
<tr>
<td>Managing Partitions</td>
<td>2-5</td>
</tr>
<tr>
<td>Enabling Write Caching</td>
<td>2-7</td>
</tr>
<tr>
<td>Default Internal Disk Configuration for a Newly-Installed System</td>
<td>2-7</td>
</tr>
<tr>
<td>Setting Up RAID Arrays on Internal Disks</td>
<td>2-9</td>
</tr>
<tr>
<td>RAID Array Overview</td>
<td>2-9</td>
</tr>
<tr>
<td>Creating a RAID-1 Array</td>
<td>2-9</td>
</tr>
<tr>
<td>Creating a RAID-0 Array</td>
<td>2-10</td>
</tr>
<tr>
<td>Adding Running RAID Arrays to the <code>/etc/mdadm.conf</code> File</td>
<td>2-11</td>
</tr>
</tbody>
</table>
### Contents

**3. Managing Data Storage Devices**  
Removing and Replacing Internal Disks  3-1  
ftSSS Management of Failed Disks  3-2  
Replacing a Failed Disk (Automatic Method)  3-3  
Configuring Safe Mode  3-4  
Speeding Up the Rate of Resynchronization  3-5  
Replacing a Failed Disk With a Used Disk  3-5  
Replacing a Failed Disk (Manual Method)  3-7  
Stopping a RAID Array and Moving It to Another System  3-10  
Periodically Checking Disks  3-10  
Using LVM  3-10  
Using ftScalable Storage Systems  3-10  
Planning for System Backups and Disaster Recoveries  3-11  
Using Device Names for the DVD Drive  3-11  
Using SAS Tape Drives  3-11  
Using USB Storage Devices  3-12  
  - USB Support in ftSSS  3-12  
  - USB Storage Devices  3-13  
  - USB Solid-State Devices  3-14  
Additional Resources  3-14

---

**4. Using ftServer Fault-Tolerant Utilities and Software**  
Using the **ftsmaint** Command  4-1  
  - **ftsmaint** Command Arguments  4-1  
  - **ftsmaint** Examples  4-7
## Contents

Displaying System Status  | 4-7
---|---
State (State) and Operation State (OP State) Values  | 4-10
Displaying the Status of a Single System Component  | 4-10
Displaying System Status  | 4-11
Bringing System Components Down and Up  | 4-12
Managing ASN Support  | 4-12
Managing Kernel Memory Dump Files  | 4-14

<table>
<thead>
<tr>
<th>5. Simple Network Management Using Net-SNMP and ftISNMP</th>
<th>5-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing and Configuring ftISNMP</td>
<td>5-1</td>
</tr>
<tr>
<td>ftISNMP Distribution</td>
<td>5-2</td>
</tr>
<tr>
<td>Configuring ftISNMP</td>
<td>5-3</td>
</tr>
<tr>
<td>The <code>snmpd.conf</code> File</td>
<td>5-3</td>
</tr>
<tr>
<td>The <code>ftlsubagent.conf</code> and <code>ftltrapsubagent.conf</code> Files</td>
<td>5-4</td>
</tr>
<tr>
<td>Configuring SNMP to Start at System Initialization</td>
<td>5-4</td>
</tr>
<tr>
<td>Configuring SNMP for Service Management</td>
<td>5-4</td>
</tr>
<tr>
<td>SNMP Foundations and Concepts</td>
<td>5-6</td>
</tr>
<tr>
<td>ftISNMP Management Commands</td>
<td>5-6</td>
</tr>
<tr>
<td>The Basic Net-SNMP Commands</td>
<td>5-7</td>
</tr>
<tr>
<td>MIBs</td>
<td>5-9</td>
</tr>
<tr>
<td>Some Objects Defined by Standard MIBs</td>
<td>5-10</td>
</tr>
<tr>
<td>SNMPv3 Support</td>
<td>5-11</td>
</tr>
<tr>
<td>SNMP’s View of a Network</td>
<td>5-11</td>
</tr>
<tr>
<td>Extensions and Fault-Tolerant SNMP Operation</td>
<td>5-12</td>
</tr>
<tr>
<td>Installing Remote Network Management Services</td>
<td>5-13</td>
</tr>
<tr>
<td>Configuring SNMP for Remote Service Management</td>
<td>5-14</td>
</tr>
<tr>
<td>Deploying SNMP Agents and Subagents</td>
<td>5-14</td>
</tr>
<tr>
<td>Verifying Traps</td>
<td>5-15</td>
</tr>
<tr>
<td>Managing SNMP</td>
<td>5-16</td>
</tr>
<tr>
<td>Customizing the SNMP Configuration</td>
<td>5-16</td>
</tr>
<tr>
<td>Testing Your SNMP Configuration</td>
<td>5-17</td>
</tr>
<tr>
<td>Managing ftServer Hardware Components</td>
<td>5-18</td>
</tr>
<tr>
<td>SNMP and MIBS</td>
<td>5-22</td>
</tr>
<tr>
<td>SNMP Network Management Station Considerations</td>
<td>5-22</td>
</tr>
<tr>
<td>Initial SNMP Testing</td>
<td>5-23</td>
</tr>
<tr>
<td>Initial Testing of <code>ftltrapsubagent</code></td>
<td>5-23</td>
</tr>
<tr>
<td>Initial Testing of <code>ftlsubagent</code></td>
<td>5-25</td>
</tr>
<tr>
<td>GET and SET Operations for ftISNMP MIB Objects</td>
<td>5-25</td>
</tr>
<tr>
<td>SRA-ftLinux-MIB OID Values and Properties</td>
<td>5-26</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>Trap Filtering</td>
<td>5-26</td>
</tr>
<tr>
<td>Trap-Filtering Capability</td>
<td>5-26</td>
</tr>
<tr>
<td>Activating and Deactivating Trap Filtering</td>
<td>5-27</td>
</tr>
<tr>
<td>Trap-Filtering Examples</td>
<td>5-27</td>
</tr>
<tr>
<td>Removing ftISNMP</td>
<td>5-36</td>
</tr>
</tbody>
</table>

### 6. Troubleshooting ftServer Systems

- **LEDs and Visual Diagnostics**
- **System Boot Problems**
  - Normal Boot Sequence
  - Possible Boot Problems
    - Missing Stratus Drivers Prevent Booting
    - Problem with the *grub* Boot Loader
    - RAID Problem
    - Automatic Reboot After Boot Monitoring Timeout
- **Problems with the VTM**
- **System Log Messages**
  - Error and Log Messages Regarding Keyboard and Mouse
- **Emulex BIOS Settings**
- **ftServer Setup BIOS Boot Settings**

### Appendix A. ftServer System States and Operation States

- **Op State:State Values**
- **Op State:Reason Definitions**

### Index
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>udev Disk Names</td>
<td>2-3</td>
</tr>
<tr>
<td>2-2</td>
<td>ftServer Enclosures: Major Devices and Paths (Front View)</td>
<td>2-29</td>
</tr>
<tr>
<td>2-3</td>
<td>ftServer Enclosures: Major Devices and Paths (Rear View)</td>
<td>2-30</td>
</tr>
<tr>
<td>5-1</td>
<td>AgentX-Enabled Extensions and Subagents</td>
<td>5-15</td>
</tr>
<tr>
<td>A-1</td>
<td>Operational State Management of ftServer System Components</td>
<td>A-1</td>
</tr>
</tbody>
</table>
Tables

Table 1-1. ftServer System-Specific Documentation 1-5
Table 1-2. Acronyms Used 1-5
Table 2-1. Default System Disk Partitions 2-8
Table 2-2. Summary of Three Common Configurations of Disk Space 2-8
Table 2-3. Ethernet Devices in ftServer Systems 2-16
Table 2-4. Device Paths 2-28
Table 4-1. Managing ASN Services 4-14
Table 5-1. SNMP Configuration Tools 5-17
Table 5-2. Set Operations Currently Implemented in ftSNMP 5-25
Table A-1. Meaning of Duplex for ftServer System Components A-2
Table A-2. Codes and Op State:State Values A-2
Table A-3. Codes and Op State:Reason Values A-4
| Example 2-1. | The `/proc/mdstat` File | 2-13 |
| Example 2-2. | The `mdadm --detail --scan --verbose` Command | 2-13 |
| Example 2-3. | The `mdadm --detail /dev/mdx` Command | 2-14 |
| Example 2-4. | Default Configuration of Embedded Ethernet Devices | 2-18 |
| Example 2-5. | Bond that Uses Static IP Addressing | 2-22 |
| Example 2-6. | Bond that Uses DHCP | 2-22 |
| Example 2-7. | `/etc/crontab` Entries to Automatically Control CPU Resynchronization | 2-26 |
| Example 2-8. | Device Path and PCI Device ID in `ftsmaint ls` Output | 2-31 |
| Example 3-1. | Pairing a Spare Internal Disk with the Running System Disk | 3-6 |
| Example 3-2. | Running `grub` | 3-9 |
| Example 4-1. | Displaying System Status with the `ftsmaint ls` Command | 4-8 |
| Example 4-2. | Viewing the State of the Bottom I/O Element | 4-10 |
| Example 4-3. | Viewing the State of Disk `sda` | 4-11 |
| Example 4-4. | Viewing the State of the Modem LEDs | 4-11 |
| Example 5-1. | Bringing a CPU-I/O Enclosure Down and Back Up | 5-19 |
| Example 5-2. | Testing Ethernet Ports | 5-20 |
| Example 5-3. | Traps that Can Occur for I/O Element 10 When Trap Filtering Is Off | 5-28 |
| Example 5-4. | Traps That Can Occur for I/O Element 10 When Trap Filtering Is On | 5-32 |
| Example 5-5. | Traps That Can Occur When Trap Filtering Is Off | 5-34 |
| Example 5-6. | Traps That Can Occur When Trap Filtering Is On | 5-35 |
| Example 6-1. | Emulex BIOS Utility | 6-8 |
The *Stratus ftServer System Administrator’s Guide for the Linux Operating System* (R003L) documents tasks and information for administrators of ftServer 2600, 4500, and 6300 systems running a supported Linux distribution and ftServer System Software for the Linux Operating System (ftSSS).

This document is intended for you if you manage or troubleshoot these ftServer systems, or develop tools and scripts for use on these systems. You should have a background knowledge of Linux or UNIX® shells, tools, and systems, and TCP/IP network server and network administration technologies.

**Revision Information**

This document is a revision. It incorporates support for ftServer 2600, 4500, and 6300 systems. Numerous changes exist throughout the manual. Notable changes include the following:

- ftServer 2600, 4500, and 6300 systems support 16 internal disks.
- This revision provides information on resynchronization in the sections “Deferring CPU Resynchronization” on page 2-25 and “Disabling System Operation During CPU Resynchronization” on page 2-26.
- The section “Using the ftsmaint Command” on page 4-1 describes new and changed arguments of the `ftsmaint` command.
- Device paths have changed; see Table 2-4 as well as Figure 2-2 and Figure 2-3.
- Starting with ftServer 2600, 4500, and 6300 systems, VTM functionality is integrated into the baseboard management controller (BMC). Thus, information about the VTM throughout the manual has changed.
- Previous revisions of this manual included a chapter on the VTM. This information now appears in *Stratus ftServer System Software: Installation for Linux Systems* (R013L).
Notation Conventions

This document uses the notation conventions described in this section.

Warnings, Cautions, and Notes

Warnings, cautions, and notes provide special information and have the following meanings:

**WARNING**

A warning indicates a situation where failure to take or avoid a specified action could cause bodily harm or loss of life.

**CAUTION**

A caution indicates a situation where failure to take or avoid a specified action could damage a hardware device, program, system, or data.

**NOTE**

A note provides important information about the operation of an ftServer system.

Typographical Conventions

The following typographical conventions are used in this document:

- The italic font introduces or defines new terms. For example:
  
  ftServer systems use replicated, *fault-tolerant* hardware to eliminate single points of failure and protect data integrity

- The bold font emphasizes words in text. For example:

  Update the BIOS **before** you install or upgrade ftSSS.
• The monospace font represents text that would appear on your display screen. The monospace bold font represents text you must type in examples that contain both user input and system output. The monospace italic font represents terms in command lines that are to be replaced by literal values. For example:

To display the state of a CPU enclosure, type a command in the following format:

```
/opt/ft/bin/ftsmaint ls n
```

If you type `/opt/ft/bin/ftsmaint ls 0` at the prompt, the following output appears:

```
H/W Path : 0
Description : CPU Node Assembly
```

• The percent sign (%) and the number sign (#) are standard default prompt signs that have a specific meaning at a command prompt. Although a prompt is sometimes shown at the beginning of a command line as it would appear on the screen, you do not type it.

  – % indicates you are logged in to a user account and are subject to certain access limitations.
  – # indicates you are logged in to the system administrator account and have superuser access. Users of this account are referred to as root. The # prompt sign used in an example indicates the command can only be issued by root.

Syntax Notation

This document uses the following format conventions for documenting commands:

• Square brackets ([ ]) enclose command argument choices that are optional. For example:

  ```
cflow [-r] [-ix] [-i] [-d num] files
  ```

• The vertical bar (|) separates mutually exclusive arguments from which you choose one. For example, the following shows two mutually exclusive, but optional, arguments:

  ```
  command [arg1 | arg2]
  ```

The following example shows two mutually exclusive arguments, one of which is required:

  ```
  command arg1 | arg2
  ```

In either case, you may use either arg1 or arg2 when you type the command.
• Ellipses (...) indicate that you can specify the preceding argument as many times as you need to on a single command line. For example,

    command [arg1 arg2 arg3 ...]

**NOTE**

Dots, brackets, and braces are not literal characters; you should **not** type them. Any list or set of arguments can contain more than two elements. Brackets and braces are sometimes nested.

**Getting Help**

If you have a technical question about ftServer system hardware or software, try these online resources first:

- **Online documentation at the StrataDOC Web site.** Stratus provides complimentary access to StrataDOC, an online-documentation service that enables you to view, search, download, and print customer documentation. You can access StrataDOC at the following Web site:

  [http://stratadoc.stratus.com](http://stratadoc.stratus.com)

  A copy of the StrataDOC CD-ROM for your system is included with this release. To order additional copies of the StrataDOC CD-ROM or to obtain copies of printed manuals, do one of the following:

  – If you are in North America, call the Stratus Customer Assistance Center (CAC) at (800) 221-6588 or (800) 828-8513, 24 hours a day, 7 days a week.
  
  – If you are located outside North America, contact your nearest Stratus sales office, CAC office, or distributor; for CAC phone numbers outside the U.S., see [http://www.stratus.com/support/cac/index.htm](http://www.stratus.com/support/cac/index.htm).

- **Online support from Stratus Customer Service.** You can find the latest technical information about an ftServer system through online product support at the Stratus Technical Support Web site:


- **Online product support for Red Hat® Linux® products.** Your primary source for support is the manufacturer who provided your software, or Red Hat Global Support Services. You can also find the latest technical information about Red Hat Enterprise and Standard Linux through online product support at the Red Hat Support Web site:

  [http://www.redhat.com/apps/support/]
If you are unable to resolve your questions with the help available at these online sites, and the ftServer system is covered by a service agreement, please contact the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative. For information about how to contact the CAC, see the http://www.stratus.com/support/cac/ Web site.

Commenting on the Documentation

To provide corrections and suggestions on the documentation, send your comments in one of the following ways:

- By clicking the site feedback link at the bottom of a Help topic. Information to identify the topic is supplied in the StrataDOC Web Site Feedback form.

- By email to Comments@stratus.com. If it is possible, please include specific information about the documentation on which you are commenting:
  - For a printed document or a document in PDF format, include the title and part number from the Notice page and the page numbers.
  - For online documentation, include the Help subject and topic title.

This information will assist Stratus Information Development in making any needed changes to the ftServer system documentation. Your assistance is most appreciated.
ftServer 2600, 4500, and 6300 systems running a supported Linux distribution together with ftServer System Software (ftSSS) for the Linux Operating System operate as fault-tolerant servers. Every ftServer system uses replicated, fault-tolerant hardware to eliminate single points of failure and protect data integrity in all areas of data handling.

The ActiveService® Network (ASN) is an optional remote-monitoring system managed by Stratus. ASN architecture built into ftServer systems supports fault-tolerant features with self-checking hardware and onboard diagnostics to detect, isolate, and report potential problems before they affect server operation.

**NOTE**

Installation of ftSSS and the Linux operating system is a bare-metal installation. You cannot install the fault-tolerant software in a guest operating system in a virtualized environment. ftSSS for the Linux Operating System supports neither Xen® nor KVM virtualization products. For virtualization on ftServer systems, install VMware® ESX™ and ftSSS for VMware vSphere™. For more information, see http://www.stratus.com/services/virtualization.htm.

This introduction to ftServer system administration contains the following topics:

- “Overview of System and Network Administration” on page 1-2
- “Unsupported Linux Tools” on page 1-4
- “System Documentation” on page 1-4
- “Additional Documentation and Resources” on page 1-5
- “Acronyms and Terms” on page 1-5
Overview of System and Network Administration

This section presents an overview of the following commonly performed system administrative tasks:

- “ftServer System Terminology”
- “Managing Data Storage Devices” on page 1-2
- “Using Stratus Fault-Tolerant Tools and Software” on page 1-3
- “Managing the System With SNMP” on page 1-3
- “Managing Virtual Technician Modules (VTMs)” on page 1-3
- “Troubleshooting ftServer Systems” on page 1-4

To perform most of the documented procedures, you need root or superuser privileges. The procedures do not always specify when you need to have root privileges.

ftServer System Terminology

Each ftServer system houses two CPU-I/O enclosures. Each CPU-I/O enclosure includes a CPU element and an I/O element, as follows:

- CPU element 0 and I/O element 10: The upper enclosure, also referred to as CPU-0, I/O-10.
- CPU element 1 and I/O element 11: The lower enclosure, also referred to as CPU-1, I/O-11.

NOTE

The terms upper and lower refer to the location of the enclosures in a rack-mounted system.

Managing Data Storage Devices

In addition to disk storage, your system supports DVD drives, tape drives, and USB storage devices. Chapter 3, “Managing Data Storage Devices,” provides a discussion of these devices and the information needed to manage them.
Using Stratus Fault-Tolerant Tools and Software

While you can use standard Linux tools to perform many system administration tasks on your ftServer systems, some tasks on fault-tolerant systems require specialized supporting utilities. In particular, ftSSS provides:

- The `/opt/ft/bin/ftsmaint` command interface (see “Using the ftsmaint Command” on page 4-1), which enables you to monitor and configure many aspects of system operation.
- The `/opt/ft/sbin/ft-bonding` command interface (see “Configuring Channel-Bonding Interfaces” on page 2-19), which enables you to configure Ethernet bonds.
- The `/opt/ft/sbin/VTMConfig` command interface (see Stratus ftServer System Software: Installation for Linux Systems (R013L)), which you use to configure VTM parameters that are not related to call-home and dial-up settings.

The VTMConfig command also allows you to configure settings for the ASN. (In previous releases, ASN settings were available only through the `/opt/ft/sbin/ASNConfig` command interface.) You can use VTMConfig to configure your server for support over the ASN and to modify VTM parameters related to ASN call-home and dial-up services. For additional information, see the Stratus ftServer System Software: Installation for Linux Systems (R013L).

Managing the System With SNMP

ftSSS includes optional utilities to allow remote support of your ftServer system. These include an extensible network administration framework and a server-monitoring utility that provides notification services. Chapter 5, “Simple Network Management Using Net-SNMP and ftlSNMP,” discusses the configuration and use of the optional ftlSNMP package implementing Simple Network Management Protocol (SNMP) for managing network objects. The ftlSNMP package is typically installed with ftSSS.

Managing Virtual Technician Modules (VTMs)

The Virtual Technician Module (VTM) console is a Web-based console that enables you, the CAC, or your authorized Stratus service representative to control, monitor, and diagnose the system. You can use the VTM console to control the host system even if the host system’s operating system is unresponsive and its network connections are lost. Stratus ftServer System Software: Installation for Linux Systems (R013L) discusses how to configure VTMs for remote access.

NOTE

Starting with ftServer 2600, 4500, and 6300 systems, VTM functionality is integrated into the baseboard management controller (BMC). In previous ftServer
system models, the VTM and BMC were separate hardware components.

Troubleshooting ftServer Systems

Problem identification, system and application diagnostics, and system configuration to resolve problems with ftServer systems are essential troubleshooting tasks. Chapter 6 discusses system features and procedures to assist you in troubleshooting ftServer systems.

Unsupported Linux Tools

CAUTION

Avoid using the Linux sysreport command, a script that collects information about system execution. The sysreport command makes the system operate in simplex mode by taking a component offline for some time, eliminating fault-tolerant operation before bringing the component back online.

CAUTION

Enabling and using the Sysrq tool causes system interruptions, because its use results in the suspension of kernel processes, which is interpreted by ftSSS as a system hang.

The Sysrq tool for writing commands to the /proc/sysrq-trigger file is not supported on ftServer systems. It is disabled by default.

System Documentation

The system documentation is available on the StrataDOC Web site and on a StrataDOC CD that was distributed with the system or ftSSS upgrade.

To view the documentation on the StrataDOC CD

1. Insert the StrataDOC CD in the DVD drive of a Linux system.
2. If necessary, mount the CD to /media/cdrecorder.
3. Double-click the index.htm file on the StrataDOC CD.

The documentation opens in a Web browser.
Additional Documentation and Resources

The following resources provide additional information that may be helpful to you in administering your ftServer system.

Red Hat Enterprise Linux

Documentation for the Red Hat Linux operating system is available at http://www.redhat.com/docs.

Stratus ftServer System Documentation

The StrataDOC media provided with your system contains the ftServer system documentation for systems that run the Linux operating system. This documentation is provided in Adobe Acrobat® Portable Document Format (PDF) and HTML format for viewing and printing.

This manual occasionally refers to other documentation that is specific to your particular ftServer system. Table 1-1 lists the system-specific documentation, all of which is available on the ftServer StrataDOC media.

Table 1-1. ftServer System-Specific Documentation

<table>
<thead>
<tr>
<th>Manual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stratus ftServer 2600, 4500, and 6300 Systems: Installation Guide</strong></td>
<td>Describes how to install and set up your ftServer 2600, 4500, and 6300 system hardware.</td>
</tr>
<tr>
<td><strong>Stratus ftServer 2600, 4500, and 6300 Systems: Operation and</strong></td>
<td>Documents how to operate, diagnose, and maintain your ftServer 2600, 4500, and 6300 system. It explains how to remove and replace the CRUs and how to interpret system operational status based on the state of the light-emitting diodes (LEDs).</td>
</tr>
<tr>
<td><strong>Maintenance Guide</strong> (R639)</td>
<td></td>
</tr>
</tbody>
</table>

Acronyms and Terms

Table 1-2 lists the acronyms and some terms used to describe tasks for administering ftServer systems.

Table 1-2. Acronyms Used (Page 1 of 2)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expanded Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN</td>
<td>ActiveService Network</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard management controller</td>
</tr>
<tr>
<td>CAC</td>
<td>Customer Assistance Center</td>
</tr>
</tbody>
</table>
Table 1-2. Acronyms Used (Page 2 of 2)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expanded Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRU</td>
<td>Customer-replaceable unit</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DIMM</td>
<td>Dual-inline memory module</td>
</tr>
<tr>
<td>Duplex</td>
<td>The state of a device in an ftServer system in which the device has a running and healthy partner. In this case, the device can be removed without interrupting system operation.</td>
</tr>
<tr>
<td>DST</td>
<td>Daylight saving time</td>
</tr>
<tr>
<td>EULA</td>
<td>End-user licensing agreement</td>
</tr>
<tr>
<td>ftsmaint</td>
<td>A command tool for managing your ftServer system's fault-tolerant functions.</td>
</tr>
<tr>
<td>ftSSS</td>
<td>ftServer System Software for the Linux Operating System</td>
</tr>
<tr>
<td>IPL</td>
<td>Initial Program Load</td>
</tr>
<tr>
<td>MIB</td>
<td>SNMP Management Information Base</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean time between failures</td>
</tr>
<tr>
<td>OSM</td>
<td>OpState Manager</td>
</tr>
<tr>
<td>SAS</td>
<td>Serial Attached SCSI</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial ATA</td>
</tr>
<tr>
<td>Simplex</td>
<td>The state of a device in an ftServer system in which the device does not have a running and healthy partner. In this case, you cannot remove the device without disrupting the system operation.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>VFAT</td>
<td>Virtual file allocation table</td>
</tr>
<tr>
<td>VTM</td>
<td>Virtual Technician Module</td>
</tr>
</tbody>
</table>
Chapter 2
Configuring the ftServer System

This chapter discusses the following topics:

- “Configuring Internal Disk Storage” on page 2-2
- “Setting Up RAID Arrays on Internal Disks” on page 2-9
- “Ethernet Devices” on page 2-15
- “Other System Configuration Information” on page 2-23
- “Additional Documentation and Resources” on page 2-31

At system startup, the operating system probes hardware for legacy devices and attached devices that are not already configured for use on the system. Often, the device is recognized and automatically supported, requiring no direct configuration.

While the operating system may recognize legacy devices, ftSSS does not support them as fault-tolerant devices. To be supported as a fault-tolerant device, a device must have a special hardened driver that supports surprise removal and fault management by ftSSS.

Some system components, such as data storage, may require additional configuration. The following sections discuss them, as well as some of the automated features of the ftServer system that support fault-tolerant operation and ease system administration.
Configuring Internal Disk Storage

The internal storage of your ftServer system supports Serial Attached SCSI (SAS) disks. For information on removing and inserting disks, see the operation and maintenance guide for your system, as listed in Table 1-1.

This section discusses the following topics:

- “Internal Disk Naming” on page 2-2
- “Internal Disk Storage Restrictions” on page 2-4
- “The Console Log and the /var/log/messages File” on page 2-4
- “Managing Partitions” on page 2-5
- “Enabling Write Caching” on page 2-7
- “Default Internal Disk Configuration for a Newly-Installed System” on page 2-7

Internal Disk Naming

Your ftServer system supports eight disks in each CPU-I/O enclosure, for a total of 16 disks in each system. The 16 internal storage disks are given static (persistent) user-device (udev) names based on their slot. This name is associated with the slot, not the disk.

You can use udev names with standard Linux commands; however, do not use udev names with ftsmaint. With ftsmaint, you use device paths. For information, see “Understanding Device Paths” on page 2-27.

In the upper CPU-I/O enclosure, the slots are, from left to right, top to bottom, as follows:

<table>
<thead>
<tr>
<th>/dev/sda</th>
<th>/dev/sdc</th>
<th>/dev/sde</th>
<th>/dev/sgd</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sdb</td>
<td>/dev/sdd</td>
<td>/dev/sdf</td>
<td>/dev/sdh</td>
</tr>
</tbody>
</table>

In the lower CPU-I/O enclosure, the slots are, from left to right, top to bottom, as follows:

<table>
<thead>
<tr>
<th>/dev/sdi</th>
<th>/dev/sdk</th>
<th>/dev/sdm</th>
<th>/dev/sdo</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sdj</td>
<td>/dev/sdl</td>
<td>/dev/sdn</td>
<td>/dev/sdp</td>
</tr>
</tbody>
</table>

Figure 2-1 shows the udev names for these disk slots in a fully-populated system. See also Figure 2-2 for the device paths that ftSSS associates with these slots.
NOTE

Because the *kernel* names for these devices are assigned on a first-come/first-served basis and are not persistent across disk swaps and reboots, determining which physical device a kernel name refers to can be difficult. Kernel names appear in the `/var/log/messages` and `/proc/mdstat` files. See your Red Hat Linux documentation for information about the `udevinfo` command, which translates between kernel names and *udev* names, static device naming, and *udev* naming in general.

The Linux operating system allows many possible configurations of these sixteen disks. To simplify administration and reduce confusion, this section presents recommended configurations in ftServer systems.

For fault tolerance, the disks are paired based on vertical grouping of the disks in the CPU-I/O enclosures; sda is paired with sdi, sdb with sdj, sdc with sdk, and so on. RAID-1 arrays are created by placing one mirror on each disk of the pair. For example, RAID array `/dev/md0` occupies `/dev/sda1` and `/dev/sdi1`, where `/dev/sda1` and `/dev/sdi1` are partitions within the disks `/dev/sda` and `/dev/sdi`, respectively.
Internal Disk Storage Restrictions

CAUTION

In the ftServer system internal disk slots, insert only hard drives provided by Stratus. Inserting any other type of device may cause data loss or system failure.

You may use any slots for any disks, with the following restrictions:

- If you are booting from an internal disk, you must install the system boot disk in the upper left-hand slot of the top enclosure (/dev/sda) and its mirror in the upper left-hand slot of the lower enclosure (/dev/sdi).
- Use RAID-1 to mirror the disks in one enclosure with the corresponding disks in the other enclosure for fault tolerance. (Do not mirror disks in the same internal storage enclosure.)

RAID-1 directs I/O flow to the appropriate disks in the two CPU-I/O enclosures. When a CPU-I/O enclosure (or a disk in it) is pulled, the RAID-1 mirrors are broken, the other CPU-I/O enclosure becomes simplex, and its disk status LED starts blinking yellow. (Pulling the CRU would cause all disk LEDs in the remaining CRU to blink yellow. Pulling one disk would cause only its partner's LED to blink yellow.) A blinking yellow LED indicates that the device is no longer safe to pull. For complete information on LEDs, see the operation and maintenance guide for your system, as listed in Table 1-1.

When a CRU is reinserted, the driver spins up the disks within that CRU, and ftSSS administratively adds the mirrors back into their RAID arrays. The other CRU remains simplex until all mirror synchronization completes.

The Console Log and the /var/log/messages File

The system console displays messages from the internal storage subsystem. This includes messages when disks are inserted and removed and when disk errors occur. The console messages are also in the system log (/var/log/messages). Tailing the messages file while configuring disks is very helpful.

```
# tail -f /var/log/messages
```

Since some disk-configuration operations produce considerable console output, it can be helpful to log on to another session.
Managing Partitions

You can use the `fdisk` or `sfdisk` utilities to display and change a disk’s partition table and geometry (see `fdisk(8)` and `sfdisk(8)` for details). During the Linux operating system installation, all of the mirrored boot partitions are created as type 0xfd (Linux RAID autodetect). After the installation, use the `fdisk` command to add data disks with the type 0x83 (Linux). Both disks of a RAID pair must have the same geometry, partition table, and type.

You can use the `fdisk` command to manage disk partitions. The following example uses the internal storage enclosure disk `sdb`.

**To display the partition table**

1. Type the `fdisk` command.

   ```bash
   # fdisk /dev/sdb
   ``

   The number of cylinders for this disk is set to 17849.
   There is nothing wrong with that, but this is larger than 1024, and could in certain setups cause problems with:
   1) software that runs at boot time (e.g., old versions of LILO)
   2) booting and partitioning software from other OSs (e.g., DOS FDISK, OS/2 FDISK)

   Command (m for help):

2. Type the `p` argument of the `fdisk` command.

   Command (m for help): `p`

   Disk /dev/sdb: 146.8 GB, 146815737856 bytes
   255 heads, 63 sectors/track, 17849 cylinders
   Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot Start End Blocks Id System
   /dev/sdb1 1 17849 143372061 83 Linux

   Command (m for help):

3. In this example, there is one partition, `sdb1`, that is 143,372,061K blocks long. Type the `q` command to quit, or continue with other commands, as required.

   The following example creates a new partition table and adds a primary partition, `sdb1`, of type 0xfd on `sdb`.

**To create a new partition table and add a partition**

1. If `fdisk` is not already running, type the `fdisk` command.

   ```bash
   # fdisk /dev/sdb
   ``

   The number of cylinders for this disk is set to 17849.
   There is nothing wrong with that, but this is larger than 1024, and could in certain setups cause problems with:

   (Continued on next page)
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
Command (m for help):

2. Type the o command to create a new empty DOS partition table. **Note the caution displayed by the command.**

Command (m for help): o
Building a new DOS disklabel. Changes will remain in memory only, until you decide to write them. After that, of course, the previous content won't be recoverable.

The number of cylinders for this disk is set to 17849.
There is nothing wrong with that, but this is larger than 1024, and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be corrected by write
Command (m for help):

3. Type the n command to add a new partition.

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)

4. Type e or p to specify the desired type.

   p
   Partition number (1-4):

5. Type the partition number you want to assign (the choices depend on the type specified).

   Partition number (1-4): 1
   First cylinder (1-8924, default 1):

6. Type the desired starting cylinder number for the partition, or press Enter to accept the default (this example accepts the default).

   Using default value 1
   Last cylinder or +size or +sizeM or +sizeK (1-8924, default 8924):
7. Type the desired last cylinder number for the partition, the size in megabytes or kilobytes, or press Enter to accept the default (this example accepts the default).

    Using default value 8924
    Command (m for help): 

8. Type the t command.

    Command (m for help): t
    Selected partition 1
    Hex code (type L to list codes):

9. Press Enter to accept the default ID (83). Type fd if you want the partition system ID to be Linux RAID autodetect.

    Hex code (type L to list codes): fd
    Changed system type of partition 1 to fd (Linux RAID autodetect)
    Command (m for help):

10. Type the w command to write the partition table to the disk and exit fdisk.

    Command (m for help): w

Enabling Write Caching

    You can enable write caching for internal disks. However, only do so if the system is protected by a UPS.

Default Internal Disk Configuration for a Newly-Installed System

    By default, the Linux operating system is installed on a RAID array that contains disks in slots 10/40/1 and 11/40/1. Before and during installation, these disks are named sda and sdb. After ftSSS is fully installed, these disks receive their persistent names, sda and sdi.

Table 2-1 describes the partitions on the system disks after the installation of the Linux operating system. The table assumes that the system disks reside in slots 10/40/1 and 11/40/1. Table 2-2 provides further information about approximate sizes of disks and mount points, based on installed physical memory.
### Table 2-1. Default System Disk Partitions

<table>
<thead>
<tr>
<th>Mount Points</th>
<th>Size</th>
<th>RAID Array</th>
<th>Mirrored Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>/boot</td>
<td>256 MB</td>
<td>/dev/md0</td>
<td>/dev/sda1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>/dev/sdi1</td>
</tr>
<tr>
<td>(swap)</td>
<td>12 GB</td>
<td>/dev/md1</td>
<td>/dev/sda2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>/dev/sdi2</td>
</tr>
<tr>
<td>/ (root)</td>
<td>12 to 32 GB (depending on disk size)</td>
<td>/dev/md2</td>
<td>/dev/sda3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>/dev/sdi3</td>
</tr>
</tbody>
</table>
| /var/crash   | /var/crash must be large enough to hold the entire contents of physical memory, so its size is dependent on the size of installed memory:  
- If installed memory is less than or equal to 32 GB, then the partition is 32 GB. If sufficient space is not available, the partition may shrink to accommodate the available space, but not to less than the amount of installed memory.  
- If installed memory is greater than 32 GB, up to 96 GB, then the partition is 96 GB.  
Allocation is adjusted by 3.25% for file system overhead. | /dev/md3 | /dev/sda5 |
|              |                       |              | /dev/sdi5           |

### Table 2-2. Summary of Three Common Configurations of Disk Space

<table>
<thead>
<tr>
<th>Mount Point/Disk Space</th>
<th>73 GB System Disk With Up To 32 GB Memory</th>
<th>146 GB System Disk With Up To 32 GB Memory</th>
<th>146 GB System Disk With More Than 32 GB Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total available disk space</td>
<td>68 GB</td>
<td>135 GB</td>
<td>135 GB</td>
</tr>
<tr>
<td>/boot</td>
<td>0.25 GB</td>
<td>0.25 GB</td>
<td>0.25 GB</td>
</tr>
<tr>
<td>(swap)</td>
<td>12 GB</td>
<td>12 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>/ (root)</td>
<td>22 GB</td>
<td>32 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>/var/crash</td>
<td>33 GB</td>
<td>33 GB</td>
<td>99 GB</td>
</tr>
<tr>
<td>Unused</td>
<td>0 GB</td>
<td>59 GB</td>
<td>0 GB</td>
</tr>
</tbody>
</table>
Setting Up RAID Arrays on Internal Disks

This section discusses the following topics related to creating RAID arrays for the internal disk drives:

- “RAID Array Overview” on page 2-9
- “Creating a RAID-1 Array” on page 2-9
- “Creating a RAID-0 Array” on page 2-10
- “Adding Running RAID Arrays to the /etc/mdadm.conf File” on page 2-11
- “Mounting a File System” on page 2-11
- “Checking the Current State of RAID” on page 2-12

RAID Array Overview

RAID is the basis for fault-tolerant file system availability. As disks come in and go out of service, the only way to keep the file system available is to mirror it on multiple disks, with a disk in each CPU-I/O enclosure.

All of the file systems are created on RAID devices. ftSSS supports RAID-1 (mirrored) and RAID-0 (striped) on RAID-1 on internal disks. You configure the RAID-0 array with RAID-1 devices, since the underlying devices must be fault tolerant.

The default format for device names for a RAID array consists of the letters md and a number from 0 through 128 (for example, /dev/md23). The number must be unique among the running RAID arrays. Device files are created for the first 128 RAID arrays. Use the mknod command (see mknod(1)) to create additional device files as needed. The number is the minor device number, and it is also used in the name.

The smaller numbers are used by the installer, so it is convenient to add new RAID arrays above 10. When RAID arrays are intended to be moved between systems, use numbers that are unique among all of the systems.

NOTE
To ensure fault-tolerant operation of your system, use only the mdadm command to create RAID arrays and only use device names of the default format.

Creating a RAID-1 Array

1. Select a pair of same-sized disks and insert them into two corresponding slots in different CPU-I/O enclosures. This example uses the disk in the left-most slot of the second row of the upper CPU-I/O enclosure (the udev name of the slot is sdb) and the lower CPU-I/O enclosure (the udev name of the slot is sdj). See Figure 2-1.
2. When the disks have spun up, partition them for the desired RAID array, as described in “Managing Partitions” on page 2-5. You can mark the partitions with code 83.

3. To create and start the RAID array, type a command similar to the following:

```
# mdadm -C /dev/md20 -b internal --level=1 --raid-devices=2 /dev/sdb1
   /dev/sdj1
```

This command creates the RAID array and starts it. The `-b internal` option implements Red Hat Linux RAID-1 fast resync, which can greatly reduce the amount of time the arrays need to resynchronize. To prevent system instability, use this option when you create the array, instead of using the `--grow` option at a later time.

**NOTE**

When an array is created, `/proc/mdstat` shows that disks are in the process of resynchronizing, but the LEDs on those disks do not light. Although `/proc/mdstat` reports a resynchronization in progress, none is occurring and no disk I/O is involved. In this case, ignore the resynchronization information in `/proc/mdstat`.

To see the status of the new RAID array, type a command similar to the following:

```
# mdadm --detail /dev/md20
```

4. To start the new RAID array each time the system boots, see “Adding Running RAID Arrays to the /etc/mdadm.conf File” on page 2-11.

**Creating a RAID-0 Array**

When the desired file system is larger than a single disk, use RAID-0 to combine multiple RAID-1 arrays into a single RAID array.

This example assumes that two RAID-1 arrays have been created: `md20`, consisting of the partitions `sdb1` and `sdj1`; and `md21`, consisting of the partitions `sdc1` and `sdk1`.

**To create a RAID-0 array**

1. Select a pair of RAID-1 arrays.
2. Make the RAID array with the following command:

```
# mdadm --create /dev/md30 --level=0 --raid-devices=2 /dev/md20
   /dev/md21
```

This command creates the RAID array and starts it.
3. To show the active RAID array, type the following command:
   
   ```
   # mdadm -Q --detail /dev/md30
   ```

4. To start the new RAID array each time the system boots, see “Adding Running RAID Arrays to the `/etc/mdadm.conf` File” on page 2-11.

Adding Running RAID Arrays to the `/etc/mdadm.conf` File

The `/etc/mdadm.conf` file, which specifies which RAID arrays will load at boot time, is created during installation. By default, this file contains one line for each RAID array that is created during installation. If you add disks to the system, you can add the arrays to the `/etc/mdadm.conf` file so the new RAID arrays will load at boot time.

To load RAID arrays at each reboot

1. Generate a list of the running arrays:
   
   ```
   # mdadm --detail --scan --v
   ```

2. Copy the output of the command, except for the `Array` lines that refer to the boot disks, `sda` and `sdb`.

3. In a text editor, open the `/etc/mdadm.conf` file and paste the copied output into the file. Save and close the file.

Mounting a File System

The RAID arrays you create by following the instructions in “Creating a RAID-1 Array” on page 2-9 and “Creating a RAID-0 Array” on page 2-10 are raw disk block devices. To use the file system, you make it a journaling (EXT3) file system and mount it.

1. Make the file system an EXT3 journaling file system by typing a command similar to the following:
   
   ```
   # mkfs.ext3 /dev/md30
   ```

2. Mount the file system on a convenient mount point (for example, `/mnt/big_data`) by typing commands similar to the following:
   
   ```
   # mkdir /big_data
   # mount /dev/md30 /mnt/big_data
   ```

3. Verify that the file system is mounted by doing one or both of the following:

   - Type a `df` command, similar to the following, which shows the size of the file system:
     
     ```
     # df /mnt/big_data
     ```
• Type an `ls` command, similar to the following, which shows the `lost+found` directory in the file system:

```
# ls -l /mnt/big_data
```

4. Add the mount to the `/etc/fstab` file, so the file system is mounted each time the system is rebooted.

5. Reboot the system to verify that the file system is mounted.

   **NOTE**

   For data fault-tolerance, do not use a single disk that is not part of a RAID-1 array.

### Checking the Current State of RAID

Two sources provide information about the current state of RAID: the `/proc/mdstat` file and the `mdadm --detail` command.

The `/proc/mdstat` file provides an overview of active RAID devices, disk mirror status, and disk resynchronization progress, but uses kernel device names that do not correspond to ftServer user-space device names. These names can cause confusion, and you cannot use them to identify particular disks.

The `/sbin/mdadm --detail` command uses ftSSS user-space device names, enabling you to identify the disks described in the command output with particular physical disks. However, the `mdadm --detail --scan` command, which provides an overview of running mirrors, does not display disk resynchronization progress. To see resynchronization progress, you must issue `mdadm --detail` on a particular mirror.

Therefore, use these sources as follows:

- Use the `/proc/mdstat` file (see Example 2-1) when you need to check only the resynchronization progress on a particular mirror, since `/proc/mdstat` shows the resynchronization status for all mirrors.
- Use the following two commands to check the resynchronization status of a particular mirror:
  - `mdadm --detail --scan --verbose` (see Example 2-2) to get a summary of the running mirrors
  - `mdadm --detail /dev/xxx` (see Example 2-3) to see disk resynchronization status of a particular device (represented by `xxx`).
Example 2-1 shows the contents of a sample `/proc/mdstat` file. The disk device names (`sd*`) do not correspond to the names that ftSSS installation assigns to internal disks based on their CPU-I/O enclosure and slot location.

**Example 2-1. The `/proc/mdstat` File**

```bash
# cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdq1[0] sdr1[1]
  264960 blocks [2/2] [UU]
  bitmap: 0/33 pages [0KB], 4KB chunk

md1 : active raid1 sdq2[0] sdr2[1]
  4192896 blocks [2/2] [UU]
  bitmap: 0/128 pages [0KB], 16KB chunk

md3 : active raid1 sdr5[2] sdq5[0]
  29358656 blocks [2/1] [U_]
  [.........................] recovery = 2.4% (706240/29358656)
  finish=5.4min speed=88280K/sec
  bitmap: 0/224 pages [0KB], 64KB chunk

md2 : active raid1 sdq3[0] sdr3[1]
  33551680 blocks [2/2] [UU]
  bitmap: 3/128 pages [12KB], 128KB chunk
```

Example 2-2 shows the output of the `mdadm` command, which displays the `udev` disk device names. The command output is an overview of running mirrors, though without disk resynchronization status.

**Example 2-2. The `mdadm --detail --scan --verbose` Command**

```bash
# mdadm --detail --scan --verbose
ARRAY /dev/md2 level=raid1 num-devices=2 metadata=0.90
  UUID=23281db8:a5d5d3c0:03984b9c:a327a71c
  devices=/dev/sda3,/dev/sdi3
ARRAY /dev/md3 level=raid1 num-devices=2 metadata=0.90 spares=1
  UUID=e15b2957:b2b78bf5:71312b37:999ea42a
  devices=/dev/sda5,/dev/sdi5
ARRAY /dev/md1 level=raid1 num-devices=2 metadata=0.90
  UUID=d55a97e:ae05f13ec3dd20b0:073cc136
  devices=/dev/sda2,/dev/sdi2
ARRAY /dev/md0 level=raid1 num-devices=2 metadata=0.90
  UUID=189bdcc5:fd9ca4eb:d23b4f2e:3c10a447
  devices=/dev/sda1,/dev/sd1
```
Example 2-3 shows the use of the `mdadm` command to display the resynchronization progress of a particular device, md2.

**Example 2-3. The `mdadm --detail /dev/mdx` Command**

```bash
# mdadm --detail /dev/md2
/dev/md3:
    Version : 0.90
    Creation Time : Mon Aug 31 14:30:11 2009
    Raid Level : raid1
    Array Size : 29358656 (28.00 GiB 30.06 GB)
    Used Dev Size : 29358656 (28.00 GiB 30.06 GB)
    Raid Devices : 2
    Total Devices : 2
    Preferred Minor : 3
    Persistence : Superblock is persistent

    Intent Bitmap : Internal

    Update Time : Thu Oct 29 09:46:34 2009
    State : active, degraded, recovering
    Active Devices : 1
    Working Devices : 2
    Failed Devices : 0
    Spare Devices : 1

    Rebuild Status : 72% complete

    UUID : e15b2957:b2b78bf5:71312b37:999ea42a
    Events : 0.23004

    Number   Major   Minor   RaidDevice State
    0        65      5        0      active sync  /dev/sda5
    2        65      21       1      spare rebuilding  /dev/sdi5
```
Ethernet Devices

Network-interface card (NIC) naming in ftSSS is different from other Linux systems. ftSSS gives physical devices names that correspond to their hardware location. After installing ftSSS, the interfaces associated with the Ethernet adapters are operational and default bonds are created.

This section discusses the following topics:

- “Device Naming of Ethernet Ports”
- “Monitoring and Configuring Channel-Bonding Interfaces” on page 2-17
- “MAC Addresses” on page 2-22

Device Naming of Ethernet Ports

On many Linux systems, Ethernet port devices are assigned names based on the order of discovery at system startup. The configuration may change dynamically when hardware failures occur, repairs are made, or when an administrator adds or removes components.

Creating new Ethernet port device names when new hardware is installed, tracking the name of a device while it is removed and replaced and matching it up again, or deleting the name would be difficult and the results confusing.

Therefore, ftSSS assigns to network devices names that are derived from their physical location in the system. A sample Ethernet port name is `eth100200`.

Ethernet port names are developed according to the following scheme:

- The prefix `eth`
- 10 or 11, indicating the I/O element device path
- 01, 02, 03, 04, or 06, indicating the slot number
- Two final digits, based on PCI device and function number

To list the names of all Ethernet port devices installed on the system, type the following command:

```
# ifconfig -a | grep HW
```

Table 2-3 lists the Ethernet interface device names and other information for Ethernet adapters in CPU-I/O enclosures, assuming that all slots are populated by Ethernet adapters. For additional information on device paths, see “Understanding Device Paths” on page 2-27.
Table 2-3. Ethernet Devices in ftServer Systems  *(Page 1 of 2)*

<table>
<thead>
<tr>
<th>Device</th>
<th>Location and Device Path</th>
<th>Ethernet Interface Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded 10/100/1000-Mbps Ethernet PCI adapter</td>
<td>CPU-0, I/O-10, slot 6, port 0 10/6</td>
<td>eth100600</td>
</tr>
<tr>
<td>Embedded 10/100/1000-Mbps Ethernet PCI adapter</td>
<td>CPU-0, I/O-10, slot 6, port 1 10/6</td>
<td>eth100601</td>
</tr>
<tr>
<td>Embedded 10/100/1000-Mbps Ethernet PCI adapter</td>
<td>CPU-1, I/O-11, slot 6, port 0 11/6</td>
<td>eth110600</td>
</tr>
<tr>
<td>Embedded 10/100/1000-Mbps Ethernet PCI adapter</td>
<td>CPU-1, I/O-11, slot 6, port 1 11/6</td>
<td>eth110601</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-0, I/O-10, PCI slot 1, port 0 10/1</td>
<td>eth100100</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-0, I/O-10, PCI slot 1, port 1 10/1</td>
<td>eth100101</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-0, I/O-10, PCI slot 2, port 0 10/2</td>
<td>eth100200</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-0, I/O-10, PCI slot 2, port 1 10/2</td>
<td>eth100201</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-1, I/O-11, PCI slot 1, port 0 11/1</td>
<td>eth110100</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-1, I/O-11, PCI slot 1, port 1 11/1</td>
<td>eth110101</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-1, I/O-11, PCI slot 2, port 0 11/2</td>
<td>eth110200</td>
</tr>
<tr>
<td>Ethernet PCIe adapter (optional)</td>
<td>CPU-1, I/O-11, PCI slot 2, port 1 11/2</td>
<td>eth110201</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional PCIe or PCI-X slot</td>
<td>CPU-0, I/O-10, PCI slot 3, port 0 10/3</td>
<td>eth100300</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-10, PCI slot 3, port 1 10/3</td>
<td>eth100301</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-10, PCI slot 4, port 0 10/4</td>
<td>eth100400</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-10, PCI slot 4, port 1 10/4</td>
<td>eth100401</td>
</tr>
</tbody>
</table>
By default, the embedded physical Ethernet interfaces (100600, 110600, 100601, and 110601 in Table 2-3) are bound together into two channel-bonding interfaces, called bond0 and bond1, as follows:

- **bond0**: 100600 and 110600
- **bond1**: 100601 and 110601

The two channel-bonding interfaces are set to operate in active-backup mode (mode 1) with Dynamic Host Configuration Protocol (DHCP) enabled.

In many cases, no additional configuration is necessary of these embedded interfaces. However, you may want to change the default configuration to better meet your particular networking requirements.

If the system contains additional network adapters, or if you add network adapters, bind their ports into channel-bonding interfaces. Place one port from each enclosure in each bonded-pair.

The default ftServer bonding mode is active-backup (also sometimes called Adapter Fault Tolerance, or AFT). All Linux bonding modes are supported.

---

**NOTE**

Consider the following when configuring the channel bonding mode.

1. When a CPU-I/O enclosure is running diagnostics, such as when it is being brought into service, its expansion PCI slots are temporarily powered up. If one of the

---

### Table 2-3. Ethernet Devices in ftServer Systems (Page 2 of 2)

<table>
<thead>
<tr>
<th>Device</th>
<th>Location and Device Path</th>
<th>Ethernet Interface Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-11, PCI slot 3, port 0 11/3</td>
<td>eth110300</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-11, PCI slot 3, port 1 11/3</td>
<td>eth110301</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-11, PCI slot 4, port 0 11/4</td>
<td>eth110400</td>
</tr>
<tr>
<td>Ethernet PCI adapter in optional high-profile PCIe or PCI-X slot</td>
<td>CPU-0, I/O-11, PCI slot 4, port 1 11/4</td>
<td>eth110401</td>
</tr>
</tbody>
</table>
the PCI slots contains an optional Ethernet PCI adapter (that is, a NIC), the adapter can signal to a connected network switch that the adapter is ready for traffic even though the operating system has not configured the adapter. If the adapter is part of a channel bonding interface with a switch-assisted mode, such as Bal-RR or Bal-Xor, a few network packets from the switch can get lost during this interval.

2. The TCP protocol recovers the packets because TCP resends the lost packets after its time-out period. Other network protocols, such as UDP and ICMP, do not resend lost packets.

You configure and administer the Ethernet interfaces on your ftServer system just as you would on any standard Linux system. Additionally, you can use the following tools:

- The /opt/ft/bin/ftsmaint command to obtain information about the fault-tolerant status of the interfaces, described in “Monitoring Channel-Bonding Interfaces” on page 2-18
- The /opt/ft/sbin/ft-bonding tool, described in “Configuring Channel-Bonding Interfaces” on page 2-19

Monitoring Channel-Bonding Interfaces

You can monitor the fault-tolerant status of channel-bonding interfaces by using the ftsmaint command. Example 2-4 shows the default configuration of the embedded Ethernet devices.

Example 2-4. Default Configuration of Embedded Ethernet Devices

```
# /opt/ft/bin/ftsmaint lsVnd
Virtual Network Device (VND) Groups
===================================
Group Name   Status  Inet Address    RX Errors  TX Errors  Collisions
---------------------------------------------------------------------
bond0        ONLINE  134.111.78.103          0          0           0
bond1        ONLINE  192.168.4.10            0          0           0
bond2        OFFLINE -                       0          0           0
bond3        OFFLINE -                       0          0           0
bond4        OFFLINE -                       0          0           0
bond5        OFFLINE -                       0          0           0
bond6        OFFLINE -                       0          0           0
bond7        OFFLINE -                       0          0           0
bond8        OFFLINE -                       0          0           0
bond9        OFFLINE -                       0          0           0
```
(Continued on next page)
VND Group Members
=================

<table>
<thead>
<tr>
<th>Member</th>
<th>Group Name</th>
<th>Status</th>
<th>Interface</th>
<th>Link State</th>
<th>Link Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth100600</td>
<td>bond0</td>
<td>DUPLEX</td>
<td>UP LINK</td>
<td>100Mb/s-FD</td>
<td></td>
</tr>
<tr>
<td>eth100601</td>
<td>bond1</td>
<td>DUPLEX</td>
<td>UP LINK</td>
<td>100Mb/s-FD</td>
<td></td>
</tr>
<tr>
<td>eth110600</td>
<td>bond0</td>
<td>DUPLEX</td>
<td>UP LINK</td>
<td>100Mb/s-FD</td>
<td></td>
</tr>
<tr>
<td>eth110601</td>
<td>bond1</td>
<td>DUPLEX</td>
<td>UP LINK</td>
<td>100Mb/s-FD</td>
<td></td>
</tr>
</tbody>
</table>

In Example 2-4, there are two online channel-bonding interfaces (bonds), bond0 and bond1, each composed of two physical interfaces (members). The output shows the four physical slave interfaces in the system and also shows their status and the name of the bond to which they belong. Note that three other channel-bonding interfaces are defined by default, but they are not configured and are therefore offline.

You can monitor additional information about the currently installed channel-bonding and physical interfaces by running the Linux `ifconfig` tool.

### Configuring Channel-Bonding Interfaces

You can use the `/opt/ft/sbin/ft-bonding` tool to bond pairs of Ethernet ports that have been newly added to the system or to change the configuration of existing bonds.

**NOTES**

1. The `/opt/ft/sbin/ft-bonding` tool uses only the bond files that already exist. The installation program creates only bond0 and bond1. To add Ethernet ports to other bonds, first create a new bond file by copying an existing bond file (for example, `ifcfg-bond2`) in the `/etc/sysconfig/network-scripts` directory to another file.

2. The `/opt/ft/sbin/ft-bonding` tool creates the bonds to operate in active-backup mode (mode 1) with Dynamic Host Configuration Protocol (DHCP) enabled. Edit the bond file to change these settings. See Example 2-5 and Example 2-6 for reference.

**Subcommands for the `/opt/ft/sbin/ft-bonding` tool include:**

- `/opt/ft/sbin/ft-bonding list`

  Lists each bond and its Ethernet ports.
• /opt/ft/sbin/ft-bonding none
  Removes all Ethernet bonds.

• /opt/ft/sbin/ft-bonding single
  Adds all Ethernet ports to a single bond.

• /opt/ft/sbin/ft-bonding paired
  Creates a default set of Ethernet bonds, binding pairs of Ethernet ports according to a default configuration.

  The default configuration pairs ports so that a bond contains one port from each enclosure. If an Ethernet adapter is installed in only one enclosure (no adapter is installed in its matching slot in the other enclosure), these ports are left unbonded.

• /opt/ft/sbin/ft-bonding config
  Starts an interactive session, prompting you to supply the name of the bond and the ports that should be members of the bond.

  Type done at any prompt to exit from the session. Then activate the changes made to the configuration file.

When you type the /opt/ft/sbin/ft-bonding none, /opt/ft/sbin/ft-bonding single, or /opt/ft/sbin/ft-bonding paired command, or complete the interactive configuration steps, the changes to the configuration file are made immediately. You can undo the changes by typing another command, such as /opt/ft/sbin/ft-bonding none.

You can also use standard Linux tools to configure and administer channel-bonding interfaces. The ifcfg-* files in the /etc/sysconfig/network-scripts directory control the configuration of channel-bonding interfaces. You can modify existing channel bond configurations by editing the bond’s ifcfg-bondn file or the bond’s slaves’ interface ifcfg-eth* files. Additionally, you use standard Linux network utilities like ifdown, ifup, service, ifconfig, ip, and route.

By default, the system supports five channel-bonding interfaces. In the unlikely event that you must configure more than five bonds (up to a maximum of 10), modify the options line in the /etc/modprobe.d/ft-network.conf file so that max_bonds=x, where x is the desired number of channel-bonding interfaces. Perform the following procedure to activate configuration-file modifications.

To activate configuration-file modifications
1. Type the ifdown command to stop all network interfaces.
2. Type the rmmod command to unload the bonding kernel module. This disables network access.
3. Type the `modprobe` command to reload the bonding module. This enables network access with the newly designated number of channel-bonding interfaces.

4. If necessary, type an `ifup bondN` command for each bonded interface you wish to restart.

You can configure each bond with its own bonding mode by adding a line to the `/etc/sysconfig/network-scripts/ifcfg-bondN` file. Add the line `BONDING_OPTS="mode=x"`, where `x` is the desired mode of operation.

If you want to change the mode from the default setting (mode 1, active-backup mode) for all bonds, modify the options line in the `/etc/modprobe.d/ft-network.conf` file so that `mode=x`, where `x` is the desired mode of operation. After you change the mode, activate the configuration-file modifications.

**NOTES**

1. The `/etc/modprobe.d/ft-network.conf` file must contain at least one alias for an active bond, or bonding cannot occur.

2. The `/etc/modprobe.d` directory should contain no more than one `ft-network.conf` file.

**To add two physical interfaces and configure a new bond**

1. Install the first Ethernet PCI adapter in a supported slot in one CPU-I/O enclosure. Find and write down the interface device name for each port on this newly installed adapter. See “Device Naming of Ethernet Ports” on page 2-15 for details.

2. Install the second Ethernet PCI adapter in the same slot in the other CPU-I/O enclosure.

**NOTE**

When adding a pair of Ethernet PCI adapters to the system, be sure to install one adapter in the upper CPU-I/O enclosure and the other in the lower CPU-I/O enclosure, in same-numbered slots. This configuration is necessary to maintain fault tolerance. If you install both devices in the same enclosure and that enclosure fails, you lose connectivity.

Find and write down the interface device name for each port on this newly installed adapter. See “Device Naming of Ethernet Ports” on page 2-15 for details.
3. Create a new bond file (for example, ifcfg-bond2) in the
   /etc/sysconfig/network-scripts directory. Use the contents of an existing
   bondn file as a guide.

   The following are examples of bond file entries that show the lines for specifying
   two bonds, one that uses static IP addressing and another that uses DHCP to
   obtain an IP address.

   **Example 2-5. Bond that Uses Static IP Addressing**

   ```
   DEVICE=bond2
   ONBOOT=yes
   BOOTPROTO=None  IPADDR=192.168.1.152 NETMASK=255.255.255.0
   USERCTL=no
   GATEWAY=192.168.1.1  <this line goes in only 1 file>
   ```

   **Example 2-6. Bond that Uses DHCP**

   ```
   DEVICE=bond2
   ONBOOT=yes
   BOOTPROTO= blackmail
   USERCTL=no
   ```

4. Create two new physical interface configuration files for the two new physical
   interfaces. Use the contents of an existing ifcfg-eth* file as a guide. Be sure to
   use the device names of the newly installed adapters (see step 2).

5. Type the following command to bring up the new interface:

   `# ifup bond2`

### MAC Addresses

You can use the `ifconfig` command to determine the current MAC address of an
Ethernet interface. Or, you can examine the interface's address file in the
`sys/class/net/interfacename` directory.

For the embedded Ethernet adapter interfaces, Ethernet MAC addresses are
algorithmically generated from a `base` MAC address assigned to the machine as a
whole. Each physical device receives a different MAC address. Because of this, a
channel-bonding interface (and all of its member devices) may get a different MAC
address from one reboot to the next, depending on which member device is available
first (based on which CPU-I/O enclosure is used during the boot).
Other System Configuration Information

In addition to setting up storage and network devices, you may want to perform the following tasks to set up your system:

- Configure the ASN software on your system to allow the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative to monitor system alarms and perform remote troubleshooting. See *Stratus ftServer System Software: Installation for Linux Systems* (R013L) and the *Stratus ActiveService Network Configuration Guide* (R072) for instructions.
- Configure the video display.
- Manage the system clock.
- Defer CPU resynchronization.
- Disable system operation during CPU resynchronization.

You also need to perform the following configuration tasks, using standard Linux procedures:

- Configure the IP address for the bond0 and bond1 interfaces (static or DHCP, and gateway in `/etc/sysconfig/network-scripts/ifcfg-bond0` and `/etc/sysconfig/network-scripts/ifcfg-bond1`)
- Configure DNS resolution for the system (`/etc/nsswitch.conf` and `/etc/resolv.conf`)  
- Configure static routes for the system (`/etc/sysconfig/static-routes`)
- Configure the system hostname (`/etc/hosts` and `/etc/sysconfig/network`)
- Configure the system time zone (`/etc/sysconfig/clock`). See “Managing the System Clock” on page 2-24 for related information.

As you perform these configuration tasks as well as other system administrative tasks, you need to understand and use device paths, as “Understanding Device Paths” on page 2-27 describes.

Configuring the System Video Display

ftSSS configures your system’s video output to a default setting, and you typically do not need to change the video-display settings. The system is strictly limited in some of its parameters. For instance, the screen resolution is limited to 1600x1200 pixels. However, it is possible, though not advisable, to change the video configuration.
If you do change video settings, use a text editor to change the entries in the /etc/X11/xorg.conf file. Use one of the configured video modes that the ftSSS installation program installed in the xorg.conf file.

To do this, select one of the available modes from the list for the pixel depth you are using, which is present as a comment in the xorg.conf file. Replace the Modes line of the desired pixel depth with your preferred video mode. Changes made to the xorg.conf file are preserved during an upgrade.

**CAUTION**

Using other means to configure the video—including any of those available from a Red Hat utility—may result in loss of system fault tolerance, may cause the system to boot only in text mode, or may return an error message.

### Managing the System Clock

By default, the installation of the Linux operating system sets the time zone of the system clock to Coordinated Universal Time (UTC), not Local Time. Do not change this setting and make sure any kickstart file you provide sets the time to UTC.

**NOTE**

Using UTC ensures that times in system logs are not duplicated after a time change to or from daylight saving time (DST, or *summer* time).

You may see the following message after the system boots or after you attempt to use the `system-config-time` utility:

```
Cannot access the Hardware Clock via any known method.
Use the --debug option to see the details of our search for an access method.
```

You may safely disregard this message.

The following message does not indicate a problem with the system. The clock will be properly reset and you can safely ignore the message.

```
Losing some ticks... checking if CPU frequency changed
```
Deferring CPU Resynchronization

For a variety of reasons (for example, replacement of a failed CPU enclosure or recovery from a transient CPU error), a CPU in your system may need to be put back into service and resynchronized to return the system to duplexed operation. During this resynchronization period, system performance is sluggish and the system cannot respond to network connections; therefore, it is important to set the timeout period or number of retries for network applications large enough to prevent timeouts. The length of the resynchronization period is proportional to the amount of system memory configured.

By default, resynchronization occurs as soon as the inactive CPU element is determined to be operational, or when the CPU-I/O enclosure is replaced. The priority is to return the system to fully duplexed operation as quickly as possible. However, if your application is sensitive to a delay of this nature, you can defer resynchronization to a more convenient time, such as an off-peak period.

To defer return of an offline CPU enclosure to service, enter the following command as the root user:

```
# /opt/ft/bin/ftsmaint bringupPolicy defer
```

Thereafter, if a CPU element goes out of service, the system runs simplexed until one of the following events occurs:

- You set `bringupPolicy` to `enable`.
- The `ftsmaint bringUp` command is executed for the CPU element.
- The system restarts.

**NOTE**
Whenever the system restarts, the `bringupPolicy` setting is temporarily ignored, and the CPUs resynchronize automatically, even if `bringupPolicy` is set to `defer`. After the system has finished booting, the set policy again takes effect.

**CAUTION**
While your system is running simplexed, it is not fault tolerant. Therefore, you should limit the length of the period during which resynchronization is deferred to the minimum necessary.
To re-enable CPU resynchronization (the default setting), and immediately resynchronize any CPU currently in the deferred state, enter the following command:

```bash
# /opt/ft/bin/ftsmaint bringupPolicy enable
```

To display the current setting of the `bringupPolicy`, enter the following command:

```bash
# /opt/ft/bin/ftsmaint bringupPolicy list
```

To schedule specific periods of the day to enable or defer CPU resynchronization, use the `cron` utility to run the `ftsmaint bringupPolicy` command at predetermined times.

To schedule CPU bringup options with the `cron` utility, edit the `/etc/crontab` file to include scheduled executions of the `ftsmaint bringupPolicy` command, and save the file.

**Example 2-7** shows the lines to add to the `/etc/crontab` file to defer CPU resynchronizations during a peak period from 6:00 AM to 6:15 PM each day (i.e., resynchronization will be done only before 6:00 AM or after 6:15 PM).

**Example 2-7. `/etc/crontab` Entries to Automatically Control CPU Resynchronization**

```bash
# Defer CPU bringup at 6AM every day
0 6 * * * root /opt/ft/bin/ftsmaint bringupPolicy defer
#
# Enable CPU bringup at 6:15PM every day
15 18 * * * root /opt/ft/bin/ftsmaint bringupPolicy enable
```

**Disabling System Operation During CPU Resynchronization**

When a CPU that has been offline is brought into service and needs to be synchronized with the running CPU, ftSSS normally allows the system to continue operating during a portion of the synchronization period. However, some applications may interact with the system during this operational period in such a way as to prevent the CPUs from synchronizing. To avoid this problem, you can now use the `ftmod_blackout_only` parameter in the `/etc/sysconfig/modules/00-1sb-ft-ftmod.modules` file to instruct the system to suspend operation during the entire synchronization period.
To disable system operation during CPU resynchronization

1. Edit the /etc/sysconfig/modules/00-1sb-ft-ftmod.modules file. By default, the file contains the following lines:

```bash
#!/bin/sh
# Copyright (c) 2008 Stratus Technologies Bermuda Ltd.
for i in button ftmod
    do
        logger -p kern.info -t `basename ${0}` Loading module: $i
        modprobe $i || 
        logger -s -p kern.error -t `basename ${0}` modprobe
        $i failed.
    done
```

Edit the `for i in button ftmod` line by adding quotation marks ("") and the `ftmod_blackout_only_cpu_bringup=1` option, so that the resulting line is the following:

```bash
for i in button “ftmod ftmod_blackout_only_cpu_bringup=1”
```

2. Save the file.

3. Reboot the system.

You can enable system operation during a portion of the synchronization period again by removing the `ftmod_blackout_only_cpu_bringup=1` parameter from the file, saving it, and rebooting the system.

### Understanding Device Paths

Most ftServer subsystems and components are addressable by device paths, and you must use these device paths in certain commands and procedures. For example, you must use device paths with the `ftsmaint` command. Device paths uniquely identify devices in an ftServer system. In the output of some commands, devices are also represented by device IDs, which may change as a result of normal system events. Thus, device IDs may vary but device paths remain unchanged. For further information, see the following sections:

- “Device Paths” on page 2-27
- “Device IDs” on page 2-30

### Device Paths

Table 2-4 lists device paths in an ftServer system. For controllers, the table includes sample device IDs. Figure 2-2 and Figure 2-3 show device paths with the devices. For more information on device IDs, see “Device IDs” on page 2-30. For a complete list of Ethernet interface device names, see Table 2-3.
<table>
<thead>
<tr>
<th>Device</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Combined CPU/IO (CPU)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Top Enclosure</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>DIMMs (addressed by slot)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0/1 – 0/12</td>
</tr>
<tr>
<td>Processors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0/21, 0/22</td>
</tr>
<tr>
<td>Baseboard Temp#n Sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0/130</td>
</tr>
<tr>
<td>Baseboard Fan #n Sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0/140 – 0/144</td>
</tr>
<tr>
<td>Combined CPU/IO (I/O)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
</tr>
<tr>
<td>PCIe adapter devices (in slots on motherboards)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/1, 10/2</td>
</tr>
<tr>
<td>PCI adapter devices (in optional high-profile PCIe or PCI-X slots)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/3, 10/4</td>
</tr>
<tr>
<td>Network controller</td>
<td></td>
</tr>
<tr>
<td>Ethernet controller: Intel Corporation 82</td>
<td></td>
</tr>
<tr>
<td>Network interface</td>
<td>10/6</td>
</tr>
<tr>
<td></td>
<td>0b:00.0, 0b:00.1</td>
</tr>
<tr>
<td></td>
<td>eth100600,</td>
</tr>
<tr>
<td></td>
<td>eth100601</td>
</tr>
<tr>
<td>Display controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/7</td>
</tr>
<tr>
<td>VGA compatible controller: Matrox graphic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0c:00.0</td>
</tr>
<tr>
<td>Serial bus controllers</td>
<td></td>
</tr>
<tr>
<td>USB controllers: Intel Corporation 82801J</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/8</td>
</tr>
<tr>
<td></td>
<td>0a:1a.0, 0a:1a.7</td>
</tr>
<tr>
<td>Serial bus controllers</td>
<td></td>
</tr>
<tr>
<td>USB controllers: Intel Corporation 82801J</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/9</td>
</tr>
<tr>
<td></td>
<td>0a:1d.0, 0a:1d.1, 0a:1d.2, 0a:1d.7</td>
</tr>
<tr>
<td>Bridge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/10</td>
</tr>
<tr>
<td>Internal disk controller</td>
<td></td>
</tr>
<tr>
<td>Disk drives 1 - 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/40</td>
</tr>
<tr>
<td></td>
<td>10/40/1 (sda) –</td>
</tr>
<tr>
<td></td>
<td>10/40/8 (sdh)</td>
</tr>
<tr>
<td>2x PCIe or PCI-X Riser Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/70</td>
</tr>
<tr>
<td>Baseboard management controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/120</td>
</tr>
<tr>
<td>Optional ftScalable Storage system</td>
<td></td>
</tr>
<tr>
<td>RAID controller tray</td>
<td></td>
</tr>
<tr>
<td>expansion tray</td>
<td></td>
</tr>
<tr>
<td></td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>71</td>
</tr>
<tr>
<td>Callout</td>
<td>Device</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>1</td>
<td>CPU-0, I/O-10</td>
</tr>
<tr>
<td>2</td>
<td>Internal disk drive: 1</td>
</tr>
<tr>
<td>3</td>
<td>Internal disk drive: 2</td>
</tr>
<tr>
<td>4</td>
<td>Internal disk drive: 3</td>
</tr>
<tr>
<td>5</td>
<td>Internal disk drive: 4</td>
</tr>
<tr>
<td>6</td>
<td>Internal disk drive: 5</td>
</tr>
<tr>
<td>7</td>
<td>Internal disk drive: 6</td>
</tr>
<tr>
<td>8</td>
<td>Internal disk drive: 7</td>
</tr>
<tr>
<td>9</td>
<td>Internal disk drive: 8</td>
</tr>
<tr>
<td>10</td>
<td>CPU-1, I/O-11</td>
</tr>
<tr>
<td>11</td>
<td>Internal disk drive: 1</td>
</tr>
<tr>
<td>12</td>
<td>Internal disk drive: 2</td>
</tr>
<tr>
<td>13</td>
<td>Internal disk drive: 3</td>
</tr>
<tr>
<td>14</td>
<td>Internal disk drive: 4</td>
</tr>
<tr>
<td>15</td>
<td>Internal disk drive: 5</td>
</tr>
<tr>
<td>16</td>
<td>Internal disk drive: 6</td>
</tr>
<tr>
<td>17</td>
<td>Internal disk drive: 7</td>
</tr>
<tr>
<td>18</td>
<td>Internal disk drive: 8</td>
</tr>
</tbody>
</table>
Other System Configuration Information

Figure 2-3. ftServer Enclosures: Major Devices and Paths (Rear View)

A device ID is in the format $nn:nn.n$, also displayed as $nn, nn, nn$. Values in a device ID for PCI adapters represent the following:

$$PCI_{-BUS}\_SLOT\_IN\_BUS\_FUNCTION\_WITHIN\_DEVICE.$$ 

Values for $PCI_{-BUS}$ and $SLOT\_IN\_BUS$ vary based on the slot where the PCI adapter is inserted. Values for $PCI_{-BUS}$ can further vary based on the presence and location of other options in the system. Thus, whenever possible, you should identify a PCI adapter by device path instead of device ID. (For information on device paths, see “Device Paths” on page 2-27.)
If you must associate a device ID of a PCI adapters with a device path, and thus, a particular slot, use the command `ftsmaint ls`. The command output typically includes the device ID and its corresponding device path, which is listed in the line above the device ID.

Example 2-8 shows an excerpt from output of the command `ftsmaint ls`. The excerpt displays a line with the device ID `06:00.0`, and the preceding line with the device path `10/1`. Thus, on this system, device ID `06:00.0` corresponds to the device path `10/1`, so you know that the Fibre Channel PCI adapter `06:00.0` is located in slot 1 in CPU-I/O enclosure 10. (Example 6-1 shows output of the Emulex BIOS Utility that includes the device `06,00,00`, which corresponds to the Fibre Channel PCI adapter `06:00.0`.)

**Example 2-8. Device Path and PCI Device ID in `ftsmaint ls` Output**

<table>
<thead>
<tr>
<th>H/W Path</th>
<th>Description</th>
<th>State</th>
<th>OPState</th>
<th>FRev</th>
<th>Fct</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/1</td>
<td>Serial Bus Ctrlrs</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>06:00.0</td>
<td>Fibre Channel: Emulex Corp Saturn:</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Additional Documentation and Resources**

*Linux System Administrator’s Guide* v0.8, Linux Documentation Project:

http://www.ibiblio.org/pub/Linux/docs/linux-doc-project/system-admin-guide/
http://unthought.net/Software-RAID.HOWTO/

*Managing RAID on Linux*, Derek Vadala, O'Reilly & Associates, 2003:
http://www.oreilly.com/catalog/mraidlinux/
Chapter 3
Managing Data Storage Devices

This chapter discusses the following topics:

- “Removing and Replacing Internal Disks”
- “Stopping a RAID Array and Moving It to Another System” on page 3-10
- “Using LVM” on page 3-10
- “Using ftScalable Storage Systems” on page 3-10
- “Planning for System Backups and Disaster Recoveries” on page 3-11
- “Using Device Names for the DVD Drive” on page 3-11
- “Using SAS Tape Drives” on page 3-11
- “Using USB Storage Devices” on page 3-12
- “Additional Resources” on page 3-14

Removing and Replacing Internal Disks

For disk fault tolerance, disk mirrors must be maintained when disks or CPU-I/O enclosures are removed and replaced. For information about the recommended mirroring configuration for internal disks, see “Internal Disk Naming” on page 2-2.

When you remove and then reinsert a pulled disk into a running system, ftSSS attempts to match it with an existing disk. If it finds a match, it automatically adds the mirrored partitions on the inserted disk back into the existing RAID arrays and resynchronizes them.

Similarly, if you replace a failed disk, ftSSS automatically adds the replacement disk to a running RAID array.

To remove a failed disk

1. So that you do not lose any data, make sure the disk you are removing is not the only member of a mirror (in a SIMPLEX state). See “Displaying the Status of a Single System Component” on page 4-10.
If the disk is in a SIMPLEX state and you do not want to lose the information on the disk, insert a disk in the corresponding slot of the other CPU-I/O enclosure and allow the disks to synchronize. However, mirroring of the replacement disk occurs automatically only when the system has not been rebooted after the partner of the SIMPLEX disk was removed.

If you are removing a disk that has been removed from service because of errors, the disk will be in a BROKEN state and you can go to step 2. See “ftSSS Management of Failed Disks” on page 3-2” for information about how ftServer systems react to errors on a mirror.

If the disk is not in a SIMPLEX or BROKEN state, type the following command to remove it from service:

```
# ftsmaint bringDown path
```

For *path*, specify the value for the internal disk, as shown in Figure 2-1.

2. Remove the physical disk from its slot.

For related information, see the following topics:

- “ftSSS Management of Failed Disks”
- “Replacing a Failed Disk (Automatic Method)” on page 3-3
- “Configuring Safe Mode” on page 3-4
- “Speeding Up the Rate of Resynchronization” on page 3-5
- “Replacing a Failed Disk With a Used Disk” on page 3-5
- “Replacing a Failed Disk (Manual Method)” on page 3-7
- “Stopping a RAID Array and Moving It to Another System” on page 3-10
- “Periodically Checking Disks” on page 3-10

**ftSSS Management of Failed Disks**

When a disk or partition experiences a fault, ftSSS determines whether the disk has experienced an unacceptable number of errors by calculating its mean time between failures (MTBF). To view the MTBF of a component, issue the command `ftsmaint ls path` (for information, see “ftsmaint Command Arguments” on page 4-1).

If the MTBF is not yet below the assigned MTBF threshold, ftSSS removes the disk, or the partitions on the disk, from its RAID-1 mirrors and then adds them back.
Removing and Replacing Internal Disks

If the MTBF is less than the assigned threshold, ftSSS removes any partitions on the affected disk from their RAID mirrors and removes the disk from service. If the system is configured to send alerts to the ASN, ftSSS sends an alert.

NOTES

1. The last active disk of a RAID set is never removed from service, even if errors are reported against it.
2. The alert signals the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative to send a replacement disk.

Every time an active disk is pulled, all outstanding I/O is returned as errors. When a disk is pulled, all RAID members or mirrors that have active I/O on the missing disk are marked faulty, though these may not reflect all RAID arrays that use the disk.

When ftSSS removes a disk from service, the disk of the remaining active mirror and the CPU-I/O enclosure that contains the remaining active disk enter a simplex state, and are no longer safe to pull. A blinking yellow LED on the disk drive indicates that the disk drive is in a simplex state and is unsafe to remove.

CAUTION

Do not remove a disk that is in a simplex state. Doing so could cause a data loss or halt system operation.

For descriptions of commands used to manage the MTBF settings, see “ftsmaint Command Arguments” on page 4-1. For information about MTBF statistics, see the Stratus ftServer Systems: Technical Reference Guide (R550).

Replacing a Failed Disk (Automatic Method)

When you need to replace a failed disk, ftSSS can automatically add the replacement disk to a running RAID array, provided the following conditions exist:

- The replacement disk must be blank, as defined by the current safe mode setting. If safe mode is active, zero the disk's partition table and RAID superblocks. Then remove and reinsert the disk to start the automatic disk replacement.
- You do not reboot the system or stop and restart the OpState Manager (OSM), an ftSSS storage plug-in, after you remove the failed disk until you have inserted the replacement disk and it has synchronized with its partner. The information necessary to perform automatic disk replacement is not persistent, so if OSM is restarted, the replacement disk must be paired using a different method.
- The failed disk must have been paired with one (and only one) partner disk. For example, if /dev/md4 consisted of partitions sda1 and sdb1, and /dev/md5
consisted of sdb2 and sdc2, automatic disk replacement would not work for disk sdb. In addition, partition numbers on the failed disk and its partner, for any partitions belonging to RAID-1 arrays, must be the same.

- The failed disk must belong to a RAID-1 array on top of a disk or partition. If the failed disk belongs to a RAID-0 array (even it is also part of a RAID-1 array), the blank disk will not be added to the RAID array.

**NOTE**

If the running member of the RAID array was a system disk, the boot loader (grub) is added to the newly-inserted disk.

**To replace a failed disk (automatic method)**

1. While the system and RAID array are running, remove the failed disk.
2. Insert a blank disk.

   The blank disk is automatically added to the array.

If you must reboot the system after you have removed the failed disk, but before you insert the new disk, see “Replacing a Failed Disk (Manual Method)” on page 3-7.

If you are replacing the failed disk with a disk that is not blank, see “Replacing a Failed Disk With a Used Disk” on page 3-5.

**Configuring Safe Mode**

By default, the OSM configuration file, /opt/ft/osm/config.xml, configures this automatic pairing of disks in safe-mode. In safe mode, a newly inserted disk is considered blank if it has no valid partition table or RAID superblocks.

Add the following entry in the OSM configuration file to configure safe mode:

```
<entry key="blankDiskSafeMode" value="true"/>
```

To allow a newly inserted disk to be considered blank even if it has a valid partition table or RAID superblocks, as long as it does not belong to a running RAID array, specify that automatic pairing of disks not operate in safe mode by replacing the word true with false so that the file contains the following entry:

```
<entry key="blankDiskSafeMode" value="false"/>
```

Because OSM preferences are only read at start-up time, you must reboot the system for a change to take effect.
Speeding Up the Rate of Resynchronization

To speed up the rate at which internal disks resynchronize, you can change the default value of the `dev/raid/speed_limit_min` parameter from 1000 to 200000.

**CAUTION**

While increasing the `dev/raid/speed_limit_min` value greatly accelerates the pace of resynchronization, it degrades system performance.

To see the current maximum and minimum speed limits, type the following commands, which in this case return values of 200000 and 1000, respectively:

```
# cat /proc/sys/dev/raid/speed_limit_max
200000
# cat /proc/sys/dev/raid/speed_limit_min
1000
```

To increase the speed limit to 200,000 immediately, in `/etc/rc.local`, type the following command:

```
# echo 200000 >/proc/sys/dev/raid/speed_limit_min
```

To set the kernel parameter to the higher speed limit so that the system boots with those values, type the following commands in `/etc/sysctl.conf`:

```
# dev.raid.speed_limit_max = 200000
# dev.raid.speed_limit_min = 200000
```

Replacing a Failed Disk With a Used Disk

If you are replacing the failed disk with a disk that is not blank, remove the failed disk, insert the replacement disk, and type the following command:

```
# /opt/ft/bin/duplex_blank_disk
```

If the replacement disk contains partitions or a partition table, the command prompts you to confirm that you want to delete the information on the disk.

Example 3-1 shows the command prompts and sample responses for pairing a spare internal disk (in slot `sdi`) with the running system disk (in slot `sda`). See Figure 2-1 and Figure 2-2 for illustrations and lists of device paths for disk devices.
Example 3-1. Pairing a Spare Internal Disk with the Running System Disk

```bash
# /opt/ft/bin/duplex_blank_disk

Device Path ID of blank disk (e.g. 10/40/1 or 70/1): 11/40/1

Device node(s) for 11/40/1: /dev/sdi

Is this the correct blank disk device? (yes/no) y

Device Path ID of source disk (e.g. 10/40/1 or 70/1): 10/40/1

Device node(s) for 10/40/1: /dev/sda

Is this the correct source disk device? (yes/no) y

Source disk is partitioned: partitioning blank disk to match.

Source disk partition 1 belongs to RAID 1 /dev/md0.

Adding blank disk partition 1 to RAID 1 /dev/md0.
mdadm: hot added /dev/sdi1
Source disk partition 2 belongs to RAID 1 /dev/md2.

Adding blank disk partition 2 to RAID 1 /dev/md2.
mdadm: hot added /dev/sdi2

Source disk partition 3 belongs to RAID 1 /dev/md1.

Adding blank disk partition 3 to RAID 1 /dev/md1.
mdadm: hot added /dev/sdi3

Waiting for resync to complete before grubbing /dev/sdi1.

Grubbing /dev/sdi1

Note that the /opt/ft/bin/duplex_blank_disk command creates the partitions and runs the grub boot loader on the boot partition of the replacement disk.
Replacing a Failed Disk (Manual Method)

If you cannot replace the disk while the system is running, perform the following steps:

- While the system is shut down, remove the defective disk and insert a spare disk.

  NOTE

  Replacement disks can be new disks or disks recycled from other systems. If the disk has been previously used, zero the spare disk after you boot the system and verify that the spare disk is not in use.

- Boot the system.
- Partition the spare disk to match the running disk.
- Add partitions on the spare disk to RAID-1 arrays.
- Run the grub boot loader (only if the running disk is the system disk).

The following procedures demonstrate how you replace the boot disk in CPU-I/O enclosure 11.

To verify that the spare disk is not in use

Type the following commands and check the resulting output:

```bash
# mdadm --detail --scan
# swapon -s
# cat /etc/mtab
```

To zero the spare disk

1. Zero the spare disk’s RAID superblocks by typing a command such as the following for each partition on the spare disk (substitute the device node of the partition for sdi1 in this example):

   ```bash
   # mdadm --zero-superblock /dev/sdi1
   ```

   NOTE

   Zeroing the disk’s RAID superblocks takes very little time but may not remove everything from the disk. If you are concerned about this, zero the entire disk as described in the following step.

2. Remove the partition table by typing a command such as the following (substitute the device node of the disk for sdi in this example):

   ```bash
   # dd if=/dev/zero of=/dev/sdi bs=512k count=1
   ```
To partition the spare disk to match the running disk

1. Save the partition table of the running disk to a file with a command such as:
   
   ```
   # sfdisk -d /dev/sda > sda_partition_table
   ```

2. Write the saved partition table to the spare disk with a command such as:
   
   ```
   # sfdisk /dev/sdi < sda_partition_table
   ```

Occasionally, `sfdisk` returns the following error while writing the saved partition table to the spare disk:

```
Checking that no-one is using this disk right now ... 
BLKRRPART: Input/output error
```

This error indicates that the disk is currently in use, so you should not partition it. Perform the following steps to correct this error:

1. Unmount all file systems.
2. Swap off all swap partitions on this disk.
3. Use the `--no-reread` flag to suppress this check.
4. Use the `--force` flag to overrule all checks.

**NOTE**

The preceding error does not occur if the spare disk already contained a valid partition table.

If you are sure that the spare disk is not in use, force `sfdisk` to write the partition table by using the `--no-reread` flag.

To add partitions on the spare disk to RAID-1 arrays

1. Type the following command to determine which RAID-1 arrays the running disk belongs to:
   
   ```
   # mdadm --detail --scan
   ARRAY /dev/md2 level=raid1 num-devices=2
   UUID=5ddb14c7:d5e0b2d6:ad80086d:8db2a245
devices=/dev/sda2
   ARRAY /dev/md1 level=raid1 num-devices=2
   UUID=3838df6e:60cafe7e:695d0f62:de94e821
devices=/dev/sda3
   ARRAY /dev/md0 level=raid1 num-devices=2
   UUID=3e4ad330:c8ee5dfc:f48bd88a:401ada25
devices=/dev/sdal
   ```
2. Add each partition on the spare disk to the RAID-1 array containing the corresponding partition on the running disk with commands like the following:

   # mdadm -a /dev/md0 /dev/sdi1
   mdadm: hot added /dev/sdi1

   # mdadm -a /dev/md1 /dev/sdi3
   mdadm: hot added /dev/sdi3

   # mdadm -a /dev/md2 /dev/sdi2
   mdadm: hot added /dev/sdi2

Perform the following procedure only if the running disk is the system disk.

To run grub

If the running disk is the system disk, run the grub boot loader on the boot partition of the spare disk, after resynchronization is complete on that partition. Example 3-2 shows a typical use of grub.

Example 3-2. Running grub

   # /sbin/grub
   GNU GRUB  version 0.95  (640K lower / 3072K upper memory)
   [ Minimal BASH-like line editing is supported. For the first word, TAB lists possible command completions. Anywhere else TAB lists the possible completions of a device/filename.]

   grub> device (hd0) /dev/sdi

   grub> root (hd0,0)
   Filesystem type is ext3fs, partition type 0xfd

   grub> setup (hd0)
   Checking if "/boot/grub/stage1" exists... no
   Checking if "/grub/stage1" exists... yes
   Checking if "/grub/stage2" exists... yes
   Checking if "/grub/e2fs_stage1_5" exists... yes
   Running "embed /grub/e2fs_stage1_5 (hd0)"... 16 sectors are embedded.
   succeeded
   Running "install /grub/stage1 (hd0) (hd0)1+16 p (hd0,0)/grub/stage2 /
   /grub/grub.conf"..
   . succeeded
   Done.
   grub> quit

On your own system, replace the /dev/sdi shown in Example 3-2 with the device node for your spare disk. In the root (hd0,0) command, the second zero is the number of the partition on which to load the boot loader. Because grub partitions are zero-based rather than one-based, these commands actually indicate that partition 1 on /dev/sdi has the boot loader.
Stopping a RAID Array and Moving It to Another System

1.Unmount the file system (if one is mounted) and stop the array by typing commands similar to the following:

```
# umount /dev/md30
# mdadm -S /dev/md30
```

2. Make sure that the RAID array no longer appears in `/proc/mdstat` file.

3. On the system from which you are removing the array, delete the entries for the array from the `/etc/fstab` and `/etc/mdadm.conf` files.

4. On the system to which you are moving the array, add entries for the array to the `/etc/fstab` and `/etc/mdadm.conf` files.

5. Start the RAID array. Type a command similar to the following:

```
# mdadm -A /dev/md30
```

**NOTE**

Never remove both member disks of a RAID-1 array. The Linux operating system does not support that operation.

Periodically Checking Disks

To periodically check or repair a disk, Red Hat Enterprise Linux uses the tool `/etc/cron.weekly/99-raid-check`. For a link to documentation of standard Linux tools, see “Red Hat Enterprise Linux” on page 1-5.

Using LVM

ftSSS imposes no specific restrictions on the use of Logical Volume Manager (LVM). However, for fault-tolerance, use LVM on internal-disk RAID arrays or external multipath devices.

Using ftScalable Storage Systems

ftServer systems also support external ftScalable Storage systems. See the following manuals for information about installing, configuring, monitoring, and administering ftScalable Storage systems:

- *ftScalable Storage: Getting Started Guide* (R601)
- *ftScalable Storage: Operation and Maintenance Guide* (R600)
- *ftScalable Storage: Commands Reference Manual* (R599)
Planning for System Backups and Disaster Recoveries

Your ftServer system provides many safeguards against losing data due to hardware failures. However, it is still important to perform regular backups and enact a good disaster-recovery program.

**CAUTION**

Do not perform full backups of the `/proc` or `/sys` file systems. Performing complete backups of the `/proc` or `/sys` file system (or the root), or otherwise indiscriminately reading files in those systems (for example, with the `cat` command) can cause a CPU element to be temporarily taken out of service. Back up required files or subtrees only, and use care in reading files in these file systems.

Using Device Names for the DVD Drive

An ftServer system supports one DVD drive, which may appear as the following device names when you list the contents of the `/dev` directory:

- When CPU-0, I/O-10 is active: `/dev/cdrom`, `/dev/cdrw`, `/dev/cdwriter`, `/dev/dvd`, `/dev/dvdrw`, `/dev/dvdwriter`, `/dev/scd0`
- When CPU-1, I/O-11 is active: `/dev/cdrom`, `/dev/cdrw`, `/dev/cdwriter`, `/dev/dvd`, `/dev/dvdrw`, `/dev/dvdwriter`, `/dev/scd1`

In the Computer browser, the drives appear as cdrecorder.

Using SAS Tape Drives

ftServer 2600, 4500, and 6300 systems with an installed U106 Eight-Port SAS PCI-Express Adapter support attachment of SAS tape drives.

Autoloader tape drives may require configuration into an operational mode that is fully addressable by applications through switch settings on the drive. The operation manual for the drive should provide you with needed configuration information.

SAS tape drives are addressable as `/dev/st*` devices. Miscellaneous SCSI devices such as scanners are generally mapped as `/dev/sg*` devices. The Linux operating system also allows some non-SCSI devices to be addressable as SCSI pseudo-devices. This can be useful in allowing certain SCSI software packages to work with non-SCSI devices.
Using USB Storage Devices

This section describes ftSSS support for USB devices in general, and specifically for the following USB storage devices:

- USB Floppy Drives
- USB Solid-State Devices

USB Support in ftSSS

USB storage devices, including floppy-disk, hard-disk, and solid-state storage, are supported through the SCSI driver. These devices appear as SCSI devices. You can get information about these devices by running the command `/usr/bin/lsscsi`.

When you connect a USB storage device to the USB bus, the SCSI driver scans it once and assigns a name (for example, `/dev/sd1`).

Use the following commands to find out the device name of a USB storage device, create a directory as the mount point, and mount the device:

```
# /usr/bin/lsscsi

[61:0:0:0] disk USB DISK 2.0 PMAP /dev/sdw
```

```
# mkdir /media/floppy
# mount /dev/sdw1 /media/floppy
```

The ftSSS installation disables the automounting of a USB storage device. To simplify the mounting process of these devices, you can put a record for a USB storage device in the `/etc/fstab` file, but use the `noauto` option.

⚠️ CAUTION

Remember to include the `noauto` option, or the system will fail to boot if the device is not present.

⚠️ CAUTION

Before removing the device, make sure that it is not being used. If a file system is mounted, unmount it (and make sure the `umount` command completes) before unplugging.
the device. The `umount` command flushes any buffered pages back to the device, so failing to wait for `umount` to complete can cause data corruption.

NOTES

1. An important consequence of the fact that the SCSI subsystem scans USB storage devices only on connection is that removing a disk from a drive does not cause a rescan. You must remove and reconnect the device to cause a rescan.

2. During failovers, access to USB storage devices is not robust.

3. If an AC switch occurs, some USB storage devices are not properly reset and disappear from `ftsmaint` output. To reset these devices, you must remove and reconnect the device.

4. When you remove and reconnect a device, the device name may change if the SCSI subsystem has added other devices while it was removed.

If the active CPU-I/O enclosure fails over to the other enclosure, a mounted USB disk-drive device may become unusable. If this happens, remove the device from the system and then insert it back in the system.

USB storage devices are not bootable devices.

Most floppy disks and solid-state devices come with a virtual file allocation table (VFAT) file system. You can create `ext-2` or other file systems on the device as well.

**USB Storage Devices**

A connected USB storage device appears as follows in `/proc/scsi/scsi` (as well as `/var/log/messages`).

```
Host: scsi2 Channel: 00 Id: 00 Lun: 00
Vendor: Model: USB DISK 2.0 Rev: PMAP
Type: Direct-Access ANSI SCSI revision: 02
```
The system log shows details about the device:

```
usb 1-4: new high speed USB device using ehci_hcd and address 4
usb 1-4: configuration #1 chosen from 1 choice
Initializing USB Mass Storage driver...
scsi2 : SCSI emulation for USB Mass Storage devices
usbcore: registered new driver usb-storage
USB Mass Storage support registered.
    Vendor: Model: USB DISK 2.0 Rev: PMAP
    Type: Direct-Access ANSI SCSI revision: 00
SCSI device sdq: 501760 512-byte hdwr sectors (257 MB)
sdq: Write Protect is off
sdq: assuming drive cache: write through
SCSI device sdq: 501760 512-byte hdwr sectors (257 MB)
sdq: Write Protect is off
sdq: assuming drive cache: write through
sdq: sdq1
sd 2:0:0:0: Attached scsi removable disk sdq
sd 2:0:0:0: Attached scsi generic sg17 type 0
```

**USB Solid-State Devices**

The following is an example of the `/proc/scsi/scsi` display for a solid-state device.

```
Host: scsi5 Channel: 00 Id: 00 Lun: 00
    Vendor: LEXAR    Model: JUMPDRIVE SECURE Rev: 3000
    Type:   Direct-Access                    ANSI SCSI revision: 02
```

The system log provides details about the device, including its size:

```
scsi5 : SCSI emulation for USB Mass Storage devices
    Vendor: LEXAR    Model: JUMPDRIVE SECURE Rev: 3000
    Type:   Direct-Access                    ANSI SCSI revision: 02
SCSI device sdaz: 506880 512-byte hdwr sectors (260 MB)
```

**Additional Resources**

*Linux Allocated Devices, LANANA*: [http://www.lanana.org/docs/device-list/devices.txt](http://www.lanana.org/docs/device-list/devices.txt)
ftSSS provides a special command interface, ftsmaint, for managing the fault-tolerant components of your ftServer system. It also includes a monitoring and diagnostic package, the ASN, that enables your ftServer system to interact with the Stratus ASN. When you configure the ASN on your ftServer system, the CAC can receive alarm notifications when faults or other significant events occur on your system, and can remotely diagnose problems.

This chapter discusses the following topics:

- “Using the ftsmaint Command” on page 4-1
- “Managing ASN Support” on page 4-12
- “Managing Kernel Memory Dump Files” on page 4-14

**Using the ftsmaint Command**

The /opt/ft/bin/ftsmaint command provides a control interface for managing your ftServer system’s fault-tolerant functions. For information about using the ftsmaint command and using device path enumeration to manage specific devices in your system, see the following sections:

- “ftsmaint Command Arguments” on page 4-1
- “ftsmaint Examples” on page 4-7

**ftsmaint Command Arguments**

The ftsmaint command arguments support both device query and management tasks. Some of the command arguments apply only to certain devices or systems, which you must specify following the command argument.

Most of the ftsmaint command task arguments require an enumerated hardware-specification argument, indicated by path in the command descriptions. You can view a list of valid hardware path values by typing the ftsmaint ls command. Any hardware path value shown in ftsmaint ls output can be used as a path...
argument. For example, the 10/2 path in the following command displays information about the PCI adapter in slot 2 of I/O element 10:

```
# /opt/ft/bin/ftsmaint ls 10/2
```

Some of the task arguments of most interest to a system administrator are as follows. For a full description of `ftsmaint`, see the `man` page.

- **`ftsmaint inventory [-c]`**
  This command displays complete device information for the purpose of ASN inventory reports. Default output is to `/var/tmp/inventory.out`, or standard output if you use `-c`.

- **`ftsmaint ls path`**
  This command displays the status of the hardware specified by the value of `path`. Specifying a path displays a detailed status of the hardware at that path. Omitting `path` displays a less-detailed table of all fault-tolerant devices on the system. See “Understanding Device Paths” on page 2-27 for information on device path values and “Displaying the Status of a Single System Component” on page 4-10 for examples of this command.

  Output from `ftsmaint ls path` reflects what the OSM reports about the state of a component. Because of system latency, the output may not reflect the immediate state of the device. However, you cannot, as a result of this discrepancy, issue a command that would take the system offline. (See `ftsmaint bringDown`.)

  To verify the actual state of the device, check the state of its LED.

- **`ftsmaint lsLong`**
  This command displays the status of all fault-tolerant devices on the ftServer system and the status of empty devices, such as unpopulated slots. This command also displays details about the BMC (which provides VTM functionality) at 10/120 or 11/120. This command is useful to study the addressable fault-tolerant devices that can be queried or controlled with ftSSS software.

- **`ftsmaint lsPeriph`**
  This command displays information about peripheral devices, such as the DVD drive and modem.

- **`ftsmaint lsSystem`**
  This command displays general information about the system, including the model number, part number, and serial number.
• **ftsmaint lsVND**
  This command displays the status (including the IP address) of the Ethernet channel-bonding interfaces in the ftServer system.

• **ftsmaint acSwitch [10 | 11]**
  If you do not specify the device path of an I/O element, this command toggles the active compatibility of the I/O elements between I/O element 10 and I/O element 11. For example, if I/O element 10 is the active (primary) element (the one with the PRIMARY system LED on), then issuing an acSwitch command makes I/O element 11 the active element. If you do specify an I/O element, it forces the specified enclosure to active compatibility status.

• **ftsmaint bringDown path**
  This command removes from service the CPU element, I/O element, or internal disk specified by *path*. No other devices are supported. When you bring down a device, the effect on the system is the same as physically removing it.

  **NOTE**
  The **ftsmaint bringDown** command will not permit you to bring down a device in a SIMPLEX state, because this would disable the system or make a resource unavailable.

• **ftsmaint bringUp path**
  This command brings into service the CPU element, I/O element, internal disk, or PCI slot specified by *path*. No other devices are supported.

• **ftsmaint bringUpPolicy cpu_policy**
  This command either displays the current bringup policy or it changes the CPU bringup policy to *cpu_policy*, if specified.

• **ftsmaint burnProm fw_file path**
  This command updates the firmware contained in the file *fw_file* into one EPROM device, which is specified by *path*. This command can be used to update only BMC and BIOS firmware.

• **ftsmaint dump path**
  This command creates a dump of the CPU element specified in the *path* argument. A CPU dump is stored in the
  `/var/crash/YYYY-MM-DD-hh:mm/vmcore`, where *nn* indicates a device path.
Using the *ftsmaint* Command

- **ftsmaint identify [start|stop] path**
  This command starts or stops the LEDs on the device specified by *path*. The device can be a CPU element, an I/O element, or an internal disk.

- **ftsmaint jumpSwitch path**
  This command transfers processing to the CPU element specified by *path*, making that CPU-I/O enclosure the primary enclosure.

  See Table 2-4 for *path* values for these devices.

- **ftsmaint memCheck**
  This command tests the integrity of the system’s memory.

- **ftsmaint runDiag path**
  This command starts diagnostics on the CPU element or I/O element specified by *path*.

- **ftsmaint setPriority level path**
  This command sets the priority level (high, mid, or low) of the CPU element specified by *path* to the value in the *level* argument.

- **ftsmaint -version**
  This command returns the build number of the *ftsmaint* command on your system. This number coincides with the build number of ftSSS installed on the system.

The following *ftsmaint* command arguments allow you to monitor and manage the ASN, the BMC, and the VTMs:

- **ftsmaint lsVtmConfig path**
  This command displays VTM settings (including the VTM network address), as specified in *path* (10/120 or 11/120).

- **ftsmaint showVtmConfig**
  This command displays the BMC configuration, as it exists on the local disk.

- **ftsmaint renewVtmDhcp**
  This command releases and renews Ethernet IP addresses for both BMCs. This command requires root access.

- **ftsmaint showAsnConfig**
  This command displays the ASN configuration, as it exists on the local disk.
• **ftsmaint burnBmcs file**
  This command uses the firmware file `file` to burn firmware on both BMCs. This command requires root access.

The following **ftsmaint** command arguments allow you to control the modem:

• **ftsmaint powerOn modem**
  This command supplies electrical power to the modem.

• **ftsmaint powerOff modem**
  This command removes electrical power from the modem.

• **ftsmaint resetModem**
  This command restores modem settings to their factory default values.

• **ftsmaint takeModem**
  This command transfers control of the modem from the BMC to the host. The **ftsmaint** alias for `takeModem` is `modem2host`. This command requires root access.

• **ftsmaint giveModem**
  This command transfers control of the modem from the host to the BMC. The **ftsmaint** alias for `giveModem` is `modem2bmc`. This command requires root access.

The BMC controls the modem until one of the following occurs:

- `takeModem` is issued
- 10 minutes elapses and no connection is established.

  The 10-minute timeout period starts when `giveModem` is issued, so if an active connection is not established within 10 minutes, control reverts to the host.

  The 10-minute timeout starts again when a successful modem connection to the BMC is terminated. So if a connection is established and closed within 10 minutes, and then a second connection is attempted, the 10-minute timeout period begins again at the second connection attempt.

• **ftsmaint modemStatus**
  This command displays the current owner of the modem, the host or the BMC.
The following additional `ftsmaint` command arguments allow you to modify factory presets for sensors and MTBF (for an explanation of MTBF, see the *Stratus ftServer Systems: Technical Reference Guide* (R550)):

**CAUTION**

Do not modify these settings unless instructed to do so by the CAC or your authorized Stratus service representative, as doing so may affect the fault tolerance of your system.

- **ftsmaint clearMtbf path**
  This command clears the MTBF value of the CPU element, I/O element, internal disk, or PCI slot specified by `path`.

- **ftsmaint resetMtbf path**
  This command resets the MTBF value of the CPU element, I/O element, internal disk, or PCI slot specified by `path`.

**NOTE**

Do not use this feature to retain a faulty or degraded device in service. It may be useful if the MTBF for a device has been degraded by testing or configuration error.

- **ftsmaint setMtbfThresh evict|replace fault-class value path**
  This command sets the eviction or replacement MTBF threshold for fault class (specified by `fault-class`) of the CPU element, I/O element, internal disk, or PCI slot specified by `path` to `value`. To determine values for `fault-class` and `value`, use `ftsmaint ls path`.

- **ftsmaint setMtbfMinFaults fault-class count path**
  This command sets the MTBF minimum fault count (specified by `count`) for fault class (specified by `fault-class`) of the CPU element, I/O element, internal disk, or PCI slot, as specified by `path`. To determine values for `fault-class` and `count`, use `ftsmaint ls path`. 
• ftsmaint setMtbfType policy path
This command sets the MTBF type to policy on the CPU element, I/O element, internal disk, or PCI slot. Values of the policy argument are as follows:

- useThreshold
- neverRestart
- alwaysRestart

• ftsmaint setSensorThresh th_name value path
This command sets the threshold specified by th_name on the sensor device specified by path to value. The th_name argument can take one of the following values:

- uf (upper fatal)
- uc (upper critical)
- unc (upper noncritical)
- lf (lower fatal)
- lc (lower critical)
- lnc (lower noncritical)

The operational states for the sensors are as follows:

- Fatal: above uf or below lf
- Critical: above uc or below lc
- Warning: above unc or below unc
- Normal: default

ftsmaint Examples
The following sections provide examples of how to use the ftsmaint command:

• “Displaying System Status”
• “State (State) and Operation State (OP State) Values” on page 4-10
• “Displaying the Status of a Single System Component” on page 4-10
• “Bringing System Components Down and Up” on page 4-12

Displaying System Status
To display the status of the fault-tolerant devices and subsystems in your ftServer system, type the following command:

# ftsmaint ls
Example 4-1 shows sample output from the command.

Example 4-1. Displaying System Status with the ftsmaint ls Command

```
# ftsmaint ls
```

<table>
<thead>
<tr>
<th>H/W Path</th>
<th>Description</th>
<th>State</th>
<th>OPState</th>
<th>FRev</th>
<th>Fct</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Combined CPU/IO</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>*</td>
<td>2</td>
</tr>
<tr>
<td>0/0</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/1</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/2</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/3</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/4</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/5</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/6</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/7</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/8</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/9</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/10</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/11</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/12</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/21</td>
<td>Intel(R) Xeon(R) CPU E5504 @ 2.00GHz</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/130</td>
<td>Baseboard Temp#0 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/140</td>
<td>Baseboard Fan1#0 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/141</td>
<td>Baseboard Fan2#0 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/142</td>
<td>Baseboard Fan3#0 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/143</td>
<td>Baseboard Fan4#0 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0/144</td>
<td>Baseboard Fan5#0 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>Combined CPU/IO</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>*</td>
<td>0</td>
</tr>
<tr>
<td>1/1</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/2</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/3</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/4</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/5</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/6</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/7</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/8</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/9</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/10</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/11</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/12</td>
<td>DIMM</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/21</td>
<td>Intel(R) Xeon(R) CPU E5504 @ 2.00GHz</td>
<td>ONLINE</td>
<td>ONLINE</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/130</td>
<td>Baseboard Temp#1 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/140</td>
<td>Baseboard Fan1#1 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/141</td>
<td>Baseboard Fan2#1 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/142</td>
<td>Baseboard Fan3#1 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/143</td>
<td>Baseboard Fan4#1 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/144</td>
<td>Baseboard Fan5#1 Sensor</td>
<td>-</td>
<td>NORMAL</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>Combined CPU/IO</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>10/1</td>
<td>-</td>
<td>MISSING</td>
<td>EMPTY</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10/2</td>
<td>-</td>
<td>MISSING</td>
<td>EMPTY</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10/5</td>
<td>Mass Storage Ctrlr</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>05:00.0</td>
<td>SCSI storage controller: LSI Logic / Symb</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

(Continued on next page)
### Using the ftsmaint Command

10/6  Network Ctrlr ONLINE DUPLEX - 0
0b:00.0 Ethernet controller: Intel Corporation 82 ONLINE DUPLEX - -
eth100600 Network Interface ONLINE DUPLEX - -
0b:00.1 Ethernet controller: Intel Corporation 82 ONLINE DUPLEX - -
eth100601 Network Interface ONLINE DUPLEX - -
10/7  Display Ctrlr ONLINE DUPLEX - 0
0c:00.0 VGA compatible controller: Matrox Graphic ONLINE DUPLEX - -
10/8  Serial Bus Ctrlrs ONLINE ONLINE - 0
0a:1a.0 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
0a:1a.7 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
10/9  Serial Bus Ctrlrs ONLINE ONLINE - 0
0a:1d.0 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
0a:1d.1 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
0a:1d.2 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
0a:1d.7 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
10/10 Bridge ONLINE ONLINE - 0
10/40 Internal Disk Enclosure - - - -
10/40/1 Disk Drive ONLINE DUPLEX 0004 0
10/70 2x PCI-X Riser Card - - - -
10/120 Baseboard Management Ctrlr ONLINE DUPLEX * -
11     Combined CPU/IO ONLINE DUPLEX - 0
11/1  - MISSING EMPTY - -
11/2  - MISSING EMPTY - -
11/5  Mass Storage Ctrlr ONLINE DUPLEX - 0
3f:00.0 SCSI storage controller: LSI Logic / Symb ONLINE DUPLEX - -
11/6  Network Ctrlr ONLINE DUPLEX - 0
45:00.0 Ethernet controller: Intel Corporation 82 ONLINE DUPLEX - -
eth110600 Network Interface ONLINE DUPLEX - -
45:00.1 Ethernet controller: Intel Corporation 82 ONLINE DUPLEX - -
eth110601 Network Interface ONLINE DUPLEX - -
11/7  Display Ctrlr ONLINE DUPLEX - 0
46:00.0 VGA compatible controller: Matrox Graphic ONLINE DUPLEX - -
11/8  Serial Bus Ctrlrs ONLINE ONLINE - 0
44:1a.0 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
44:1a.7 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
11/9  Serial Bus Ctrlrs ONLINE ONLINE - 0
44:1d.0 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
44:1d.1 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
44:1d.2 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
44:1d.7 USB Controller: Intel Corporation 82801JI ONLINE ONLINE - -
11/10 Bridge ONLINE ONLINE - 0
11/40 Internal Disk Enclosure - - - -
11/40/1 Disk Drive ONLINE DUPLEX 0005 0
11/70 2x PCI-X Riser Card - - - -
11/120 Baseboard Management Ctrlr ONLINE DUPLEX * -

IO Enclosure 10 is the Active Compatibility Node.

This is an ftServer 4500 system, P-Package P4500-2S, Serial# 5000000945.

* Use lsLong to see this value.
State (State) and Operation State (OP State) Values

Table A-2 describes the values that are used in the State and OP State columns.

Displaying the Status of a Single System Component

Before you remove a component that is duplexed for fault tolerance, verify that it is not in a simplex state. To verify the state of a component, type a command in the following format:

```
# ftsmaint ls path
```

For path, specify the correct value for the component, as listed in Table 2-4.

The value of Op State specifies whether the device is in a simplex state. The value is generally either DUPLEX or SIMPLEX.

The following lists some example commands and the resulting output.

In Example 4-2, the bottom I/O element is listed as having a State of ONLINE and an OP State of DUPLEX. The value of SECONDARY for Reason indicates that it is operating as the backup I/O element.

Example 4-2. Viewing the State of the Bottom I/O Element

```
# ftsmaint ls 11
H/W Path                 : 11
Description              : Combined CPU/IO
State                    : ONLINE
Op State                 : DUPLEX
Reason                   : SECONDARY
Modelx                   : 062-02800
Artwork Rev              : 0
ECO Level                : 0
Min Partner ECO Level    : 0
Serial #                 : 2AK050007
Active Compat Node       : false
Logic Revision           : 364
MTBF Policy             : useThreshold
MTBF Fault Class: uncorrectable
Fault Count: 0
Last Timestamp: -
Replace Threshold: 0
Evict Threshold: 7889400
Value: 0
Minimum Count: 4
```
In Example 4-3, the disk in the left-most top slot of the top enclosure is listed as having a State of ONLINE and an Op State of DUPLEX.

**Example 4-3. Viewing the State of Disk sda**

```
# ftsmaint ls 10/40/1
H/W Path : 10/40/1
Description : Disk Drive
State : ONLINE
Op State : DUPLEX
Reason : NONE
Modelx : SEAGATE:ST973451SS
Firmware Rev : 0005
Serial #: 3PD1ZMJA00009909LNTT
Device Name : disk_a
Udev Device Names : /dev/sda
Kernel Device Names : sdq
MTBF Policy : useThreshold
MTBF fault class: critical noncritical
Fault Count: 0 0
Last Timestamp: -
Replace Threshold : 0 0
Evict Threshold : 2147483647 604800
Value: 0 0
Minimum Count: 1 4
```

**Displaying System Status**

If you are located remotely from the ftServer system, you can view the state of LEDs on some components. To view the state of a component’s LEDs, type a command in the format `ftsmaint ls path`. For example, to view the state of the modem, type the command in Example 4-4.

**Example 4-4. Viewing the State of the Modem LEDs**

```
# ftsmaint ls modem
Present : True
Power : True
Attention : False
Identify : False
Reset Held : False
Power Fault : False
Owner : Host
```

In addition, LED s on the system report the overall operational status of the system. For information on these LEDs, see the operation and maintenance guide for your system, as listed in Table 1-1.
Managing ASN Support

You can also view the status of the system remotely using the VTM console. For information, see Stratus ftServer System Software: Installation for Linux Systems (R013L) and the Stratus ftServer Virtual Technician Module User’s Guide (R642).

Bringing System Components Down and Up

You can use the ftsmaint command to bring down and restart a fault-tolerant subsystem. After bringing up a system, it attempts to synchronize and duplex the corresponding components automatically.

To take the bottom I/O element out of service and then bring it back into service, type the following commands:

```
# /opt/ft/bin/ftsmaint bringDown 11
# /opt/ft/bin/ftsmaint bringUp 11
```

**NOTE**

Before removing a component that is duplexed for fault tolerance, verify that it is not in a simplex state. See “Displaying the Status of a Single System Component” on page 4-10.

When you issue the bringUp command and all the system components are healthy, the CPU elements return to lockstep, the internal disks resynchronize, and the system resumes duplex operation.

Managing ASN Support

The ASN enables the CAC to provide remote monitoring, diagnosis, troubleshooting, and problem-resolution services to your systems over a secure network. With ASN connectivity, your system can send alerts (call-home alarm messages) to the CAC when unusual events occur on the system. If the operating system is not running or is not responding, the VTM can connect through its own network port or the modem. After verifying a hardware problem, your authorized Stratus service representative can send out a replacement CRU.

Access to the ASN requires a service contract with Stratus or an authorized Stratus service representative. For information on setting up ASN on your system, see Stratus ftServer System Software: Installation for Linux Systems (R013L). For information on configuring your system for ASN support on the Stratus ASN Web site, see the Stratus ActiveService Network Configuration Guide (R072).
Your system can connect to the ASN through:

- A network port, if Internet access is available—Internet-based ASN connects over a secure path to your authorized Stratus service representative. Internet connectivity provides faster, more reliable connections than a dialup modem.
- A modem, if installed

NOTES

1. Do not use the ASN modem for other purposes. The ASN provides continuous system monitoring. It requires dedicated assignment to a system serial port, as well as a dedicated modem and telephone line for switched line communications.

2. A dedicated phone line provides the most reliable service for the modem. ASN calls routed through a PBX may be slow due to load on the PBX, or may not complete successfully due to disconnections. If you must use a PBX, do not route the telephone extension through a switchboard; instead, provide a direct-dial analog number.

ASN software includes the **ft-sra_asn** service, which controls the **sra_alarm** and **sra_ras** daemons. These daemons generate alarm messages.

NOTE

The **sra_alarm** and **sra_ras** services will not run until the ASN is configured.

ASN logging appends event messages to the system log file by default (which is `/var/log/messages`, by default).

The **sra_alarm** daemon passes **libft** events to **libASNAlarm.so**, which matches state and reason codes of the event record against an internal list that is generated using `/etc/opt/ft/asn/sra_alarm/ASN_Alarm_Config`. If an operational state (opstate) and reason combination is set to generate an alarm, an ASN alarm will be generated.

Table 4-1 specifies the commands, which vary by release, that manage ASN services.
Table 4-1. Managing ASN Services

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To check the status of running ASN services</td>
<td>service ft-sra_asn status</td>
</tr>
<tr>
<td>To stop ASN services</td>
<td>service ft-sra_asn stop</td>
</tr>
<tr>
<td>To start ASN services</td>
<td>service ft-sra_asn start</td>
</tr>
<tr>
<td>To restart ASN services</td>
<td>service ft-sra_asn restart</td>
</tr>
</tbody>
</table>

To reinstall ASN on your ftServer system

1. Remove ASN by typing the following command:
   
   `rpm -e lsb-ft-asn`


   Type **YES** when the prompt asks if you want to install ASN.

Managing Kernel Memory Dump Files

**CAUTION**

To ensure that the ftServer dumping mechanism works successfully, do not enable Diskdump or Netdump. Diskdump or Netdump can interfere with the completion of an ftServer dump.

At the time of a crash, the system creates a memory dump. After the system restarts, the dump is automatically written in a compressed format to a disk file in

/var/crash/YYYY-MM-DD-HH:mm:ss/vmcore, and an alert is logged to the ASN. When the ASN starts, it reads its notification log, and when the system reaches run level 3 or 5, it files an alert to the ASN server to which it is configured to report. If authorized, the CAC can log into the system and obtain the dump file for analysis if required. Or, you can send the dump file to them.

It is important that you monitor and maintain sufficient free space in the /var/crash directory. Back up old crash dump data before deleting it.
Chapter 5
Simple Network Management
Using Net-SNMP and ftlSNMP

This chapter describes Simple Network Management Protocol (SNMP) for ftServer systems, ftlSNMP. After describing ftlSNMP installation and configuration, this chapter introduces SNMP concepts, for administrators who are new to SNMP. If you are reading this chapter for the first time, you should first read Release Notes: Stratus ftServer System Software for the Linux Operating System (R005L).

This chapter discusses the following topics:

- “Installing and Configuring ftlSNMP” on page 5-1
- “SNMP Foundations and Concepts” on page 5-6
- “Installing Remote Network Management Services” on page 5-13
- “Managing SNMP” on page 5-16
- “SNMP and MIBS” on page 5-22
- “SNMP Network Management Station Considerations” on page 5-22
- “Initial SNMP Testing” on page 5-23
- “Trap Filtering” on page 5-26
- “Removing ftlSNMP” on page 5-36

Installing and Configuring ftlSNMP

When installing ftSSS, you have the option of installing ftlSNMP. If you choose not to install ftlSNMP when you install ftSSS, you can install it later by rerunning the ftSSS installation program and selecting to install ftlSNMP. Installing ftlSNMP this way will not reinstall packages already installed on the system, and therefore not affect unrelated configurations.
On ftServer systems running a supported Linux distribution together with ftSSS, SNMP is composed of two separate packages:

- **Net-SNMP** (*net-snmp*), which is installed during the Linux operating system installation. SNMP is a widely used protocol for monitoring network equipment (for example, routers), computer equipment, and devices such as uninterruptible power supplies (UPS). Net-SNMP is a suite of applications used to implement SNMP v1, SNMP v2c, and SNMP v3 using both IPv4 and IPv6. This suite includes:
  - Various command-line applications for retrieving, manipulating, converting, and displaying information
  - A daemon application for receiving SNMP notifications
  - An extensible agent for responding to SNMP queries for management information
  - A library for developing new SNMP applications

See [www.net-snmp.org](http://www.net-snmp.org) for more information about Net-SNMP.

- **ftlSNMP** (*lsb-ft-snmp*), which is installed with ftSSS. The ftlSNMP package consists of the following components:
  - **SRA-ftLinux-MIB**—This MIB supports ftServer’s fault-tolerant hardware.
  - **ftlsubagent**—This subagent supports SRA-ftLinux-MIB SNMP GET and SET operations.
  - **ftltrapsubagent**—This subagent supports SRA-ftLinux-MIB traps.
  - Various startup, restart, and shutdown scripts
  - Man pages

ftlSNMP binaries are built with performance optimizations for use with the Net-SNMP version in the supported release of the Linux operating system. The *Release Notes: Stratus ftServer System Software for the Linux Operating System* (R005L) describes the supported release of the Linux operating system.

**ftlSNMP Distribution**

This ftlSNMP distribution is provided as a single binary RPM package on the ftSSS distribution named *lsb-ft-snmp-7.0.4-nnn.x86_64.rpm*, where *nnn* is the ftServer build number.

Files in the ftlSNMP package are located in the following directories:

- `/etc/opt/ft/snmp`—Contains the fault-tolerant subagent configuration templates and the Net-SNMP master agent configuration template.
Installing and Configuring ftlSNMP

Simple Network Management Using Net-SNMP and ftlSNMP

5-3

- /etc/opt/ft/snmp/scripts—Contains the start, stop, and restart scripts.
- /opt/ft/doc/lsb-ft-snmp-n.n.n—Contains the ftlSNMP README file.
- /opt/ft/mibs—Contains the ftServer SRA-ftLinux-MIB file.
- /opt/ft/sbin—Contains the ftServer fault-tolerant subagents (ftlsubagent and ftltrapsubagent).
- /opt/ft/share/man/en/man8—Contains the man pages for the fault-tolerant subagent.

Configuring ftlSNMP

To configure ftlSNMP, edit the following files:

- /etc/opt/ft/snmp/snmpd.conf (see “The snmpd.conf File” on page 5-3 and snmpd.conf(5))

**NOTE**

The ftSSS installation automatically creates snmpd.conf in the /etc/opt/ft/snmp directory, while Net-SNMP creates it in the /etc/snmp directory. You should use the /etc/opt/ft/snmp version because it is the directory that the ftlSNMP scripts reference.

- /etc/opt/ft/snmp/ftlsubagent.conf (see “The ftlsubagent.conf and ftltrapsubagent.conf Files” on page 5-4)
- /etc/opt/ft/snmp/ftltrapsubagent.conf (see “The ftlsubagent.conf and ftltrapsubagent.conf Files” on page 5-4)

These files are created when you install or upgrade ftlSNMP, provided that they do not already exist. If they already exist, installing or upgrading ftlSNMP does not overwrite them. Use the information in the template files (for example, /etc/opt/ft/snmp/snmpd.conf.template) as a guide when editing the files. However, values of parameters to be set in these files are system-, network-, and SNMP-manager specific.

**The snmpd.conf File**

ftlSNMP requires agentX services. Therefore, keep the following two lines at the end of the snmpd.conf file:

```
master agentx
agentxTimeout 60
```

To avoid timeouts when the subagents are running under abnormal system stress (for example, 80% CPU usage and disks heavily stressed), raise the value of
agentxTimeout, which specifies a number of seconds. If a timeout occurs, there will be a short delay while the subagents reinitialize their communications.

The ftlsubagent.conf and ftltrapsubagent.conf Files

These files require no editing for default operation, but you may want to adjust logging. You can change the trace level from off to brief or verbose as desired, or as suggested by the CAC to aid in diagnosing any problems. Debugging information will be logged.

These files contain the following configuration lines:

- sraTraceLevel off
- sraTraceLog /var/opt/ft/log/ftlsubagents.log

With sraTraceLevel set to brief, data flows to and from ftlSNMP external items are traced. With sraTraceLevel set to verbose, internal items are also traced. You can also change the location of the log file.

Agent and subagent startup and shutdown events are logged separately in syslog.

With trace levels other than off, logs may grow rapidly (depending on the number of managed objects and their activity). In order to limit the size of the logs, you can use logrotate to manage log size and archiving. See logrotate(8).

Configuring SNMP to Start at System Initialization

The ft-snmp initialization script is installed from the lsb-ft-snmp package to the /etc/init.d directory, and the ft-snmp service is added. During system initialization, the ft-snmp service is automatically started at run level 3, 4, or 5. This initialization script provides start, stop, restart, and status functionality.

**NOTE**

- ft-snmp service replaces the snmpd service provided by the Linux operating system, which is disabled when ft-snmp is used. Do not enable the snmpd service provided by the Linux operating system.

Configuring SNMP for Service Management

To use SNMP securely, you need to create an SNMPv3 user account. SNMPv3 user accounts allow local and remote access to SNMP services.

Use an SNMPv3 user account when the manager and master agent are on separate networks.
CAUTION

Failure to use SNMPv3 when communicating over a public network is a server and network security risk.

SNMP V3 includes true authentication and encryption. The three authentication models are NoAuthNoPriv, authNoPriv, and authPriv. Note that you must have auth status for encryption.

An SNMP engine identifier takes the first IP address as the default that identifies the agent in the device. Each device must have a user login account for the device.

SNMPv3 also has concepts of groups, views, and privileges for access control. These are referred to as the view-based access control model (VACM) and user-based security model (USM).

The following procedure demonstrates how to create an SNMPv3 user account and includes some values that you can change to suit your requirements.

To create an SNMPv3 user

1. Stop SNMP services by typing the following command:

   ```
   # service ft-snmp stop
   ```

2. Edit `/etc/opt/ft/snmp/snmpd.conf`, and add the following lines:

   ```
   rwuser admin
   rwuser v3user
   createUser admin MD5 AdminPassword DES
   group v3usergroup usm admin
   group v3usergroup usm v3user
   view v3view included .1.3.6.1
   access v3usergroup "" usm authNoPriv exact v3view v3view v3view
   ```

3. Start SNMP services by typing the following command:

   ```
   # service ft-snmp start
   ```

4. Clone the newly created admin user to a new v3user user by typing the following command:

   ```
   # snmpusm -v3 -u admin -n "" -l authNoPriv -a MD5 -A AdminPassword localhost create v3user admin
   ```
5. Change the v3user user's authentication and encryption passwords by typing the following command:

```
# snmpusm -v3 -u v3user -x DES -n "" -l authNoPriv -a MD5 -A AdminPassword localhost passwd AdminPassword NewPassword
```

These commands clone an initial (template) SNMPv3 user account, admin, as a v3user user account, and then change the password of v3user user account.

When you run `start_snmp`, you can use this v3user user name and its password in SNMPv3 `snmpwalk` and `snmpget` commands, as shown in the following example:

```
# snmpwalk -v 3 -t 40 -l authNoPriv -u v3user -A NewPassword -x DES localhost 1.3.6.1.4.1.458
```

### SNMP Foundations and Concepts

The Net-SNMP and ftlSNMP packages support the SNMP protocol and many of the capabilities of SNMP for managing network objects using protocols and interface features described in numerous Internet Engineering Task Force (IETF) documents. Net-SNMP and ftlSNMP are packages for network administration that compatibly support ftServer fault-tolerant operations using standard network communications. There are few network administration tools available that readily support fault-tolerant capabilities of networked systems and devices. ftlSNMP allows ftServer systems to be monitored and managed by any remote-networked system running SNMP-based network management software.

Net-SNMP provides a functional network administration package for use on ftServer systems to meet identified customer needs. ftlSNMP is a unique extension of Net-SNMP that provides the SRA-ftLinux-MIB to define manageable systems and components of ftServer Linux-based systems. ftServer subagents and an accompanying MIB provide SNMP support and services for fault-tolerant operations.

### ftlSNMP Management Commands

To start `ftl-snmp`, type the following command:

```
# service ft-snmp start
```

To stop `ftl-snmp`, type the following command:

```
# service ft-snmp stop
```

To stop and then restart `ftl-snmp`, type the following command:

```
# service ft-snmp restart
```
Use the preceding commands for most situations. The following commands are also available to deal with special situations.

**CAUTION**

However, you should **not** normally use them except under the guidance of the CAC, as starting and stopping agents in untested order can have unforeseen consequences.

- **start_all_subagents, stop_all_subagents, restart_all_subagents**—These commands start, stop, and restart only the subagents.
- **start_ftlsubagent, stop_ftlsubagent, restart_ftlsubagent**—These commands start, stop, and restart only ftlsubagent.
- **start_ftltrapsubagent, stop_ftltrapsubagent, restart_ftltrapsubagent**—These commands start, stop, and restart only ftltrapsubagent.
- **start_snmp_daemon, stop_snmp_daemon, restart_snmp_daemon**—These commands start, stop, and restart only snmp_daemon (the master agent).

**The Basic Net-SNMP Commands**

These tools provide a basic set of features for exercising and managing objects using a standard command syntax and core functionality:

**NOTE**

Although these commands are documented as user commands (man (1)), you should treat SNMP utilities as the administrative tools they are, and closely limit privileges to execute these commands.

- **snmpwalk**—This command uses SNMP GETNEXT requests to query a network entity for a tree of information that maps the managed objects by object ID hierarchically. See snmpwalk(1). While this can return much information, take care not to use this command on a heavily loaded network, since it can add significantly to traffic.
- **snmpget**—This command queries a single SNMP object using an SNMP GET request. See snmpget(1).
- **snmpgetnext**—This command uses GETNEXT requests to query network entities for information.
- **snmpgetbulk**—This command uses the SNMP GETBULK request to query a network entity for quantities of information. See snmpgetbulk(1).
• **snmpdf**—This command replicates `df` command functionality on a network-accessible drive. The `snmpdf` command checks disk space on the remote machine by examining the system's `HOST-RESOURCES-MIB hrStorageTable`, or a UCD-SNMP-MIB `dskTable` value. See `snmpdf(1)`.

• **snmpstatus**—This command queries a network entity to retrieve significant information about a communicating object. See `snmpstatus(1)`. The following information is retrieved:
  - The IP address of the entity.
  - A textual description of the entity (`sysDescr.0`)
  - The uptime of the entity's SNMP agent (`sysUpTime.0`)
  - The sum of received packets on interfaces (`ifInUCastPkts.* + ifInNUCastPkts.*`)
  - The sum of transmitted interface packets (`ifOutUCastPkts.* + ifOutNUCastPkts.*`)
  - The number of IP input packets (`ipInReceives.0`)
  - The number of IP output packets (`ipOutRequests.0`)

• **snmptranslate**—This command converts object ID values into more easily understood forms. See `snmptranslate(1)`.

• **snmptable**—This command repeatedly uses SNMP `GETNEXT` or `GETBULK` requests to get information on a network entity, which is specified as, and must be mapped by, a table. See `snmptable(1)`.

• **snmpset**—This command uses the SNMP `SET` request to control, or set information on, a network entity. See `snmpset(1)`.

• **snmptrap**—This command uses the SNMP `TRAP` operation to send information to a network manager when a trigger condition is met. See `snmptrap(8)`.

• **snmpinform**—This command essentially works like `snmptrap`, but uses a different form of signal, and can require a response in order to suppress resending. See `snmptrap(1)`.

• **snmptest**—This command is a flexible test utility that can send a variety of signals and retrieve a variety of information. It is best used within shell scripts that can hide its complexity and focus on particular test queries. See `snmptest(1)`.

• **snmpnetstat**—This command is a powerful data retrieval tool to query a remote system and retrieve a variety of information about communications objects. See `snmpnetstat(1)`.

• **snmpdelta**—This command is a tool used to monitor values of a network object over time, and respond if the values deviate from established parameters. See `snmpdelta(1)`.
MIBs

A management information base (MIB) uses ISO Abstract Syntax Notation 1 to assign a unique object identifier to any object to be managed by SNMP. This syntax is a hierarchical model that is intended to provide unique object identification. Under this notation, there is conceptually only one true MIB; everything fits within it. To the extent that developers observe syntactic standards, various MIB definitions will not conflict, because a MIB should use only unique identifiers. Thus Net-SNMP and other SNMP implementations allow a large number of MIBs to be loaded from various paths at initialization, under the presumption that all identifications are unique. In current standard SNMP implementations, at least the IETF MIB-II definitions supporting RFC1213 must be used. RFC1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II can be downloaded from the IETF Web site.

SNMPv1 MIBs supported only strings of data, but later MIBs typically use a columnar layout of information that can be easily manipulated by a scripting language that handles textual data, such as Perl. The supplied MIBs are stored in the /opt/ft/mibs and /usr/share/snmp/mibs directories in the default search path.

NOTE

The ftSSS installation automatically creates the SRA-ftLinux-MIB file in the /opt/ft/mibs directory, while Net-SNMP creates its MIBs in the /usr/share/snmp/mibs directory.

MIBs can be stored in a variety of locations, but running SNMP agents must still be directed to the location of a MIB the first time it is to be used, if the MIB is added after the agents have already started.

If the MIB was not in the path when the SNMP services were started (and SRA-ftLinux-MIB exported), the following example shows how to identify the SRA-ftLinux-MIB file to the SNMP tools:

```
# snmpget -m SRA-ftLinux-MIB -v 2c -c public myhost.com ftcBdState.1
SRA-ftLinux-MIB::ftcBdState.1 = INTEGER: duplex(21)
```

As you begin to develop your own MIB (or MIBs) for your management requirements, you can save a lot of work by adopting defined variables from other MIBs. A large number of MIBs are defined by the IETF and are available as plain text files. You should use standardized MIBs where they define objects to avoid non-standard implementation of networked objects.
Do not change standard MIBs. If you need additional object definitions, you can add another MIB or create your own. The MIB-defined objects can be queried and data recovered that provides a basis for SNMP agent operations. You can create scripts that the SNMP agent or a subagent executes according to MIB definitions.

Some Objects Defined by Standard MIBs

For a practical implementation of SNMP, a number of objects simply must be defined. Some of these are introduced here.

For UDP or TCP/IP communications and collection of statistical data about communications and communications channels, MIB-II defines some necessary objects. MIB-II defines these objects for querying:

```
  system
  interfaces
  at
  ip
  icmp
  tcp
  udp
  snmp
```

The Net-SNMP implementation requires basic support of the Host Resources MIB. The objects defined in RFC1514 Host Resources MIB include:

```
  hrSystem
  hrStorage
  hrDevice
  hrSWRun
  hrSWRunPerf
  hrSWininstalled
  hrSWRunID
```

**NOTE**

A Host Resources MIB should support these objects, which are defined in RFC1514. A Newer Host Resources MIB may comply with RFC2790, which extends and replaces RFC1514. The Net-SNMP Host Resources MIB implementation has been tested for the RFC1514 features.
The Net-SNMP package also implements the Net-SNMP version of the UCD Extensions MIB, which defines these objects:

- prTable
- memory
- laTable
- systemStats
- fileTable

**SNMPv3 Support**

SNMPv3 support includes implementation of IETF RFCs 3410 through 3418. The third version of the Simple Network Management Protocol, presented by the IETF as the Internet Standard Management Framework RFC3410, SNMPv3 incorporates elements of SNMPv1 and SNMPv2, and shares the same basic modular architecture. This framework consists of four structures: a data definition language (SMIv1), a management information base (MIB) defining management information, a separately defined communication protocol, and security and administration applications and engines.

Features of SNMP version 1, SNMP version 2, and SNMP version 3 are not mutually exclusive. IETF Best Current Practices 74 (BCP74) describes how to implement these protocols compatibly on networks and on internetworked environments so that objects can be managed using the least sophisticated protocol required. In this way, networked and internetworked objects may be managed using SNMPv1, for example, without becoming obsoleted if the network is commingled into a larger network where objects are managed using SNMPv2 or SNMPv3.

This is necessary because the SNMP schema treats all networks as potentially a single network, providing for addressing every object uniquely with a single MIB. Accordingly, implementing conformant extensions to SNMP should not cause interoperability conflicts with existing standards-conforming SNMP implementations. In the SNMP network universe, any number of SNMP servers can exist, and they can manage the objects they know about using SNMPv1, SNMPv2, SNMPv3, and with confidence that any SNMPv4 or subsequent protocol that may be defined will not obsolete existing SNMP servers and their managed objects.

**SNMP’s View of a Network**

SNMPv1 defines a simple and robust internet protocol-based communications method for tracking the status of and managing almost any network-interactive item that is sufficiently defined as an object in a MIB.

SNMP normally uses UDP protocol implemented on socket-based IP communications, but may also be implemented using TCP/IP and another IP-based protocol, and also
on non-IP protocols such as RS-232 serial communications by spoofing an IP-based communication or by piggybacking it on another transmission or transfer protocol. SNMP can also take advantage of common security enhancements implemented over IP, such as the Secure Socket Layer and other encryption, authentication, and remote access technologies provided by, for example, ssh, the Openssh package.

SNMPv2 expands management capabilities of SNMPv1 by providing a mechanism for more easily defining the managed objects that SNMP communicates with. SNMP refines SNMPv2 definitions and adds important security features. Net-SNMP supports SNMPv1, SNMPv2, and SNMPv3 protocols. Because of the simple basic structure of SNMP, applications developed for any SNMP implementation tend to be easily adaptable and useful with other SNMP implementations.

Conceptually, every managed object on a network is uniquely identifiable. SNMP uses ISO Abstract Syntax Notation Standard 1 (ASN.1) to place every SNMP object within the internet hierarchy of managed objects. All these unique managed objects can be managed by their defined characteristics in the MIB. While in the theoretical schema there is only one MIB, it is usual to refer to any file that provides SNMP MIB definitions as a MIB. MIBs can be formally registered and entered into defined namespace or used locally as experimental MIBs.

An SNMP server only knows of objects for which it has definitions. This allows distributed SNMP services to co-exist on networks without interfering with each other. SNMP agents can, however, interact. SNMP agents can act as subagents of a master agent. A managed object can be a host computer or subsystem, an arbitrary interactive device, or a software application (including an operating system), basically anything whose interactivity over the network can be defined in a MIB so that it can be interfaced via SNMP.

Extensions and Fault-Tolerant SNMP Operation

While Net-SNMP supports the security features of SNMPv3, it can also interact compatibly with distributed SNMP services that use SNMPv1 and SNMPv2. Net-SNMP is the most widely-adopted open source SNMP package. This facilitates interfacing the Net-SNMP and ftSNMP implementations with other servers deploying Net-SNMP-based distributed SNMP services and service management utilities in a heterogeneous network environment. Net-SNMP has been ported to Linux, UNIX, and other operating systems. Note, however, that the Net-SNMP and ftSNMP combined packages provide support only for ftServer systems running a supported Linux distribution together with ftSSS.

The Net-SNMP and ftSNMP packages encourage deployment of distributed SNMP services on heterogeneous networks featuring both ftServer systems running a supported Linux distribution together with ftSSS, and ftServer hosts running other supported operating systems. The Net-SNMP and ftSNMP packages also can be used
to complement ASN alarm and notification functions to strengthen server management support for Linux administrators. See “Managing ASN Support” on page 4-12.

The Net-SNMP and ftlSNMP packages interact with and manage networked objects defined in MIB files. The ftlSNMP package includes the SRA-ftLinux-MIB file (SRA-ftLinux-MIB.txt) to support fault-tolerant ftServer systems. Net-SNMP also supports MIB-II and Host Resource MIB features. The ftlSNMP package follows the SNMP master/agent daemon management model, and extends the basic model using AgentX subagents. This allows the subagents associated with different MIBs to be kept separate so that failure of one does not bring down the others. Also, the ftltrapsubagent was kept separate from the ftlsubagent to avoid blocking on serious traps. AgentX extensions are defined in RFC2741, Agent Extensibility (AgentX) Protocol version 1. RFC2741 defines a standardized framework for extensible SNMP agents, and then defines master agents and subagents as processing daemons. An AgentX protocol is defined for communication between an AgentX-capable master agent and subagents. RFC2741 also defines elements of procedure for an AgentX daemon to process SNMP protocol messages.

Traditional CMU SNMP management utilities are modestly refined and enhanced in Net-SNMP. Most of the ftlSNMP extensions to Net-SNMP come through added MIB definitions and correspondingly augmented configuration files for managing SNMP agent and subagent daemons.

**Installing Remote Network Management Services**

The remote host (management) system must have an SNMP system installed that supports SNMPv3 (an example is the Red Hat Net-SNMP distribution; the following sample procedures are based on that distribution).

Transfer the SRA-ftLinux-MIB.txt file to the management system and install it in /opt/ft/mibs (or wherever the management system stores its MIBs). You can use ftp to transfer the MIB file from the ftServer system to the management system as long as the two systems can communicate with each other over a network.

Run these commands to set up MIB path environment variables and reinitialize Net-SNMP:

```
# export MIBDIRS=/usr/share/snmp/mibs:/opt/ft/mibs
# export MIBS=ALL
# service snmpd restart
```

The SNMP manager now can execute commands to manage a network-accessible ftServer system running the Linux operating system and the Net-SNMP and ftlSNMP packages.
To receive traps, configure the `/etc/opt/ft/snmp/snmpd.conf` file on the ftServer system, adding `trapsink` entries pointing to the management server running `snmptrapd`. The configuration lines should look something like this:

```
trapcommunity  public
trapsink        192.168.33.75  public
trap2sink       192.168.33.75  public
```

In this sample, the community is `public`. This would not be the usual case on an Internet-accessible system.

**Configuring SNMP for Remote Service Management**

The procedure for configuring Net-SNMP is very similar to “Configuring SNMP for Service Management” on page 5-4, which describes enabling remote services by adding SNMP users and groups. If you are using a network management station, you may have some other procedure provided with your software.

**Deploying SNMP Agents and Subagents**

The basic SNMP model has a master agent on the SNMP server system, with behavior configured by MIBs. The master agent manages one or more subagents. Typically, a single subagent is used per system (including the SNMP server system). However, with AgentX extensions, multiple agents can be deployed on a system, performing different tasks under control of the master agent. Even a MIB-II subagent can be extended to provide new functionality using AgentX. Although logging is flexible, on some SNMP systems logging is simply merged with syslog output. In the default ftlSNMP configuration, logging is configured as shown in Figure 5-1.
By default, `snmpd.log`, `ftlsubagent.log`, and `ftltrapsubagent.log` are located in `/var/opt/ft/log`. You can relocate the subagent logs by modifying `/etc/opt/ft/snmp/ftlsubagent.conf` and `/etc/opt/ft/snmp/ftltrapsubagent.conf` (see “The ftlsubagent.conf and ftltrapsubagent.conf Files” on page 5-4). If you have `sraTraceLevel` set to `brief` or `verbose` in these files, you may want to relocate the logs to a file system with ample space.

**Verifying Traps**

You can easily verify traps using `snmptrapd` on a remote Linux management system with Net-SNMP installed.

1. On the remote Linux system, set up Net-SNMP to autostart, and verify it using the `chkconfig` command, or manually start Net-SNMP.

2. On the `ftServer` system with the Linux operating system, `ftSSS`, Net-SNMP, and `ftlSNMP` installed, configure `/etc/opt/ft/snmp/snmpd.conf` with `trapsink` entries that point to the IP address of a remote management system running `snmptrapd`, by adding lines as follows:

   ```plaintext
   trapcommunity  public
   trapsink        ip_address  public
   trap2sink       ip_address  public
   ```

   In this example, `ip_address` is the IP address of the remote management system.
3. Start (or restart) SNMP using the `/etc/opt/ft/snmp/scripts/start_snmp`
   (or `/etc/opt/ft/snmp/scripts/restart_snmp`) command for changes to
take effect.

4. From the remote management system, you can view the traps as they are
generated, by tailing `/var/log/messages` (or wherever the remote management
system is configured to log `snmptrapd` messages):

   ```
   # tail -f /var/log/messages
   ```

Pulling CPU-I/O enclosures and/or pulling Ethernet cables on the ftServer system will
generate traps, as will exercising the system using the `ftsmaint` command.

## Managing SNMP

The following sections discuss how to manage SNMP on your system:

- “Customizing the SNMP Configuration”
- “Testing Your SNMP Configuration” on page 5-17
- “Managing ftServer Hardware Components” on page 5-18

**NOTE**

The sample command lines in the remainder of this
chapter are for general guidance only. Some of the
command-line details and command output shown—for
instance, PCI adapter device names—may differ from
what is applicable to your system.

### Customizing the SNMP Configuration

The following examples include accessing information on an object by either its
symbolic object identifier (OID) or the OID's corresponding entry name. To successfully
map an entry name to a MIB, or to have the output expressed with text instead of OIDs,
you must use one of several options to express the list of MIBs and MIB directories
available. Table 5-1 describes the methods of specifying this list.
Testing Your SNMP Configuration

The following are some Net-SNMP commands that you can use to test or exercise MIBs. If you run these remotely, the target name and IP address will differ.

To walk the SRA-ftLinux-MIB file:

```
# snmpwalk -v 1 -c public -t 120 localhost 1.3.6.1.4.1.458
# snmpwalk -v 2c -c public localhost 1.3.6.1.4.1.458
```

To walk the ftServer ftcPcidevcnf table:

```
# snmpwalk -v 2c -c public localhost 1.3.6.1.4.1.458.107.1.2.5.2.1
```

To walk the ftServer EtherState by its OID name:

```
# snmpwalk -v 2c -c public localhost ftcEtherState
```
To use SNMPv3 with `snmpwalk`:

```
# snmpwalk -v 3 -l authNoPriv -u v3user -A new_passwd localhost
  system
```

```
# snmpwalk -v 3 -l authNoPriv -u v3user -A new_passwd localhost
  1.3.6.1.4.1.458
```

In these command examples, `v3user` and `new_passwd` are the user name and password set up in “Configuring SNMP for Service Management” on page 5-4.

Managing ftServer Hardware Components

In the following command examples, `v3user` and `new_passwd` are the user name and password set up in “Configuring SNMP for Service Management” on page 5-4.

To bring down a CPU element

Note that a final octet 1 identifies CPU element 0 and a final octet 2 identifies CPU element 1.

```
# snmpset -v 3 -t 40 -l authNoPriv -u v3user -A new_passwd localhost
  1.3.6.1.4.1.458.107.1.2.1.2.3.1.13.1 s test
```

To bring up a CPU element

```
# snmpset -v 3 -t 40 -l authNoPriv -u v3user -A new_passwd localhost
  1.3.6.1.4.1.458.107.1.2.1.2.3.1.11.1 s test
```

To bring down an I/O element

Note that a final octet 1 identifies I/O element 10 and a final octet 2 identifies I/O element 11.

```
# snmpset -v 3 -t 40 -l authNoPriv -u v3user -A new_passwd localhost
  1.3.6.1.4.1.458.107.1.2.1.3.3.1.14.1 s test
```

To bring up an I/O element

```
# snmpset -v 3 -t 40 -l authNoPriv -u v3user -A new_passwd localhost
  1.3.6.1.4.1.458.107.1.2.1.3.3.1.12.1 s test
```

Examples

This sections shows two examples of using the SNMP commands:

- Bringing a CPU-I/O enclosure down and back up
- Testing Ethernet ports
Example 5-1. Bringing a CPU-I/O Enclosure Down and Back Up

This example shows how to use ftsmaint commands to confirm the actions you perform with SNMP commands. The examples show only relevant portions of the ftsmaint command output.

Issue the following command to check the status of CPU element 0, I/O element 10:

```bash
# /opt/ft/bin/ftsmaint ls 0
```

<table>
<thead>
<tr>
<th>H/W Path</th>
<th>Description</th>
<th>State</th>
<th>Op State</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Combined CPU/IO</td>
<td>ONLINE</td>
<td>DUPLEX</td>
<td>SECONDARY</td>
</tr>
</tbody>
</table>

The command output shows that CPU element 0 is online and duplexed, so it is safe to remove if from service. To bring down CPU element 0 by invoking the ftcCpubdInitiateBringDown command, use the whole numeric OID for that command (1.3.6.1.4.1.458.107.1.2.1.2.3.1.13) plus the CPU element 0 index (1) as the final octet. Thus, the complete OID is:

```
1.3.6.1.4.1.458.107.1.2.1.2.3.1.13.1
```

The following example assumes that the community string “private” has been defined in /etc/opt/ft/snmp/snmpd.conf.

```bash
# snmpset -v 1 -c private localhost 1.3.6.1.4.1.458.107.1.2.1.2.3.1.13.1 s test
```

```
SRA-ftLinux-MIB::ftcCpubdInitiateBringDown.3 = STRING: "test"
```

To check that the CPU-I/O enclosure status has changed:

```bash
# /opt/ft/bin/ftsmaint ls 0
```

<table>
<thead>
<tr>
<th>H/W Path</th>
<th>Description</th>
<th>State</th>
<th>Op State</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Combined CPU/IO</td>
<td>OFFLINE</td>
<td>REMOVED_FROM_SERVICE</td>
<td>OK_FOR_BRINGUP</td>
</tr>
</tbody>
</table>

To bring CPU element 0 back up by invoking the ftcCpubdInitiateBringUp command, use the numeric OID (see “SRA-ftLinux-MIB OID Values and Properties” on...
page 5-26) for that command (1.3.6.1.4.1.458.107.1.2.1.2.3.1.11), again followed by CPU element 0’s index:

```bash
# ./snmpset -v 1 -c private localhost 
1.3.6.1.4.1.458.107.1.2.1.2.3.1.11.1 s test
```

SRA-ftLinux-MIB::ftcCpubdInitiateBringUp.3 = STRING: "test"

If you check CPU element 0’s status immediately, you can see that it has started initializing:

```bash
#/opt/ft/bin/ftsmaint ls 0

H/W Path : 0
Description : Combined CPU/IO
State : INRESET
Op State : INITIALIZING
Reason : NONE
...
```

After a while, it is fully back up again:

```bash
#/opt/ft/bin/ftsmaint ls 0

H/W Path : 0
Description : Combined CPU/IO
State : ONLINE
Op State : DUPLEX
Reason : PRIMARY
...
```

**Example 5-2. Testing Ethernet Ports**

You can test Ethernet ports for proper traps and changes to OIDs. On an ftServer system running a supported Linux distribution together with ftSSS, Ethernet ports are uniquely identified.

When testing cable pulls or bringdowns, the system should generate traps, and the data that ftServer MIB objects returned should reflect these changes.

One approach is to set up an `snmptrapd` on a Linux system to verify the traps as they are generated (see “Verifying Traps” on page 5-15) and to run `snmpwalk` on the SRA-ftLinux-MIB file before and after a fault insertion to verify object data changes. A `diff` of these two walks will reveal changes that ftServer MIB objects return.

This example shows tests on dual-port 10/100/1000-Mbps Ethernet PCI adapters installed in slot 1 of both CPU-I/O enclosures.
Determine the instance name of the Ethernet device and which slot it is in:

1. Run an `snmpwalk` on `ftcEtherInstanceName` OID. This gives you a list of EtherInstance names mapped to Ethernet device names:

   ```
   # snmpwalk -v 1 -c private -t 40 localhost ftcEtherInstanceName
   ```

   ```
   SRA-ftLinux-MIB::ftcEtherInstanceName.1 = STRING: "eth100600"
   SRA-ftLinux-MIB::ftcEtherInstanceName.2 = STRING: "eth100601"
   SRA-ftLinux-MIB::ftcEtherInstanceName.3 = STRING: "eth110600"
   SRA-ftLinux-MIB::ftcEtherInstanceName.4 = STRING: "eth110601"
   SRA-ftLinux-MIB::ftcEtherInstanceName.5 = STRING: "lo"
   SRA-ftLinux-MIB::ftcEtherInstanceName.6 = STRING: "sit0"
   ```

2. Run an `snmpwalk` on `ftcEtherDevPathID` OID. This gives you a list of EtherDevPath names mapped to EtherInstance names:

   ```
   # snmpwalk -v 1 -c private -t 40 localhost ftcEtherDevPathID
   ```

   ```
   SRA-ftLinux-MIB::ftcEtherDevPathID.1 = STRING: "[10/6]"
   SRA-ftLinux-MIB::ftcEtherDevPathID.2 = STRING: "[10/6]"
   SRA-ftLinux-MIB::ftcEtherDevPathID.3 = STRING: "[11/6]"
   SRA-ftLinux-MIB::ftcEtherDevPathID.4 = STRING: "[11/6]"
   SRA-ftLinux-MIB::ftcEtherDevPathID.5 = STRING: "[unknown]"
   SRA-ftLinux-MIB::ftcEtherDevPathID.6 = STRING: "[unknown]"
   ```

   The instances to check for when pulling cables are the following:

<table>
<thead>
<tr>
<th>Instance Name</th>
<th>Instance Name (I/O element / Slot)</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftcEtherInstanceName.3</td>
<td>10/6</td>
<td>eth100600</td>
</tr>
<tr>
<td>ftcEtherInstanceName.4</td>
<td>10/6</td>
<td>eth100601</td>
</tr>
<tr>
<td>ftcEtherInstanceName.5</td>
<td>11/6</td>
<td>eth110600</td>
</tr>
<tr>
<td>ftcEtherInstanceName.6</td>
<td>11/6</td>
<td>eth110601</td>
</tr>
</tbody>
</table>

   State changes include DUPLEX, SIMPLEX, BROKEN, and, of course, various counters such as frames and collisions. (See "Op State:State Values" on page A-2 for information about states.)

3. Run `snmpwalk` on the `ftcEtherState` OID before and after pulling each cable:
In practice, you will actually redirect your `snmpwalk` output to files for before and after `diff` comparison. For example, in your work area, run `snmpwalk` for the entire SRA-ftLinux-MIB file and dump that data to a file. Pull the cable, then run `snmpwalk` again and dump it to another file.

Finally, run `diff` on the two files to see all ftServer objects that have changed because of the fault insertion. You may want to put these commands into a shell script for easier testing.

### SNMP and MIBS

The SRA-ftLinux-MIB file maps ftServer device definitions for management by Net-SNMP and ftlSNMP. These device definitions map to addressable devices in the `/proc` virtual file system. ftlSNMP can retrieve operation state data on these devices. The contents of SRA-ftLinux-MIB provide useful remarks about objects that can be managed. Table 2-4 lists device paths of hardware components for ftServer systems running a supported Linux distribution together with ftSSS. Appendix A describes the system states and operational states in an ftServer system. You can use ftlSNMP to track and log these states, and to control some operations. See Table A-2 and Table A-3 for a complete list of operational states.

### SNMP Network Management Station Considerations

The ftlSNMP package provides SNMP subagents. Net-SNMP and ftlSNMP do not provide an SNMP-capable network management station (NMS). However, you can use a commercial or open source NMS to manage the Net-SNMP and ftlSNMP packages remotely; you can also manage these packages directly from a remote system using Net-SNMP. The SRA-ftLinux-MIB file must be provided on the managing host(s) and must support the ftSSS release installed on the managed system(s). If different systems use different Linux operating system releases, the SRA-ftLinux-MIB file must reconcile differences or your SNMP NMS will not be able to manage mismatched object IDs.

The MIBs in ASN.1 encoded text form are located in `/opt/ft/mibs`, `usr/share/snmp/mibs`, and subordinate directories by default. Note that the SRA-ftLinux-MIB file is present in the `/opt/ft/mibs` directory and is named SRA-ftLinux-MIB.txt.
Load all of the MIB files you require into the SNMP NMS; certainly, SRA-ftLinux-MIB will be necessary to manage ftServer objects. Configure the SNMP NMS to avoid verbose OID printouts that may clutter the display. The minimum part of the OID needs to be displayed to provide the object's unique name.

**NOTES**

1. Net-SNMP and ftlSNMP do not require the SNMP NMS, and the package does not provide one. Choice, installation, and configuration of the SNMP NMS is your responsibility.

2. The SRA-ftLinux-MIB file is only useful for managing ftServer Linux-based systems.

**Initial SNMP Testing**

On a system with an SNMP-aware NMS, you start the NMS before starting SNMP servers.

Start the master agent and the ftlSNMP subagents by typing:

```bash
# service ft-snmp start
```

After this command completes, master agent and subagent processes with the names `snmpd`, `ftlsubagent`, and `ftltrapsubagent` should be running. Verify this:

```bash
# ps ax | egrep 'snmp|agent'
```

Any errors or warnings generated during the startup script's execution are posted to `syslog` and `stderr`. See “Deploying SNMP Agents and Subagents” on page 5-14 for the default destinations of messages logged by the master agent and subagent processes and “The `ftlsubagent.conf` and `ftltrapsubagent.conf` Files” on page 5-4 for information on how to change the location of the subagent logs.

There are many other commands available for managing Net-SNMP and ftlSNMP. See “ftlSNMP Management Commands” on page 5-6 and `ftl SNMP_scripts(8)` for descriptions of other commands, and read comments in the script files.

To terminate these processes, type:

```bash
# service ft-snmp stop
```

**Initial Testing of ftltrapsubagent**

The `ftltrapsubagent.conf` file allows you to control trap filtering. For detailed information about controlling trap filtering, see “Trap Filtering” on page 5-26.
To perform initial testing of ftlttrapsubagent, determine whether a system enclosure can be safely brought down.

NOTES

1. Do not use this procedure on a deployed network host.

2. Before continuing, read ftsmaint(8) for information on single-digit device path IDs, and “Understanding Device Paths” on page 2-27 if you have not already done so.

Select an enclosure that can be safely brought down. To get a listing of options, type:

```
# /opt/ft/bin/ftsmaint ls
```

To get a report on a single enclosure (see “ftsmaint Examples” on page 4-7 for an explanation of hw_path), type:

```
# /opt/ft/bin/ftsmaint ls hw_path
```

The output of ftsmaint must show that both the CPU elements and the I/O elements of the enclosures are ONLINE and DUPLEXED before either of them can be brought down. The SAFE TO PULL LED on each enclosure will also be steady green.

NOTE

The ftsmaint command will not allow you to bring down an enclosure unless it is duplexed.

Suppose that CPU 1, I/O 11 is duplexed. You can bring it down (leaving its partner, CPU 0, I/O 10, functioning) with the following commands:

```
# /opt/ft/bin/ftsmaint bringDown 11
# /opt/ft/bin/ftsmaint bringDown 1
```

NOTE

The term DIAGNOSTICS may appear when remotely bringing down an CPU-I/O enclosure. This term is typically returned if a diagnostic test is in progress, without regard to whether the test will succeed or fail. DIAGNOSTICS is a transient state.
Use the following command to bring the CPU-I/O enclosure up again:

```
# /opt/ft/bin/ftsmaint bringUp 11
# /opt/ft/bin/ftsmaint bringUp 1
```

**Initial Testing of ftlsubagent**

Use the `snmpwalk` tool to perform a `get next` operation on a system where an SNMP master agent is running. See `snmpwalk(1)`. For example, for the `ftcPcidevcnf` table:

```
# ./snmpwalk -Os -c public -v 1 -t 40 localhost
   1.3.6.1.4.1.458.107.1.2.5.2.1
...  
ftcPcidevcnfMasterDataParityError  
iso.3.6.1.4.1.458.107.1.2.5.2.1.14.0 = INTEGER: 2  
iso.3.6.1.4.1.458.107.1.2.5.2.1.14.1 = INTEGER: 2  
...  
ftcPcidevcnfSignaledSERR  
iso.3.6.1.4.1.458.107.1.2.5.2.1.15.0 = INTEGER: 2  
iso.3.6.1.4.1.458.107.1.2.5.2.1.15.1 = INTEGER: 2  
...  
ftcPcidevcnfDetectedParityError  
iso.3.6.1.4.1.458.107.1.2.5.2.1.16.0 = INTEGER: 2  
iso.3.6.1.4.1.458.107.1.2.5.2.1.16.1 = INTEGER: 2  
...  
```

Notice that the `snmpwalk` tool can provide symbolic decoding of absolute numbers/OIDs.

**GET and SET Operations for ftSNMP MIB Objects**

See the `SRA-ftLinux-MIB.txt` file a list of the objects that have `GET` and `SET` operations. **Table 5-2** lists the operations.

**Table 5-2. Set Operations Currently Implemented in ftSNMP**

<table>
<thead>
<tr>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ftcCpubdBurnFirmware</code></td>
</tr>
<tr>
<td><code>ftcCpubdClearMTBF</code></td>
</tr>
<tr>
<td><code>ftcCpubdInitiateBringDown</code></td>
</tr>
<tr>
<td><code>ftcCpubdInitiateBringUp</code></td>
</tr>
<tr>
<td><code>ftcCpubdSetCPUPBoardPriority</code></td>
</tr>
<tr>
<td><code>ftcIobdInitiateBringUp</code></td>
</tr>
<tr>
<td><code>ftcIobdSetMTBFThreshold</code></td>
</tr>
<tr>
<td><code>ftcIobdSetMtbfType</code></td>
</tr>
<tr>
<td><code>ftcEtherClearMTBF</code></td>
</tr>
<tr>
<td><code>ftcEtherSetMTBFThreshold</code></td>
</tr>
</tbody>
</table>
Trap Filtering

This section discusses the following topics:

- "Trap-Filtering Capability" on page 5-26"
- "Activating and Deactivating Trap Filtering" on page 5-27"
- "Trap-Filtering Examples" on page 5-27

Trap-Filtering Capability

ftlSNMP provides the ability to filter out transitional traps. Traps are messages that inform you about network events. Hardware components that go in and out of service trigger a number of traps that are seen at the management client. Some of these traps are actually transitional state information for devices. For example, when you bring up a CPU element, the CPU board’s state changes from DIAGNOSTICS to Initializing, Online, and then Duplex. However, if you are interested in only the end-state (for example, Online and Duplex), the trap-filtering capability is useful.

Another reason to use the trap-filtering capability is that some SNMP traps are triggered by obvious reason codes. For example, when you bring down an I/O element, the display controller with the device path 10/0 or 11/0 will change state from Duplex to Offline with the reason code of Parent Empty. If you are not interested in this type of trap, use the trap-filtering capability.
Activating and Deactivating Trap Filtering

To activate trap filtering, specify the following configuration line in the 
/etc/opt/ft/snmp/ftltrapsubagent.conf file:

    sraTrapFiltering on

When you activate trap filtering, traps with the following operational states are filtered out:

- DUMPING
- DIAGNOSTICS
- DIAGNOSTICS_PASSED
- INITIALIZING
- SYNCING
- FIRMWARE_UPDATE
- FIRMWARE_UPDATE_COMPLETE
- UNKNOWN

Traps with the following reason codes are also filtered out:

- PARENT_EMPTY
- PARENT_BROKEN

To deactivate the trap-filtering capability, change the above configuration line as follows:

    sraTrapFiltering off

By default, trap filtering is turned off (that is, sraTrapFiltering is set to off in the configuration file).

Trap-Filtering Examples

Example 5-3 shows some traps that can occur when I/O element 10
(ftcTrapDevicePathID.0 = STRING: "10 0) is brought down and trap filtering
is off.

    NOTE

The following examples show sample data only. Data from
your system may be different.
Example 5-3. Traps that Can Occur for I/O Element 10 When Trap Filtering Is Off

RFC1213-MIB::sysUpTime.0 = Timeticks: (11829) 0:01:58.29
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 0"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING:
"20051206134938.609247-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (11929) 0:01:59.29
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PRIMARY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING:
"20051206134939.616628-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (12030) 0:02:00.30
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 40 1"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING:
"20051206134940.622184-300"

(Continued on next page)
RFC1213-MIB::sysUpTime.0 = Timeticks: (12130) 0:02:01.30
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 40 1"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "ONLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206134941.625363-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (12231) 0:02:02.31
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 5"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206134942.629238-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (12431) 0:02:04.31
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206134944.633611-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (12435) 0:02:04.35
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 0"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PARENT_EMPTY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206134944.633611-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (12535) 0:02:05.35
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0

(Continued on next page)
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 2"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PARENT_EMPTY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206134945.675906-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (14244) 0:02:22.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 3"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PARENT_EMPTY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206134945.675906-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (14444) 0:02:24.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 4"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PARENT_EMPTY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206135004.762343-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (17244) 0:02:52.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 5"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PARENT_EMPTY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206135032.759280-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (18744) 0:03:07.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0

(Continued on next page)
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 6"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PARENT_EMPTY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206135047.759920-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (20244) 0:03:22.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 6"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206135102.760559-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (21744) 0:03:37.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 40 1"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "REMOVED"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206135117.760098-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (23244) 0:03:52.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 120"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PRIMARY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206135132.761581-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (26444) 0:04:24.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 120"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"

(Continued on next page)
Example 5-4 shows some traps that can occur when I/O element 10 (ftcTrapDevicePathID.0 = STRING: "10 0") is brought down and trap filtering is on.

Example 5-4. Traps That Can Occur for I/O Element 10 When Trap Filtering Is On

RFC1213-MIB::sysUpTime.0 = Timeticks: (4223) 0:00:42.23
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 0"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141302.277883-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (5445) 0:00:54.45
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "PRIMARY"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141314.504766-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (5546) 0:00:55.46
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "OFFLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141315.508290-300"

(Continued on next page)
RFC1213-MIB::sysUpTime.0 = Timeticks: (5746) 0:00:57.46
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 40 1"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141317.514636-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (5847) 0:00:58.47
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "11 40 1"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "ONLINE"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141318.517971-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (5948) 0:00:59.48
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 6"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141319.534567-300"

RFC1213-MIB::sysUpTime.0 = Timeticks: (6064) 0:01:00.64
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "10 5"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "SIMPLEX"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "20051206141320.697382-300"

(Continued on next page)
Example 5-5 shows some traps that can occur when CPU element 1 (ftcTrapDevicePathID.0 = STRING: "2") is brought up and trap filtering is off.

Example 5-5. Traps That Can Occur When Trap Filtering Is Off

RFC1213-MIB::sysUpTime.0 = Timeticks: (461810) 1:16:58.10
SNMPv2-MIB::snmpTrapOID.0 = OID:
SRA-ftLinux-MIB::ftcTrapGenericInformationTrap.0
SRA-ftLinux-MIB::ftcTrapDevicePathID.0 = STRING: "2 120"
SRA-ftLinux-MIB::ftcTrapAlertType.0 = STRING: "OPSTATE_CHANGE"
SRA-ftLinux-MIB::ftcTrapGenName.0 = STRING: "REMOVED"
SRA-ftLinux-MIB::ftcTrapGenDetailInfo.0 = STRING: "NONE"
SRA-ftLinux-MIB::ftcTrapGenAction.0 = STRING: "UNKNOWN"
SRA-ftLinux-MIB::ftcTrapGenEventTimeStampWithOffsetFromUTC.0 = STRING: "200512061438.510919-300"

(Continued on next page)
Example 5-6 shows some traps that can occur when CPU element 0 (ftcTrapDevicePathID.0 = STRING: "0") is brought up and trap filtering is on.
Removing ftlSNMP

Whenever possible, avoid manual removal of the Net-SNMP and ftlSNMP packages. Use the standard Linux operating system and ftSSS installation and upgrade procedures to manage Net-SNMP and ftlSNMP installations and upgrades.

To remove ftlSNMP

1. Stop all server SNMP processes by typing the following command:

```
# service ft-snmp stop
```

2. To remove the installed binary RPM, type the following command:

```
# rpm -e lsb-ft-snmp
```
This chapter discusses the following topics:

- “LEDs and Visual Diagnostics”
- “System Boot Problems”
- “Problems with the VTM” on page 6-5
- “System Log Messages” on page 6-5
- “Emulex BIOS Settings” on page 6-6
- “ftServer Setup BIOS Boot Settings” on page 6-8

This chapter provides information that will help you use available ftServer system and Linux operating system tools to diagnose system problems. For information on online diagnostic codes, see the Stratus ftServer Virtual Technician Module User’s Guide (R642). In many cases, you will be able to identify the source of the problem. If you cannot, contact the CAC.

**LEDs and Visual Diagnostics**

ftServer systems have a number of LEDs that can provide information of diagnostic value. For a complete explanation of the location and interpretation of LEDs in your system, see the troubleshooting chapter in the operation and maintenance guide for your system, as listed in Table 1-1.

**System Boot Problems**

If you experience problems in booting the system, the following information may help you diagnose the problem.

- “Normal Boot Sequence” on page 6-2
- “Possible Boot Problems” on page 6-2
- “Error and Log Messages Regarding Keyboard and Mouse” on page 6-6
Also, refer to the following related information:

- *Stratus ftServer System Software: Installation for Linux Systems* (R013L), for instructions for booting in Linux rescue mode
- *Stratus ftServer Virtual Technician Module User’s Guide* (R642), for instructions for procedures you perform with the VTM console

**Normal Boot Sequence**

The active CPU-I/O enclosure (that is, the primary enclosure, as indicated by the PRIMARY system LED) initiates the boot by starting the BIOS. The BIOS set-up program includes a configurable list of bootable devices. By default, the BIOS searches for a bootable partition in the disk enclosure, from top to bottom, left to right, and then in the DVD drive. (For information on changing the default BIOS settings, see “ftServer Setup BIOS Boot Settings” on page 6-8.) For a successful boot, the active CPU-I/O enclosure must have access to a bootable medium.

For example, when you boot the top CPU-I/O enclosure, the BIOS searches for a boot partition on *sda* (the top, left-most drive), then *sdb, sdc, sdd, sde, sdf, sdg, and finally sdh*. The boot sequence fails if the BIOS does not find a bootable partition. If the boot fails, the system switches the active CPU-I/O enclosure and the search for a bootable partition continues with *sdi*.

**NOTE**

If a RAID array fails to start, the boot stops and enters a debug shell. A typical cause for this failure is a configuration error in */etc/fstab* or in */etc/mdadm.conf*. Exiting the shell forces a reboot.

**Possible Boot Problems**

A problem in booting the system may be associated with missing or corrupt fault-tolerant drivers, the grub boot loader, or RAID.

**Missing Stratus Drivers Prevent Booting**

If required fault-tolerant drivers are not present at boot time, and if the system’s fault-tolerant policy is set to prevent booting when ftSSS drivers are missing (the default setting), the following prompt appears at the console:

```
This system is not fault tolerant because reason
Type "NON-FT-BOOT" to allow login for repair:
```
In the output, *reason* is one of the following:

- ERROR building Stratus kernel objects -- see *logfile*
- ERROR: missing Stratus kernel objects -- see *logfile*
- ERROR: incorporating Stratus kernel objects -- see *logfile*

In the output above, *logfile* is the name of a file that contains relevant details.

To override the system’s fault-tolerant policy and allow the system to boot to a non-fault-tolerant state, at the console, type `NON-FT-BOOT` and press *Enter*.

If you provide any other response three times, the system starts the boot process again.

**Problem with the grub Boot Loader**

If the system boots and hangs before the operating system is loaded, it may be a problem with the *grub* boot loader. Reinstall grub in the master boot record (MBR) on the problem disk.

**To manually run grub**

1. Insert the Red Hat Enterprise Linux media (disk #1 of a CD set) into the DVD drive.
2. Enter the BIOS setup program to set the DVD as the boot device.
   a. When the system is booting and displays the message *Press the F2 key to enter setup*, press *ESC*. The Boot Menu appears.
   b. On the Boot Menu, select *USB CDROM* and press *Enter*.
3. After the system boots, and *as soon as the boot prompt appears*, type the following line at the *boot* prompt and press *Enter*:
   ```
   # boot: linux rescue
   
   NOTE
   You must type something (at least one character) on the boot prompt line before its timeout period expires. Otherwise, the boot will proceed with incorrect parameters and the keyboard will be disabled. If this happens, you can recover by power-cycling the system and booting again.
   ```
4. After several minutes, the Language prompt appears. Follow the prompts.
5. Type the following command:
   ```
   chroot /mnt/sysimage
   ```
6. Run `/sbin/grub` by typing the following command and responses. Note that these commands apply when only the two boot disks are inserted:

```
# /sbin/grub
```

```
grub> device (hd0) /dev/sda
grub> root (hd0,0)
grub> setup (hd0)
grub> device (hd0) /dev/sdb
grub> root (hd0,0)
grub> setup (hd0)
grub> quit
```

Both system disks are now bootable.

7. Shut down the system and eject the media.

Incorrect grub parameters can also cause problems in booting. Do not change the parameters from the defaults set when the operating system was installed.

---

**CAUTION**

In particular, specifying the grub `noapic` option can make the operating system unbootable.

---

**RAID Problem**

If a RAID-1 array has one type 0xfd (Linux RAID autodetect) mirror and one 0x83 (Linux) mirror, at boot, the RAID array is started in degraded mode using the type 0xfd mirror, and the type 0x83 mirror is not automatically added. You can add the mirror with `mdadm`. To fix this problem, just change the partition type with `fdisk`.

The system supports RAID-1 arrays that consist of type 0x83 mirrors. (Type 0xfd mirrors are used on the boot disk, but type 0x83 mirrors are used for other disks.)

You can create partitions of type 0x83, create RAID-1 arrays with them, and then create a RAID-0 array from the RAID-1 arrays. If you want to start the RAID-0 arrays automatically, add entries for them to `/etc/mdadm.conf`. Otherwise, the RAID-0 arrays are not started.

---

**Automatic Reboot After Boot Monitoring Timeout**

When the system is booted into certain modes, such as RAID repair mode, the system heartbeat is not enabled. After a defined period (the default is 10 minutes), the system is automatically rebooted if a heartbeat has not been received. If your troubleshooting and repair requires more than the defined period, you must disable boot monitoring in the BIOS during the boot sequence.
To disable boot monitoring

1. When the system is booting and the progress bar has started to fill, press F2 to enter the BIOS Setup program. An *Entering Setup* message appears, but it may take several minutes for the BIOS Setup program to run.

2. Use the **RIGHT ARROW** key to select the **Server** tab.

3. On the **Server** menu, use the **DOWN ARROW** key to select **Monitoring Configuration**. Press **ENTER**.

4. On the **Monitoring Configuration** menu, use the **DOWN ARROW** key to select **OS Boot Monitoring**.

5. Select **OS Boot Monitoring** and use the **PLUS SIGN (+)** key to change the value to **Disabled**.

6. Press **ESC** to exit from the submenu.

7. In the **Setup Confirmation** dialog box, select **Yes** and press **ENTER** to save the new settings and exit from the BIOS Setup program.

After resolving the problem, reenable boot monitoring during the next boot by following the same procedure, but in step 5, change the value to **Enabled**.

⚠️ **CAUTION**

Boot monitoring is one of the fault-tolerant features of your ftServer system. You must reenable it for full fault tolerance.

### Problems with the VTM

If your system is experiencing technical difficulties with remote video, remote power control, call-home functionality, or dial-in, issuing the command `ftsmaint acSwitch` may fix the problem. This command will reset the primary VTM to the primary I/O element, if it is not already so set, which may enable the VTM to resume remote control of power and network traffic.

### System Log Messages

System log messages contain information on the operation state of the system. The file `/var/log/messages` contains system log messages. You can find logs that are specific to ftServer systems in the directory `/var/opt/ft/log`.

See “Op State:State Values” on page A-2 and “Op State:Reason Definitions” on page A-4 for explanations of some of the terminology you may see in these messages.
Error and Log Messages Regarding Keyboard and Mouse

In the system log or at system boot, you may see stderr messages. These and similar messages may occur multiple times. They are not a cause for concern if the system boots without undue delay, and when the operating system presents you with the logon prompt, it is appropriately presented on your display device and your input devices are supported to interact with the system. The messages are an unavoidable result of the order in which drivers need to be loaded during the Linux operating system boot process.

Emulex BIOS Settings

If you are installing your system for the first time or replacing a failed HBA, the HBAs you ordered from Stratus already have the appropriate settings for your storage configuration. You need to access or modify the Emulex BIOS settings only if:

- You want to verify that your HBAs arrived with the correct settings.
- You need to change the Fibre Channel topology setting, autoscan setting, or other settings for troubleshooting purposes.
- Your system contains additional, non-boot HBAs on which you must disable the Emulex BIOS to prevent boot problems. (You enable the Emulex BIOS only on boot HBAs, which connect to the Linux boot volume.)

The following procedure describes how to configure the Emulex BIOS settings for boot and non-boot HBAs.

**NOTE**

You may also need to modify the ftServer BIOS settings to configure the appropriate boot parameters. See “ftServer Setup BIOS Boot Settings” on page 6-8 for information about configuring the default production boot settings.

To configure the Emulex BIOS settings

1. Start or restart your system.
2. When the BIOS POST messages appear, press Alt + E to enter the Emulex BIOS Utility.
3. In the top-level menu, select the HBA you want to configure. To select each item in the tool, press the number key associated with that item, then press Enter.
   
   If the menu lists more than one HBA, as in Example 6-1, determine the location and function (boot or non-boot) of each HBA, then select an HBA to configure.

4. Select option 2 for Configure this Adapter’s Parameters.
5. Select option 1 for **Enable or Disable BIOS**.

6. Do one of the following:
   - If you are configuring a boot HBA, select option 1 to enable the BIOS. You must enable the BIOS on a boot HBA to allow the system to boot properly from the Linux boot volume. Continue with step 7.
   - If you are configuring a non-boot HBA, select option 2 to disable the BIOS. You must disable the BIOS on any non-boot HBA to prevent the system from searching for boot volumes on these HBAs. Continue with step 13.

7. Press **Esc** to return to the **Configure this Adapter’s Parameters** menu.

8. Select option 4 for **Topology Selection**.

9. Select the appropriate option for **Auto Topology**, the boot method that the system tries first upon powering up.

   The default setting is option 1 (**Loop first**). This setting generally works for all configurations, but if your system is not booting correctly, you can try setting option 2 (**Pt to Pt first**).

10. Press **Esc** to return to the **Configure this Adapter’s Parameters** menu.

11. Select option 6 for **Auto Scan Setting**.

12. Select option 3 for **First LUN 0 device**.

13. If you need to configure additional HBAs in this CPU-I/O enclosure, press **Esc** twice to return to the top-level menu of the Emulex BIOS Utility and repeat steps 3-13 as necessary. Otherwise, continue with step 14.

14. Select **x** to exit, and **Y** to reboot the system now.

   When the system restarts, verify that the setting works correctly. Then, if necessary, shut down the system and continue this procedure to duplicate the BIOS settings on HBAs in the secondary CPU-I/O enclosure.

15. Determine which CPU-I/O enclosure is the primary enclosure, as indicated by the PRIMARY system LED. Then, follow these steps to make the secondary enclosure the active enclosure:

   a. Remove the power cord from the primary enclosure for 10 seconds.
   b. Reinsert the power cord. The PRIMARY system LED on the secondary enclosure is now lit, indicating that it has become the primary enclosure.
   c. Lift the power-switch cover, and press the button for 2 or 3 seconds to restart the system.

16. Repeat steps 2-14 to duplicate the Emulex BIOS settings on the HBAs in the second enclosure.
If your system contains more than one Emulex HBA in each CPU-I/O enclosure, the top-level menu of the Emulex BIOS Utility contains an entry for each adapter, as in Example 6-1. Then, if necessary, determine the location and function (boot or non-boot) of each Emulex HBA.

**Example 6-1. Emulex BIOS Utility**

Emulex LightPulse BIOS Utility, WB2.11a0
Copyright (c) 1997-2008 Emulex. All rights reserved.

Emulex Adapters in the System:

1. LPe1150-E: PCI Bus, Device, Function (7B,00,00)
2. LPe1150-E: PCI Bus, Device, Function (06,00,00)

**Determine the Location and Function of An HBA**

1. Make note of the device ID at the end of each HBA entry in output of the Emulex BIOS Utility. Example 6-1 displays 7B,00,00 and 06,00,00.
2. Use the device ID and device path in output from the `ftsmaint ls` command to determine the physical location of each HBA, as explained in “Device IDs” on page 2-30. In Example 2-8, the device ID 06,00,00 corresponds to the device path 10/1.

   If necessary, use Figure 2-3 as well as the illustrations in the operation and maintenance guide for your system (as listed in Table 1-1) to locate the PCI slots in the system.

3. Using the information you collected in step 2, determine which HBA in the Emulex BIOS Utility is a boot HBA and which HBAs are non-boot HBAs. A boot HBA connects to an external storage system that contains the Linux boot volume. Non-boot HBAs connect to external storage systems that contain additional, non-boot volumes.
4. Use this information to configure the Emulex BIOS settings.

**ftServer Setup BIOS Boot Settings**

Through the course of various installation or maintenance procedures, your system boot settings may have been changed. You can use the following procedure to restore the proper settings for booting from internal or external storage.

**To configure ftServer Setup BIOS settings**

1. If necessary, start or restart your system.
2. As the system begins to boot, press F2 to enter the ftServer Setup program.
3. In the **Boot** menu, select **PCI SCSI** as the top boot device to make it the first bootable device on the system. (To move **PCI SCSI** to the top of the list, highlight it, then press the plus-sign key (+) to move it up in the list.)

4. In the **Server** menu, select the **Monitoring Configuration** tab, then set **Boot Monitoring** to **Enabled**. Use the plus-sign key (+) or minus-sign key (-) to change the value.

5. In the **Advanced** menu, click **Option ROM Configuration** and do one of the following:
   - To boot the system from an internal disk, set the **Embedded SAS Option ROM** value to **Enabled** and make sure that the other option ROMs are set to **Disabled**.
   - To boot the system from a LUN in a SAN, set the **Embedded SAS Option ROM** value to **Disabled** and make sure that the option ROM for the PCI slot that contains the boot HBA (the HBA connected to the boot volume) is set to **Enabled**. Also, to prevent boot conflicts, ensure that the option ROMs for PCI slots that contain non-boot HBAs (HBAs connected to non-boot volumes) are set to **Disabled**.

6. Save the BIOS configuration (press **F10**), then exit to continue booting the system.

Note that you may also need to modify the Emulex BIOS settings to boot from the external storage enclosure. See “**Emulex BIOS Settings**” on page 6-6 for information about configuring the default production boot settings.
Figure A-1 illustrates the State and operational states (OP State) changes in an ftServer system.

**Figure A-1. Operational State Management of ftServer System Components**

The device’s physical states (State) can be Empty, Removed, Shot, or Broken, and the OP State value is the same value as the State value. More typically, the component is in an Online state, and the OP State value is Simplex or Duplex.

A device enters the Removed state by administrative command, which the system then treats as an Empty state. However, you can use an administrative command to restart a device in a Removed state. You can only restart a device in an Empty state by physically removing it (if actually present) and inserting the device or its replacement.
System software assigns the state \textit{Shot} based on a failure threshold or MTBF calculation. A device transitions from a \textit{Shot} state to an operational state when the device is automatically returned to service, or to \textit{Broken} state through a defined system administrative process. A device in a \textit{Broken} state requires intervention: an administrator can choose to return the device to service or may physically remove the device.

If a device is in the \textit{Unknown} state, ftServer software tries to return the device to service and a known state by initializing it and performing diagnostic tests on it. If the component passes the diagnostic tests, ftServer software brings the device into the \textit{Online} state for fault-tolerant operations. A partnered device on an ftServer system typically reaches a \textit{Simplex} state (if its partner is missing or not functioning) or a \textit{Duplex} state. The interpretation of \textit{Duplex} depends on the individual device type, as shown in \textit{Table A-1}.

\textbf{Table A-1. Meaning of \textit{Duplex} for ftServer System Components}

<table>
<thead>
<tr>
<th>Component</th>
<th>Meaning of Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU element</td>
<td>A partner CPU element is present and online, and the two partners are synchronized and running in lockstep.</td>
</tr>
<tr>
<td>I/O element</td>
<td>A partner I/O element is present, online, and able to become primary (to assume \textit{active compatibility}).</td>
</tr>
<tr>
<td>I/O device</td>
<td>A partner I/O device (for example, an Ethernet adapter) is present, online, and available for failover.</td>
</tr>
<tr>
<td>Disk drive</td>
<td>A partner disk drive is online, and the partitions of the two partners are mirrored and synchronized.</td>
</tr>
</tbody>
</table>

\textbf{Op State:State Values}

\textit{Table A-2} lists and describes \textit{SRA-ftLinux-MIB} codes and \textit{Op State:State} values for ftServer systems running a supported Linux distribution and ftSSS.

\textbf{Table A-2. Codes and \textit{Op State:State} Values (Page 1 of 2)}

<table>
<thead>
<tr>
<th>Code</th>
<th>\textit{Op State:State Value}</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UNKNOWN</td>
<td>The state of a component could not be determined.</td>
</tr>
<tr>
<td>2</td>
<td>EMPTY</td>
<td>The component slot does not have a component present, or the component does not have power.</td>
</tr>
<tr>
<td>3</td>
<td>REMOVED</td>
<td>A component is present in the slot, but main power is not turned on and the component is out of service.</td>
</tr>
</tbody>
</table>
### Table A-2. Codes and Operation States (Page 2 of 2)

<table>
<thead>
<tr>
<th>Code</th>
<th>Operation State Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>SHOT</td>
<td>A component has an error and was taken out of service by system logic. When in this state, the component is electrically isolated from the rest of the system.</td>
</tr>
<tr>
<td>5</td>
<td>BROKEN</td>
<td>A component has a problem; an associated reason (see Table A-3) describes the problem. This is a terminal state; some user action must occur to change this state. User actions that cause a transition out of the BROKEN state include bringing the component up or down, or removing the component.</td>
</tr>
<tr>
<td>6</td>
<td>DUMPING</td>
<td>A CPU-I/O enclosure is recovering crash dump information.</td>
</tr>
<tr>
<td>7</td>
<td>DIAGNOSTICS</td>
<td>A component is running diagnostics.</td>
</tr>
<tr>
<td>8</td>
<td>DIAGNOSTICS_PASSED</td>
<td>A component has passed diagnostics.</td>
</tr>
<tr>
<td>9</td>
<td>INITIALIZING</td>
<td>Software is preparing a device to be brought online.</td>
</tr>
<tr>
<td>11</td>
<td>FIRMWARE_UPDATE</td>
<td>Board firmware code is being updated.</td>
</tr>
<tr>
<td>12</td>
<td>FIRMWARE_UPDATE_COMPLETE</td>
<td>Board firmware code is updated.</td>
</tr>
<tr>
<td>14</td>
<td>OFFLINE</td>
<td>The unit has been brought down.</td>
</tr>
<tr>
<td>15</td>
<td>STOPPED</td>
<td>The driver has stopped the component; the component is no longer running.</td>
</tr>
<tr>
<td>19</td>
<td>ONLINE</td>
<td>The unit can be communicated with.</td>
</tr>
<tr>
<td>20</td>
<td>SIMPLEX</td>
<td>A component is online and has no partner; it is not safe to remove this component. Applies to components that can be partnered.</td>
</tr>
<tr>
<td>21</td>
<td>DUPLEX</td>
<td>The component is online and has a partner component that is running in lockstep, mirrored, or available for failover (depending on the type of component). This component is safe to remove. Applies to components that can be partnered.</td>
</tr>
</tbody>
</table>
Op State:Reason Definitions

Table A-3 lists and describes SRA-ftLinux-MIB codes and Op State:Reason value for ftServer systems running a supported Linux distribution and ftSSS.

Table A-3. Codes and Op State:Reason Values

<table>
<thead>
<tr>
<th>Code</th>
<th>Op State:Reason Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UNKNOWN</td>
<td>The cause is not known.</td>
</tr>
<tr>
<td>2</td>
<td>NONE</td>
<td>No reason is available.</td>
</tr>
<tr>
<td>3</td>
<td>BELOW_MTBF</td>
<td>The current MTBF is below the MTBF threshold specified for this component.</td>
</tr>
<tr>
<td>4</td>
<td>DIAGNOSTICS_FAILED</td>
<td>This component failed diagnostic testing.</td>
</tr>
<tr>
<td>5</td>
<td>HARDWARE_INCOMPATIBLE</td>
<td>The component hardware is incompatible with the online system hardware.</td>
</tr>
<tr>
<td>6</td>
<td>HOLDING_DUMP</td>
<td>Bring-up failed for dump is in process.</td>
</tr>
<tr>
<td>9</td>
<td>MEDIA_DISCONNECT</td>
<td>Simplex state was entered because a cable was unplugged.</td>
</tr>
<tr>
<td>10</td>
<td>FIRMWARE_BURN_FAIL</td>
<td>Failed to update the enclosure’s BIOS or firmware.</td>
</tr>
<tr>
<td>11</td>
<td>FIRMWARE_FILE_NOT_FOUND</td>
<td>The entered firmware file path is either incorrect or the file does not exist.</td>
</tr>
<tr>
<td>12</td>
<td>FIRMWARE_FILE_ERROR</td>
<td>There was an error in the firmware image on disk.</td>
</tr>
<tr>
<td>13</td>
<td>FIRMWARE_PROM_ERROR</td>
<td>Could not write to the firmware PROM.</td>
</tr>
<tr>
<td>14</td>
<td>AUTOBURN_DISABLED</td>
<td>Cannot match a new enclosure’s BIOS or firmware with that of the existing enclosure.</td>
</tr>
<tr>
<td>16</td>
<td>PRIMARY</td>
<td>With duplex devices, this indicates that the specific device is primary in the pair.</td>
</tr>
<tr>
<td>17</td>
<td>SECONDARY</td>
<td>With duplex devices, this indicates that the specific device is secondary in the pair.</td>
</tr>
</tbody>
</table>
A
acronyms, 1-5
acSwitch argument of ftsmaint command, 4-3
active compatibility, A-2
active-backup mode, 2-17
ASN (ActiveService Network), 1-1
command interface, 1-3
installing, 4-14
managing, 4-13
services, 4-14
restarting, 4-14
ASNConfig command, location of, 1-3
B
backing up a system, 3-11
Bal-RR channel bonding mode, packet loss, 2-18
Bal-Xor channel bonding mode, packet loss, 2-18
bare-metal installation, 1-1
BIOS
changing settings of Setup program, 6-5
troubleshooting boot settings, 6-8
updating firmware, 4-3
BMC
updating firmware, 4-3, 4-5
VTM functionality, 1-3
bonding. See channel-bonding interfaces
boot disks, restrictions, 2-4
booting the system
disabling Boot Monitoring, 6-5
Emulex BIOS settings, 6-6
enabling boot monitoring, 6-9
ftServer BIOS settings, 6-8
normal sequence, 6-2
problems, 6-1, 6-2
bringDown argument of ftsmaint command, 4-3
bringUp argument of ftsmaint command, 4-3
bringUpPolicy argument of ftsmaint command, 4-3
Broken state, A-1
build number, determining, 4-4
burnBmcs argument of ftsmaint command, 4-5
burnProm argument of ftsmaint command, 4-3
C
call home
alarm messages, 4-12
troubleshooting, 6-5
channel-bonding interfaces, 2-17
active-backup mode, 2-17
configuring, 2-20
modes, limitations, 2-17
monitoring, 2-18
clearMtbf argument of ftsmaint command, 4-6
clock, 2-24
collection
channel-bonding interfaces, 2-19
DNS resolution, 2-23
Ethernet ports, 2-19
ftlSNMP, 5-2
IP addresses for bonds, 2-23
RAID arrays, 2-9
static routes, 2-23
system host name, 2-23
system time zone, 2-23, 2-24
core log, 2-4
Coordinated Universal Time (UTC), 2-24
CPU elements, 1-2
bring down, 4-3
bring up, 4-3
dump, 4-3
LEDs, 4-4
removing from service, 4-3
resynchronization, 2-25
returning to service, 4-3
temporarily out of service, 3-11
CPU-I/O enclosures
  illustration, 2-29
  numbering of, 1-2

D

data, backup limitations, 3-11
device ID, 2-30
devices
  bringing down, 4-3
device ID, 2-30
device paths, 2-27, 2-30
disks
  naming, 2-12
  enumeration, 5-22
  Ethernet PCI adapters, 2-15
DHCP
  renewing settings, 4-4
  using for VTM ports, 4-4
dial-in, troubleshooting, 6-5
disaster recovery, 3-11
disks
  device names, 2-13
  inserting, 3-1
  mirror status, 2-12
  removing, 3-1
  removing from service, 4-3
  replacing, 3-3
  returning to service, 4-3
displaying resynchronization progress, 2-14
documentation, 1-5, 2-31
  ftScalable Storage systems, 3-10
  ftServer systems, 1-5
drivers
  fault-tolerant, 2-1
  ftSSS and boot problems, 6-2
  hardened, 2-1
  missing, 6-2
  SCSI, 3-12
  USB support, 3-12
dump argument of ftsmaint command, 4-3
dumps, CPU, 4-3
duplex LED indicator, 5-24
Duplex OP State value, A-1, A-3
DVD drive, device name, 3-11

E

elements
  CPU, 1-2
  resynchronization, 2-25
  temporarily out of service, 3-11
  I/O, 1-2
    device ID, 2-15
    removing from service, 4-3
    returning to service, 4-3
Empty state, A-1
Emulex BIOS, resetting factory defaults, 6-6
error log messages
  keyboard, 6-6
  mouse, 6-6
Ethernet adapters
  adding, 2-21
  names, 2-15
Ethernet ports
  bonding of embedded, 2-17
  channel bonding, 2-17
  MAC addresses, 2-22
  naming in ftSSS, 2-15
  renewing IP addresses, 4-4
  testing, 5-20
EXT3 file systems, 2-11

F

failed disk
  managing, 3-2
  removing, 3-1
  replacing, 3-3, 3-5, 3-7
fault tolerance
  bonding mode, 2-17
  boot monitoring, 6-5
  disks, 2-3, 3-1
  ftSSS software, 1-1, 1-3
  hardened drivers, 2-1
  hardware, 1-1
  RAID disk arrays, 2-4, 2-9
  SNMP, 5-2, 5-12
  software, 4-1
  utilities, 4-1
file systems
  EXT3, 2-11
  journaling, 2-11
  lost+found directory, 2-12
  mounting, 2-11
  RAID, 2-9
size, 2-11
verifying creation, 2-11
VFAT, 3-13

files
/etc/crontab, 2-26
/etc/fstab, 3-10, 3-12
/etc/mdadm.conf, 2-11, 3-10
/etc/modprobe.d/ft-network.conf, 2-20
/etc/opt/ft/snmp/ftlsubagent.conf, 5-3
/etc/opt/ft/snmp/ftltrapsubagent.conf, 5-3
/etc/opt/ft/snmp/snmpd.conf, 5-3
/etc/X11/xorg.conf, 2-24
/opt/ft/osm/config.xml, 3-4
/proc/mdstat, 2-12, 3-10
/var/log/messages, 2-4, 2-4, 6-5
00-1sb-ft-ftmod.modules, 2-26
bond, 2-19
dump, 4-3, 4-14
ftSNMP, 5-2
README, 5-3
ifcfg-*, 2-20
SRA-ftLinux-MIB, 5-3

firmware
BIOS, updating, 4-3
BMC, updating, 4-5
ftSNMP, 5-1
agents, 5-14
configuration files, 5-3
configuring, 5-2
for remote service management, 5-14
description, 5-2
extensions, 5-12
GET operations, 5-25
installing, 5-1, 5-2
inventory, 5-2
management commands, 5-6
managing, 5-16
MIBs, 5-9, 5-22
objects defined by, 5-10
README file, 5-3
removing, 5-36
SET operations, 5-25
SRA-ftLinux-MIB, 5-22
subagents, 5-14
testing the configuration, 5-17
uninstalling, 5-36
verifying traps, 5-15
ftlsubagent
description, 5-2
initial testing, 5-25
ftltrapsubagent
description, 5-2
initial testing, 5-23
ftScalable Storage systems, 3-10
ftServer Setup. See BIOS
ftServer systems
documentation, 1-5
system administration, 1-1
troubleshooting, 1-4, 6-1
ftsmaint command, 4-1
acSwitch, 4-3
bringDown, 4-3
bringUp, 4-3
bringUpPolicy, 4-3
burnBmcs, 4-5
burnProm, 4-3
clearMtbfs, 4-6
dump, 4-3
examples, 4-7
giveModem, 4-5
identify, 4-4
inventory, 4-2
jumpSwitch, 4-4
location of, 1-3
ls, 4-2
lsLong, 4-2
lsPeriph, 4-2
lsSystem, 4-2
lsVND, 4-3
lsVtmConfig, 4-4
memCheck, 4-4
modemStatus, 4-5
powerOff modem, 4-5
powerOn modem, 4-5
renewVtmDhcp, 4-4
resetmodem, 4-5
resetMtbfs, 4-6
runDiag, 4-4
setMtbfsMinFaults, 4-6
setMtbfsThresh, 4-6
setMtbfsType, 4-7
setPriority, 4-4
setSensorThresh, 4-7
showAsnConfig, 4-4
showVtmConfig, 4-4
takeModem, 4-5
task arguments, 4-1
using, 4-1
-version, 4-4

ftSSS
acronyms, 1-5
and LVM, 3-10
build number, 4-4
commands, 1-3
disk management, 3-1
drivers, 6-2
failed disk management, 3-2
ftsmaint command, 4-1
legacy devices in, 2-1
management command, ftssm, 4-1
NIC naming, 2-15
operational states, 5-22, A-1
optional tools, 1-3
replacement disk management, 3-3
SNMP, 5-1
support for RAID levels, 2-9
tape drive support, 3-11
tools, 1-3
USB floppy drive support, 3-13
USB support, 3-12
user-space device names, 2-12
utilities, 1-3
video configuration, 2-23

G
giveModem argument of ftssm, 4-5
grub boot loader, 3-4, 3-9
problems, 6-3

H
hard-disk drives
disk names, 2-2
management of disk partitions, 2-5
storage allocation, 2-7
supported SCSI disks, 2-2
system-console messages, 2-4
hardware
fault-tolerant, 1-1
managing, 5-18
self checking, 1-1
HBAs
configuring non-boot adapters, 6-6
diagnosing Emulex BIOS settings, 6-6
diagnosing ftServer BIOS settings, 6-8
host name of system, configuring, 2-23

I
I/O elements, 1-2
bring down, 4-3
bring up, 4-3
device ID, 2-15
ftsmaint acSwitch, 4-3
LEDs, 4-4
numbering of, 1-2
removing from service, 4-3
returning to service, 4-3
identify argument of ftssm, 4-1
command, 4-2
installing
ftlSNMP, 5-1, 5-2
remote network management services, 5-13
system boot disk, 2-4
internal storage, 2-2
default configuration, 2-7
removing and replacing disks, 3-1
inventory argument of ftssm
command, 4-2

J
jumpSwitch argument of ftssm
command, 4-4

K
kernel memory dump file management, 4-14
kernel names, 2-3

L
LEDs, 6-1
disks, 2-4, 2-10
identifying components, 4-4
operational status of system, 4-11
SAFE TO PULL indicator, 5-24
legacy devices, 2-1
USB storage device, 3-13
Index

Linux operating system, 1-1
logical volume manager (LVM) and ftSSS, 3-10
logrotate, 5-4
logs
  console, 2-4
details of USB device, 3-14
for traces, 5-4
message, 6-5
SNMP, 5-15
ls argument of ftsmaint command, 4-2
lsLong argument of ftsmaint command, 4-2
lsPeriph argument of ftsmaint command, 4-2
lsscsi command, 3-12
lsSystem argument of ftsmaint command, 4-2
lsVND argument of ftsmaint command, 4-3
lsVtmConfig argument of ftsmaint command, 4-4

M
MAC addresses, 2-22
management
  data storage devices, 1-2
  Ethernet devices, 2-15
  partitions, 2-5
  SNMP, 5-1
mdadm command
  creating RAID arrays, 2-9, 2-10
  --detail argument, 2-12
device names in output, 2-13
displaying resynchronization progress, 2-14
mdadm.conf file and adding RAID arrays, 2-11
mdstat file, 2-10
  overview of active RAID devices, 2-12
  sample, 2-13
memCheck argument of ftsmaint command, 4-4
memory sizes, 2-7
MIB (management information base), 5-9, 5-22
  objects defined by, 5-10
  SRA-ftLinux-MIB, 5-9
mirrors
  boot disk, 2-4
default partitions, 2-8
  problems, 6-4
  RAID-1 arrays, 2-3
  resynchronization status, 2-12
missing drivers, 6-2
model number of system, displaying, 4-2
modem
  ASN connection, 4-12
  controlling with ftsmaint, 4-5
  viewing state of, 4-11
modemStatus argument of ftsmaint command, 4-5
monitoring system remotely, 4-12
MTBF, A-2
disk, 3-2
  settings, 4-6
  SNMP set commands, 5-25

N
names
  disk devices, 2-12
  Ethernet devices, 2-15
  USB devices, 3-12
Net-SNMP, 5-1, 5-22
  basic commands, 5-7
description, 5-2
network management stations (NMS), 5-22
network-interface cards (NICs)
  naming in ftSSS, 2-15
  See also Ethernet ports, 2-17
noauto option, 3-12

O
Op State
  Reason values, A-4
  State values, A-2
  viewing, 4-10
OpState Manager (OSM), 3-3

P
packets, lost, 2-18
part number of system, displaying, 4-2
partitions, managing, 2-5
PCI slots
  LEDs, 4-4
  removing from service, 4-3
  returning to service, 4-3
physical states, A-1
power control (remote), troubleshooting, 6-5
powerOff modem argument of ftsmaint command, 4-5
powerOn modem argument of ftsmaint command, 4-5
proc/mdstat file, 2-12

R
RAID, 2-4, 2-9
arrays, 2-4
creating, 2-9
creating RAID-0 arrays, 2-10
creating RAID-1 arrays, 2-9
device names, 2-9
loading at boot, 2-11
mounting file systems, 2-11
overview, 2-9
state information, 2-12
levels supported, 2-9
problems, 6-4
restrictions, 2-4
README file for SNMP, 5-3
reason values of Op State, A-4
Red Hat Linux
99-read-check tool, 3-10
documentation, 1-5
RAID-1 fast resync, 2-10
remote
access to SNMP services, 5-4
monitoring, 4-12
network management services, 5-13
power control, 6-5
viewing of status, 4-12
Removed state, A-1
removing ftlSNMP, 5-36
renewVtmDhcp argument of ftsmaint command, 4-4
resetmodem argument of ftsmaint command, 4-5
resetMtbf argument of ftsmaint command, 4-6
resynchronization progress, displaying for disks, 2-14
rpm
package, 5-2
removing installed binary RPM, 5-36
runDiag argument of ftsmaint command, 4-4
S
SAFE TO PULL LED, 5-24
serial number, displaying system, 4-2
setMtbfMinFaults argument of ftsmaint command, 4-6
setMtbfThresh argument of ftsmaint command, 4-6
setMtbfType argument of ftsmaint command, 4-7
setPriority argument of ftsmaint command, 4-4
setSensorThresh argument of ftsmaint command, 4-7
shells for debugging, 6-2
Shot state, A-1, A-3
showAsnConfig argument of ftsmaint command, 4-4
showVtmConfig argument of ftsmaint command, 4-4
simplex state or operation
bringing down a device, 4-3, 4-10
CPU element operation, 2-25
CPU-I/O enclosure, 2-4
disk, 3-1, 3-3
Ethernet devices, 5-21
ftsmaint bringDown command, 4-3
LED indicator, 5-24
Op State, 4-10, A-1, A-3
SNMP (Simple Network Management Protocol), 5-1
See also ftlSNMP and Net-SNMP
basic Net-SNMP commands, 5-7
concepts, 5-6
configuring for remote service management, 5-14
configuring for service management, 5-4
configuring to start at system initialization, 5-4
fault-tolerant operation, 5-12
initial testing, 5-23
managing, 5-16
managing hardware, 5-18
testing a configuration, 5-17
testing Ethernet ports, 5-20
traps. See traps
view of a network, 5-11
snmpset command, 5-18
snmptrapd daemon, 5-15
snmpwalk command, 5-17
sra_ras service, starting, 4-14
SRA-ftLinux-MIB, 5-22
description, 5-2
GET operations, 5-25
OID values and properties, 5-26
SET operations, 5-25
states, physical, A-1
storage
ftScalable storage system, 2-28, 3-10
internal disk storage, 2-2
restrictions, 2-4
managing data storage devices, 3-1
troubleshooting
Emulex BIOS settings, 6-6
ftServer BIOS settings, 6-8
USB storage devices, 3-12
sysreport command, 1-4
Sysrq tool, 1-4
sysrq-trigger file, 1-4
system
administration, 1-1
backup, 3-11
boot
normal sequence, 6-2
problems, 6-1, 6-2
clock, 2-24
devices
bringing down, 4-12
bringing up, 4-12
controlling, 4-12
disks, 2-7
restrictions, 2-4
displaying information, 4-2
log messages, 6-5
remote monitoring, 4-12
system log file, 4-13
T
takeModem argument of ftsmaint command, 4-5
testing
Ethernet ports, 5-20
failed diagnostic testing, A-4
ftlsubagent, 5-25
ftltrapsubagent, 5-23
SNMP, 5-23
SNMP configuration, 5-17
time zone configuration, 2-23, 2-24
traps
filtering
activating, 5-27
deactivating, 5-27
description, 5-26
description, 5-26
description, 5-26
examples, 5-27
ftltrapsubagent, 5-2, 5-3, 5-13
ftltrapsubagent.conf, 5-4, 5-15, 5-23
ftltrapsubagent.log, 5-15
receiving through snmp.conf, 5-14
restart_ftltrapsubagent, 5-7
snmptrap, 5-8
snmptrapd, 5-15
start_ftltrapsubagent, 5-7
stop_ftltrapsubagent, 5-7
verifying, 5-15
troubleshooting, 1-4, 6-1
call home, 6-5
dial-in, 6-5
Emulex BIOS settings, 6-6
ftServer BIOS settings, 6-8
ftServer systems, 6-1
remote power control, 6-5
using ASN, 4-12
video, 6-5

U
udev disk device names, 2-2
displaying, 2-13
umount command, 3-12
USB storage devices, 3-13
automounting, 3-12
entries in /etc/fstab, 3-12
names, 3-12
restoring after enclosure failure, 3-13
solid-state, 3-14
storage, 3-12
UTC. See Coordinated Universal Time

V
version argument of the ftsmaint command, 4-4
video
configuration, 2-23
displaying, 2-13
PowerPC code (PPC), 2-12
troubleshooting, 6-5
Virtual Network Devices (VND). See VND
visual diagnostics, 6-1
VND, 2-18
  ftsmaint lsVND command, 4-3
VTM
  displaying information about, 4-2, 4-4
  managing, 1-3
VTM console, 1-3
VTMConfig command, 1-3