

Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10

系统操作和管理指南



手册代码: C120-E679-24ZH
2018年3月

版权所有© 2007, 2018, Fujitsu Limited。保留所有权利。

Oracle 和/或其附属公司对于本材料的部分内容提供了技术意见和审阅。

Oracle 和/或其附属公司与 Fujitsu Limited 各自拥有或控制与本文档所述产品和技术相关之知识产权，并且此类产品、技术及本文档受著作权法、专利和其他知识产权法及国际条约的保护。

本文档以及它所介绍的产品和技术按照限制其使用、复制、分发和反汇编的许可证进行分销。未经 Oracle 和/或其附属公司与 Fujitsu Limited 及其相应许可方（若有）的事先书面许可，严禁以任何形式、通过任何方式复制此产品或技术及本文档的任何部分。向您提供本文档并非授权您对于文档所述产品或技术之任何明示或默示之权利或许可，并且本文档不包含或表示 Oracle、Fujitsu Limited 或其各自任何附属公司方面的任何承诺。

本文档以及其所述的产品和技术可能融合了第三方的知识产权，这些产权的著作权属于这些供应商和/或是供应商授权给 Oracle 和/或其附属公司及 Fujitsu Limited，包括软件和字体技术。

依照 GPL 或 LGPL 的条款，在最终用户请求时，如果可行，则提供由 GPL 或 LGPL 管控的源代码的副本。请联系 Oracle 和/或其附属公司或 Fujitsu Limited。此分发可能包括第三方开发的材料。产品的一些部分可能源于 Berkeley BSD 系统，并获得了加州大学的授权。

UNIX 是 The Open Group 的注册商标。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。

Fujitsu 和 Fujitsu 徽标是 Fujitsu Limited 的注册商标。

SPARC Enterprise、SPARC64、SPARC64 徽标和所有 SPARC 商标是 SPARC International, Inc.在美国和其他国家/地区的商标或注册商标，并应按照许可证的规定使用。

其他名称可能是各自所有者的商标。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

免责声明：Oracle 和 Fujitsu Limited 和/或任何附属公司授予的与本文档或其所述任何产品或技术之仅有保证均在所提供相关产品或技术的许可证协议中明确说明。

除非此类协议明确规定，ORACLE 或 FUJITSU LIMITED 和/或其附属公司对于按原样提供的此类产品或技术或本文档不做任何类型（明示或默示）的陈述或保证。所有明示或默示之条件、陈述和保证，包括但不限于对适销性、特定用途适用性或非侵权的默示担保，均被免责，除非此类免责被法律视为无效。

除非此类协议明确规定，在适用法律允许的范围内，无论任何情况下，依据任何法理，Oracle 或 Fujitsu Limited 和/或其任何附属公司对于任何第三方的收入或利润损失、使用或数据损失、业务中断，或者任何间接、特殊、意外或连带损害，均不承担责任，即使事先被告知可能会发生此损害。

文档按原样提供，所有明示或默示之条件、陈述和保证，包括但不限于对适销性、特定用途适用性或非侵权的默示担保，均被免责，除非此类免责被法律视为无效。

目录

前言 xxiii

第1章 概括了解 SPARC M12/M10 1

1.1 SPARC M12/M10 的基础知识 1

1.2 XSCF 固件基本知识 4

1.2.1 XSCF 概览 4

1.2.2 XSCF 功能 4

1.2.3 XSCF 功能 9

1.2.4 主/备用/从 XSCF 的机制 12

1.2.5 不同型号间 XSCF 配置的差异 12

1.3 网络配置 14

1.3.1 网络连接概述 14

1.3.2 XSCF-LAN 端口号和功能以及防火墙 20

1.4 虚拟机监控程序基本知识 21

1.5 Oracle VM Server for SPARC 基本知识 22

1.6 OpenBoot PROM 基本知识 23

第2章 登录和注销 XSCF 25

2.1 连接系统管理终端 25

2.1.1 通过串行端口连接 25

2.1.2 串行连接中终端可用的功能 28

2.1.3 通过 XSCF-LAN 端口连接 29

2.1.4 XSCF-LAN 连接中终端可用的功能 32

2.2	登录 XSCF Shell	33
2.2.1	如何使用串行连接登录 XSCF shell	33
2.2.2	如何经由 XSCF-LAN 通过 SSH 连接登录 XSCF shell	35
2.2.3	如何经由 XSCF-LAN 通过 Telnet 连接登录 XSCF shell	36
2.3	从 XSCF Shell 注销	37
2.4	登录 XSCF Web	37
2.4.1	必须事先设置的项目	37
2.4.2	支持的浏览器	38
2.4.3	Web 浏览器必须启用的功能	38
2.4.4	如何用 XSCF Web 登录	38
2.5	从 XSCF Web 注销	39
2.6	可连接的用户数	40
第3章	配置系统	41
3.1	XSCF 设置前提工作	41
3.1.1	设置前的初始工作	41
3.1.2	支持信息	42
3.1.3	设置的用户界面以及如何访问	42
3.1.4	顺利配置 XSCF	43
3.2	了解 XSCF 固件设置的内容	43
3.2.1	设置使用 XSCF 的项目	43
3.2.2	检查主 XSCF	44
3.2.3	备用 XSCF 上可执行的功能	46
3.2.4	在 man 页检查命令选项的详情	46
3.3	从 XSCF Shell 设置	47
3.4	从 XSCF Web 设置	51
3.5	创建/管理 XSCF 用户	52
3.5.1	XSCF 用户帐户	52
3.5.2	密码和密码策略	52
3.5.3	用户权限类型	53
3.5.4	检查与 XSCF 用户帐户相关的设置项目和命令	55
3.5.5	XSCF 用户帐户注册流程	55

3.5.6	确认已注册的用户	56
3.5.7	确认/更改密码策略	57
3.5.8	添加一个 XSCF 用户帐户并设置密码	59
3.5.9	设置用户权限	60
3.5.10	启用/禁用用户帐户	60
3.5.11	启用/禁用登录锁定功能	61
3.5.12	使用 LDAP 管理 XSCF 用户帐户	62
3.5.13	使用 Active Directory 管理 XSCF 用户帐户	67
3.5.14	使用 LDAP over SSL 管理 XSCF 用户帐户	83
3.6	设置 XSCF 时间/日期	98
3.6.1	了解 XSCF 时间和物理分区时间之间的关系	99
3.6.2	逻辑域的时间管理策略	100
3.6.3	查看与时间有关的设置项目和命令	100
3.6.4	设置时区	101
3.6.5	设置夏令时	102
3.6.6	设置系统时间	103
3.6.7	同步控制域时间和 XSCF 时间	104
3.6.8	将 XSCF 指定为 NTP 服务器	105
3.6.9	将 XSCF 指定为 NTP 客户端	106
3.6.10	配置由 XSCF 使用的 NTP 服务器	107
3.6.11	配置 NTP 服务器的 DNS 轮循	108
3.6.12	指定/取消 NTP 服务器首选	109
3.6.13	设置 XSCF 层次值	110
3.6.14	更改 XSCF 本地时钟的时钟地址	111
3.7	配置用于登录 XSCF 的 SSH/Telnet 服务	113
3.7.1	检查与 SSH 和 Telnet 相关的设置项目和命令	113
3.7.2	启用/禁用 SSH 和 Telnet 服务	114
3.7.3	设置 SSH 服务主机密钥	115
3.7.4	注册/删除 SSH 服务的用户公钥	116
3.7.5	设置 SSH/Telnet 服务超时时间	117
3.8	配置用于登录 XSCF 的 HTTPS 服务	117

- 3.8.1 使用外部或 Intranet 中的证书颁发机构的流程 118
- 3.8.2 使用自签名证书颁发机构时的流程 118
- 3.8.3 检查与 HTTPS 有关的设置和命令 119
- 3.8.4 启用/禁用 HTTPS 服务 119
- 3.8.5 使用外部或 Intranet 中的证书颁发机构导入 Web 服务器证书 120
- 3.8.6 配置自签名证书颁发机构并创建 Web 服务器证书 121
- 3.9 配置 XSCF 网络 123
 - 3.9.1 通过 XSCF 网络使用服务 123
 - 3.9.2 了解 XSCF 网络接口 123
 - 3.9.3 XSCF 网络接口配置 125
 - 3.9.4 了解网络组子网 127
 - 3.9.5 了解使用 SSCP 设置的 IP 地址 127
 - 3.9.6 检查与 XSCF 网络相关的设置项目和命令 129
 - 3.9.7 配置 XSCF 网络的流程 130
 - 3.9.8 启用/禁用 XSCF 网络，并设置 XSCF-LAN IP 地址和网络掩码 131
 - 3.9.9 设置接管 IP 地址 133
 - 3.9.10 设置 SSCP 的 IP 地址 134
 - 3.9.11 设置 XSCF 主机名和域名 136
 - 3.9.12 设置 XSCF 路由 137
 - 3.9.13 设置 XSCF 的 DNS 140
 - 3.9.14 给 XSCF 网络设置 IP 数据包筛选规则 142
 - 3.9.15 应用 XSCF 网络设置 143
 - 3.9.16 检查 XSCF 网络连接状态 145
- 3.10 配置审核以强化 XSCF 安全 146
 - 3.10.1 审核 146
 - 3.10.2 了解审核术语 147
 - 3.10.3 管理审核 148
 - 3.10.4 检查与审核有关的设置项目和命令 149
 - 3.10.5 审核流程 150
 - 3.10.6 显示/设置审核策略 152
 - 3.10.7 启用/禁用审核 153

3.10.8	删除审核日志数据	154
3.10.9	查看审核日志	155
3.10.10	管理备用 XSCF 的审核日志	156
第4章	按照使用型号配置系统	157
4.1	设置/确认系统海拔高度	157
4.1.1	设置系统海拔高度	157
4.1.2	检查系统的海拔高度设置	158
4.2	控制系统启动	158
4.2.1	设置/确认预热时间	159
4.2.2	设置/确认启动等待时间	160
4.3	启用/禁用双回路供电	161
4.3.1	启用双回路供电	161
4.3.2	禁用双回路供电	162
4.3.3	确认双回路供电设置	162
4.4	降低功耗	163
4.4.1	设置功耗上限	163
4.4.2	处理因电源异常造成的温度/负荷异常	165
4.4.3	降低未使用的或低利用率硬件的功耗	166
4.5	连接 DVD 驱动器	170
4.5.1	使用外部 DVD 驱动器	170
4.5.2	使用外部 DVD 驱动器安装 Oracle Solaris	173
4.6	使用远程存储	177
4.6.1	远程存储是什么?	177
4.6.2	远程存储网络配置	178
4.6.3	使用远程存储的方法	185
4.6.4	终端和浏览器的使用要求	186
4.6.5	Oracle Solaris 的设置	189
4.6.6	远程存储软件的版本	189
4.6.7	远程存储设备的路径和别名	190
4.6.8	远程存储注意事项	190
4.6.9	使用远程存储的流程	191

4.6.10	配置与远程存储一同使用的 XSCF-LAN	193
4.6.11	XSCF Remote Storage Server (XSCF 远程存储服务器) 的状态	194
4.6.12	使用远程存储时连接到介质	195
4.6.13	从 Oracle Solaris 使用远程存储	200
4.6.14	从介质断开/结束远程存储	203
4.6.15	其他注意事项和操作	206
第5章 CPU 激活 209		
5.1	CPU 激活的基本概念	209
5.2	CPU 激活密钥	210
5.3	添加 CPU 内核资源	212
5.3.1	将 CPU 内核添加到物理分区和逻辑域的工作流程	212
5.3.2	购买添加的 CPU 激活	212
5.3.3	检查 CPU 激活密钥	213
5.3.4	登录 CPU 激活密钥	213
5.3.5	分配 CPU 内核资源到物理分区	214
5.3.6	将 CPU 内核添加到逻辑域	216
5.3.7	保存逻辑域配置信息	217
5.4	删除 CPU 内核资源	217
5.4.1	删除 CPU 激活的工作流程	217
5.4.2	移除逻辑域中的 CPU 内核	218
5.4.3	释放物理分区中的 CPU 内核资源	218
5.4.4	检查将被删除的 CPU 激活密钥	218
5.4.5	删除 CPU 激活密钥	219
5.5	移动 CPU 内核资源	219
5.5.1	CPU 激活移动工作流程	219
5.5.2	检查将被移动的 CPU 激活密钥	220
5.6	查看 CPU 激活信息	221
5.6.1	查看 CPU 激活注册和设置信息	221
5.6.2	检查 COD 日志	222
5.6.3	查看 CPU 激活密钥信息	222

5.6.4	查看已激活 CPU 内核资源的使用状况	223
5.7	保存/恢复 CPU 激活密钥	224
5.7.1	保存 CPU 激活密钥	224
5.7.2	恢复 CPU 激活密钥	225
5.8	CPU 激活异常的故障排除	225
5.8.1	使用中的 CPU 内核数量超过了已激活的 CPU 内核数量	225
5.8.2	工作中的 CPU 内核数量因为故障下降到 CPU 激活的数量	226
5.9	CPU 激活的重要注意事项	226
第6章	启动/停止系统	229
6.1	启动系统	229
6.1.1	从输入电源开启到系统启动的流程	229
6.1.2	使用电源开关	230
6.1.3	使用 <code>poweron</code> 命令	232
6.2	停止系统	233
6.2.1	从系统停止到输入电源关闭的流程	234
6.2.2	系统停止之前保存逻辑域配置信息	234
6.2.3	停止整个系统	235
6.3	重新启动系统	236
6.4	禁止在开机时启动 Oracle Solaris	236
第7章	控制物理分区	239
7.1	配置物理分区	239
7.2	设置物理分区运行模式	239
7.2.1	搭载在物理分区上的 CPU 和 CPU 运行模式	240
7.2.2	检查恢复供电/设置自动上电时电源的操作	245
7.3	开启物理分区	247
7.4	关闭物理分区	249
7.5	更改物理分区的配置	250
第8章	控制逻辑域	251
8.1	配置逻辑域	251
8.2	配置 Oracle Solaris 内核区	252
8.2.1	Oracle Solaris 内核区的硬件和软件要求	252

- 8.2.2 Oracle Solaris 内核区上的 CPU 管理 252
- 8.2.3 Oracle Solaris 内核区注意事项 252
- 8.3 从 XSCF Shell 切换到控制域控制台 253
 - 8.3.1 如何从 XSCF shell 切换到目标控制域控制台 253
 - 8.3.2 适当情况下连接到控制域控制台 254
- 8.4 从控制域控制台返回 XSCF Shell 254
 - 8.4.1 如何从控制域控制台切换到 XSCF shell 254
 - 8.4.2 从控制域控制台注销 255
- 8.5 启动逻辑域 255
- 8.6 关闭逻辑域 256
- 8.7 按顺序关闭逻辑域 257
 - 8.7.1 域表 (ldomTable) 257
 - 8.7.2 域信息 (ldom_info) 资源 258
- 8.8 检查 CPU 激活信息 258
- 8.9 设置控制域的 OpenBoot PROM 环境变量 259
 - 8.9.1 XSCF 固件可设置 OpenBoot PROM 环境变量 259
 - 8.9.2 设置控制域的 OpenBoot PROM 环境变量 260
 - 8.9.3 查看控制域的 OpenBoot PROM 环境变量 262
 - 8.9.4 初始化控制域的 OpenBoot PROM 环境变量 262
- 8.10 域控制台日志功能 263
 - 8.10.1 禁用控制台日志功能的方法 263
 - 8.10.2 启用控制台日志功能的方法 263
 - 8.10.3 服务域要求 264
 - 8.10.4 虚拟控制台组表 (ldomVconsTable) 264
 - 8.10.5 控制台资源 264
- 8.11 更改逻辑域的配置 265
- 8.12 设置逻辑域时间 265
- 8.13 收集管理程序转储文件 266
 - 8.13.1 管理程序转储基本知识 266
 - 8.13.2 管理程序转储功能的命令 266
 - 8.13.3 使用管理程序转储时的注意事项 268

8.14	管理与 CPU 插槽相关联的逻辑域资源	269
8.14.1	CPU 插槽约束条件概述	269
8.14.2	CPU 插槽约束条件的硬件和软件要求	270
8.14.3	CPU 插槽约束条件的限制	270
8.14.4	使用 CPU 插槽约束条件创建可靠性高的逻辑域	270
8.14.5	将内存镜像配置到 CPU 芯片	271
8.14.6	移除控制域中与 CPU 插槽相关联的资源	273
8.14.7	将 CPU 插槽约束条件配置到逻辑域配置	275
8.15	设置物理分区动态重新配置策略	276
8.15.1	物理分区动态重新配置策略	276
8.15.2	资源减少策略的详情	276
8.15.3	如何变更 PPAR DR 策略	279
8.16	设置逻辑域的最大页面大小	280
8.16.1	逻辑域的最大页面大小	280
8.16.2	较大的最大页面大小的优点	281
8.16.3	较大的最大页面大小的缺点	281
8.16.4	设置和变更逻辑域的最大页面大小	282
8.16.5	查看逻辑域的最大页面大小	284
第9章	管理系统日报	285
第10章	故障的预防和应对措施	287
10.1	了解故障排除和相关功能	288
10.2	故障发生时通过电子邮件接收通知	288
10.2.1	电子邮件通知功能的特点	289
10.2.2	故障通知详情	289
10.2.3	检查与电子邮件通知相关的设置项目和命令	291
10.2.4	电子邮件通知的设置流程	291
10.2.5	设置 SMTP 服务器的主机名、端口号、回复电子邮件地址和验证方法	292
10.2.6	设置通知的目标电子邮件地址和启用/禁用电子邮件通知功能	292
10.3	通过 SNMP 代理监控/管理系统状态	293
10.3.1	SNMP 基本知识	293

10.3.2	SNMP 相关术语	294
10.3.3	MIB 定义文件基本知识	295
10.3.4	陷阱基本知识	296
10.3.5	查看与 SNMP 代理相关的设置项目和命令	298
10.3.6	SNMP 代理设置流程	299
10.3.7	在 SNMP 代理上设置系统管理信息，并启用/禁用 SNMP 代理	301
10.3.8	设置 SNMPv3 陷阱	302
10.3.9	禁用到 SNMPv3 预期目标主机的陷阱	303
10.3.10	启用/禁用 SNMPv1 和 SNMPv2c 通信	304
10.3.11	设置 SNMPv1 和 SNMPv2c 陷阱	304
10.3.12	禁用对 SNMPv1 和 SNMPv2c 预期主机的陷阱	305
10.3.13	恢复 SNMP 设置的默认值	305
10.3.14	设置 USM 管理信息	306
10.3.15	设置 VACM 管理信息	307
10.4	监控系统	308
10.4.1	了解主机看门狗功能/实时检查的机制	308
10.4.2	控制监控和服务器操作	309
10.5	了解故障降级机制	310
10.6	查看发生故障的硬件资源	310
10.6.1	使用 list-domain 命令查看故障的内存或 CPU	311
10.6.2	使用 list-device 命令查看故障的内存或 CPU	311
10.7	设置故障 CPU 内核的自动更换	311
10.7.1	自动更换 CPU 内核的条件	311
10.7.2	更改自动更换策略的方法	313
10.7.3	更改最大重试次数计数器和重试间隔的方法	314
10.8	设置恢复模式	314
10.9	建立冗余组件配置	315
10.10	保存/恢复 XSCF 设置信息	315
10.10.1	了解如何保存/恢复 XSCF 设置信息	315
10.10.2	保存 XSCF 设置信息	316

10.10.3	恢复 XSCF 设置信息	317
10.11	保存/恢复 XSCF 中的逻辑域配置信息	318
10.11.1	保存/显示逻辑域配置信息	318
10.11.2	恢复逻辑域配置信息	320
10.12	在 XML 文件中保存/恢复逻辑域配置信息	321
10.12.1	保存/确认逻辑域配置信息	322
10.12.2	恢复逻辑域配置信息	323
10.13	保存/恢复 OpenBoot PROM 环境变量	324
10.13.1	保存 OpenBoot PROM 环境变量	324
10.13.2	恢复 OpenBoot PROM 环境变量	326
10.14	保存/恢复硬盘中的内容	327
10.15	重启逻辑域	328
10.16	在逻辑域中引起崩溃	329
10.16.1	在来宾域中引起崩溃	329
10.16.2	在控制域中引起崩溃	329
10.17	重启物理分区	330
10.18	将服务器恢复为出厂默认状态	331
10.18.1	了解初始化命令	332
10.18.2	初始化服务器	332
10.19	使用延迟转储收集崩溃转储文件	333
第11章	查看系统状态	335
11.1	查看系统配置/状态	335
11.1.1	查看与系统配置/状态相关的设置项目和命令	335
11.1.2	查看系统安装的组件	336
11.1.3	查看系统环境	339
11.1.4	查看故障/降级组件	343
11.1.5	查看 PCI 扩展单元状态	344
11.2	查看物理分区	347
11.2.1	查看有关物理分区和逻辑域配置/状态的项目和命令	347
11.2.2	查看物理分区配置	347
11.2.3	查看物理分区操作状态	350

11.2.4	查看内存镜像模式设置	351
11.2.5	查看 PSB 状态	352
11.2.6	查看逻辑域状态	353
第12章	检查日志和信息	355
12.1	检查 XSCF 保存的日志	355
12.1.1	检查日志类型和参考命令	355
12.1.2	如何查看日志	358
12.1.3	检查错误日志	359
12.1.4	检查监视信息日志	361
12.1.5	检查电源日志	361
12.1.6	检查事件日志	363
12.1.7	检查控制台日志	363
12.1.8	检查崩溃日志	364
12.1.9	检查 IPL 日志	364
12.1.10	检查审核日志	365
12.1.11	检查 COD 日志	366
12.1.12	检查活动目录日志	367
12.1.13	检查 LDAP over SSL 日志	367
12.1.14	检查温度历史日志	368
12.1.15	使用快照将日志保存到文件	368
12.1.16	将日志保存到本地 USB 设备	369
12.1.17	通过网络将日志保存在使用 XSCF Web 的终端	370
12.1.18	通过网络将日志保存在使用快照指定的服务器	370
12.2	检查警告和通知信息	370
12.2.1	检查信息类型和参考方法	370
12.2.2	处理通知信息	372
第13章	切换到锁定/维护模式	375
13.1	了解锁定模式和维护模式的差异	375
13.2	切换操作模式	376
第14章	配置高可靠性系统	379
14.1	配置内存镜像	379

14.1.1	内存镜像概述	379
14.1.2	配置内存镜像	380
14.2	配置硬件 RAID	381
14.2.1	硬件 RAID 基础知识	381
14.2.2	FCode 实用程序命令	385
14.2.3	硬件 RAID 的注意事项	385
14.2.4	硬件 RAID 操作前的准备工作	387
14.2.5	创建硬件 RAID 卷	389
14.2.6	删除硬件 RAID 卷	393
14.2.7	管理硬件 RAID 卷的热备盘	394
14.2.8	检查硬件 RAID 卷的状态和磁盘驱动器	395
14.2.9	检查出现故障的磁盘驱动器	397
14.2.10	更换出现故障的磁盘驱动器	398
14.2.11	重新启用硬件 RAID 卷	399
14.2.12	指定硬件 RAID 卷为启动设备	401
14.3	使用 LDAP 服务	401
14.4	使用 SAN 启动	402
14.5	使用 iSCSI	402
14.6	SPARC M12/M10 和 I/O 设备的远程电源管理	402
14.6.1	SPARC M12/M10 的远程电源管理功能	402
14.6.2	了解远程电源管理的连接形式	403
14.6.3	远程电源管理的结构	406
14.6.4	设置远程电源管理之前	407
14.6.5	设置远程电源管理的流程	407
14.6.6	检查远程电源管理设置	408
14.6.7	初始化远程电源管理设置	409
14.6.8	启用/禁用远程电源管理功能	409
14.6.9	创建管理文件	409
14.6.10	启用/禁用 XSCF 的远程电源管理功能使用的 IPMI 服务	410
14.6.11	获取远程电源管理组的设置信息	411
14.6.12	设置远程电源管理组	411

14.7	使用不间断电源	411
14.8	使用验证启动	412
14.8.1	验证启动基础知识	412
14.8.2	验证启动启动验证的机制	412
14.8.3	验证启动用 X.509 公共密钥证书	413
14.8.4	验证启动策略	413
14.8.5	支持验证启动的 Oracle Solaris 和 XCP 的版本	415
14.8.6	验证启动支持的范围	415
14.8.7	注意事项和限制	416
14.8.8	查看验证启动相关的设置项目和命令	417
14.8.9	验证启动的设置流程	417
14.8.10	注册 X.509 公共密钥证书	419
14.8.11	启用/禁用已注册的 X.509 公共密钥证书	421
14.8.12	删除已注册的 X.509 公共密钥证书	424
14.8.13	查看已注册的 X.509 公共密钥证书	426
14.8.14	设置验证启动策略	427
14.8.15	查看验证启动策略	428
第15章	扩展系统配置	429
15.1	更改虚拟 CPU 配置	429
15.2	更改内存配置	431
15.3	PCIe 端点设备的动态重新配置功能	432
15.3.1	将物理 I/O 设备添加到 I/O 域	434
15.3.2	从 I/O 域移除物理 I/O 设备	434
15.4	使用 PCI 扩展单元	435
15.4.1	检查 PCI 扩展单元	436
15.4.2	控制 PCI 扩展单元的电源	436
15.4.3	连接 PCI 扩展单元系统配置的注意事项	437
15.5	扩展 SPARC M12-2S/M10-4S	439
第16章	更新 XCP 固件	441
16.1	固件更新的基础知识	441
16.1.1	要更新固件的类型	441

16.1.2	固件更新的特点	442
16.1.3	固件更新的机制	442
16.1.4	版本匹配	444
16.1.5	使用多个 XSCF 时更新	444
16.2	更新固件之前	444
16.2.1	更新注意事项	444
16.2.2	更新文件交付方法和格式	445
16.2.3	检查固件版本的方法	445
16.2.4	更新方法和工作时间	446
16.3	更新流程	447
16.4	准备 XCP 映像文件	448
16.5	更新固件	448
16.5.1	在拥有一个 XSCF 的系统上更新 XCP	448
16.5.2	更新具有多个 XSCF 的模块化架构配置系统上的 XCP	453
16.6	从 XSCF Web 更新固件	462
16.7	部件更换时固件版本匹配	468
16.7.1	输入电源开启情况下添加/更换时固件版本的匹配	468
16.7.2	输入电源关闭情况下添加/更换时固件版本的匹配	469
16.8	固件更新期间出现故障	472
16.9	与固件更新相关的常见问题	473
第17章	更新 Oracle Solaris 和 Oracle VM Server for SPARC	475
第18章	故障排除	477
18.1	关于 XSCF 的故障排除	477
18.2	使用 RESET 开关的注意事项	480
18.3	常见问题/FAQ	481
18.4	使用 XSCF 进行系统故障排除	482
附录 A	SPARC M12/M10 系统设备路径列表	485
A.1	SPARC M12-1 设备路径	485
A.2	SPARC M12-2 设备路径	488
A.2.1	对应初始安装 1-CPU 配置の場合	488
A.2.2	对应初始安装 2-CPU 配置の場合	491

A.3	SPARC M12-2S 设备路径	494
A.3.1	对应初始安装 1-CPU 配置的场所	494
A.3.2	对应初始安装 2-CPU 配置的场所	498
A.4	SPARC M10-1 设备路径	504
A.5	SPARC M10-4 设备路径	507
A.5.1	对应初始安装 2-CPU 配置的场所	507
A.5.2	对应初始安装 4-CPU 配置的场所	510
A.6	SPARC M10-4S 设备路径	513
A.6.1	对应初始安装 2-CPU 配置的场所	513
A.6.2	对应初始安装 4-CPU 配置的场所	518
附录 B	识别基于 WWN 的 SAS2 设备	523
B.1	全球通用名称 (WWN) 语法	523
B.2	probe-scsi-all 命令输出概要	524
B.3	使用 probe-scsi-all 命令识别磁盘槽	524
B.3.1	使用 probe-scsi-all 命令识别磁盘槽的示例 (SPARC M12-1/ M12-2/M12-2S/M10-1/M10-4/M10-4S)	524
B.4	识别磁盘槽	527
B.4.1	使用 format 命令 (Oracle Solaris 11)	527
B.4.2	使用 diskinfo 命令 (Oracle Solaris 11)	529
B.4.3	使用 diskinfo 命令 (Oracle Solaris 10)	531
附录 C	XSCF Web 页面列表	533
C.1	页面概要	533
C.2	了解菜单配置	535
C.3	可用页面	539
C.3.1	本页面显示系统、物理分区和逻辑域的状态	539
C.3.2	操作物理分区的页面	540
C.3.3	配置服务器的页面	543
C.3.4	维护服务器页面	553
C.3.5	查看日志的页面	555
附录 D	XSCF MIB 信息	557
D.1	MIB 对象标识	557

D.2	标准 MIB	559
D.3	扩展 MIB	559
D.3.1	XSCF 扩展 MIB 对象	560
D.4	陷阱基本知识	561
附录 E	Oracle VM Server for SPARC 的 SPARC M12/M10 系统特定功能	563
E.1	按顺序关闭逻辑域	563
E.2	CPU 激活支持	563
E.3	检查发生故障的资源	564
E.3.1	确认使用 list-domain 子命令时是否发生了内存或 CPU 故障	564
E.3.2	显示使用 list-device 子命令时是否发生了内存或 CPU 故障	564
E.4	自动更换故障的 CPU	564
E.5	管理程序转储	564
E.6	域控制台日志功能	565
E.7	CPU 插槽限制条件	565
附录 F	SAS2IRCU 实用程序命令示例	567
F.1	显示 sas2ircu 识别的 SAS 控制器列表	567
F.2	查看硬件 RAID 卷的信息	568
F.3	添加硬件 RAID 卷	572
F.4	查看硬件 RAID 卷的配置状态	574
F.5	创建硬件 RAID 卷的热备盘	575
F.6	删除硬件 RAID 卷的热备盘	576
F.7	删除硬件 RAID 卷	577
F.8	识别硬件 RAID 卷的默认磁盘驱动器	578
附录 G	SPARC M12-1/M10-1 XSCF 启动模式功能	585
G.1	功能概述	585
G.1.1	XSCF 启动模式功能是什么?	585
G.1.2	使用状态	586
G.2	限制和注意事项	586
G.2.1	系统安装时的限制和注意事项	586
G.2.2	系统操作时的限制和注意事项	587
G.2.3	维护时的限制	587

G.3	配置步骤	588
附录 H	OpenBoot PROM 环境变量和命令	591
H.1	SCSI 设备查看	591
H.2	不支持的 OpenBoot PROM 环境变量	591
H.3	不支持的 OpenBoot PROM 命令	592
H.4	启用安全模式的行为	593
附录 I	如何指定启动设备	595
I.1	内置存储器的设备路径	595
I.2	使用 PHY 编号指定的方法	596
I.3	使用目标 ID 指定的方法	597
I.4	使用 SAS 地址指定的方法	598
I.5	使用卷设备名指定的方法	599
附录 J	DVD 驱动器别名列表	601
J.1	外部 DVD 驱动器别名	601
J.1.1	SPARC M12-1 外部 DVD 驱动器别名	601
J.1.2	SPARC M12-2 外部 DVD 驱动器别名	602
J.1.3	SPARC M12-2S 外部 DVD 驱动器别名	602
J.1.4	SPARC M10-1 外部 DVD 驱动器别名	605
J.1.5	SPARC M10-4 外部 DVD 驱动器别名	605
J.1.6	SPARC M10-4S 外部 DVD 驱动器别名	605
J.2	远程存储 DVD 驱动器别名	607
J.2.1	SPARC M12-1 远程存储 DVD 驱动器别名	607
J.2.2	SPARC M12-2 远程存储 DVD 驱动器别名	607
J.2.3	SPARC M12-2S 远程存储 DVD 驱动器别名	607
J.2.4	SPARC M10-1 远程存储 DVD 驱动器别名	608
J.2.5	SPARC M10-4 远程存储 DVD 驱动器别名	608
J.2.6	SPARC M10-4S 远程存储 DVD 驱动器别名	608
附录 K	CPU 激活临时许可证	611
K.1	CPU 激活临时许可证是什么?	611
K.2	CPU 激活临时许可证的使用条款和注意事项	612
K.3	相关命令	613

K.3.1	使用 CPU 激活临时许可证的命令	613
K.3.2	使用 CPU 激活临时许可证时的相关命令	613
K.4	使用 CPU 激活临时许可证的流程和步骤	614
K.4.1	XCP 2330 及更高版本的流程和步骤	614
K.4.2	XCP 232x的流程和步骤	623
K.4.3	功能过期或禁用的情况	629
K.5	CPU 激活临时许可证的事件通知	633
K.5.1	通知的类型	633
K.5.2	通知示例	633
K.6	其他重要注意事项	635
K.6.1	PPAR DR 和 CPU 激活临时许可证	635
K.6.2	尝试再次使用 CPU 激活临时许可证时（仅适用于 XCP 232x）	635
K.6.3	移动 CPU 激活密钥（删除/移动）	636
K.6.4	ldm 命令的输出	636
索引		639

前言

本文档介绍了在安装后从 Oracle 或 Fujitsu 对 SPARC M12/M10 系统进行设置和管理的方法。操作任何 SPARC M12/M10 系统时，请阅读必要的部分。

在阅读本文档之前，建议您阅读《Fujitsu SPARC M12 快速指南》或《Fujitsu M10/SPARC M10 系统 快速指南》。

在日本 Fujitsu 将 Fujitsu SPARC M12 作为 SPARC M12 销售。
Fujitsu SPARC M12 和 SPARC M12 是相同的产品。

在日本 Fujitsu 将 Fujitsu M10 作为 SPARC M10 销售。
Fujitsu M10 和 SPARC M10 是相同的产品。

适用对象

本文档适用于精通计算机和 Oracle Solaris 的系统管理员。

相关文档

在以下网址可以找到适用于您服务器的全部文档。

- Sun Oracle 软件相关文档（Oracle Solaris 等）
<http://docs.oracle.com/en/>
- Fujitsu 文档
全球网站
<http://www.fujitsu.com/global/products/computing/servers/unix/sparc/downloads/manuals/>
日语网站
<http://www.fujitsu.com/jp/products/computing/servers/unix/sparc/downloads/manual/>

有关使用 SPARC M12 的系统，请参见 "[与 SPARC M12 相关的文档](#)" 中列出的手册。

有关使用 SPARC M10 的系统，请参见 "[与 SPARC M10 相关的文档](#)" 中列出的手册。

与 SPARC M12 相关的文档

手册名称 (*1)

《Fujitsu SPARC M12 产品说明》
《Fujitsu SPARC M12 快速指南》
《Fujitsu SPARC M12 入门指南》 (*2)
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information》 (*2)
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide》
《Software License Conditions for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10》
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security Guide》
《Fujitsu SPARC Servers/SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual》
《Fujitsu SPARC M12-1 安装指南》
《Fujitsu SPARC M12-2 安装指南》
《Fujitsu SPARC M12-2S 安装指南》
《Fujitsu SPARC M12 PCI Card Installation Guide》
《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 系统 操作和管理指南》
《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide》 (*3)
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists》
《Fujitsu SPARC M12-1 Service Manual》
《Fujitsu SPARC M12-2/M12-2S Service Manual》
《Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》
《PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》
《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Glossary》
《External USB-DVD Drive user guide》

*1 列出的手册如有变更，恕不另行通知。

*2 本产品提供印刷的手册。

*3 本文档特别适用于 SPARC M12/M10 和 FUJITSU ETERNUS 磁盘存储系统。

与 SPARC M10 相关的文档

手册名称 (*1)

《Fujitsu M10/SPARC M10 系统 产品说明》
《Fujitsu M10/SPARC M10 系统 快速指南》

手册名称 (*1)

《Fujitsu M10/SPARC M10 系统 入门指南》 (*2)

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information》 (*2)

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide》

《Software License Conditions for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10》

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security Guide》

《Fujitsu SPARC Servers/SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual》

《Fujitsu M10-1/SPARC M10-1 安装指南》

《Fujitsu M10-4/SPARC M10-4 安装指南》

《Fujitsu M10-4S/SPARC M10-4S 安装指南》

《Fujitsu M10/SPARC M10 Systems PCI Card Installation Guide》

《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 系统 操作和管理指南》

《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide》 (*3)

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists》

《Fujitsu M10-1/SPARC M10-1 Service Manual》

《Fujitsu M10-4/Fujitsu M10-4S/SPARC M10-4/SPARC M10-4S Service Manual》

《Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》

《PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》

《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Glossary》

《External USB-DVD Drive user guide》

*1 列出的手册如有变更，恕不另行通知。

*2 本产品提供印刷的手册。

*3 本文档特别适用于 SPARC M12/M10 和 FUJITSU ETERNUS 磁盘存储系统。

安全注意事项

在使用或处理 SPARC M12/M10 之前，请仔细阅读以下文档：

- 《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information》
- 《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide》

文本惯例

本手册使用以下字体和符号来表示特定类型的信息。

字体/符号	含义	示例
AaBbCc123	您输入的内容，对比屏幕上的计算机输出内容。 本字体用于表示命令输入。	XSCF> adduser jsmith
AaBbCc123	命令、文件和目录的名称；屏幕上的计算机输出。 此字体表示文框内的命令输出示例。	XSCF> showuser -P User Name: jsmith Privileges: useradm auditadm
《 》	表示参考手册的名称。	请参阅《Fujitsu M10-1/SPARC M10-1 安装指南》。
" "	表示章节名、项目、按钮或菜单。	请参阅 "第 2 章 网络连接"。

文本中的命令语法

当 XSCF 命令有 (8) 或 (1) 的节号时，从文本中被省略。
有关命令的详情，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

命令行界面 (CLI) 语法

命令语法如下：

- 必须将要求输入一个值的变量设为斜体。
- 可选元素必须括在 [] 中。
- 可选关键词的一组选项必须括在 [] 中并由 | 隔开。

文档的反馈

如果您对本文档有任何意见建议或要求，请抽出几分钟时间告知我们，指明手册代码、手册标题和页码，并在以下网站陈述您的观点：

- 全球网站
<http://www.fujitsu.com/global/contact/>
- 日语网站

<http://www.fujitsu.com/jp/products/computing/servers/unix/sparc/contact/>

概括了解 SPARC M12/M10

本章概括介绍了 SPARC M12/M10 系统，并介绍了配套软件和固件。

- SPARC M12/M10 的基础知识
- XSCF 固件基本知识
- 网络配置
- 虚拟机监控程序基本知识
- Oracle VM Server for SPARC 基本知识
- OpenBoot PROM 基本知识

1.1 SPARC M12/M10 的基础知识

本节对 SPARC M12/M10 系统进行简要介绍。

SPARC M12/M10 是使用 SPARC 处理器和 Oracle Solaris 的 UNIX 服务器系统。CPU 激活允许以一个内核为单位扩展资源。SPARC M12-2S/M10-4S 使用模块化架构系统，以便系统可以根据预期的业务用途和业务规模进行合理配置。该服务器可以以多种方式应用：作为最适合应用于在云计算时代数据中心的数据库服务器、作为对高吞吐量要求很高的 Web 服务器或应用服务器。

以下型号可支持各种预期用途。

- SPARC M12-1
这种最多具有六个内核的 单CPU 紧凑型设计旨在节省空间和提高性能。
- SPARC M12-2
本型号最多由两个 CPU 组成，每个 CPU 最多有 12 个内核。
- SPARC M12-2S
本型号最多由两个 CPU 组成，每个 CPU 最多有 12 个内核。通过模块化架构 (BB) 系统，可以根据所需的性能调整连接的 SPARC M12-2S 单元的数量。通过将 SPARC M12-2S 单元直接连接到另一个 BB，可以将配置扩展到多达四个 BB。此外，使用接线盒的系统支持最多 16 个 BB 的配置，并可扩展到最多 32 个 CPU -- 可扩展性得到保证。

- SPARC M10-1
这种最大具有 16 个内核的 单CPU 紧凑型设计旨在节省空间和提高性能。
- SPARC M10-4
本型号最多由四个 CPU 组成，每个 CPU 最多有 16 个内核。
- SPARC M10-4S
本型号最多由四个 CPU 组成，每个 CPU 最多有 16 个内核。通过模块化架构 (BB) 系统，可以根据所需的性能调整连接的 SPARC M10-4S 单元的数量。通过将 SPARC M10-4S 单元直接连接到另一个 BB，可以将配置扩展到多达四个 BB。此外，使用接线盒的系统支持最多 16 个 BB 的配置，并可扩展到最多 64 个 CPU -- 可扩展性得到保证。

注 - 如果使用模块化架构系统，则同一配置中不能混装 SPARC M12-2S 和 SPARC M10-4S。

系统配置

本节介绍系统配置。

图 1-1 显示了一个系统配置的示例，其中由模块化架构系统连接多个 SPARC M12-2S 或多个 SPARC M10-4S。具有模块化架构配置的单个 SPARC M12-2S/M10-4S 单元是一个模块化架构。通过组合一个或多个模块化架构模块来配置物理分区 (PPAR)。

图 1-2 介绍了 SPARC M12-1/M12-2/M10-1/M10-4 的系统配置示例。单个 SPARC M12-1/M12-2/M10-1/M10-4 单元无法具有模块化架构配置，但有时称为物理分区。请注意，单机配置中的 SPARC M12-2S 和 SPARC M10-4S 有时也称为物理分区。

图 1-1 SPARC M12-2S/M10-4S 系统配置示例

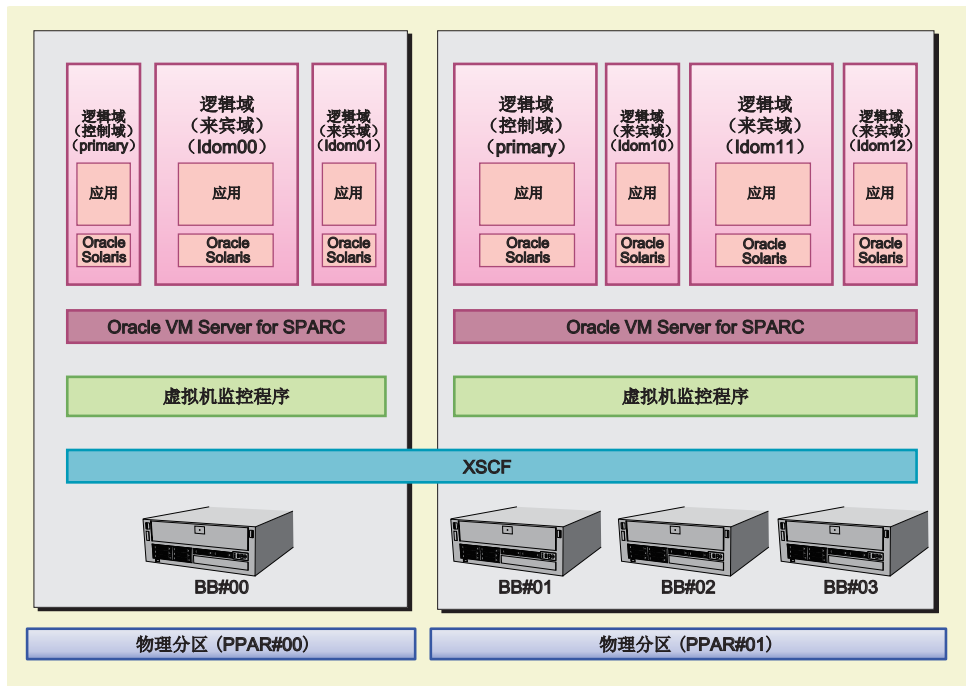
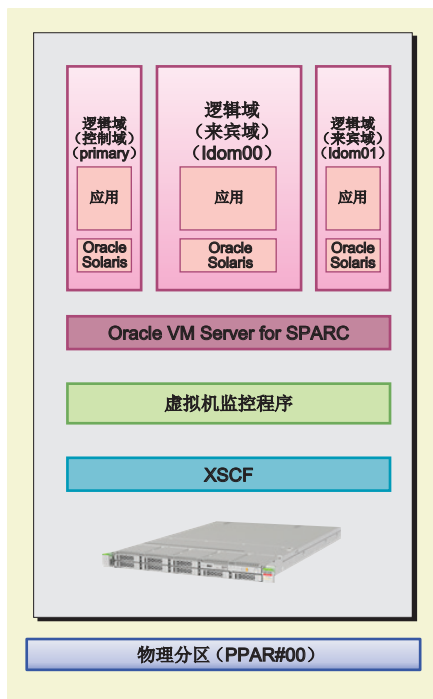


图 1-2 SPARC M12-1/M12-2/M10-1/M10-4 系统配置示例



以下几个小节说明 "物理分区" 和 "逻辑域", 它们是系统配置的关键。

配置物理分区

如需配置 SPARC M12-2S 或 SPARC M10-4S 系统, 需通过组合同一型号的一个或多个模块化架构来配置物理分区 (PPAR)。配置物理分区称为分区, 将得到的配置对象称为物理分区 (PPAR)。使用 XSCF 固件 (系统管理固件) 来配置物理分区。

在 图 1-1 所示的示例中, PPAR#00 是其中一个模块化架构 (BB), 将 BB#00 配置为物理分区 PPAR#00。类似地, 从 BB#01、BB#02 和 BB#03 配置物理分区 PPAR#01。

一旦配置了物理分区, 物理分区上的硬件资源将分配给逻辑域。

请注意, 由于 SPARC M12-1/M12-2/M10-1/M10-4 型号是由单个单元所组成, 因此只能配置一个物理分区。

配置逻辑域

物理分区将 CPU、内存、I/O 设备和其他硬件资源分配给逻辑域。使用 Oracle VM Server for SPARC 软件配置逻辑域。

配置后的逻辑域在软件中被处理成 UNIX 系统。Oracle Solaris 和应用程序可以安装在逻辑域并分别执行任务。在 图 1-1 所示的示例中, 通过分配物理分区 PPAR#00 的硬件资源配置了逻辑域 primary、ldom00 和 ldom01。

同样, 逻辑域 primary、ldom10、ldom11、和 ldom12 被配置了物理分区 PPAR#01 的硬件资源。

其中一个分配了物理分区资源的逻辑域用于控制所有逻辑域的域。这被称为控制域。控

制域就是逻辑域控制器，也用于处理物理分区和逻辑域之间的通信。

系统所需的固件/软件

物理分区使用 XSCF 固件和逻辑域、Oracle VM Server for SPARC 来实现。即使对于仅有控制域的配置，也需要 Oracle VM Server for SPARC。

在 XSCF 固件和 Oracle VM Server for SPARC 之间，在系统内部进行监控和管理整个系统的通信。用户不需要关注。

SPARC M12/M10 系统中的 XSCF 固件和 Oracle VM Server for SPARC 之间的接口由名为虚拟机监控程序的固件实现。

"1.2 XSCF 固件基本知识" 和后续章节将介绍系统中使用的固件和软件。

1.2 XSCF 固件基本知识

本节概括介绍 XSCF 固件的功能。

1.2.1 XSCF 概览

XSCF 固件是 SPARC M12/M10 中的标准内置系统控制设备。XSCF 固件独立运行在服务器处理器的专用处理器（服务处理器）上。每个 SPARC M12/M10 系统的机箱包含一个完整的 XSCF 固件包，用于与逻辑域进行通讯并管理整个系统。当使用模块化架构 (BB) 系统组合多个服务器时，服务器通过接线盒 (XBBBOX) 与其他服务器互连。每一个接线盒中有一个运行 XSCF 固件的服务处理器。

服务器电源处于开启状态时，XSCF 固件运行并持续监控服务器的操作是否正确，甚至在逻辑域没有运行或物理分区电源关闭时也能保持运行和监控状态。还能按照需求改变服务器配置和进行服务器的电源开启和关闭操作。

此外，XSCF 固件包括可提供监视、管理和控制系统的功能的用户接口。

在本手册中，XSCF 固件可能被称为 XSCF。包含搭载服务处理器的主板（用于运行 XSCF 固件）可能被称为 XSCF 单元。

1.2.2 XSCF 功能

内置用户界面可用于日常服务器操作和维护

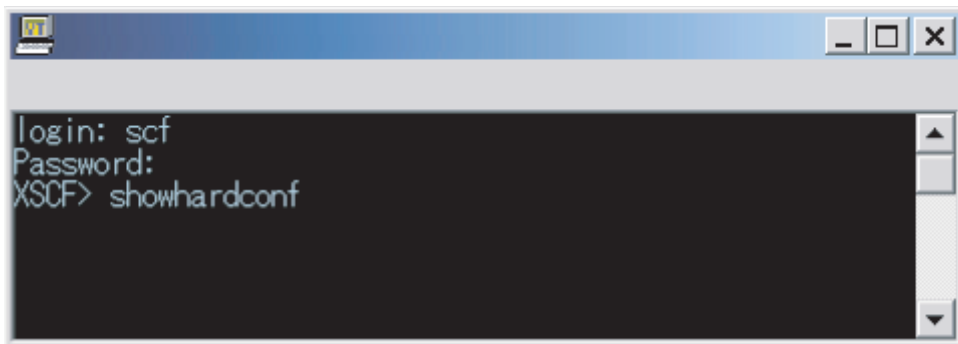
从命令行或 Web 浏览器访问 XSCF 您可以把握服务器状态、操作服务器和维护服务器。

- **XSCF shell（命令行界面）**

您可以通过串行线直接将用户 PC 连接到服务器或将 XSCF LAN 连接到以太网，您可以使用 SSH 服务或 Telnet 服务实现通信。这将使 PC 可作为 XSCF shell 终端，执行 XSCF shell 命令。在 XSCF shell 中，您可以切换到控制台，从而让您操作控制域（以下称控制域控制台）。

图 1-3 是 XSCF shell 终端的示例。

图 1-3 XSCF shell 终端的示例

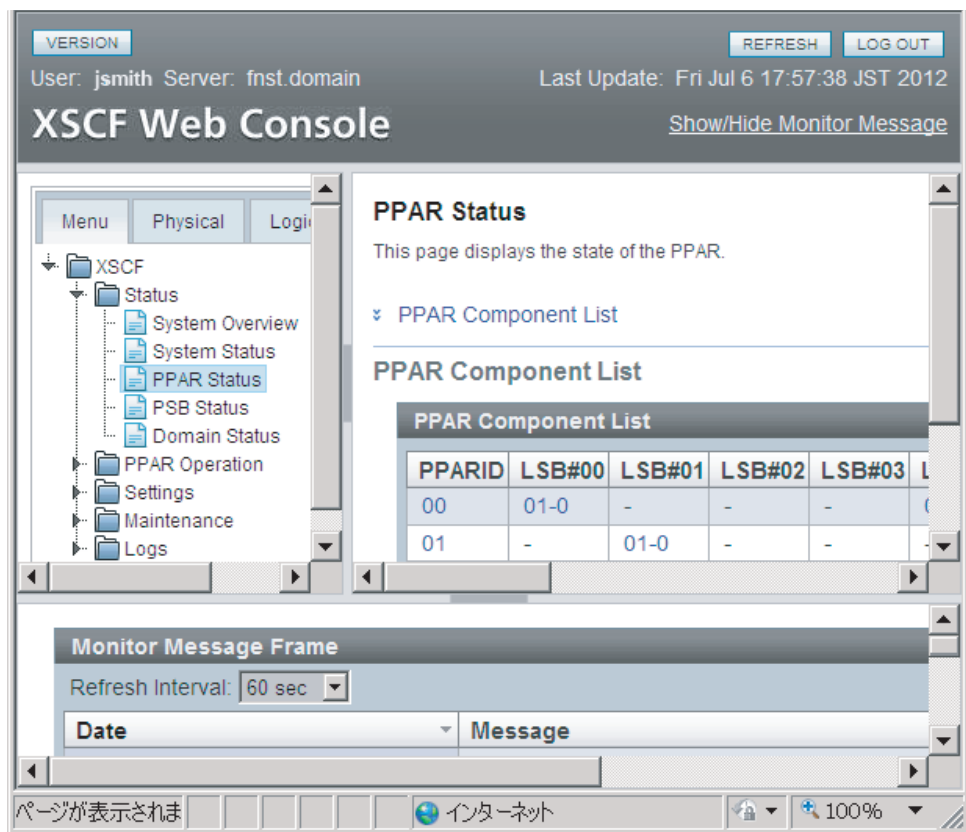


- **XSCF Web**（浏览器用户界面）

本界面允许您通过以太网将用户 PC 连接到 XSCF LAN，并且使用 HTTPS 或 SSL/TLS 协议实现通信。因此，您可以使用 PC 上的 Web 浏览器来使用 XSCF Web 控制台。通过 XSCF Web，您可以分层次显示组件，查找想要操作的菜单，从而减少用户的操作负担和降低服务器管理成本。

图 1-4 显示了使用 XSCF Web 控制台的示例。

图 1-4 XSCF Web 控制台示例



模块化架构配置中的 XSCF

当使用模块化架构系统配置系统时，接线盒 (XBBOX) 也包含 XSCF。将 XSCF 安装在服务器和 XBBOX 中实现了高度可靠的系统。

注 - 如果使用模块化架构系统配置系统，则该配置中不能混装 SPARC M12-2S 和 SPARC M10-4S 机箱。

图 1-5 显示了 4BB 配置中 SPARC M12-2S 或 SPARC M10-4S 系统的示例，其中机箱直接互连。

图 1-5 SPARC M12-2S/M10-4S 系统 XSCF 配置（无接线盒）示例

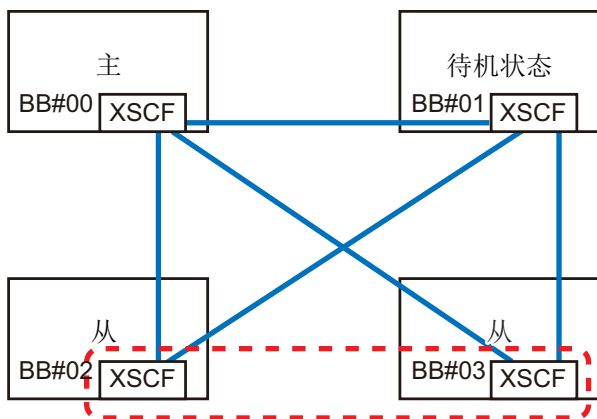
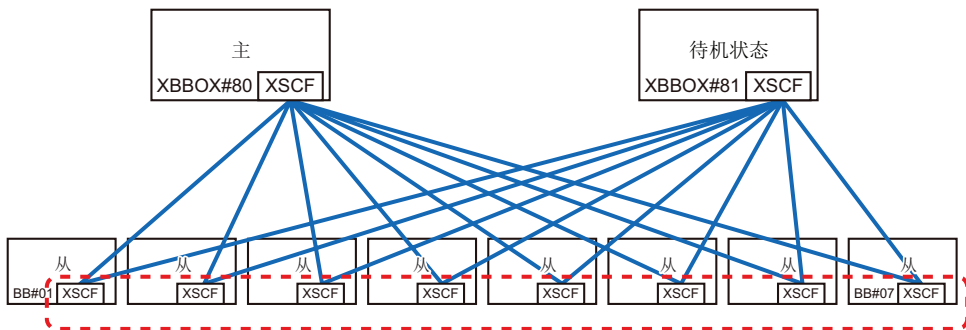


图 1-6 显示了 8BB 配置（有接线盒）中 SPARC M12-2S 或 SPARC M10-4S 的示例。

图 1-6 SPARC M12-2S/M10-4S 系统 XSCF 配置（有接线盒）示例



模块化架构配置中的 XSCF 分为三个角色：主、备用和从。有关详情，请参见“1.2.4 主/备用/从 XSCF 的机制”。

外部接口

SPARC M12/M10 中的单个机箱和接线盒安装有以下与 XSCF 相关的连接器（端口）和 LED。用户、系统管理员和现场工程师可以使用这些接口和 XSCF 固件来监视和操作服务器。

有关各接口的位置和连接方法的详情，请参见以下任一内容。

- 所使用服务器《安装指南》中的“查看外部接口端口规格”
- 所使用服务器《Service Manual》中的“Understanding the LED Indications”
- 串行端口
串行端口用于通过 XSCF shell 配置服务器和查看服务器状态。串行端口 (RS-232C) 使用 RJ-45 连接器。串行端口和 PC 间通过 RS-232C 串行跨接线进行连接。如果使用 LAN 线连接，则需要使用 RJ-45/RS-232C 转换线或转换连接器。
- XSCF-LAN 端口（以太网端口）
XSCF-LAN 端口为 LAN 接口，可让系统管理员通过以太网操作服务器。通过 XSCF-LAN 端口，系统管理员可以使用 XSCF shell 或 XSCF Web 配置服务器或查看服务器状态。有两个 XSCF-LAN 端口。两个端口都使用 RJ-45 接口。每个端口仅

支持带自动协商的 10Base-T/100Base-TX/1000Base-T。XSCF-LAN 的连接速度/连接方式无法设置。

- USB 端口
一个 USB 端口 (Type-A) 装配在前面板, 两个 USB 端口装配在后面板用于连接 USB 设备。例如将 DVD 驱动器连接在 USB 端口, 进行 Oracle Solaris 的安装。后面板上的 XSCF 专用 USB 端口支持 USB 1.1 或 USB2.0 接口。用于保存和恢复 XSCF 硬件信息以及收集日志信息。
- LED
以下 LED 对应 XSCF 和 XSCF-LAN。
 - READY LED (绿色)
READY LED 亮起绿色。输入电源开启后, READY LED 立即开始闪烁。闪烁表示 XSCF 正在启动和初始化。XSCF 初始化结束后, LED 停止闪烁并保持亮起。
 - CHECK LED (琥珀色)
CHECK LED 亮起琥珀色。输入电源开启后, CHECK LED 立即亮起。但是, 硬件正常运行时, CHECK LED 保持熄灭。硬件发生某种故障时它会亮起。
 - MASTER LED (绿色, 仅适用于 SPARC M12-2S/M10-4S 系统)
MASTER LED 亮起绿色。在具有多个 XSCF 的系统中, MASTER LED 表示 SPARC M12-2S 机箱、SPARC M10-4S 机箱或有主 XSCF 的接线盒。对于主 XSCF 它会亮起, 对于备用 XSCF 和从 XSCF 会熄灭。
 - LINK SPEED (绿色或琥珀色)
每个 XSCF-LAN 端口都配置 Link Speed LED, 亮起绿色或琥珀色。对于 1000-Mbps LAN 连接, Link Speed LED 亮起琥珀色, 对于 100-Mbps LAN 连接亮起绿色。对于 10-Mbps LAN 连接则熄灭。
 - ACT LED (绿色)
每个 XSCF-LAN 端口都有 ACT LED, 亮起绿灯。正在发送或接收数据时, 此指示灯绿色闪烁。不发送或接收数据时, 此指示灯熄灭。
- SP 到 SP 通讯端口协议 (SSCP 端口)
在具有模块化架构配置和多个 XSCF 的系统中, 以下连接器 (端口) 安装在每个 SPARC M12-2S 或 SPARC M10-4S 机箱和接线盒上, 因为通讯是在服务处理器之间进行。有关 XSCF 之间的连接配置, 请参见《Fujitsu SPARC M12-2S 安装指南》中的 "第4章 设置模块化架构配置中的 SPARC M12-2S" 或《Fujitsu M10-4S/SPARC M10-4S 安装指南》中的 "第4章 配置模块化架构连接"。
 - SPARC M12-2S/M10-4S 侧
XSCF DUAL 控制端口: 1 个端口。本端口将主和备用 XSCF 连接在一起。
XSCF BB 控制端口: 3 个端口。这些端口将主和备用 XSCF 连接到从 XSCF。
 - 接线盒侧
XSCF DUAL 控制端口: 1 个端口。本端口将主和备用 XSCF 连接在一起。
XSCF BB 控制端口: 19 个端口。这些端口将主和备用 XSCF 连接到从 XSCF。

1.2.3 XSCF 功能

XSCF shell 和 XSCF Web

XSCF 提供 XSCF shell 和 XSCF Web，让用户能够查看服务器状态、操作服务器、查看物理分区状态、操作物理分区和显示控制台。

系统初始化和初始诊断

在输入电源开启时或 XSCF 重新启动时，XSCF 执行初始自诊断，以检测并通知用户 XSCF 中的任何故障。它也进行 XSCF 的初始硬件设置，并也初始化启动 Oracle Solaris 所需的硬件。

系统配置识别和物理分区配置管理

XSCF 按机箱管理 CPU、内存和 I/O 系统资源，显示系统配置的状态，并创建和更改物理分区配置。

在 SPARC M12-2S 和 SPARC M10-4S 中，用户可以通过将一个机箱 (1BB) 的模块化架构系统作为最小单位来连接多个机箱，从而配置物理分区。机箱 (BB)、物理分区配置单元按逻辑编号 (LSB 编号) (由逻辑域识别) 管理。

另外，通过与虚拟机监控程序固件的连接，XSCF 固件会监视由 Oracle VM Server for SPARC 软件配置的逻辑域使用的内存、CPU 和 I/O 资源。

注 - 一个 SPARC M12/M10 单元的系统组成一个物理分区。

故障监视和 RAS 功能

XSCF 批量控制/监控服务器以使系统稳定运行。检测到系统故障时，立即开始收集硬件日志，进行分析，识别故障的位置并确定故障的状态。XSCF 显示服务器状态，并根据需要执行部件降级、物理分区降级和系统重置以防止其他故障的发生。XSCF 可保证整个系统的可靠性、可用性和可服务性 (RAS)。

监控目标 如下。

- 监控和管理硬件配置
- 监控网络配置
- 监控散热单元，如风扇单元和环境温度
- 监控物理分区和逻辑域的状态
- 监控外设的故障

向系统管理员通知故障信息的功能

XSCF 始终在监控系统操作。XSCF 提供以下服务来通知系统管理员故障信息。

- 不依赖于 Oracle Solaris 操作的服务器监视功能
- 从远程位置远程控制服务器
- 发生故障时电子邮件通知
- 使用 SNMP 代理功能进行陷阱通知

信息传送和日志记录

XSCF 收集并储存有关系统故障的信息。故障发生后，硬件故障信息能够识别故障内容和故障的位置，同时立即为用户提供准确、易懂的服务器故障预测。有关错误消息和日志的详情，请参见“第12章 检查日志和信息”。

显示如下信息。

- 系统启动时的初始诊断信息
- 网络配置监控中检测到的配置错误信息
- 监测到部件故障时的错误信息
根据电源、风扇、系统板、内存、CPU 和其它组件监控中故障检测的信息，系统管理员能够立即确认需要更换的部件。
- 监测到环境故障时的错误信息
监测服务器温度和 CPU 温度可以防止由于温度升高造成的系统不稳定。

收集如下信息。

- 错误日志
- 监视信息日志
- 电源日志
- 事件日志
- 控制台日志
- 崩溃日志
- IPL 日志
- 审核日志
- COD 日志
- 温度历史记录日志
- 活动目录日志
- LDAP over SSL 日志

XSCF 用户帐户管理

XSCF 管理使用 XSCF 的用户帐户。下面列出 XSCF 管理用户帐户的主要权限类型。根据用户帐户类型（称为用户权限），提供可以操作的 XSCF shell 和 XSCF Web。

- 系统管理员
- 物理分区管理员
- 操作员
- 现场工程师

安全

XSCF 通过 SSH 和 SSL/TLS 提供加密和审核功能。系统运行时它会记录操作错误和无效访问。系统管理员能够使用日志调查系统故障或无效访问的原因。

协助活动部件的更换

在活动部件更换中，XSCF 使用 XSCF shell 来协助维护工作。执行维护命令时，显示维护菜单。用户可按照菜单执行维护工作。

控制台重定向功能

XSCF 提供向各物理分区中的 Oracle Solaris 的 OS 控制台（控制域控制台）产生输出的功能。通过执行到 XSCF 的 SSH (Secure Shell) 或 Telnet 连接，XSCF 可以用作 OS 控制台。

CPU 激活注册/管理功能

使用 XSCF 注册 CPU 激活密钥可以永久使用服务器 CPU 资源。在服务器投入运行之前，需要为一个或多个 CPU 购买 CPU 激活许可。

需要额外的 CPU 资源时，XSCF 可执行添加 CPU 激活密钥的工作。需要减少 CPU 资源时，XSCF 可执行移除 CPU 激活密钥的工作。
有关 CPU 内核资源使用的详情，请参见“第5章 CPU 激活”。

固件更新功能

使用 XSCF Web 和 XSCF shell 命令，您可以下载新固件（XSCF 固件、OpenBoot PROM 固件、POST 固件或虚拟机监控程序固件），而无需关闭物理分区。您还可以不必关闭其它物理分区电源，即可应用固件更新。请注意，如果在物理分区启动时您更新 OpenBoot PROM 固件、POST 固件或虚拟机监控程序固件，则在物理分区重新启动时该更新被应用。有关固件更新的详情，请参见“第16章 更新 XCP 固件”。

绿色 IT 功能

Oracle Solaris、虚拟机监控程序和 XSCF 会停止向未运行的组件供电以降低功耗。此外，XSCF 可以控制功耗上限以降低系统功耗。如果超过上限，XSCF 会立即确定系统供电的状态并关闭或切断电源。

时间控制

SPARC M12/M10 将 XSCF 时钟设置为系统参考时间。

在物理分区启动时，SPARC M12/M10 系统的物理分区与 XSCF 时钟时间同步。与虚拟机监控程序固件联动时，XSCF 管理与控制域的时间差。

物理分区动态重新配置 (PPAR DR) 功能

在模块化架构配置中，XSCF 支持在系统运行时动态更改物理分区的配置所需的工作。物理分区 (PPAR DR) 的动态重新配置使您能够在物理分区正在运行时添加或删除物理分区的模块化架构（SPARC M12-2S 或 SPARC M10-4S）。有关 PPAR DR 功能的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

注 - 在 SPARC M12-1/M12-2/M10-1/M10-4 中，无法使用 PPAR DR 功能。

1.2.4 主/备用/从 XSCF 的机制

在 SPARC M12-2S 或 SPARC M10-4S 由模块化架构系统连接的系统中，每个 SPARC M12-2S 或 SPARC M10-4S 机箱和接线盒都安装了一个 XSCF。根据其作用将 XSCF 分为三种类型。

- 主 XSCF
系统只包含一个主 XSCF。除了监视和管理整个系统之外，主 XSCF 还管理安装有 XSCF 的 SPARC M12-2S、SPARC M10-4S 或接线盒。为了双重化，备用 XSCF 作为主 XSCF 的备份运行。
- 从 XSCF
从 XSCF 是除主 XSCF 以外的其他 XSCF。从 XSCF 仅监视和管理安装有 XSCF 的 SPARC M12-2S、SPARC M10-4S 或接线盒。
- 备用 XSCF
此 XSCF 作为主 XSCF 的备份运行。它也称为待机 XSCF。一个备用 XSCF 包含在从 XSCF 中。

主 XSCF 和备用 XSCF 互相监控。如果主 XSCF 发生故障，主 XSCF 可以切换到备用 XSCF，因此系统操作和管理不会中断。

主 XSCF 通过专用线缆，采用称作内部服务处理器通信协议 (SSCP) 的 XSCF 专用协议连接到从 XSCF。针对主 XSCF 的设置通过 SSCP 应用在从 XSCF 上。针对指定物理分区的设置只应用在属于 PPAR 的 XSCF 上。

1.2.5 不同型号间 XSCF 配置的差异

本节介绍如何配置 XSCF 以及如何在 SPARC M12/M10 的相应配置中监视和管理系统。

SPARC M12-1/M12-2/M10-1/M10-4 和单机配置中的 SPARC M12-2S/M10-4S

SPARC M12-1/M12-2/M10-1/M10-4 和单机配置中的 SPARC M12-2S/M10-4S 都具有仅有一个 XSCF 的配置。没有备用 XSCF 或主 XSCF。

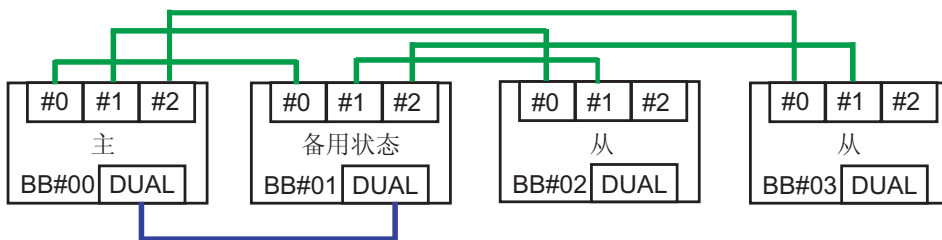
模块化架构配置中的 SPARC M12-2S/M10-4S（无接线盒）

无接线盒的模块化架构配置中的 SPARC M12-2S/M10-4S 系统最多配置四个 SPARC M12-2S 或 SPARC M10-4S 机箱，因此配置最多可以有四个 XSCF。在该配置中，BB#00 或 BB#01 机柜中的 XSCF 是主 XSCF 或 XSCF。如果主 XSCF 发生错误，备用 XSCF 会切换到主 XSCF。BB#02 和 BB#03 机柜固定为从 XSCF。

- 连接形式
主 XSCF（图 1-7 中的 BB#00）的 XSCF BB 控制端口连接到每个从 XSCF 上网络 ID 为 0（图 1-7 中的 BB#01 至 BB#03 的 #0 端口）的 XSCF BB 控制端口。
备用 XSCF（图 1-7 中的 BB#01）的 XSCF BB 控制端口连接到每个从 XSCF 上网络 ID 为 1（图 1-7 中的 BB#02 和 BB#03 的 #1 端口）的 XSCF BB 控制端口。主 XSCF 和备用 XSCF 通过 XSCF DUAL 控制端口连接。从 XSCF 只连接到主 XSCF 和备用 XSCF。

- XSCF 控制流程
主 XSCF 监控和管理所有 XSCF。原则上，在主 XSCF 中对 XSCF 进行各种设置。对主 XSCF 所做的设置应用在所有从 XSCF 上，包括通过 SSCP 网络的备用 XSCF。此外，对给定的 SPARC M12-2S 或 SPARC M10-4S 机箱使用主 XSCF 进行的设置也将反映在预期的 SPARC M12-2S 或 SPARC M10-4S 机箱中的备用 XSCF 和从 XSCF 上。

图 1-7 XSCF 连接（适用于模块化架构配置中的 SPARC M12-2S/M10-4S（无接线盒））

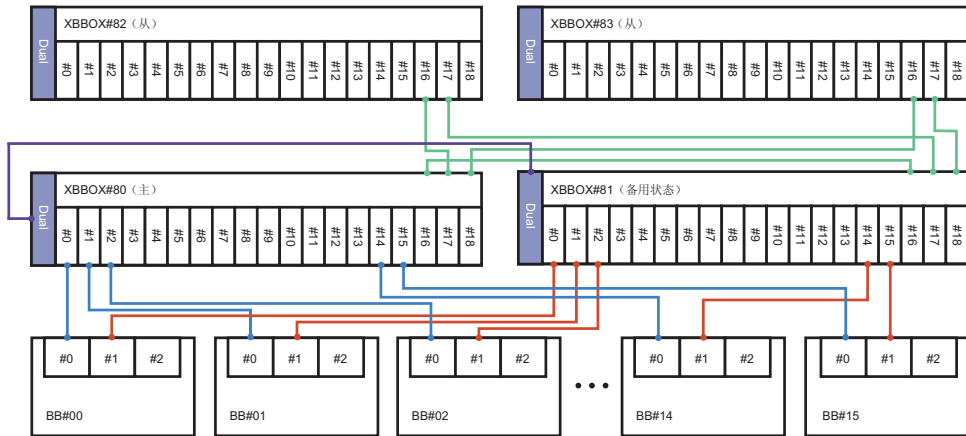


模块化架构配置中的 SPARC M12-2S/M10-4S（有接线盒）

模块化架构配置中的 SPARC M12-2S 或 SPARC M10-4S（有接线盒）最多配置 16 个 XSCF，接线盒最多配置四个 XSCF。在该配置中，XBBOX#80 或 XBBOX#81 接线盒中的 XSCF 是主 XSCF 或备用 XSCF。XBBOX#82 和 XBBOX#83 接线盒中的 XSCF，以及所有 SPARC M12-2S 或 SPARC M10-4S 机箱中的 XSCF 都被固定为从 XSCF。

- 连接形式
 - 至接线盒的连接
主 XSCF (XBBOX#80) 连接到每个从 XSCF 上网络 ID 为 16（图 1-8 中的 XBBOX#81 至 XBBOX#83 的 #16 端口）的 XSCF BB 控制端口。备用 XSCF (XBBOX#81) 连接到每个从 XSCF 上网络 ID 为 17（图 1-8 中的 XBBOX#82 和 XBBOX#83 的 #17 端口）的 XSCF BB 控制端口。主 XSCF 和备用 XSCF 通过 XSCF DUAL 控制端口连接。不能连接到除主 XSCF 和备用 XSCF 以外的任何 XSCF。
 - 至 SPARC M12-2S/M10-4S 的连接
主 XSCF (XBBOX#80) 连接到每个从 XSCF 上网络 ID 为 0（图 1-8 中的 BB#00 至 BB#15 的 #0 端口）的 XSCF BB 控制端口。备用 XSCF (XBBOX#81) 连接到每个从 XSCF 上网络 ID 为 1（图 1-8 中的 BB#00 至 BB#15 的 #1 端口）的 XSCF BB 控制端口。固定为从 XSCF (BB#00 到 BB#15) 的 XSCF 只连接到主 XSCF 和备用 XSCF。
- XSCF 控制流程
主 XSCF 监控和管理所有 XSCF。原则上，在主 XSCF 中对 XSCF 进行各种设置。对主 XSCF 所做的设置应用在所有从 XSCF 上，包括通过 SSCP 网络的备用 XSCF。此外，对给定的 SPARC M12-2S 或 SPARC M10-4S 机箱使用主 XSCF 进行的设置也将反映在预期的 SPARC M12-2S 或 SPARC M10-4S 机箱中的备用 XSCF 和从 XSCF 上。

图 1-8 XSCF 连接（适用于模块化架构配置中的 SPARC M12-2S/M10-4S（有接线盒））



1.3 网络配置

1.3.1 网络连接概述

本节概括介绍系统操作的网络连接。

系统由两个主要网络组成。一个是用户网络，另一个是系统控制网络。

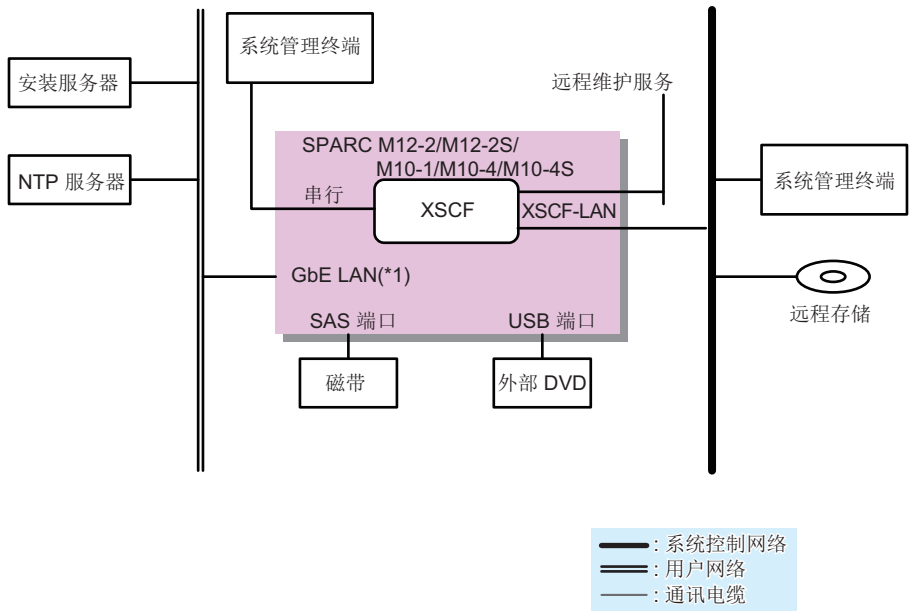
- 用户网络
用户网络用于运行已配置的业务系统。根据业务需要做出相应的配置后，用户网络可以连接到其它服务器、PC 和外设。
用户网络连接到外部 Internet 时，需要通过安装防火墙或采取其他必要的安全措施。
- 系统控制网络（XSCF 网络）
系统控制网络（XSCF 网络）用于维护和管理系统。本网络还可用于对 XSCF 固件进行操作，该固件用于监控管理系统、电源开启/关闭操作以及组件的更换作业。如果要执行远程系统控制操作，可配置一个设置有系统控制网络的环境。
系统控制网络也可以连接到用户网络，因此必须采取更高安全措施（如安装防火墙软件）以防止对于系统控制网络的非法外部访问。
根据具体情况，采用串行或 LAN 连接，使用终端（系统管理终端）维护和管理系统。有关系统管理终端的连接形式，请参见“2.1 连接系统管理终端”。

以下示例显示了 SPARC M12/M10 系统配置。

图 1-9 显示了使用一个 SPARC M12/M10 的配置。
系统管理终端通过串行端口或系统控制网络连接到 XSCF-LAN 端口。远程存储通过系

统控制网络连接到 XSCF-LAN 端口。GbE LAN 端口或 10GbE LAN 端口通过用户网络连接到安装服务器和其他服务器。此外，SAS 端口连接到外部 SAS 接口设备，如磁带单元，USB 端口连接到外部 USB 接口设备，如外部 DVD 驱动器。

图 1-9 SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S 的单机配置的连接配置示例

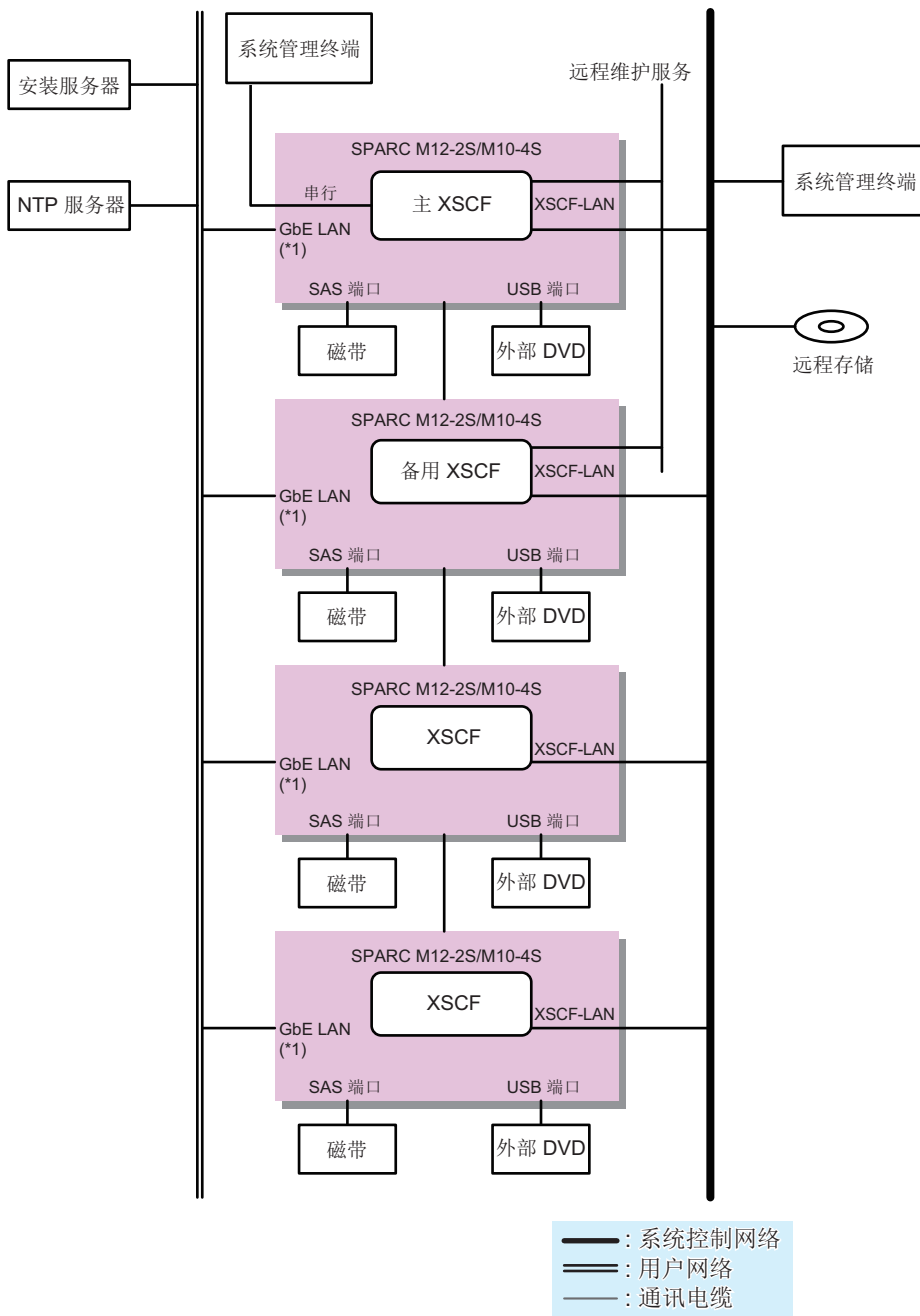


*1 SPARC M12-1/M12-2/M12-2S 使用 10GbE LAN

图 1-10 显示了四个 SPARC M12-2S 或 SPARC M10-4S 单元不使用接线盒而连接的配置。

系统管理终端通过系统控制网络连接到主 XSCF 的串行端口或连接到主 XSCF 和备用 XSCF 的 XSCF-LAN 端口。四个 SPARC M12-2S 单元的 10GbE LAN 端口或四个 SPARC M10-4S 单元的 GbE LAN 端口通过用户网络连接到安装服务器和其他服务器。此外，SAS 端口连接到外部 SAS 接口设备，如磁带单元，USB 端口连接到外部 USB 接口设备，如外部 DVD 驱动器。

图 1-10 SPARC M12-2S/M10-4S 连接的配置示例（无接线盒）

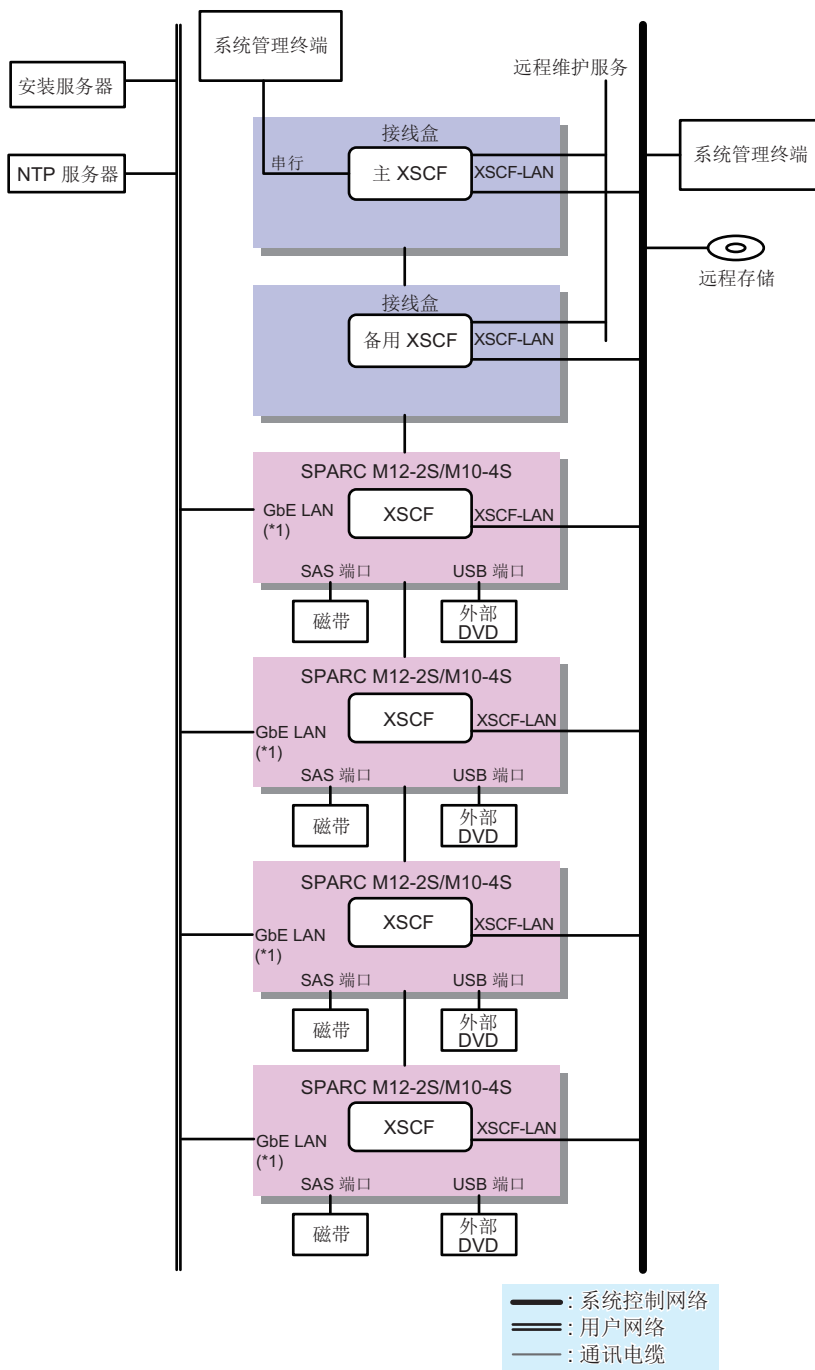


*1 SPARC M12-2S 使用 10GbE LAN

图 1-11 显示了多个 SPARC M12-2S 或 SPARC M10-4S 单元通过接线盒连接的配置。系统管理终端通过系统控制网络连接到接线盒中的主 XSCF 的串行端口或连接到主 XSCF 和备用 XSCF 的 XSCF-LAN 端口。远程存储器通过系统控制网络连接到每个

SPARC M12-2S 或 SPARC M10-4S 单元的 XSCF-LAN。
SPARC M12-2S 的 10GbE LAN 端口或 SPARC M10-4S 的 GbE LAN 端口通过用户网络连接到安装服务器和其他服务器。此外，SPARC M12-2S 或 SPARC M10-4S 单元的 SAS 端口连接到外部 SAS 接口设备，如磁带单元，USB 端口连接到外部 USB 接口设备，如外部 DVD 驱动器。

图 1-11 SPARC M12-2S/M10-4S 连接的配置（有接线盒）

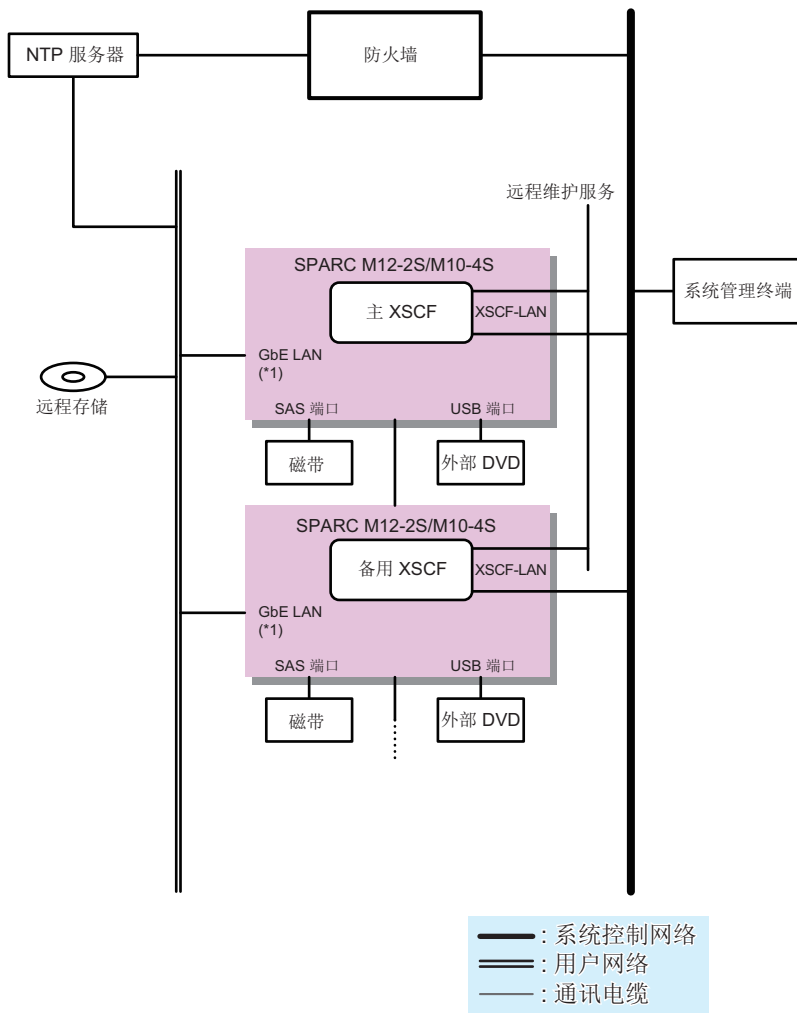


*1 SPARC M12-2S 使用 10GbE LAN

图 1-12 显示了通过防火墙连接系统控制网络 and 用户网络的配置。这里，如需使用 NTP 服务器以同步 XSCF 的时间，需通过防火墙连接用户网络上的

NTP 服务器。通过防火墙的连接可以保护 XSCF 免于用户网络上的安全威胁。对于放置在用户网络上的远程存储，您可以通过配置防火墙中的远程存储访问，保护免受安全威胁的同时将其连接到 XSCF-LAN。

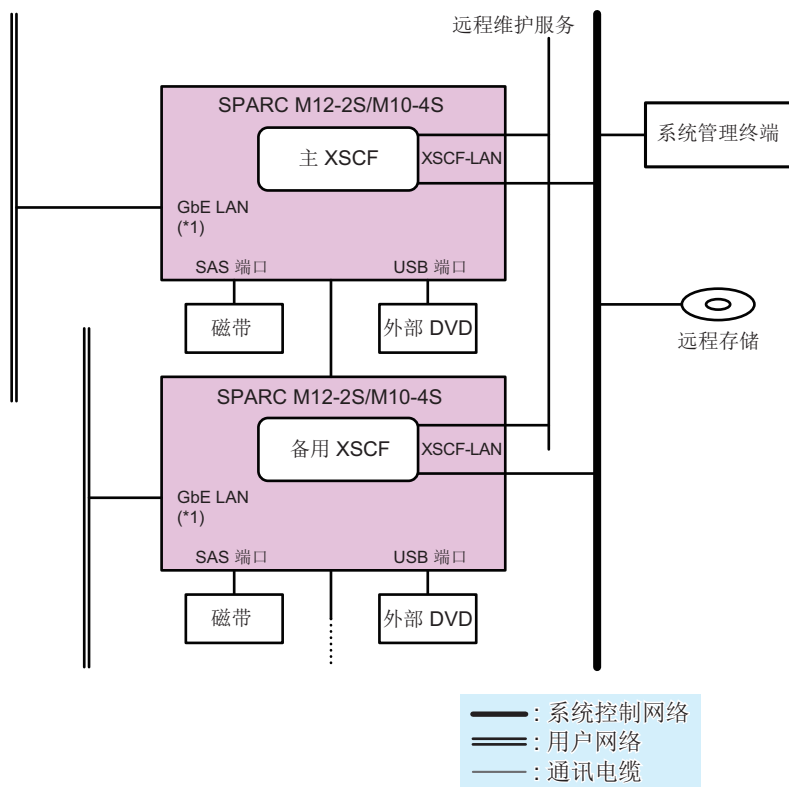
图 1-12 连接系统控制网络 and 用户网络的配置



*1 SPARC M12-2S 使用 10GbE LAN

图 1-13 显示了模块化架构配置中的系统，其中每个 SPARC M12-2S 或 SPARC M10-4S 单元连接到单独的用户网络。分离连接到每个 SPARC M12-2S 单元的 10GbE LAN 的用户网段或连接到每个 SPARC M10-4S 单元的 GbE LAN 的用户网段可以降低来自用户网络上安全威胁的风险。模块化架构配置中的每个 SPARC M12-2S 或 SPARC M10-4S 单元的系统控制网络不能分离。

图 1-13 分离每个服务器用户网段的配置



*1 SPARC M12-2S 使用 10GbE LAN

1.3.2 XSCF-LAN 端口号和功能以及防火墙

表 1-1 列出了 XSCF-LAN 端口使用的端口号和 XSCF 使用的功能。为了防止对 XSCF 的非法访问和攻击，建议在进行外部网络连接时配置一个防火墙。安装防火墙时，您需要按照要求允许数据包通过端口。

表 1-1 XSCF-LAN 端口号、功能和连接方向

端口号/协议	功能	连接方向 (*)
21/TCP	XSCF shell 外部传输 (FTP)	XSCF -> 外部网络 (21)
22/TCP	XSCF shell (SSH)	外部网络 -> XSCF (22)
	XSCF shell 外部传输 (SSH)	XSCF -> 外部网络 (22)
23/TCP	XSCF shell (Telnet)	外部网络 -> XSCF (23)
25/TCP	电子邮件通知和远程维护服务	XSCF -> 外部网络 (25)
53/TCP	DNS	XSCF (53) -> 外部网络 (53)
53/UDP		

表 1-1 XSCF-LAN 端口号、功能和连接方向 (续)

端口号/ 协议	功能	连接方向 (*)
80/TCP	XSCF shell 外部传输 (HTTP)	XSCF -> 外部网络 (80)
110/TCP	通过 POP 验证电子邮件通知, 通过 POP 验证远程维护服务	XSCF -> 外部网络 (110)
123/UDP	与 NTP 服务器时间同步 从 NTP 客户端时间同步	XSCF (123) -> 外部网络 (123) 外部网络 (123) -> XSCF (123)
161/UDP	SNMP 功能	外部网络 -> XSCF (161)
162/UDP	SNMP 陷阱功能	XSCF -> 外部网络 (162)
389/TCP	通过 LDAP 和 Active Directory 进行验证	XSCF -> 外部网络 (389)
443/TCP	XSCF Web (HTTPS) XSCF shell 外部传输 (HTTPS)	外部网络 -> XSCF (443) XSCF -> 外部网络 (443)
465/TCP	远程维护服务 (SMTP over SSL)	XSCF -> 外部网络 (465)
587/TCP	通过 SMTP 验证电子邮件通知, 通过 SMTP 验证远程维护服务	XSCF -> 外部网络 (587)
623/UDP	使用 IPMI 的远程电源管理功能	XSCF (623) <-> 外部网络 (623)
636/TCP	通过 LDAP over SSL、Active Directory 进行验证	XSCF -> 外部网络 (636)
3260/TCP	远程存储	XSCF -> 外部网络 (3260)
6481/TCP	自动服务请求 (ASR) 功能 (服务标签)	外部网络 (6481) -> XSCF (6481)
6481/UDP	(*2)	

*1 括号中的各符号和数字含义如下:

符号 ->: 表示从左到右的方向。<->: 表示从左到右或从右到左的方向。

括号中的数字: 连接端口号 对于与外部网络的连接, 可以在 XSCF 上更改网络的端口号。有关详细信息, 请参见本文档中相应功能的章节。对于与远程存储器的连接, 存储器的端口号是固定的 (3260)。

*2 ASR 功能是一种远程维护服务, 运行由 Oracle Corporation 公司提供的 Oracle Auto Service Request 软件。有关 ASR 功能的详细信息, 请参见您正在使用的软件版本的《Oracle Auto Service Request Installation and Operations Guide》。

1.4 虚拟机监控程序基本知识

本节对内置到 SPARC M12/M10 系统的虚拟机监控程序固件进行简要介绍。

虚拟机监控程序固件用于执行虚拟化。它安装在 CPU 内存单元上。

安装在逻辑域上的不同固件和软件 (如 XSCF 固件和 Oracle Solaris) 正在每个 SPARC M12/M10 系统上运行。这些固件和软件监控和管理整个系统。虚拟机监控程序固件安装在 XSCF 固件和 Oracle Solaris 之间, 用作一个界面, 将设置信息从 XSCF 传输到逻辑域并向 XSCF 通知逻辑域的状态。

虚拟机监控程序固件有如下主要功能。

- 在 XSCF 所管理物理分区与 Oracle VM Server for SPARC 所管理逻辑域之间传输信息。根据从 XSCF 传输到控制域的 PPAR 配置信息 (PCL)，Oracle VM Server for SPARC 配置逻辑域。除此以外，逻辑域配置信息和重新配置的硬件资源信息通过虚拟机监控程序传输到 XSCF 固件。

有关 PPAR 配置信息的详情，请参见“[11.2.2 查看物理分区配置](#)”。

- 传输关于逻辑域挂起或故障的信息
如果逻辑域挂起或故障，虚拟机监控程序会将逻辑域状态通知 XSCF。
- 传输关于 XSCF 和逻辑域日期和时间的信息
逻辑域中的时间设置由虚拟机监控程序通知 XSCF。与整个系统的时间有差异时，XSCF 将时间保存在逻辑域。

1.5 Oracle VM Server for SPARC 基本知识

本节概括介绍 Oracle VM Server for SPARC 软件。

Oracle VM Server for SPARC 软件用于配置逻辑域环境。在 Oracle Solaris 环境中安装并使用。

通过在 XSCF 固件组建的物理分区中灵活地分配硬件资源，如 CPU、内存和 I/O 设备，并使用这些资源配置逻辑域。这些资源被指定为虚拟硬件环境。配置的逻辑域可以运行业务应用程序，每个应用程序都在独立的 Oracle Solaris 环境中。在一个或多个 SPARC M12 或 SPARC M10 单元中构建多个虚拟硬件环境可实现更高的服务器利用率，与服务器集成相比较可降低成本。

典型的逻辑域是控制域（创建和控制其他逻辑域）以及用于业务应用程序的来宾域。在每个 SPARC M12/M10 系统中，每个物理分区创建一个控制域，以管理物理分区中配置的其他逻辑域。Oracle VM Server for SPARC 在控制域中运行，用于配置和管理来宾域。

控制域也用于通过内置的虚拟机监控程序固件，向 XSCF 固件通知逻辑域的信息。XSCF 中的设置信息也通过虚拟机监控程序固件传输到控制域。

即使逻辑域已经组建并投入业务运营，也可以通过逻辑域的操作状态重新配置 CPU、内存、I/O 设备和其它硬件资源。硬件资源重新配置也可以通过 Oracle VM Server for SPARC 实现。当一个任务临时增加系统负担时，增加硬件资源可以保持硬件资源高利用率并防止执行任务时溢出。

有关使用 SPARC M12/M10 系统中的 Oracle VM Server for SPARC 配置和重新配置逻辑域的详细信息，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。有关 Oracle VM Server for SPARC 的详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》。

1.6 OpenBoot PROM 基本知识

本节概括介绍 OpenBoot PROM。

OpenBoot PROM 提供 Oracle Solaris 启动所需的基本功能。

在 OpenBoot PROM 环境中，控制台屏幕上显示 ok 提示。您可以通过定义 OpenBoot PROM 环境变量，配置与启动与 Oracle Solaris 有关的各种功能。您可以使用以下命令之一定义 OpenBoot PROM 环境变量。

- 在 OpenBoot PROM 环境中执行 `setenv` 命令（在 ok 提示下）。
- 在 Oracle Solaris 环境中执行 `eeprom` 命令。

使用 XSCF 固件的 `setpparam` 命令可以覆盖若干 OpenBoot PROM 环境变量。

有关 OpenBoot PROM 环境变量和命令的详细信息，请参见 Oracle 公司的《OpenBoot 4.x Command Reference Manual》。

有关 SPARC M12/M10 不支持的 OpenBoot PROM 环境变量和命令的详细信息，请参见“附录 H OpenBoot PROM 环境变量和命令”。

登录和注销 XSCF

本章介绍系统管理终端的连接形式以及登录 XSCF 的方法。

- 连接系统管理终端
- 登录 XSCF Shell
- 从 XSCF Shell 注销
- 登录 XSCF Web
- 从 XSCF Web 注销
- 可连接的用户数

2.1 连接系统管理终端

本节介绍系统控制网络中系统管理终端连接的形式。有关实际的连接方法，请参见“[2.2 登录 XSCF Shell](#)”。

系统管理网络的连接形式根据连接的端口分为如下两种类型。

- 串行连接
通过串行线连接到串行端口。
- LAN 连接
通过 LAN 线连接到 XSCF-LAN 端口。

通常系统管理终端连接到串行端口进行 XSCF 固件初始设置。一旦完成 XSCF 的网络设置，即可选择串行连接和 LAN 连接。

下一小节介绍每种连接的特点。

2.1.1 通过串行端口连接

串行连接是使用串行线连接在服务器上串行端口的连接形式。如果 SPARC M12-2S 或 SPARC M10-4S 处于模块化架构配置中，将串行线连接到具有主 XSCF 的机箱。系统管理终端和主 XSCF 是 1 对 1 连接，因此系统环境安全。系统管理终端通过串行线连接

时，主 XSCF 显示登录画面。

图 2-1 串行端口 (SPARC M12-1)

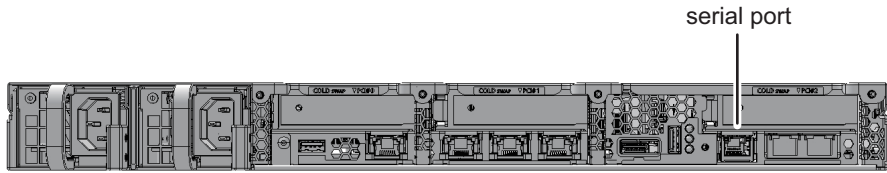


图 2-2 串行端口 (SPARC M12-2)

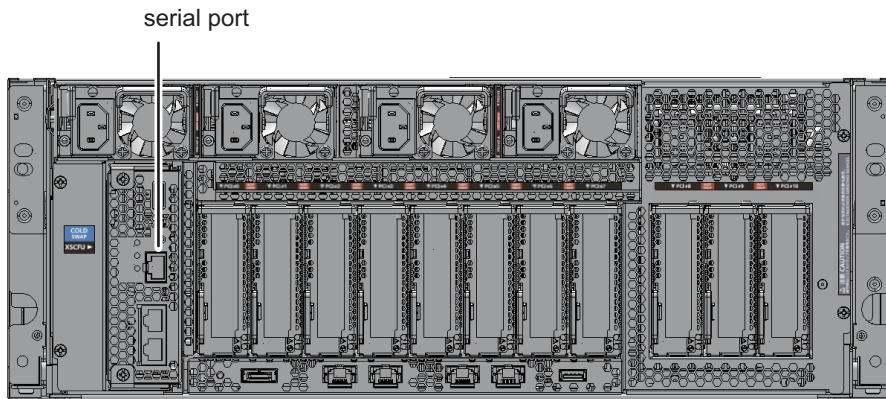


图 2-3 串行端口 (SPARC M12-2S)

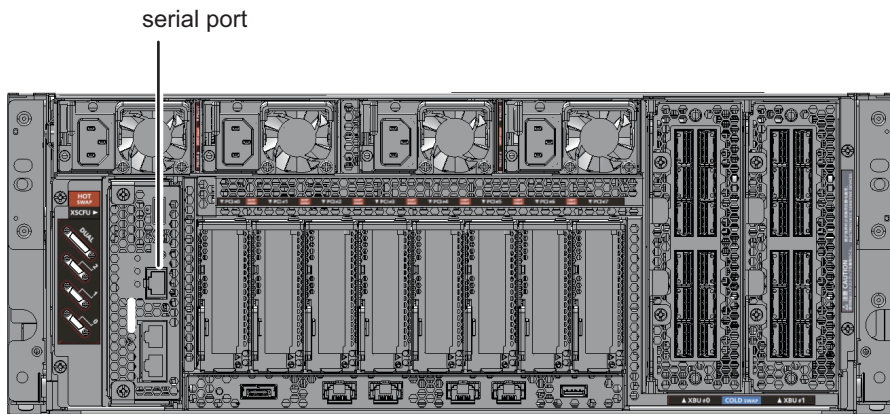


图 2-4 串行端口 (SPARC M10-1)

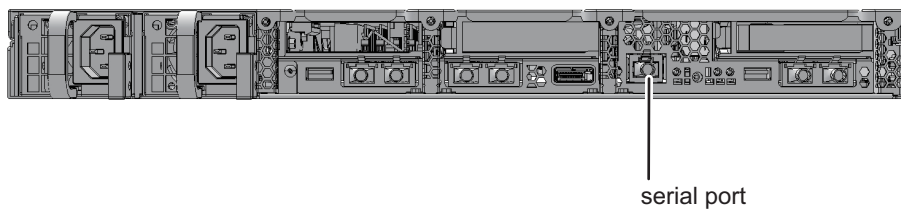


图 2-5 串行端口 (SPARC M10-4S)

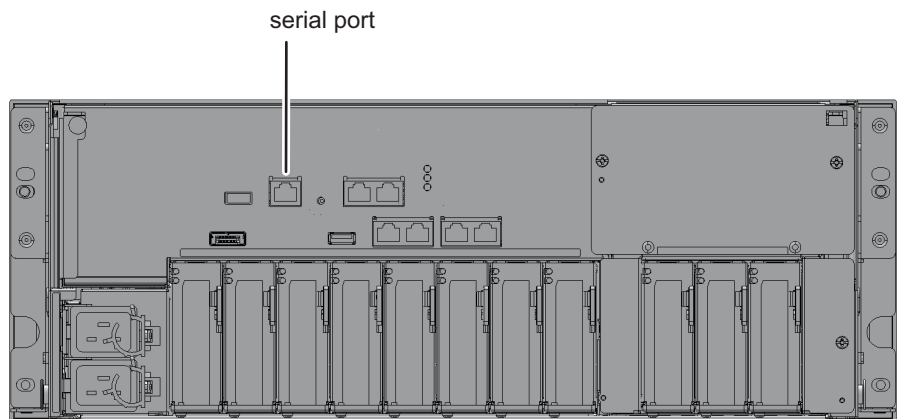
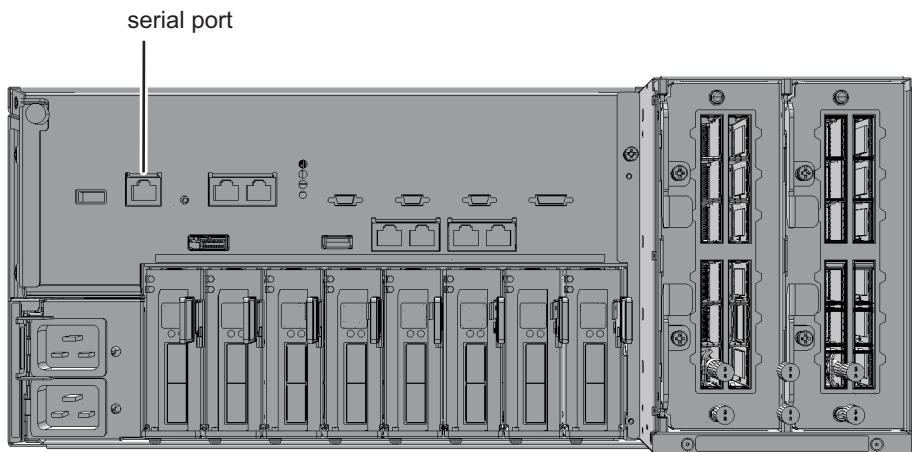


图 2-6 串行端口 (SPARC M10-4S)

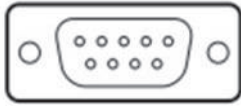


登录 XSCF 后, 您可以使用 XSCF shell。使用 XSCF 命令监控和管理系统。如果您需要监控或管理逻辑域, 可以将 XSCF shell 切换到控制域。有关切换方法, 请参见 ["8.3 从 XSCF Shell 切换到控制域控制台"](#)。

串行连接需要做好以下准备工作。

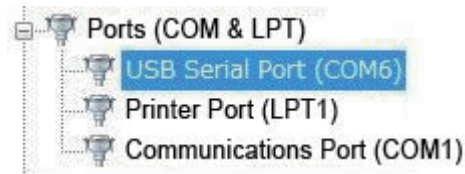
- 准备串行线
将附带的 D-Sub 9 针 RS-232C 线放在手边。如果终端没有串行端口，您需要使用 RJ-45/RS-232C 转换线、转换接头或 USB /串行转换转换线。

图 2-7 RC-232C D-Sub 9 针接口



- 准备用于连接的终端软件
使用 XSCF shell 时，请为终端软件设置 TERM=vt100。
- 确认所识别的串行端口
将串行线连接到终端，然后确认所识别的串行端口。将识别的串行端口指定为 XSCF 的串行连接端口。
以下示例显示被识别为 COM6 的串行端口。

图 2-8 确认串行端口（带设备管理器）



2.1.2 串行连接中终端可用的功能

通过连接到串行端口的终端，您可以使用 XSCF shell 和控制域的控制台（控制域控制台）。XSCF Web 不可用。

表 2-1 列出了串行连接的终端和控制台以及可用的功能。

表 2-1 串行连接终端和控制台以及可用的功能

终端类型	工作	线缆
XSCF shell 终端	<ul style="list-style-type: none">- 在连接到串行端口后您可以立即使用 XSCF shell 终端。- 您可以使用 console 命令切换到控制域控制台窗口。- 登录后，如果 XSCF shell 在规定的期间内没有操作，将被强制注销。有关 XSCF 会话超时设置的详细信息，请参见 setautologout(8) 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。	需要 RS-232C 串行跨接线。当您只有 LAN 线时，在 PC 侧需要 9 针转换线。

表 2-1 串行连接终端和控制台以及可用的功能 (续)

终端类型	工作	线缆
控制域控制台 (RW 控制台)	<ul style="list-style-type: none"> - 本 OS 控制台可用于输入/输出。从 XSCF shell 终端中，通过使用 <code>console</code> 命令指定物理分区和可写入控制台，您可以打开 RW 控制台。 - 在一个物理分区中，一次只能有一个用户（一个连接）可以使用 RW 控制台。 - 如需了解控制域控制台未被使用时的会话超时时间设置，请参见 Oracle Solaris 参考手册中关于 <code>ttymon</code> 的说明。 	
控制域控制台 (RO 控制台)	<ul style="list-style-type: none"> - 这是查看专用的 OS 控制台。从 XSCF shell 终端中，通过使用 <code>console</code> 命令指定物理分区和查看专用控制台，您可以打开 RO 控制台。 	

允许并发连接到 RW 控制台和 RO 控制台的最高数量如下：

- SPARC M12-1/M10-1: 20 个控制台
- SPARC M12-2/M10-4: 40 个控制台
- SPARC M12-2S/M10-4S (无接线盒) : 40 个用户
- SPARC M12-2S/M10-4S (有接线盒) : 70 个用户

2.1.3 通过 XSCF-LAN 端口连接

XSCF-LAN 连接是用 LAN 线连接到 XSCF-LAN 端的连接。在模块化架构配置中，将 LAN 线连接到具有主 XSCF 或备用 XSCF 的 SPARC M12-2S、SPARC M10-4S 或接线盒。

连接 LAN 线后，配置 XSCF 网络设置并通过 SSH 服务或 Telnet 服务连接系统管理终端，以显示主 XSCF 的登录画面。

图 2-9 XSCF-LAN 端口 (SPARC M12-1)

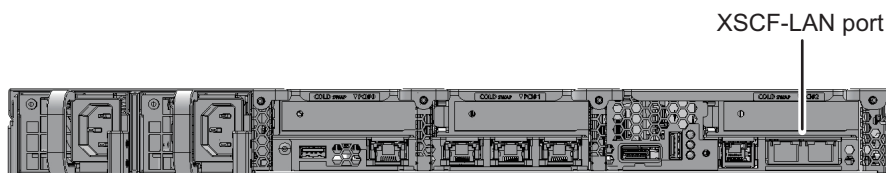


图 2-10 XSCF-LAN 端口 (SPARC M12-2)

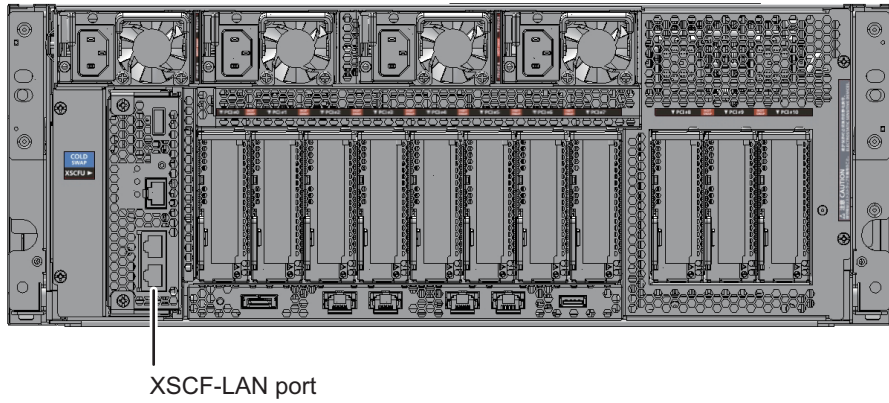


图 2-11 XSCF-LAN 端口 (SPARC M12-2S)

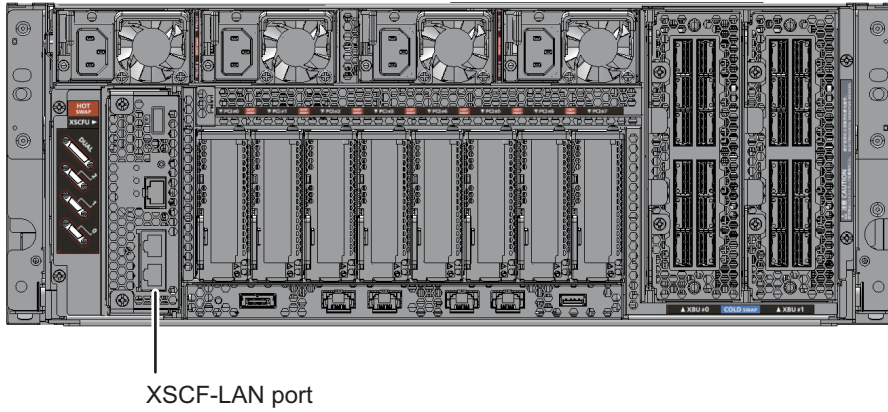


图 2-12 XSCF-LAN 端口 (SPARC M10-1)

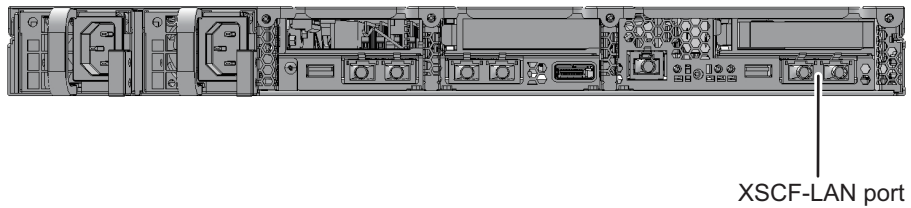


图 2-13 XSCF-LAN 端口 (SPARC M10-4)

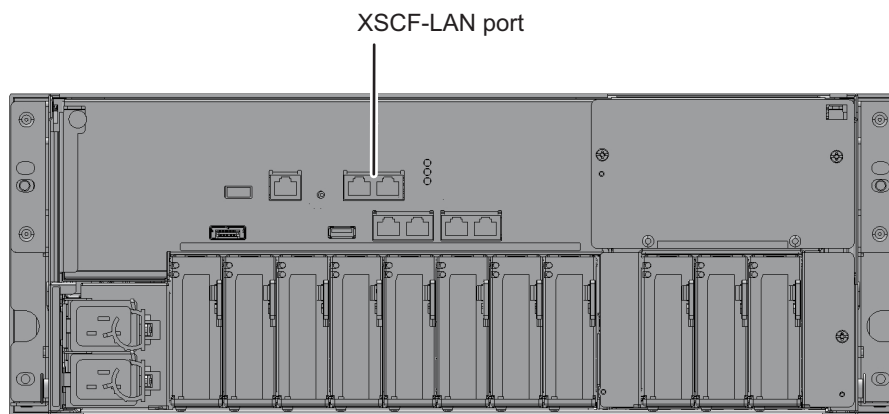
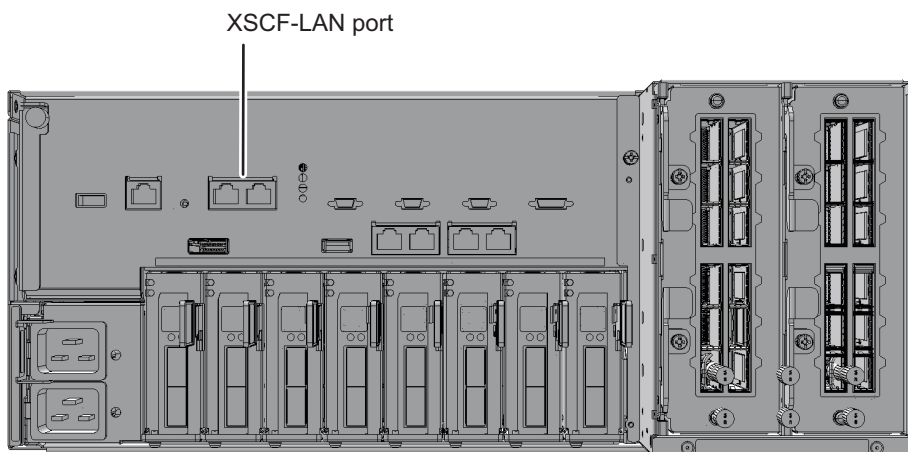


图 2-14 XSCF-LAN 端口 (SPARC M10-4S)



在通过 XSCF-LAN 端口连接到系统管理终端上，您可以使用 XSCF shell。此外，通过配置 Web 浏览器您可以使用 XSCF Web。您可以使用 XSCF 命令或 XSCF Web 来配置系统设置。

配置 XSCF 网络并通过 XSCF-LAN 连接到系统管理终端，您可使用如下功能，这些功能需要网络环境：

- 电子邮件通知
- SNMP
- 远程维护服务
- 外部 NTP 服务器连接和同步
- 远程监控和管理 XSCF

每个系统中已经配备了两个 XSCF-LAN 端口。您只能使用两个端口中的一个，例如，

根据您的系统操作，一个用于 Intranet，另一个用于 Internet。

登录 XSCF 后，您可以使用 XSCF shell。使用 XSCF 命令监控和管理服务器。如果您需要监控或管理逻辑域，可以将 XSCF shell 切换到控制域。有关切换方法，请参见 "8.3 从 XSCF Shell 切换到控制域控制台"。

LAN 连接需要做好以下准备工作。

- 准备 LAN 线
需要 5 类或超 5 类 LAN 线。
- 配置 XSCF 网络
您需要配置 XSCF 网络、SSH、Telnet 和其它服务。有关详情，请参见 "3.9 配置 XSCF 网络"。
- 准备 Web 浏览器（使用 XSCF Web）
准备一个 Web 浏览器。有关受支持的 Web 浏览器，请参见您的服务器的最新《产品说明》。
- 准备终端软件
使用 XSCF shell 时，请为终端软件设置 TERM=vt100。

2.1.4 XSCF-LAN 连接中终端可用的功能

在连接着 XSCF-LAN 的终端上，您可以通过 SSH 或 Telnet 使用 XSCF shell 和控制域控制台。

通过 XSCF-LAN 访问可以执行电子邮件通知功能、SNMP 功能、远程维护服务功能和外部 NTP 服务器时间同步功能，以及使用 LDAP 服务器、Active Directory 服务器或 LDAP over SSL 服务器的用户验证功能。此外设置 Web 浏览器使其用于 XSCF Web。

表 2-2 列出了 XSCF-LAN 连接的终端和控制台以及可用的功能。

表 2-2 XSCF-LAN 连接的终端和控制台以及可用的功能

终端类型	工作	端口号/ 线缆
XSCF shell 终端	<ul style="list-style-type: none">- 连接到 SSH 或 Telnet 服务器后，您可使用 XSCF shell。- 和串行端口上的操作相同，您可以切换到控制域控制台窗口。- 登陆后，如果 XSCF shell 在规定的期间内没有操作，和串行端口相同，将被强制注销。	SSH:22 Telnet:23 需要 LAN 线。
控制域控制台 (RW 控制台)	<ul style="list-style-type: none">- 本 OS 控制台可用于输入/输出。从 XSCF shell 终端中，通过使用 console 命令指定物理分区和可写入控制台，您可以打开 RW 控制台。- 在一个物理分区中，一次只能有一个用户（一个连接）可以使用 RW 控制台。- 如需了解控制域控制台未被使用时的会话超时时间设置，请参见 Oracle Solaris 参考手册中关于 ttymon 的说明。	

表 2-2 XSCF-LAN 连接的终端和控制台以及可用的功能 (续)

终端类型	工作	端口号/ 线缆
控制域控制台 (RO 控制台)	- 这是查看专用的 OS 控制台。从 XSCF shell 终端中，通过使用 <code>console</code> 命令指定物理分区和查看专用控制台，您可以打开 RO 控制台。	
XSCF Web 控制台	您可通过在浏览器上指定 URL 使用 XSCF Web 控制台。	HTTPS:443 需要 LAN 线。

允许并发连接到 RW 控制台和 RO 控制台的 maximum 数量如下：

- SPARC M12-1/M10-1: 20 个控制台
- SPARC M12-2/M10-4: 40 个控制台
- SPARC M12-2S/M10-4S (无接线盒) : 40 个用户
- SPARC M12-2S/M10-4S (有接线盒) : 70 个用户

2.2 登录 XSCF Shell

本节介绍如何使用 XSCF shell 登录 XSCF。

在初始安装时使用默认账户，为登录验证创建一个用户账户。使用新的用户账户登录。有关使用默认帐户登录验证的方法详情，请参见所使用服务器《安装指南》中的“执行初始系统诊断”。有关如何创建新帐户的详细信息，请参见“3.5 创建/管理 XSCF 用户”。

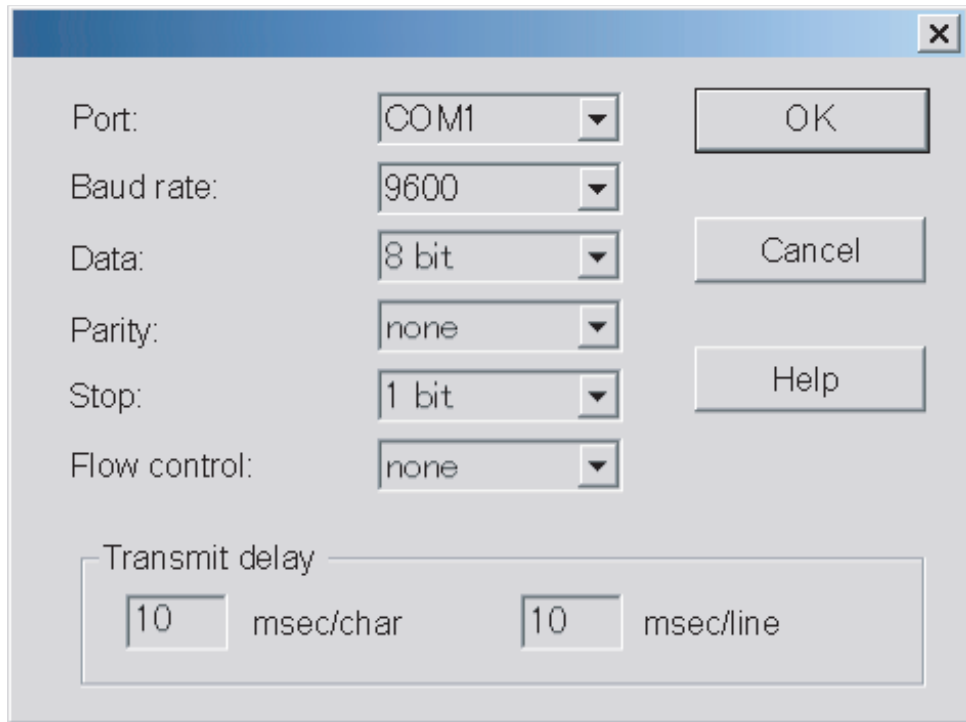
2.2.1 如何使用串行连接登录 XSCF shell

本节介绍如何将终端连接到串行端口以及如何登录 XSCF shell。

1. 检查串行线已连接到主 **XSCF** 的串行端口槽，并且正确连接到使用的 **PC** 或工作站。
2. 确认终端软件使用以下的设置：
 - 波特率：9600 bps
 - 数据长度：8 bits
 - 奇偶：无
 - 停止位：1 位
 - 流量控制：无
 - 传输延迟：非 0

图 2-15 显示了配置终端软件的示例。如果不能建立连接，请增加延迟值。

图 2-15 终端软件设置的示例



3. 建立串行连接，然后按 **[Enter]** 键。
终端变为 XSCF shell 终端，并且显示登录提示。
4. 输入 **XSCF** 用户帐户和密码以登录 **XSCF**。

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

5. 确认 **XSCF shell** 提示 (**XSCF>**) 出现。
现在，您可以使用 XSCF shell。

注 - 如果最后一次以串行连接登录到 XSCF shell 的用户在控制台命令正在执行时终止该连接，则 XSCF shell 提示符可能不会出现。
如果没有出现 XSCF shell 提示符，需输入“#.”。当正在执行控制台命令时，会出现“XSCF>”提示符。

```
XSCF>
```

2.2.2 如何经由 XSCF-LAN 通过 SSH 连接登录 XSCF shell

此处介绍的步骤假定启用了 "3.7 配置用于登录 XSCF 的 SSH/Telnet 服务" 中所述的 SSH 服务。

本节介绍如何通过 XSCF-LAN 端口使用 SSH 登录 XSCF shell。

1. 检查 LAN 线已连接到主 XSCF 的 XSCF LAN 端口槽，并且正确连接到使用的 PC 或工作站。
2. 在使用 SSH 登录前，确认事先已经预存了指纹。
如果没有预存指纹，请通过串行端口建立连接，执行 showssh 命令，然后记录主机公钥的指纹。
3. 启动 SSH 客户端，指定分配给 XSCF-LAN 或主机的 IP 地址（物理 IP 地址），如果需要，指定端口号并连接到 SSH 服务。
对于多个 XSCF 的系统，必要时指定接管 IP 地址（虚拟 IP 地址）。
4. 输入 XSCF 用户帐户和密码以登录 XSCF shell。
5. 显示主机公钥指纹是否有效的提问。请确认指纹，并确认您已正确连接到 XSCF，然后输入 "yes"。
6. 确认 XSCF shell 提示 (XSCF>) 出现。
现在，您可以使用 XSCF shell。

下面显示登录示例。

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

如需使用用户密钥建立 SSH 连接，请事先向 XSCF 注册用户公钥。有关如何注册用户公钥的详细信息，请参见 "3.7 配置用于登录 XSCF 的 SSH/Telnet 服务"。

下面显示用用户公钥登录的示例。

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

2.2.3 如何经由 XSCF-LAN 通过 Telnet 连接登录 XSCF shell

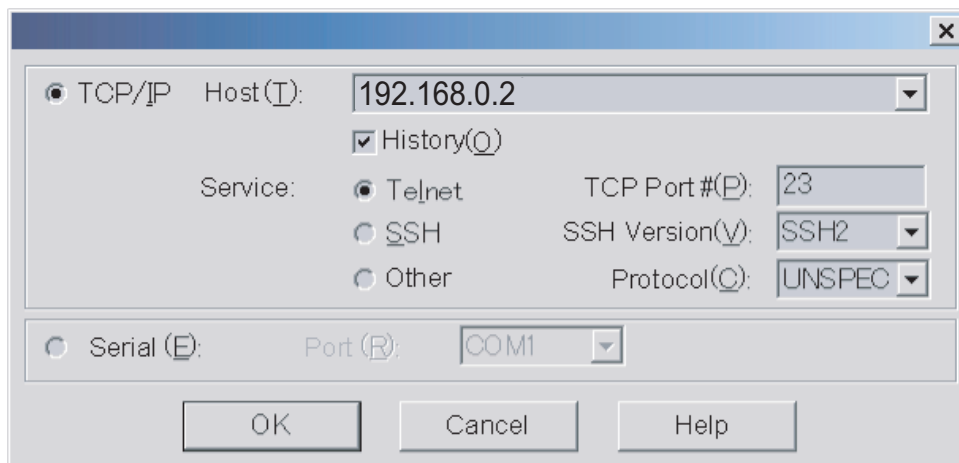
此处介绍的步骤假定启用了 "3.7 配置用于登录 XSCF 的 SSH/Telnet 服务" 中所述的 Telnet 服务。

本节介绍如何通过 XSCF-LAN 端口使用 Telnet 登录 XSCF shell。

1. 检查 LAN 线已连接到主 XSCF 的 XSCF LAN 端口槽，并且正确连接到使用的 PC 或工作站。
2. 启动终端软件，指定分配给 XSCF-LAN 或主机的 IP 地址（物理 IP 地址），指定端口 23 建立 Telnet 服务并且打开 XSCF shell 终端。
对于多个 XSCF 的系统，必要时指定接管 IP 地址（虚拟 IP 地址）。

图 2-16 显示了配置终端软件的示例。

图 2-16 终端软件设置的示例



3. 输入 XSCF 用户帐户和密码以登录 XSCF shell。
4. 确认 XSCF shell 提示 (XSCF>) 出现。
现在，您可以使用 XSCF shell。
下面示例显示成功登录。

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

2.3 从 XSCF Shell 注销

本节介绍如何从 XSCF Web 注销。

1. 执行 **exit** 命令以注销。

```
XSCF> exit
```

您已从 XSCF 中注销，XSCF 会话已断开。

登录后，如果 XSCF shell 在规定的期间内没有操作，将被强制注销。如需设置 XSCF 会话超时值，请使用 `setautologout` 命令。有关详细信息，请参见 `setautologout(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

2.4 登录 XSCF Web

本节介绍如何使用 XSCF Web 登录 XSCF。

设置 PC 连接到 XSCF-LAN 上的 Web 浏览器，您可以使用 XSCF Web。XSCF Web 不能从串行端口连接。

通过 XSCF-LAN 访问也可以执行电子邮件通知功能、SNMP 功能、远程维护服务功能和外部 NTP 服务器时间同步功能，以及使用 LDAP 服务器、Active Directory 服务器或 LDAP over SSL 服务器的用户验证功能。

XSCF Web 连接到通过采用 HTTPS 协议和 SSL/TLS 协议的用户网络连接的服务器。它能显示服务器状态，控制操作设备和浏览基于 Web 的设置信息。

当一个注册用户从 PC 中的 Web 浏览器连接到 XSCF Web 并登录 XSCF 时，浏览器显示可用的树索引和页面。有关 XSCF Web 页面信息的详情，请参见 ["附录 C XSCF Web 页面列表"](#)。

2.4.1 必须事先设置的项目

在初始设置中，XSCF Web 被禁用。使用 XSCF Web 前，需要事先配置以下设置。

- 注册一个 XSCF 用户帐户
- 启用 HTTPS 服务来使用 XSCF Web
- 使用 HTTPS 服务设置注册一个 Web 服务器证书
- 配置电子邮件通知设置（建议故障时使用）

有关启用 HTTPS 服务的步骤，请参见 ["3.8 配置用于登录 XSCF 的 HTTPS 服务"](#)。

2.4.2 支持的浏览器

XSCF Web 支持 表 2-3 中列出的 Web 浏览器。

表 2-3 支持的 Web 浏览器

Web 浏览器名	版本
Microsoft Internet Explorer	8.0, 9.0, 10.0 和 11.0
Mozilla Firefox 32 位版本	10.0 至 ESR 52

有关 Web 浏览器使用的详细信息，请参见您的服务器的最新《产品说明》。

2.4.3 Web 浏览器必须启用的功能

因为 Web 浏览器使用如下功能，所以必须设置为启用状态。

- 传输层安全性 (TLS) 版本1.2
- JavaScript
- Cookie（用于会话管理）

2.4.4 如何用 XSCF Web 登录

本节介绍如何使用 XSCF Web 登录 XSCF。

1. 检查 **LAN** 线已连接到主 **XSCF** 的 **XSCF LAN** 端口槽，并且正确连接到使用的 **PC** 或工作站。
2. 对于 **Web** 浏览器的 **URL**，请指定 **XSCF** 的 **IP** 地址或主机名并连接到 **XSCF**。

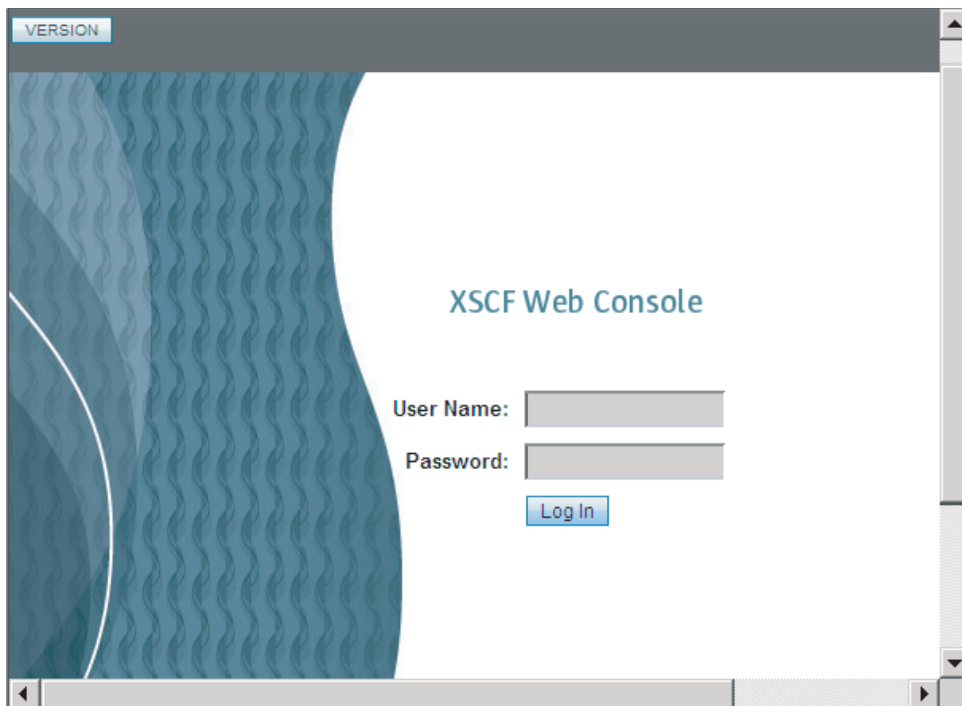
- Web 浏览器上的 URL 输入示例

```
https://192.168.111.111（输入 XSCF IP 地址 <数字>）/  
或者，  
https://XSCF-host-name（注：不是域名名称）/
```

注 - 在通信开始时，可能需要您确认证书。确认内容并接受证书。进行 HTTPS 连接时，Web 浏览器在证书完成安装之前会一直显示警告。

3. 在登录页中输入 **XSCF** 用户帐户和密码以登录 **XSCF**。
图 2-17 显示了登录页面的示例。

图 2-17 XSCF Web 登录页的示例



成功登录后，显示默认页。默认页显示一个树状视图允许您逐一选择页面。

验证失败

如果登录失败，显示登录失败信息。此外，登录失败会记录到事件日志和审核日志中。

2.5 从 XSCF Web 注销

本节介绍如何从 XSCF Web 注销。

1. 在 **XSCF Web** 页上单击 **[注销]** 按钮以注销。
您从 XSCF Web 登录页中注销 XSCF 后，将回到 XSCF Web 登录窗口。

访问状态监控

XSCF Web 监控登录其中的 XSCF 用户帐户的使用状态。XSCF Web 将已经登录但在指定期间内没有访问的帐户认定为验证过期。因此，如果您使用过期验证帐户访问 XSCF Web，会显示一个对话框提示验证过期，并返回到顶层页面。如果想要继续使用 XSCF Web，请重新登录。

您可以更改用于监控 XSCF Web 页面中验证过期的时间。监控验证过期的默认时间为 10 分钟。监控时间的范围为 1 到 255 分钟。设置监控时间请选择 **[Menu]** - **[Settings]** -

2.6 可连接的用户数

本节介绍可连接到 XSCF 的用户数。执行 `who` 命令列出登录 XSCF 的用户帐户。

- SPARC M12-1/M10-1
最多 20 个用户。在 20 个用户同时连接到 XSCF 时，对于尝试建立后续（第 21 个）连接的任何用户，访问被拒绝。
- SPARC M12-2/M12-2S/M10-4/M10-4S（无接线盒）系统
最多 40 个用户。在 40 个用户同时连接到 XSCF 时，对于尝试建立后续（第 41 个）连接的任何用户，访问被拒绝。
- SPARC M12-2S/M10-4S（有接线盒）系统
最多 70 个用户。在 70 个用户同时连接到 XSCF 时，对于尝试建立后续（第 71 个）连接的任何用户，访问被拒绝。

配置系统

本章介绍使用 XSCF 所需的设置步骤。

- XSCF 设置前提工作
- 了解 XSCF 固件设置的内容
- 从 XSCF Shell 设置
- 从 XSCF Web 设置
- 创建/管理 XSCF 用户
- 设置 XSCF 时间/日期
- 配置 XSCF 网络
- 配置用于登录 XSCF 的 SSH/Telnet 服务
- 配置用于登录 XSCF 的 HTTPS 服务
- 配置审核以强化 XSCF 安全

3.1 XSCF 设置前提工作

本节介绍在设置 XSCF 之前必须确认和执行的工作。

本说明假定服务器安装、线缆连接、系统初始诊断以及其他安装工作已经完成。

3.1.1 设置前的初始工作

在开始设置 XSCF 之前，您需要完成线缆连接、服务器的初始登录验证和其它必要工作，以便您可以从使用串行连接或 LAN 连接的终端连接到 XSCF。

系统管理员和现场工程师必须在执行以下工作之后开始设置 XSCF。

表 3-1 在开始设置 XSCF 之前完成的工作

工作	参见
使用 XSCF 默认帐户密码执行 XSCF 的初始登录验证。	所使用服务器《安装指南》中的 "登录 XSCF"。
至少注册一个具有 platadm 或 useradm 用户权限的用户帐户。	"3.5 创建/管理 XSCF 用户"

在日常操作期间，为防止操作错误，将 Mode 开关设置为 Locked。
关于模式切换的切换方法，请参见 "13.2 切换操作模式"。

3.1.2 支持信息

设置 XSCF 之前，请务必仔细阅读您的服务器的最新《产品说明》，检查软件要求和产品支持信息。

3.1.3 设置的用户界面以及如何访问

将 PC 连接到主 XSCF 以设置 XSCF。要进行各种设置，请使用 XSCF shell（命令行界面）或 XSCF Web（浏览器用户界面）访问 XSCF。

表 3-2 用户界面以及如何访问 XSCF

用户界面	如何访问 XSCF
XSCF shell (命令行界面)	从串行端口所连的 PC 中登录。 使用 SSH 或 Telnet 服务，从连接到 XSCF 专用 LAN 端口 (XSCF-LAN) 的 PC 中登录。
XSCF Web (浏览器用户界面)	使用 HTTPS 服务从安装有 Web 浏览器并连接到 XSCF-LAN 的 PC 登录。

如需使用 XSCF Web，您须首先对其进行配置。注意 XSCF 不支持有些功能的设置，如海拔设置和双电源供给设置。如需使用这些功能，请使用 XSCF shell 进行设置。有关 XSCF Web 所支持功能的详细信息，请参见 "附录 C XSCF Web 页面列表"。

设置步骤

根据连接的用户界面，设置步骤有所不同。

- 使用 XSCF shell 时
请参见 "3.3 从 XSCF Shell 设置"。
- 使用 XSCF Web 时
请参见 "3.4 从 XSCF Web 设置"。

设置信息

配置 XSCF 后，所配置的信息自动保存到 XSCF、PSU 底板或接线盒底板单元中。因此，一旦配置了 XSCF，不需要日常管理。但是，考虑到保存在服务器上信息损坏的可

能性，请定期保存/恢复 XSCF 设置信息。有关如何保存/恢复 XSCF 设置信息的详情，请参见“10.10 保存/恢复 XSCF 设置信息”。

3.1.4 顺利配置 XSCF

本节介绍在开始设置 XSCF 之前您提前应理解的内容。

在许多情况下，系统可以使用设置值和初始安装时的默认值运行。但是，需要配置服务器以适应客户环境。通过检查所使用服务器的《安装指南》已完成的工作以及事先确定项目，可使您缩短配置时间。在开始配置设置之前，考虑以下事项。

- 列出初始安装使用时已配置的所有项目（如果有）。对于后面所述项目，查看已配置给这些项目的设置信息，并确认他们不需要重新配置。
- 检查针对维护、系统管理员和物理分区是否已配置了必要的用户帐户。您还必须提前决定是使用 XSCF 的本地账户还是远程服务器上的账户数据作为您的用户账户。
- 再次检查服务器配置。检查网络地址、域配置和 CPU 激活数量等所有项目都已配置，且没有遗漏。为了确保适应用户的环境，必须采取检查措施检查出不适应用户环境的设置，例如网络地址。
- 连接到 XSCF 网络使您能够使用不同的服务。事先确定如何处理非法访问、限制主机访问以及如何进行远程维护服务（如通知）、使用什么样的标准时间。
- 为了实现节能，需要考虑服务器的操作环境。根据服务器所在的房间大小和环境温度以及其他的安装环境因素，确定服务器的启动间隔。此外，确定功耗的最大值以及类似的设定值。

3.2 了解 XSCF 固件设置的内容

本节介绍配置 XSCF 固件的详细步骤。

3.2.1 设置使用 XSCF 的项目

各种 XSCF 设置项目有如下用途：

- 使用 XSCF 固件的设置
- 配置物理分区和逻辑域的设置
- 管理/控制系统硬件的设置
- 事件通知等其他设置

本节介绍使用 XSCF 固件的设置。有关配置物理分区和逻辑域的设置，请参见“第7章 控制物理分区”和“第8章 控制逻辑域”以及参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。关于硬件（如电源等）的管理/控制设置，请参见“第4章 按照使用型号配置系统”和“第15章 扩展系统配置”。此外，其他的设置请参见相关的章节。

表 3-3 显示了使用 XSCF 固件的设置项目。有关各项目的详情，请参见表中所示内容。

表 3-3 设置使用 XSCF 的项目

设置项目	必须或可选设置	参见
用户管理	必须	3.5
时间	必须	3.6
网络	必须	3.9
SSH/Telnet 服务	可选	3.7
HTTPS 服务	可选	3.8
审核	可选	3.10
LDAP 服务	可选	3.5.12
Active Directory 服务	可选	3.5.13
LDAP over SSL 服务	可选	3.5.14

注 - 与如下设置项目有关的服务，出厂默认状态为启用。

- 用户管理
- 时间
- 网络
- 审核

3.2.2 检查主 XSCF

对于 SPARC M12-1/M12-2/M10-1/M10-4 和单机配置中的 SPARC M12-2S/M10-4S，该机箱的 XSCF 是主 XSCF。对于模块化架构配置中的 SPARC M12-2S 或 SPARC M10-4S，用户仅能访问主 XSCF 或备用 XSCF。在主 XSCF 上配置 XSCF。原则上，模块化架构配置中的主 XSCF 是安装在 ID (BB-ID) 为 0 或 1 的 SPARC M12/M10 中的 XSCF，或安装在接线盒 80 或 81 机箱中的 XSCF。备用 XSCF 是安装在具有相同编号的机箱中的 XSCF。

如果在系统运行中主 XSCF 和备用 XSCF 切换，则主 XSCF 由编号为 BB-ID 0 机柜的单元变成编号为 BB-ID 1 机柜的单元。同样，备用 XSCF 由编号为 BB-ID 1 机柜的单元变成编号为 BB-ID 0 机柜的单元。

在多个 XSCF 的系统中，主 XSCF 和备用 XSCF 的组件安装编号如下：

- SPARC M12-2S 或 SPARC M10-4S 系统（无接线盒）
 - 主 XSCF: BB#00；备用 XSCF: BB#01
 或者，
 - 主 XSCF: BB#01；备用 XSCF: BB#00
- SPARC M12-2S 或 SPARC M10-4S 系统（有接线盒）
 - 主 XSCF: XBBOX#80；备用 XSCF: XBBOX#81
 或者，
 - 主 XSCF: XBBOX#81；备用 XSCF: XBBOX#80

在多个 XSCF 的系统中，检查和连接主 XSCF 的方法如下。

- 检查 MASTER LED 并建立串行连接

对 SPARC M12-2S 或 SPARC M10-4S 或接线盒供电时，主 XSCF 初始化的完成将点亮 XSCF 单元后面板上的 MASTER LED 指示灯。将 PC 连接到相同面板上的串行端口，您可以登录到主 XSCF。

- 指定接管 IP 地址或主 XSCF IP 地址，并建立连接

主 XSCF 和备用 XSCF 分别具有 XSCF LAN#0 和 LAN#1 端口。LAN#0 端口和 LAN#1 端口通过相同子网相互连接以执行复制。

如需连接到主 XSCF，请指定 LAN#0 接管 IP 地址或 LAN#1 接管 IP 地址。即使在主和备用 XSCF 之间切换后，指定相同的接管 IP 地址也可建立到主 XSCF 的连接。

连接到主 XSCF 的另一个方法是指定主 XSCF LAN#0 或 LAN#1 IP 地址。当系统上只有一个 XSCF 或由于维护备用 XSCF 无法访问时，此方法有效。

在使用指定的 IP 地址连接主 XSCF 并登录后，执行 `showhardconf` 命令。您可以查看 SPARC M12-2S、SPARC M10-4S 或接线盒的哪一个机箱具有主 XSCF。

以下是 BB-ID 0 为主 XSCF 的示例。

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

以下是接线盒 80 为主 XSCF 的示例。

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

注 - 配置给主 XSCF 的设置应用到备用 XSCF。

3.2.3 备用 XSCF 上可执行的功能

本节介绍备用 XSCF 上可执行的功能和命令。

表 3-4 备用 XSCF 上可执行的功能

功能	命令
退出 XSCF	exit
查看手册页	man
重新启动 XSCF	rebootxscf
设置用户权限	setprivileges
查看机柜状态	showbbstatus
查看命令结束状态	showresult
查用户信息	showuser
转储固件	snapshot
切换 XSCF	switchscf
查看审核	viewaudit
查看登录的用户	who

有关各命令的详细信息，请参见其手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

3.2.4 在 man 页检查命令选项的详情

在配置 XSCF 时，在 XSCF 上执行 `man(1)` 命令查看 XSCF 命令的 man 页，其中包含操作数、选项等的说明。显示的手册页内容与《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》中的内容具有相同详细的命令信息。

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

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

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

3.3 从 XSCF Shell 设置

本节介绍从 XSCF shell 配置的流程。

详细信息请参见双引号内标题指示的章节。此外，根据客户的环境，选择是否启用或禁用设置（选项）项目。

1. **从可以进行串行连接的终端连接到 XSCF shell。**
为到服务器的串行连接设置一个安全的环境。
有关详情，请参见 ["2.2.1 如何使用串行连接登录 XSCF shell"](#)。
2. **登录 XSCF shell。**
使用初始登录验证时创建的新用户帐户登录 XSCF shell。
有关登录的详情，请参见 ["2.2 登录 XSCF Shell"](#)。
有关在初始登录验证时创建新用户帐户的详细信息，请参见 ["3.5 创建/管理 XSCF 用户"](#)。
3. **设置密码策略。**
指定密码属性，如：XSCF 用户帐户的密码有效期、字符数。
有关详情，请参见 ["3.5 创建/管理 XSCF 用户"](#)。
4. **配置审核项目（选项）。**
审核功能在审核日志中记录 XSCF 登录、注销和其它事件。默认情况下审核功能启用。审核设置需要 `auditadm` 权限。
有关详情，请参见 ["3.10 配置审核以强化 XSCF 安全"](#)。
5. **设置时间。**
设置 XSCF 时间，即系统标准时间。系统时间更新后，XSCF 重新启动，并断开 XSCF 会话。重新登录。
有关详情，请参见 ["3.6 设置 XSCF 时间/日期"](#)。

注 - 这些设置工作在初始安装时完成。如果需要更改设置值，请再次设置。

6. **配置 SSH/Telnet 服务。**
SSH 和 Telnet 可以同时启用。但是，Telnet 连接不支持安全通信协议。我们建议启用 SSH 服务时，禁用 Telnet 服务。
默认情况下，SSH/Telnet 服务被禁用。
有关详情，请参见 ["3.7 配置用于登录 XSCF 的 SSH/Telnet 服务"](#)。
7. **确认 XSCF 主机公钥。**
通过 XSCF-LAN 连接使用 SSH 服务时，执行 `showssh` 命令并记录指纹。步骤 11 介绍了通过 SSH 服务登录 XSCF shell 过程中记录指纹的内容。将主机公钥的文本数据复制到客户端指定目录内的文件。

```
XSCF> showssh
SSH status: enabled
RSA key:
```

```

ssh-rsa
AAAAB3NzaC1yc2EAAAABIWAAAIEAt0IG3wfpQnGr51znS9XtzwHcBbb/UU0LN08S
ilUXE6j+avlxdY7AFqBflwGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQ122G8pwibESrh5JmOhSxpLz13P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnb1B8/JEQI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RE1U5Pyb8F16uq96L8Q
DMswFlICMzGrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4Verb+uOfmPRpe6/kb4z++lOhtpWI9bay6CK0nrFRok+z54ez7B
rDFBQVnNzX9PyEFezJG9ziEYVUag/23LIAiLxxBmW9pqa/WxC21Ja4RQVN3009km
VwAAAIaON1LR/9Jdd7yyG18+Ue7eBBJHrCAOpkSzfzFFj5XUzQBdabh5p5Rwz+
lvriawFIZI9j2uhM/3HQdrvYSVBEdmJjaasF9hB6T/uFwP8yqtJf6Y9GdjBAhWuH8
F13pX4BtvK9IeldqCscnOuu0e2r1UoI6GICMr64FL0YYBSwfbwLIz6PSA/yKQe23
dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCAOvVlMhghuPNpX+hE19nPdBFG
zQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub

```

有关详情，请参见“3.7 配置用于登录 XSCF 的 SSH/Telnet 服务”。

8. 注册用户公钥。

在通过 XSCF-LAN 连接使用 SSH 服务的用户密钥时，为 PC 上的已注册 XSCF 用户帐户创建一个用户密钥和用户公钥，并向 XSCF 注册用户公钥。

有关详情，请参见“3.7 配置用于登录 XSCF 的 SSH/Telnet 服务”。

9. 配置 XSCF 专用网络。

配置 XSCF 网络，其中包括 XSCF-LAN IP 地址和 SSCP。允许一个以上的用户使用 SSH、Telnet 或 HTTPS 同时访问 XSCF。

执行 `applynetwork` 命令以应用网络配置。然后，执行 `rebootxscf` 命令重新启动 XSCF 并完成配置工作。XSCF 重新启动后，XSCF 会话被断开。重新登录。

有关详情，请参见“3.9 配置 XSCF 网络”。

10. 从可以进行 XSCF-LAN 连接的终端连接到 XSCF shell（选项）。

也可以通过 XSCF-LAN 连接来完成此步骤的设置工作。在此步骤中，在连接 XSCF-LAN 的 PC 上指定 IP 地址并连接到 XSCF，然后再次登录。

继续使用串行连接设置时，请转到步骤 12。

Telnet 连接不应被认为是通信的安全形式。推荐您使用 SSH 服务。在 SSH 服务登录中，会出现主机公钥的指纹是否有效的提问。确认指纹与您您在步骤 7 记录的相同并回复“yes”。如果指纹不匹配，IP 地址可能不正确或连接目的地唯一，或者可能意味着“欺骗”。再次检查 IP 地址。

```

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

```

如果已经设置了密码，在使用用户密码验证的 SSH 服务时，输入密码。

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

11. 配置 **NTP** (选项)。

配置 NTP, 使其作为 NTP 服务器或 NTP 客户端运行。在某些情况下, 您可以在配置域之后配置 NTP 设置。

有关详情, 请参见 "3.6 设置 XSCF 时间/日期"。

配置以下设置用于管理用户账户。为了管理用户账户, 事先确定是设置保存在 XSCF 中的本地用户账户, 还是设置使用 Lightweight Directory Access Protocol (LDAP)、Active Directory 或 LDAP over SSL 网络保存在目录数据库的账户数据。如需设置网络上的目录数据库, 请设置验证目录数据库的用户帐户。

如需使用 LDAP、Active Directory 或 LDAP over SSL 服务器, 需要事先下载证书, 创建公钥, 完成在目录数据库的用户注册。

因为 Active Directory 或 LDAP over SSL 用户不能将用户公钥上传至 XSCF, 您必须在使用密码验证通过 SSH 连接到 XSCF 后登录。

本手册不提供 LDAP、Active Directory 和 LDAP over SSL 的详细内容。请参见 LDAP 和 Active Directory 和 LDAP over SSL 手册。

注 - 关于支持 LDAP、Active Directory 和 LDAP over SSL 服务的 XCP 固件版本, 请参见服务器的最新《产品说明》。

12. 配置 **LDAP 服务设置** (选项)。

将 XSCF 设置为 LDAP 客户端。有关详情, 请参见 "3.5.12 使用 LDAP 管理 XSCF 用户帐户"。

13. 配置 **Active Directory 服务设置** (选项)。

将 XSCF 设置为 Active Directory 客户端。有关详情, 请参见 "3.5.13 使用 Active Directory 管理 XSCF 用户帐户"。

14. 配置 **LDAP over SSL 服务设置** (选项)。

将 XSCF 设置为 LDAP over SSL 客户端。有关详情, 请参见 "3.5.14 使用 LDAP over SSL 管理 XSCF 用户帐户"。

15. 配置 **XSCF 用户帐户**。

根据用户环境, 注册保留在本地服务器上的 XSCF 用户账户。

- 如需添加用户账户, 执行 showuser 命令并指定 -l 选项, 确认用户账户列表中没有无效账户。

- 考虑到维护工作, 一定要准备一个具有 fieldeng 用户权限的现场工程师 (FE) 用户帐户。

有关详情, 请参见 "3.5 创建/管理 XSCF 用户"。

16. 配置 **SMTP** (选项)。

配置 SMTP 以使用 XSCF 电子邮件通知功能。

有关详情, 请参见 "10.2 故障发生时通过电子邮件接收通知"。

17. 配置用于 **SNMP 代理功能** 的与 **SNMP 协议** 有关的项目 (选项)。

有关详情, 请参见 "10.3 通过 SNMP 代理监控/管理系统状态"。

18. 配置用于远程维护服务的项目（选项）。

本文档不对远程维护服务功能进行详细介绍。有关远程维护服务功能的信息，请参见您的服务器的最新《产品说明》。

通过以下步骤配置整个系统硬件管理的项目。

19. 设置海拔高度。

有关详情，请参见 "4.1 设置/确认系统海拔高度"。

注 - 这些设置工作在初始安装时完成。如果需要更改设置值，请再次设置。

20. 配置功率上限（选配）。

有关详情，请参见 "4.4 降低功耗"。

21. 配置内存镜像模式（选配）。

有关详情，请参见 "14.1 配置内存镜像"。

22. 设置空调等待时间（选项）。

设置在空调设备调整室温之前，开机程序等待的时间。

有关详情，请参见 "4.2.2 设置/确认启动等待时间"。

通过以下步骤设置物理分区的项目。

23. 设置物理分区（选项）。

设置域配置管理信息。

有关详情，请参见 "11.2 查看物理分区" 和《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

24. 设置物理分区模式（选项）。

有关详情，请参见 "7.2 设置物理分区运行模式" 和《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

25. 执行 CPU 激活的设置。

有关详情，请参见 "第5章 CPU 激活"。

26. 设置预热时间（选项）。

在 Oracle Solaris 开始运行前，设置延时时间推迟电源开启。该设置时间应用于服务器电源开启处理开始以后。此设置用于等待服务器预热和外设开启。

如果由 `setpowercapping` 命令配置了功耗上限，可能会出现所有物理分区同时开始运行并且超过功耗上限的情况。为避免这种情况，预热时间可用于错开各物理分区的运行时间。

有关详情，请参见 "4.2.1 设置/确认预热时间"。

27. 设置电源计划（选项）。

对每个物理分区设置电源计划信息。

如需设置电源计划，请使用 XSCF 固件 `setpowerschedule`、`addpowerschedule` 和 `deletepowersched` 命令。有关各命令的详细信息，请参见该命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

3.4 从 XSCF Web 设置

本节介绍使用 XSCF Web 进行必要设置的流程。详细信息请参见双引号内标题指示的章节。

如需使用 XSCF Web，您必须事先在 XSCF shell 的设置中启用 HTTPS 服务。

1. 从可以进行串行连接的终端连接到 **XSCF shell**。
有关详情，请参见 "2.2 登录 XSCF Shell"。
2. 执行 "3.3 从 XSCF Shell 设置" 中的步骤 2 到 11。使用 **XSCF shell** 执行第 7.2 节中的步骤 2 至 11 后，转到本节的下一个步骤。
3. 配置 **HTTPS**。
有关详情，请参见 "3.8 配置用于登录 XSCF 的 HTTPS 服务"。
4. 从 **Web 浏览器** 连接到 **XSCF**。
在连接 XSCF-LAN 并且安装了 Web 浏览器的 PC 上，指定主机名或 IP 地址以连接到 XSCF Web。
- Web 浏览器上的 URL 输入示例

```
https://192.168.111.111 (输入 XSCF IP 地址 <数字>) /  
或者,  
https://XSCF-host-name (注: 不是域主机名称) /
```

5. 从 **XSCF Web 控制台** 登录 **XSCF**。
使用新创建的用户账户登录。

```
<在 Web 浏览器登录验证输入的示意图>  
login:yyyy  
Password:xxxxxxxx
```

XSCF Web 浏览器窗口被称为 XSCF Web 控制台。

有关详情，请参见 "2.4 登录 XSCF Web"。

6. 设置项目与在 **XSCF shell** 中相同。从 **XSCF Web 控制台** 采用与 "3.3 从 XSCF Shell 设置" 中步骤 12 和后续步骤相同的方法对其进行配置。
有关 XSCF Web 菜单的详情，请参见 "附录 C XSCF Web 页面列表"。

注 - 如需配置 XSCF Web 菜单中没有的项目，如海拔设置和双回路供电设置，请使用 XSCF shell。

3.5 创建/管理 XSCF 用户

本节介绍如何创建/管理用于登录 XSCF 的用户帐户、密码、用户权限和密码策略。为了管理用户账户，您既可设置 XSCF 本地用户，也可设置用于 LDAP、Active Directory 或 LDAP over SSL 网络目录数据库的验证用户账户。

3.5.1 XSCF 用户帐户

使用场景

XSCF 用户帐户用于通过 SSH、Telnet 或 XSCF Web 登录 XSCF shell。

可以登录 XSCF 用户帐户的用户

如需注册一个 XSCF 用户帐户，须使用具有 `useradm` 用户权限的用户帐户登录。

可使用的 XSCF 用户帐户名

以下 XSCF 用户帐户名给系统保留，不能用于任何用户：

`root`, `bin`, `daemon`, `adm`, `operator`, `nobody`, `sshd`, `rpc`, `rpcuser`, `ldap`, `ntp`,
`admin`, `default`, `proxyuser`

如果使用 LDAP、Active Directory 或 LDAP over SSL 服务管理 XSCF 用户账户，用户账户和（如果已指定）用户身份必须在 XSCF、LDAP、Active Directory 或 LDAP over SSL 中未被使用过。有关可用字符的详细信息，请参见 `adduser(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

用户帐户数

可指定的用户帐户数为100，假定每个用户帐户平均使用10个字符。`adduser` 命令被执行后，注册一个被称为 UID 的自动分配 ID 的用户帐户。UID 是一个等于或大于 100 的整数。UID 也可被指定为任意数。此时，指定从 100 到 60000 的数值作为 UID。

登录验证失败时

如果登录验证失败，用户账户在指定的期间内被锁定。锁定帐户的功能被称为 XSCF 用户帐户锁定功能。系统管理员可以禁用或启用使用中的 XSCF 用户帐户。

3.5.2 密码和密码策略

在您注册一个 XSCF 用户帐户时，也注册一个密码。新创建的用户账户没有密码。因此，在使用 `password` 命令设置密码或将 Secure Shell (SSH) 的公钥设置给用户之前，它不能用于登录。

密码有长度、字符类型等限制。密码属性应符合称为密码策略的规则。创建用户帐户后，当前密码策略应用到创建的用户帐户。在重新设置密码策略后，密码策略应用到随后新

加的用户。您可以执行 `showpasswordpolicy` 命令确认当前密码策略。

表 3-5 显示了密码策略设置项目。

表 3-5 密码策略项目

设置项目	含义
Mindays	下次密码可以更改前，密码更改后的最小天数。0 表示该密码可以随时更改。
Maxdays	密码有效的最多天数
Warn	密码已经到期之前，发出密码过期警告后的天数
Inactive	锁定帐户前，密码过期后的天数
Expiry	该帐户仍然有效的天数 默认天数为 0。0 意味着该帐户永不过期。
Retry	允许重试更改密码的次数
Difok	新密码中包含但旧密码中未包含的字符数
Minlen	可接受的最小密码长度
Dcredit	包含数字字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的数字字符数。在这里，您可以设置此减少的最大值。
Ucredit	包含大写字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的大写字符数。在这里，您可以设置此减少的最大值。
Lcredit	包含小写字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的小写字符数。在这里，您可以设置此减少的最大值。
Ocredit	包含非字母数字字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的非字母数字字符数。在这里，您可以设置此减少的最大值。
Remember	密码历史中储存的密码数

3.5.3 用户权限类型

在添加 XSCF 用户帐户时，您需要将用户权限分配给该帐户。将用户 权限授予给用户帐户的目的是：

- 提供系统管理员对于整个服务器的操作权限
- 限制对指定物理分区的操作
- 管理用户帐户
- 配置审核
- 限制现场工程师执行的服务器操作

可以为一个用户帐户指定一个以上的用户权限。根据用户的环境和使用目的，将用户权限授予帐户。表 3-6 列出了用户权限。

表 3-6 用户权限

用户权限	概述	权限说明
pparop@n	引用指定物理分区的所有状态。	<ul style="list-style-type: none"> - 允许引用搭载在指定物理分区 (PPAR-ID: n) 上的所有硬件状态。 - 允许引用指定物理分区 (PPAR-ID: n) 的所有状态。
pparmgr@n	允许操作供电电源以及只能引用指定物理分区的状态。	<ul style="list-style-type: none"> - 允许开启/关闭电源以及重置指定物理分区 (PPAR-ID: n)。 - 允许引用搭载在指定物理分区 (PPAR-ID: n) 上的所有硬件状态。 - 允许引用指定物理分区 (PPAR-ID: n) 的所有状态。
pparadm@n	只允许管理指定物理分区。	<ul style="list-style-type: none"> - 允许控制安搭载指定物理分区 (PPAR-ID: n) 上的所有硬件。 - 允许引用搭载在指定物理分区 (PPAR-ID: n) 上的所有硬件状态。 - 允许控制所有指定物理分区 (PPAR-ID: n)。 - 允许引用指定物理分区 (PPAR-ID: n) 的所有状态。
platop	引用整个系统的状态。	可引用服务器所有的状态，但不能更改。
platadm	管理整个系统。	<ul style="list-style-type: none"> - 可以对系统执行所有硬件操作。 - 可以操纵所有的 XSCF 设置，那些需要 <code>useradm</code> 和 XSCF 审核权限的除外。 - 可以添加/删除物理分区中的硬件。 - 可对物理分区执行电源操作。 - 可以参考服务器的所有状态。
useradm	管理用户帐户。	<ul style="list-style-type: none"> - 可以创建、删除、启用和禁用用户帐户。 - 可以更改用户密码和密码配置文件。 - 可以更改用户权限。
auditop	参考审核状态。	可以参考 XSCF 审核状态和审核方法。
auditadm	控制审核。	<ul style="list-style-type: none"> - 可以控制 XSCF 审核。 - 可以删除 XSCF 审核方法。
fieldeng	允许现场工程师使用。	只允许现场工程师执行维护工作，并更改设备配置。
无	您没有用户权限。	当储存在 XSCF 的用户权限被设置为 <code>none</code> 时，用户账户的用户权限在 LDAP 中无法查出。因此，在 LDAP 中即使用户权限被设置给了用户账户，该权限被认为是 "none"。

目标物理分区的用户权限在用户权限名后附加 "@PPAR number"。(例如，PPAR-ID 01 的 `pparadm` 变成 `pparadm@1`)

一个用户帐户可以具有多个物理分区（包括目标物理分区）的权限。有关用户权限设置的详细信息，请参见 `setprivileges(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

3.5.4 检查与 XSCF 用户帐户相关的设置项目和命令

表 3-7 列出了与 XSCF 用户帐户相关的设置项目以及对应的 XSCF shell 命令。

表 3-7 与 XSCF 用户帐户相关的设置项目

设置项目	必须或可选设置	相关命令
添加/删除用户帐户	必须	showuser(8), adduser(8), deleteuser(8)
启用/禁用用户帐户	必须	enableuser(8), disableuser(8)
设置密码策略	可选	setpasswordpolicy(8), showpasswordpolicy(8)
设置一个密码	必须	password(8)
分配用户权限	必须	setprivileges(8), showuser(8)
配置锁定功能	可选	setloginlockout(8), showloginlockout(8)

表 3-8 与目录服务用户帐户有关的设置项目

设置项目	必须或可选设置	相关命令
LDAP 客户端设置	可选	showldap(8), setldap(8)
Active Directory 客户端设置	可选	showad(8), setad(8)
LDAP over SSL 客户端设置	可选	showldaps(8), setldaps(8)

注 - 关于支持 LDAP、Active Directory 和 LDAP over SSL 服务的 XCP 固件版本，请参见服务器的最新《产品说明》。

3.5.5 XSCF 用户帐户注册流程

出厂时设置的默认用户帐户被命名为“default”。如需使用任何其他用户帐户操作系统，请在 XSCF 注册。

用户帐户“default”有以下权限：

- "default" 权限: useradm 和 platadm

在默认帐户用于初始安装时的登录时，至少注册一个具有 useradm 或 platadm 用户权限的用户帐户。有关使用默认用户帐户登录验证的详情，请参见所使用服务器《安装指南》中的“登录 XSCF”。

注册流程

如需使用 LDAP、Active Directory 或 LDAP over SSL 服务通过网络上的目录服务来

管理 XSCF 用户帐户，请参见 "3.5.12 使用 LDAP 管理 XSCF 用户帐户"、"3.5.13 使用 Active Directory 管理 XSCF 用户帐户" 或 "3.5.14 使用 LDAP over SSL 管理 XSCF 用户帐户"。

系统管理员按照如下步骤注册用户账户。有关详情，请参见提示的各章节。

1. 用具有 **useradm** 权限的用户帐户登录 XSCF（参见 3.5.6 节）。
默认用户帐户 "default" 具有 useradm 权限。
2. 检查注册的用户（请参见 3.5.6 节中的 **showuser(8)**）。
添加用户帐户时，执行 **showuser** 命令并指定 **-l** 选项，并确认用户帐户列表中没有无效账户。
3. 检查/更改密码策略（请参见 3.5.7 节中的 **showpasswordpolicy(8)** 或 **setpasswordpolicy(8)**）。
4. 注册 XSCF 用户帐户（请参见 3.5.8 节中的 **adduser(8)**）。
通过使用 **adduser** 命令，注册用户帐户以适应用户环境。
5. 设置密码（请参见 3.5.8 节中的 **password(8)**）。
6. 注册用户权限（请参见 3.5.9 节中的 **setprivileges(8)**）。

有关各命令的详细信息，请参见其手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

3.5.6 确认已注册的用户

如需确认系统的已注册用户，请使用 **showuser** 命令。如需查看其他用户账户的信息，必须使用具有 useradm 权限的用户帐户才能执行此命令。

1. 执行 **showuser** 命令，查看 XSCF 的用户帐户信息。
在以下的示例中，通过指定 **-l** 选项，显示了 XSCF 用户账户的所有信息。

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

在以下的示例中，通过指定 **-p** 选项，显示了用户账户权限的信息。

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

3.5.7 确认/更改密码策略

在重新设置密码策略后，密码策略随后应用到新加的用户。使用 `showpasswordpolicy` 命令查看当前设置的密码策略。查看密码策略以后，如果您希望更改，请使用 `setpasswordpolicy` 命令。请使用具有 `useradm` 权限的用户账户执行 `setpasswordpolicy` 命令。

`setpasswordpolicy` 命令使用以下选项设置密码策略。

表 3-9 `setpasswordpolicy` 命令选项

选项	密码策略	设置内容
-n	Mindays	下次密码可以更改前，密码更改后的最小天数。0 表示该密码可以随时更改。
-M	Maxdays	密码有效的最多天数
-w	Warn	密码已经到期之前，发出密码过期警告后的天数
-i	Inactive	锁定帐户前，密码过期后的天数
-e	Expiry	该帐户仍然有效的天数
-y	Retry	允许重试更改密码的次数
-k	Difok	新密码中包含但旧密码中未包含的字符数
-m	Minlen	可接受的最小密码长度
-d	Dcredit	包含数字字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的数字字符数。在这里，您可以设置此减少的最大值。
-u	Ucredit	包含大写字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的大写字符数。在这里，您可以设置此减少的最大值。
-l	Lcredit	包含小写字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的小写字符数。在这里，您可以设置此减少的最大值。
-o	Ocredit	包含非字母数字字符的密码可能短于可接受的最小密码长度 (Minlen)。减少的字符数最多为密码中包含的非字母数字字符数。在这里，您可以设置此减少的最大值。
-r	Remember	密码历史中储存的密码数

操作步骤

1. 执行 `showpasswordpolicy` 命令以检查密码策略。

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

2. 必要时，执行 **setpasswordpolicy** 命令更改密码策略的设置。

以下示例指定以下内容：

- 重试次数最多 3 次
- 密码包含 2 个数字字符时，密码长度为 6 个或更多字符。密码不包含数字字符时，密码长度为 8 个或更多字符
- 到期时间为 60 天
- 密码到期前 15 天开始警告
- 3 作为要记住的密码的数量

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

3. 执行 **showpasswordpolicy** 命令，并确认设置。

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

注 - 系统密码策略在使用 **password** 命令时，在操作数中指定其他用户时更改无效。更改另一个用户的密码时，务必指定一个符合系统密码策略的密码。

3.5.8 添加一个 XSCF 用户帐户并设置密码

如需添加用户账户，请使用 `adduser` 命令。
请使用具有 `useradm` 权限的用户账户执行此命令。有关可用于用户帐户的名称的信息，请参见“3.5.1 XSCF 用户帐户”。

对于已经添加的用户账户，使用 `password` 命令设置密码。`password` 命令使用如下的选项设置密码的有效期。

表 3-10 password 命令选项

选项	设置内容
-e	设置用户账户的有效期，或设置失效日期。当设置为 NEVER 时，用户账户的失效日期无效。
-i	设置锁定帐户前，密码失效后的天数
-M	设置密码有效期的最多天数
-n	设置密码有效期的最少天数
-w	设置密码到期之前，发出密码过期警告后的天数

操作步骤

1. 执行 `adduser` 命令以添加一个用户帐户。
下面示例指定用户帐户名称为 `jsmith`。如果省略了 UID 指定，自动分配 UID。

```
XSCF> adduser jsmith
```

在下面示例中使用一个指定的 UID，使用 `-u` 选项添加用户帐户。

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

2. 执行 `password` 命令，并指定密码。

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

下面示例指定到期时间为 60 天，并在密码过期前 15 天开始警告。

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

3.5.9 设置用户权限

如需设置用户权限，请使用 `setprivileges` 命令。请使用具有 `setprivileges` 权限的用户帐户执行此命令。有关用户权限的类型，请参见 [表 3-6](#)。

1. 执行 `showuser` 命令，查看已启用的用户帐户信息。

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

2. 执行 `setprivileges` 命令以将用户权限分配给用户帐户。
下面是将用户权限 `useradm` 和 `auditadm` 指定给用户帐户 `jsmith` 的示例。

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

注 - `setprivileges` 命令分配指定操作数的用户权限。将一个新的用户权限添加到已分配用户权限的用户帐户，也指定现有的用户权限。

3. 执行 `showuser` 命令并确认用户权限。

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

3.5.10 启用/禁用用户帐户

使用 `adduser` 命令注册的用户账户在被注册后立即启用。必要时您可禁用已注册的 XSCF 用户帐户，然后还可再次启用。

如需禁用用户账户，请使用 `disableuser` 命令。如需启用已被禁用的用户账户，请使用 `enableuser` 命令。请使用具有 `useradm` 权限的用户账户执行 `disableuser` 和 `enableuser` 命令。

1. 执行 `showuser` 命令，查看已启用的用户帐户信息。

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

2. 执行 `disableuser` 命令以禁用一个用户帐户。
以下是指定用户账户禁用的示例。


```
XSCF> disableuser jsmith
```

3. 如需再次使用用户帐户时，执行 **enableuser** 命令以启用帐户。
以下是指定用户账户启用的示例。

```
XSCF> enableuser jsmith
```

4. 执行 **showuser** 命令，确认已启用的用户帐户信息。

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

3.5.11 启用/禁用登录锁定功能

登录锁定功能启用时，用户试图登录时 3 次失败，该用户在实现设定的时间内无法再次登录。在默认设置中，登录锁定功能禁用。

如需设置锁定时间和启用锁定功能，请使用 **setloginlockout** 命令。启用锁定功能时，请将锁定时间设置为 0 分钟以上。锁定时间值可设置在 0 到 1440 分钟之间。启用后如需禁用锁定功能，请将锁定时间设置为 0 分钟。使用 **showloginlockout** 命令确认锁定时间已设置。请使用具有 **useradm** 权限的用户账户执行 **setloginlockout** 和 **showloginlockout** 命令。

1. 执行 **showloginlockout** 命令以查看锁定功能设置。

```
XSCF> showloginlockout
90 minutes
```

2. 执行 **setloginlockout** 命令以配置锁定功能。
以下是指定锁定时间为 20 分钟并且启用锁定功能的示例。

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

下面是禁用锁定功能的示例。

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

设置的锁定时间在下次登录时有效。如果指定的时间为 0，在下次登录时锁定功能被禁用。

锁定功能在主和备用 XSCF 上都启用。如果用户账户被锁定，在审核日志中保存该信息。如果锁定功能禁用，允许用户登录的次数没有限制。

如果您希望在锁定期过期之前使用被锁定的用户账户，系统管理员可禁用锁定功能。用户帐户成功登录后，系统管理员必须再次设置锁定时间和启用锁定功能。

3.5.12 使用 LDAP 管理 XSCF 用户帐户

Lightweight Directory Access Protocol (LDAP) 是用于在网络上访问目录服务的协议。通常，SPARC M12/M10 系统上的 XSCF 用户帐户的用户验证和用户权限由本地 XSCF 管理。但是，使用 LDAP 也可通过网络的目录服务管理进行管理。另外，如果安装了多个 SPARC M12/M10 系统，则所有系统通用的 XSCF 用户帐户都可以用于 LDAP。

如需管理 XSCF 用户帐户设置，如用户验证和用户权限，请使用 LDAP 将 XSCF 配置成 LDAP 客户端。

本章介绍如何使用 LDAP 通过网络目录服务管理 XSCF 用户帐户设置。

注 - 本节不对 LDAP 服务器的配置和管理进行说明。熟悉 LDAP 服务器的管理员应设计 LDAP 服务器。

注 - 关于支持 LDAP 的 XCP 固件版本，请参见服务器的最新《产品说明》。

在 LDAP 设置中，设置与 LDAP 客户端有关的项目。设置包括 LDAP 服务器、绑定 ID、密码和搜索库等。在 LDAP 服务器中可管理 XSCF 用户信息。

表 3-11 列出了与 LDAP 设置相关的术语。

表 3-11 与 LDAP 有关的术语

术语	说明
LDAP	是 Lightweight Directory Access Protocol 的缩写。 LDAP 是用于在网络上访问目录服务的协议。
baseDN	base Distinguished name 的缩写。 在 LDAP 下，目录信息的组织结构是树状结构。如需执行一个搜索任务，指定树状结构中的子树。此时，指定目标子树的顶部的可辨别名称 (DN)。这个 DN 被简称为搜索基础 (baseDN)。
证书链	证书列表，包括用户证书和验证证书。OpenSSL 和 TLS 证书必须事先下载。
TLS	Transport Layer Security 的缩写。 这是用于通过互联网发送/接收加密信息的协议。

LDAP 设置流程

本节介绍将 XSCF 配置为 LDAP 客户端的流程。

1. 启用 **LDAP**。
2. 输入 **LDAP 服务器**的配置信息。
 - IP 地址或主机名和主 LDAP 目录端口号
 - 选项: 最多 2 个 IP 地址或主机名和备用 LDAP 目录的端口
 - 参考搜索基础可辨别名称 (DN)
 - 是否使用传输层安全 (TLS)

3. 确认 LDAP 操作是否正常。

LDAP 服务器必要的设定

- 向 LDAP 架构文件添加与用户权限有关说明。
如需将 XSCF 配置为 LDAP 客户端，在 LDAP 服务器创建一个与 XSCF 用户权限有关的 LDAP 构架文件。向构架文件添加如下说明。

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

- 向 LDIF 文件添加所需的用户属性。
向 LDIF 文件（LDAP 数据互换格式）在 LDAP 服务器添加如下的每个用户所需的属性。

表 3-12 LDIF 文件所需的属性

字段名	说明
spPrivileges	XSCF 上有效的用户权限
uidNumber	XSCF 上有效的用户 ID 号 uidNumber 必须是大于 100 的数值。使用 showuser 命令查看 UID。

以下是 LDAP 构架文件的输入示例。

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

将 XSCF 配置成 LDAP 客户端的用户验证机制

如果在 XSCF 配置 LDAP 客户端并启用时，首先在本地执行用户验证，然后在 LDAP 服务器执行。如果没有为用户指定权限而执行 setprivileges 命令，所有用户的本地权限数据被删除。然后，如果在 LDAP 中权限引用被启用，在 LDAP 中引用用户权限。当指定用户权限为 none 时，即使在 LDAP 用户有权限数据，用户也没有用户权限。

以下命令用于在 XSCF 上管理 LDAP。

```
- setlookup  
- setldap
```

Unix 加密或 MD5 加密方法用于保存在 LDAP 储存库的密码。

一旦您将 XSCF 配置成 LDAP，不用每天进行管理。

LDAP 设置项目和使用的 shell 命令

表 3-13 列出了 LDAP 设置项目和对应的 shell 命令。

表 3-13 LDAP 设置项目和使用的命令

设置项目	功能说明	Shell 命令	备注
LDAP 使用情况查看	查看关于是否 LDAP 服务器用于验证和用户权限查找的状态。	showlookup	
LDAP 使用启用/禁用	启用或禁用用于验证和用户权限查找的 LDAP 服务器的使用。	setlookup	如果指定将验证数据和用户权限数据放置在 LDAP 服务器，系统优先搜索本地区域。如果在本地没有找到目标数据，在 LDAP 服务器搜索。
客户端查看	查看 LDAP 客户端设置信息。	showldap	
绑定 ID	注册用于连接（绑定：验证）LDAP 服务器的 ID。	setldap	绑定 ID 的最大长度是 128 个字符。
密码	设置用于连接 LDAP 服务器的密码。		密码由 8 到 16 个字符组成。
搜索基础	设置 LDAP 树状搜索基础 (baseDN)。		- 如果省略这个项目，命令从树的顶部开始搜索。 - 搜索基础允许的最长字符数是 128 个。
证书链	输入 LDAP 服务器的证书链。 输入使用安全复制从远程文件输入证书链 (scp)。		- 证书链必须是 PEM 格式。 (*1) - 从远程文件使用 scp 输入证书时需要输入密码。
LDAP 服务器/端口	指定主、次 LDAP 服务器的 IP 地址和端口号。 为地址指定 IP 地址或主机名。 (例如: ldap://foobar.east, ldaps://10.8.31.14:636)		当没有指定端口号时，默认的 LDAP 端口号是 ldaps:// 636 和 ldap:// 389。
超时	设置进行 LDAP 搜索允许的最大时间（秒）。		
LDAP 测试	测试 LDAP 服务器的连接。		

*1 PEM: Privacy Enhanced Mail 的简称。为了加强隐私，发送的邮件被加密。

启用或禁用 LDAP 服务器的使用

1. 执行 **showlookup** 命令查看验证和用户权限的查找方法。
在如下的示例中，用户验证只在 XSCF 服务器进行，用户权限在 XSCF 和 LDAP 服务器查找。

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

2. 执行 **setlookup** 命令启用/禁用 LDAP 服务器的使用。
在如下的示例中，用户验证和用户权限在 LDAP 服务器启用。

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

3. 执行 **showlookup** 命令并确认查找方法。

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

设置 LDAP 服务器、端口号、绑定 ID、绑定密码、搜索基础 (baseDN) 和搜索时间 (超时期间)

1. 执行 **showldap** 命令以查看 LDAP 客户端设置。

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

2. 执行 **setldap** 命令以配置 LDAP 客户端设置。
在以下的示例中，指定了绑定 ID 和搜索基础 (baseDN)。

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

在以下的示例中，指定了绑定密码。

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

在以下的示例中，指定了主次 LDAP 服务器和端口号。

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

在以下的示例中，指定了 LDAP 搜索的超时时间。

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

3. 执行 **showldap** 命令，并确认设置。

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

安装 LDAP 服务器的证书链

1. 执行 **showldap** 命令以查看 LDAP 设置。

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

2. 执行 **setldap** 命令以输入证书链。

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

3. 执行 **showldap** 命令以确认证书链已被输入。

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

测试 LDAP 服务器的连接

1. 执行 **setldap** 命令以执行测试。

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

2. 以 **LDAP** 服务器已注册用户身份登录。使用已输入的密码确认用户验证。

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

3. 执行 **showuser** 命令，确认显示的用户权限是否和在 **LDAP** 服务器创建的权限相同。

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

3.5.13 使用 Active Directory 管理 XSCF 用户帐户

在 Active Directory 设置中，设置与 Active Directory 客户端有关的项目。设置包括 Active Directory 服务器、加载服务器证书、组名、用户权限、用户域、DNS 定位器查询等。在 Active Directory 服务器中可管理 XSCF 用户信息。

注 - 本节不对 Active Directory 服务器的配置和管理进行说明。熟悉 Active Directory 服务器的管理员应设计 Active Directory 服务器。

注 - 关于支持 Active Directory 的 XCP 固件版本，请参见服务器的最新《产品说明》。

表 3-14 列出了与 Active Directory 设置相关的术语。

表 3-14 与 Active Directory 相关的术语

术语	说明
Active Directory	Active Directory 是一个分布式目录服务，是由微软公司开发并可在 Windows 操作系统中应用。和 LDAP 目录服务相同，用于用户验证。
用户域	用户域是用于验证用户的验证域。
DNS 定位器查询	用于查询有关用户验证时 Active Directory 服务器的 DNS 服务器。

Active Directory 同时支持用户证书验证和用户访问网络资源级别的授权。Active Directory 在访问系统资源前使用验证识别指定用户，并且为了控制他们访问网络资源的权限将指定的权限授权给用户。

用户权限可在 XSCF 配置，也可从基于各用户组成员身份的网络域服务器获得。一个用户可从属于多个组。用户域是用于验证用户的验证域。Active Directory 按照用户域中配置的顺序验证用户身份。

一旦验证以后，可用以下两种方式决定用户权限：

- 在最简单的情况，用户权限由 XSCF 上的 Active Directory 设置决定。Active Directory 配有 defaultrole 参数。如果配置或设置了 defaultrole 参数，所有通过 Active Directory 验证的用户将被分配在参数中设置的用户权限。在 Active

Directory 服务器设置的用户只需要密码，无需其组成员身份。

- 如果没有配置或没有设置 defaultrole 参数，从基于用户组成员身份的 Active Directory 服务器获取用户权限。在 XSCF，组参数必须和 Active Directory 服务器的组名相对应。各组都有在 XSCF 配置的与组关联的用户权限。一旦用户验证后，用户的组成员身份用于决定用户权限。

Active Directory 设置项目和使用的 shell 命令

表 3-15 列出了设置项目和对应的 shell 命令。

表 3-15 Active Directory 相关设置项目和使用的命令

设置项目	功能说明	Shell 命令	备注
Active Directory 状态查看	查看 Active Directory 的当前状态，例如 Active Directory 和 DNS 定位器模式的启用/禁用。	showad	
Active Directory 使用启用/禁用	指定是否启用或禁用用于管理验证和用户权限的 Active Directory 服务器。	setad	默认禁用。
Active Directory 服务器查看	查看主 Active Directory 服务器或最多 5 个备用的 Active Directory 服务器的配置。	showad	端口号 "0" 代表 Active Directory 的默认端口已被使用。
Active Directory 服务器/端口	指定主 Active Directory 服务器和最多 5 个备用的 Active Directory 服务器的 IP 地址和端口号。 为地址指定 IP 地址或主机名。 如需为 Active Directory 服务器指定主机名，服务器名必须在 DNS 服务器可解析。	setad	当没有指定端口号时，使用默认端口。
服务器证书加载/删除	加载或删除主服务器和最多 5 个备用服务器的证书。	setad	移除证书时，strictcertmode 必须是禁用状。
DNS 定位器模式启用/禁用	启用或禁用 DNS 定位器模式。	setad	默认禁用。
查看 DNS 定位器查询	查看最多 5 个 DNS 定位器查询的配置。	showad	
DNS 定位器查询	配置 DNS 定位器查询。 为了决定用于用户验证的 Active Directory 服务器，DNS 定位器用于查询 DNS 服务器。	setad	为了使 DNS 定位器查询有效，DNS 和 DNS 定位器模式必须启用。
扩展搜索模式启用/禁用	启用或禁用扩展搜索模式。 扩展搜索模式只在用户帐户使用 UserPrincipalName 格式以外的指定环境时启用。	setad	默认禁用。
strictcertmode 启用/禁用	启用或禁用 strictcertmode。 如果启用 strictcertmode，服务器证书必须事先上传到服务器，当服务器证书被提出时证书签名才可被验证。	setad	默认禁用。
查看服务器证书	查看如下： - 主服务器和最多 5 个备用服务器的证书信息。 - 证书的全部内容	showad	
查看用户域	查看用户域。	showad	

表 3-15 Active Directory 相关设置项目和使用的命令 (续)

设置项目	功能说明	Shell 命令	备注
用户域	配置最多 5 个指定的用户域。使用用户名和域名之间用 "@" 符号链接的 UPN 格式或定义为 "uid = 用户名, ou = 组织单元和 dc = 域名" 的可辨别名称 (DN) 格式指定用户域。	setad	如果用户域在登录提示时被直接指定为使用 UPN 格式, 例如 "login: ima.admin@dc01.example.com", 用户域只用于本次登录。
查看 defaultrole	查看 defaultrole 设置。	showad	
defaultrole	指定通过 Active Directory 验证的分配给所有用户的用户权限。	setad	
查看组	查看管理员组、操作员组和客户组的配置。	showad	
管理员组	最多为 5 个管理员组分配组名。管理员组具有 platadm、useradm 和 auditadm 权限。这些权限无法更改。	setad	
操作员组	最多为 5 个操作员组分配组名。操作员组具有 platop 和 auditop 权限。这些权限无法更改。	setad	
客户组	最多为 5 个组分配组名和用户权限。	setad	
超时	以秒为单位配置事务超时时间。您可以指定 1 到 20 间的一个数字值。	setad	默认值为 4 秒。如果配置指定的超时时间过短, 登录进程或设置用户权限的检索可能失败。
登录启用/禁用	启用或禁用 Active Directory 验证和验证诊断信息的日志。	setad	当 XSCF 重新启动时, 此日志将被清除。
查看日志	查看 Active Directory 验证和验证诊断信息。	showad	
日志清除	清除 Active Directory 验证和验证诊断信息的日志。	setad	
默认	重置 Active Directory 设置到出厂默认状态。	setad	

配置 Active Directory 设置之前

配置 Active Directory 设置之前, 注意以下事项。

- 确认使用的是支持 Active Directory 的 XCF 版本。关于支持 Active Directory 的 XCP, 请参见最新《产品说明》。
- Active Directory 设置需要 useradm 用户权限。
- 如果 XSCF 被配置为使用 LDAP、Active Directory 或 LDAP over SSL 管理用户账户数据, 用户账户名和用户身份 (如果已指定) 必须在 XSCF、LDAP、Active Directory 或 LDAP over SSL 中未被使用过。
- 如需在 Active Directory 服务器使用主机名, 在设置 Active Directory 前必须正确地配置 DNS 设置。
- 在 Active Directory, 使用系统账户为 proxyuser 的用户账户。确认没有和其相同的用户帐户。如果存在与 proxyuser 同名的用户账户, 使用 deleteuser 命令删除。删除该帐户后, 重新启动 XSCF, 然后再使用 Active Directory。

- 如果启用了 Active Directory 并且您希望通过 telnet 登录，查询第二个和以后的备用服务器可能会超时，引起登录失败。
- 如果超时的操作数值太小，您登录到 XSCF 后，可能没有被分配到用户权限。此时，增加超时设置值并且重新尝试。
- 如果您是 Active Directory 用户，您不能将用户公钥上传到 XSCF。Active Directory 用户可使用密码验证通过 SSH 连接到 XSCF 后登录。

启用或禁用 Active Directory 服务器的使用

1. 执行 **showad** 命令以查看 Active Directory 服务器的使用情况。

```
XSCF> showad
dnslocator mode: disabled
expsearch mode: disabled
state: disabled
strictcert mode: disabled
timeout: 4
logdetail: none
```

2. 执行 **setad** 命令以启用/禁用 Active Directory 服务器的使用。
在下例中，启用 Active Directory 服务器的使用。

```
XSCF> setad enable
```

在下例中，禁用 Active Directory 服务器的使用。

```
XSCF> setad disable
```

3. 执行 **showad** 命令以确认 Active Directory 是启用还是禁用。
在下例中，启用 Active Directory。

```
XSCF> showad
dnslocator mode: disabled
expsearch mode: disabled
state: enabled
strictcert mode: disabled
timeout: 4
logdetail: none
```

设置 Active Directory 服务器和端口号

1. 执行 **showad** 命令以查看 Active Directory 服务器设置。

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

2. 执行 **setad** 命令以设置 **Active Directory** 服务器。
在以下的示例中，指定了主服务器和端口号。

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

在以下的示例中，指定了备用服务器。

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

3. 执行 **showad** 命令并确认 **Active Directory** 设置。

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

添加/删除服务器证书

1. 执行 **showad** 命令以查看服务器证书信息。

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

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

Alternate Server 2:
... <snip>

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

2. 执行 **setad** 命令添加服务器证书到 **XSCF**。

在以下的示例中，使用用户名和密码添加了主服务器的服务器证书。

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

在以下的示例中，证书的内容被复制和粘贴到屏幕，从控制台添加了备用服务器 1 的证书。按下 [Enter] 键后，按下 [Ctrl] 和 [D] 键完成添加。

```

XSCF> setad loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:
-----BEGIN CERTIFICATE-----
MIIEtjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcn5pYTEuSMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZWlzMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
[Enter]
[Ctrl]+[D]

```

3. 执行 **showad** 命令以确认服务器证书已添加。

```

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

XSCF> showad cert -i 1
Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = ap1le, CN = ap1le.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = ap1le, CN = ap1le.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)

```

4. 执行 **setad** 命令以删除主服务器证书。

```

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

```

5. 执行 **showad** 命令以确认服务器证书已删除。

```

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

```

```
version = (none)
```

移除证书时，`strictcertmode` 必须是禁用状。

启用或禁用 DNS 定位器模式

1. 执行 `showad` 命令显示 DNS 定位器模式是启用还是禁用。

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

2. 执行 `setad` 命令启用/禁用 DNS 定位器模式。
在下例中，启用 DNS 定位器模式。

```
XSCF> setad dnslocatormode enable
```

在下例中，禁用 DNS 定位器模式。

```
XSCF> setad dnslocatormode disable
```

3. 执行 `showad` 命令以确认 DNS 定位器模式是启用还是禁用。
在下例中，启用 DNS 定位器模式。

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

配置 DNS 定位器查询

注 - 设置 DNS 定位器查询之前，启用 DNS 定位器模式。

1. 执行 `showad` 命令以查看 DNS 定位器查询的配置。

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

2. 执行 **setad** 命令配置 DNS 定位器查询。

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

3. 执行 **showad** 命令并确认 DNS 定位器查询。

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

为了使 DNS 定位器查询有效，DNS 和 DNS 定位器模式必须启用。

启用/禁用扩展搜索模式

1. 执行 **showad** 命令以查看扩展搜索模式是启用还是禁用。

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

2. 执行 **setad** 命令启用/禁用扩展搜索模式。
在下例中，启用扩展搜索模式。

```
XSCF> setad expsearchmode enable
```

在下例中，禁用扩展搜索模式。

```
XSCF> setad expsearchmode disable
```

3. 执行 **showad** 命令以确认扩展搜索模式是启用还是禁用。
在下例中，启用扩展搜索模式。

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

```
timeout: 4
logdetail: none
```

启用/禁用 strictcertmode

1. 执行 **showad** 命令以查看 **strictcertmode** 是启用还是禁用。

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

2. 执行 **setad** 命令启用/禁用 **strictcertmode**。
在下例中，启用 **strictcertmode**。

```
XSCF> setad strictcertmode enable
```

在下例中，禁用 **strictcertmode**。

```
XSCF> setad strictcertmode disable
```

3. 执行 **showad** 命令并确认是启用还是禁用 **strictcertmode**。
在下例中，启用 **strictcertmode**。

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

如需启用 **strictcertmode**，服务器证书必须已经被上传到 XSCF。

设置用户域

1. 执行 **showad** 命令以查看用户域。

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



```
domain 4: (none)
domain 5: (none)
```

2. 执行 **setad** 命令以设置用户域。
在下例中，设置用户域 1。

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

在下例中，设置用户域 2。

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

3. 执行 **showad** 命令并确认用户域。

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

如果用户域在登录提示时被直接指定，例如 "login: ima.admin@dc01.example.com"，用户域只用于本次登录。

设置默认权限

1. 执行 **showad** 命令以显示默认权限。

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

2. 执行 **setad** 命令来设置默认权限。

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

3. 执行 **showad** 命令并确认默认权限。

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

设置组名和权限

1. 执行 **showad** 命令以查看组名。
下面是管理员组的示例。

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

下面是操作员组的示例。

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

下面是客户组的示例。

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

2. 执行 **setad** 命令设置组名和权限。
在下例中，设置管理员组 1。

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

在下例中，设置操作员组 1。

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

在下例中，设置客户组 1。

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

在下例中，设置客户组 1 的权限。

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

3. 执行 **showad** 命令确认组名和权限。
下面是确认管理员组的示例。

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

下面是确认操作员组的示例。

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

下面是确认客户组的示例。

```
XSCF> showad group custom
Custom Group 1
  name: CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
  roles: platadm platop
Custom Group 2
  name: (none)
  roles: (none)
Custom Group 3
  name: (none)
  roles: (none)
Custom Group 4
  name: (none)
  roles: (none)
Custom Group 5
  name: (none)
  roles: (none)
```

管理员组具有 `platadm`、`useradm` 和 `auditadm` 权限。这些权限无法更改。操作员组同样具有 `platop` 和 `auditop` 权限。这些权限无法更改。

设置超时

1. 执行 `showad` 命令查看超时时间。

```
XSCF> showad
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 4
logdetail: none
```

2. 执行 `setad` 命令以设置超时。
在以下的示例中，超时时间被设置为 10 秒。

```
XSCF> setad timeout 10
```

3. 执行 `showad` 命令确认超时时间。

```
XSCF> showad
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: none
```

启用/禁用 Active Directory 验证和验证诊断信息的日志

1. 执行 **showad** 命令以查看日志详细程度。

```
XSCF> showad
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: none
```

2. 执行 **setad** 命令以设置日志详细程度。
在以下的示例中，启用日志并将日志详细程度设置为 **trace**。

```
XSCF> setad logdetail trace
```

在下例中，禁用日志。

```
XSCF> setad logdetail none
```

3. 执行 **showad** 命令并确认日志详细程度。
以下示例中，将日志详细程度设置为 **trace**。

```
XSCF> showad
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: trace
```

查看诊断信息日志和清除日志文件

1. 执行 **showad** 命令以查看日志详细程度。

```
XSCF> showad
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: trace
```

2. 执行 **showad** 命令查看诊断信息。
在以下的示例中，实时查看诊断信息。

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

3. 执行 **setad** 命令清除诊断信息的日志文件。

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

重置 Active Directory 设置到出厂默认状态

1. 执行 **showad** 命令以查看 **Active Directory** 的设置状态。

```
XSCF> showad
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: trace
```

2. 执行 **setad** 命令将 **Active Directory** 设置恢复到默认状态。

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

3. 执行 **showad** 命令确认 **Active Directory** 设置恢复到默认状态。

```
XSCF> showad
dnslocator mode: disabled
expsearch mode: disabled
state: disabled
strictcert mode: disabled
timeout: 4
logdetail: none
```

使用 Active Directory 用户帐户登录

完成每项设置后，确认是否可使用 Active Directory 用户账户登录。

3.5.14 使用 LDAP over SSL 管理 XSCF 用户帐户

在 LDAP over SSL 设置中，设置与 LDAP over SSL 客户端有关的项目。设置包括 LDAP over SSL 服务器、加载服务器证书、组名、用户权限、用户域、DNS 定位器查询等。在 LDAP over SSL 服务器中可管理 XSCF 用户信息。

注 - 本节不对 LDAP over SSL 服务器的配置和管理进行说明。熟悉 LDAP over SSL 服务器的管理员应设计 LDAP over SSL 服务器。

注 - 关于支持 LDAP over SSL 的 XCP 固件版本，请参见最新《产品说明》。

表 3-16 列出了与 LDAP over SSL 设置相关的术语。

表 3-16 与 LDAP over SSL 有关的术语

术语	说明
LDAP over SSL	LDAP over SSL 是类似 Active Directory 的分布式目录服务。LDAP over SSL 通过使用 Secure Socket Layer (SSL)/Transport Layer Security (TLS) 技术对 LDAP 用户提供增强的安全保护。和 LDAP 目录服务相同，LDAP over SSL 用于用户验证。

LDAP over SSL 同时支持用户证书验证和用户访问网络资源级别的授权。LDAP over SSL 在访问系统资源前使用验证识别指定用户，并且为了控制他们访问网络资源的权限将指定的权限授权给用户。

用户权限可在 XSCF 配置，也可从基于各用户组成员身份的网络域服务器获得。一个用户可从属于多个组。用户域是用于验证用户的验证域。LDAP over SSL 按照用户域中配置的顺序验证用户身份。

一旦验证以后，可用以下两种方式决定用户权限：

- 在最简单的情况，用户权限由 XSCF 上的 LDAP over SSL 设置决定。LDAP over SSL 配有 defaultrole 参数。如果配置或设置了 defaultrole 参数，所有通过 LDAP over SSL 验证的用户将被分配在参数中设置的用户权限。在 LDAP over SSL 服务器设置的用户只需要密码，无需其组成员身份。
- 如果没有配置或没有设置 defaultrole 参数，从基于用户组成员身份的 LDAP over SSL 服务器获取用户权限。在 XSCF，组参数必须和 LDAP over SSL 服务器的组名相对应。各组都有在 XSCF 配置的与组关联的用户权限。一旦用户验证后，用户的组成员身份用于决定用户权限。

LDAP over SSL 设置项目和使用的 shell 命令

表 3-17 列出了设置项目和对应的 shell 命令。

表 3-17 LDAP over SSL 设置项目和使用的命令

设置项目	功能说明	Shell 命令	备注
查看 LDAP over SSL 状态	查看当前 LDAP over SSL 的状态，例如启用/禁用 LDAP over SSL 和 usemapmode。	showldapssl	
LDAP over SSL 使用的启用/禁用	指定是否启用或禁用用于管理验证和用户权限的 LDAP over SSL 服务器。	setldapssl	默认禁用。
查看 LDAP over SSL 服务器	查看主 LDAP over SSL 服务器或最多 5 个备用的 LDAP over SSL 服务器的配置。	showldapssl	端口号 "0" 代表 LDAP over SSL 的默认端口已被使用。
LDAP over SSL 服务器/端口	指定主 LDAP over SSL 服务器和最多 5 个备用的 LDAP over SSL 服务器的 IP 地址和端口号。 为地址指定 IP 地址或主机名。 如需为 LDAP over SSL 服务器指定主机名，服务器名必须在 DNS 服务器可解析。	setldapssl	当没有指定端口号时，使用默认端口。
服务器证书加载/删除	加载或删除主服务器和最多 5 个备用服务器的证书。	setldapssl	移除证书时，strictcertmode 必须是禁用状。
usermapmode 启用/禁用	启用/禁用 usermapmode。 当启用时，通过 usermap 操作数指定的非用户域的用户属性，用于用户认证。	setldapssl	默认禁用。
查看 usermap	查看 usermap 设置。	showldapssl	
usermap	配置 usermap。 usermap 用于用户验证。	setldapssl	为了使用 usermap，必须启用 usermapmode。
strictcertmode 启用/禁用	启用或禁用 strictcertmode。 如果启用 strictcertmode，服务器证书必须事先上传到服务器，当服务器证书被提出时证书签名才可被验证。	setldapssl	默认禁用。
查看服务器证书	查看如下： - 主服务器和最多 5 个备用服务器的证书信息。 - 证书的全部内容	showldapssl	
查看用户域	查看用户域。	showldapssl	
用户域	配置最多 5 个指定的用户域。用户域被指定为可辨别名称 (DN) 格式。	setldapssl	
查看 defaultrole	查看 defaultrole 设置。	showldapssl	
defaultrole	指定通过 LDAP over SSL 验证的分配给所有用户的用户权限。	setldapssl	
查看组	查看管理员组、操作员组和客户组的配置。	showldapssl	
管理员组	最多为 5 个管理员组分配组名。管理员组具有 platadm、useradm 和 auditadm 权限。这些权限无法更改。	setldapssl	

表 3-17 LDAP over SSL 设置项目和使用的命令 (续)

设置项目	功能说明	Shell 命令	备注
操作员组	最多为 5 个操作员组分配组名。操作员组具有 <code>platop</code> 和 <code>auditop</code> 权限。这些权限无法更改。	<code>setldapssl</code>	
客户组	最多为 5 个组分配组名和用户权限。	<code>setldapssl</code>	
超时	以秒为单位配置事务超时时间。您可以指定 1 到 20 间的一个数字值。	<code>setldapssl</code>	默认值为 4 秒。如果配置指定的超时时间过短，登录进程或设置用户权限的检索可能失败。
登录启用/禁用	启用/禁用 LDAP over SSL 验证和验证诊断信息的日志。	<code>setldapssl</code>	当 XSCF 重新启动时，此日志将被清除。
查看日志	查看 LDAP over SSL 验证和验证诊断信息。	<code>showldapssl</code>	
日志清除	清除 LDAP over SSL 验证和验证诊断信息的日志。	<code>setldapssl</code>	
默认	重置 LDAP over SSL 设置到出厂默认状态。	<code>setldapssl</code>	

配置 LDAP over SSL 设置之前

配置 LDAP over SSL 设置之前，注意以下事项。

- 确认使用的是支持 LDAP over SSL 的 XCP 版本。关于支持 LDAP over SSL 的 XCP，请参见最新《产品说明》。
- LDAP over SSL 设置需要 `useradm` 用户权限。
- 如果 XSCF 被配置为使用 LDAP、Active Directory 或 LDAP over SSL 管理用户账户数据，用户账户名和用户身份（如果已指定）必须在 XSCF、LDAP、Active Directory 或 LDAP over SSL 中未被使用过。
- 如需在 LDAP over SSL 服务器使用主机名，在设置 LDAP over SSL 前必须正确地配置 DNS 设置。
- 在 LDAP over SSL，使用系统账户为 `proxyuser` 的用户账户。确认没有和其相同的用户帐户。如果存在与 `proxyuser` 同名的用户账户，使用 `deleteuser` 命令删除。删除该帐户后，重新启动 XSCF，然后再使用 LDAP over SSL。
- 如果超时的操作数值太小，您登录到 XSCF 后，可能没有被分配到用户权限。此时，增加超时设置值并且重新尝试。
- LDAP over SSL 用户无法将用户公钥上传到 XSCF。LDAP over SSL 用户可使用密码验证通过 SSH 连接到 XSCF 后登录。

启用/禁用 LDAP over SSL 服务器的使用

1. 执行 `showldapssl` 命令以查看 LDAP over SSL 服务器的使用情况。

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

2. 执行 **setldapssl** 命令以启用/禁用 **LDAP over SSL** 服务器的使用。
在下例中，启用 LDAP over SSL 服务器的使用。

```
XSCF> setldapssl enable
```

在下例中，禁用 LDAP over SSL 服务器的使用。

```
XSCF> setldapssl disable
```

3. 执行 **showldapssl** 命令并确认 **LDAP over SSL** 是启用还是禁用。
在下例中，启用 LDAP over SSL。

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

设置 LDAP over SSL 服务器和端口号

1. 执行 **showldapssl** 命令以查看 **LDAP over SSL** 服务器的设置。

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

```
Alternate Server 5
  address: (none)
  port: 0
```

2. 执行 **setldapssl** 命令以设置 **LDAP over SSL** 服务器。
在以下的示例中，指定了主服务器和端口号。

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

在以下的示例中，指定了备用服务器。

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

3. 执行 **showldapssl** 命令并确认 **LDAP over SSL** 服务器的设置。

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

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

添加/删除服务器证书

1. 执行 **showldapssl** 命令以查看服务器证书信息。

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

```

valid until = (none)
version = (none)

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

Alternate Server 2:
... <snip>

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

```

2. 执行 **setldapssl** 命令添加服务证书到 **XSCF**。
在以下的示例中，使用用户名和密码添加了主服务器的服务器证书。

```

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

```

在以下的示例中，证书的内容被复制和粘贴到屏幕，从控制台添加了备用服务器 1 的证书。按下 [Enter] 键后，按下 [Ctrl] 和 [D] 键完成添加。

```

XSCF> setldapssl loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:
-----BEGIN CERTIFICATE-----
MIIEtjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMQ2FsaWZvcn5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXNOZWlzMURUwEwYDVQQLEwxTeXNOZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
[Enter]
[Ctrl]+[D]

```

3. 执行 **showldapssl** 命令以确认服务器证书已添加。

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

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

4. 执行 **setldapssl** 命令以删除主服务器证书。

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

5. 执行 **showldapssl** 命令以确认服务器证书已删除。

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

移除证书时，`strictcertmode` 必须是禁用状。

启用/禁用 `usermapmode`

1. 执行 **showldapssl** 命令以查看 `usermapmode` 是启用还是禁用。

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

```
logdetail: none
```

2. 执行 **setldapssl** 命令启用/禁用 **usermapmode**。
在下例中，启用 **usermapmode**。

```
XSCF> setldapssl usermapmode enable
```

在下例中，禁用 **usermapmode**。

```
XSCF> setldapssl usermapmode disable
```

3. 执行 **showldapssl** 命令以确认是启用还是禁用 **usermapmode**。
在下例中，启用 **usermapmode**。

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

设置或清除 usermap

1. 执行 **showldapssl** 命令以查看 **usermap** 的配置。

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

2. 执行 **setldapssl** 命令以配置 **usermap**。
在下例中，设置属性信息。

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

在下例中，设置绑定 DN。

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

在下例中，设置绑定密码。

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

在下例中，设置搜索基础。

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

3. 执行 **showldapssl** 命令，并确认 **usermap**。

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

4. 执行 **setldapssl** 命令以清除 **usermap**。

在下例中，清除属性信息。

```
XSCF> setldapssl usermap attributeInfo
```

在下例中，清除绑定 DN。

```
XSCF> setldapssl usermap binddn
```

在下例中，清除绑定密码。

```
XSCF> setldapssl usermap bindpw
```

在下例中，清除搜索基础。

```
XSCF> setldapssl usermap searchbase
```

5. 执行 **showldapssl** 命令以确认 **usermap** 已清除。

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

为了使用 **usermap**，必须启用 **usermapmode**。

启用/禁用 **strictcertmode**

1. 执行 **showldapssl** 命令以查看 **strictcertmode** 是启用还是禁用。

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

2. 执行 **setldapssl** 命令启用/禁用 **strictcertmode**。
在下例中，启用 **strictcertmode**。

```
XSCF> setldapssl strictcertmode enable
```

在下例中，禁用 **strictcertmode**。

```
XSCF> setsetldapssl strictcertmode disable
```

3. 执行 **showldapssl** 命令并确认是启用还是禁用 **strictcertmode**。
在下例中，启用 **strictcertmode**。

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

如需启用 **strictcertmode**，服务器证书必须已经被上传到 XSCF。

设置用户域

1. 执行 **showldapssl** 命令以查看用户域。

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

2. 执行 **setldapssl** 命令以设置用户域。
在下例中，设置用户域 1。

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


在下例中，设置用户域 2。

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

3. 执行 **showldapssl** 命令并确认用户域。

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

设置默认权限

1. 执行 **showldapssl** 命令以查看默认权限。

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

2. 执行 **setldapssl** 命令来设置默认权限。

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

3. 执行 **showldapssl** 命令并确认默认权限。

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

设置组名和权限

1. 执行 **showldapssl** 命令以查看组名。

下面是管理员组的示例。

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

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

下面是操作员组的示例。

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

下面是客户组的示例。

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

2. 执行 `setldapssl` 命令设置组名和权限。

在下例中，设置管理员组 1。

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

在下例中，设置操作员组 1。

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

在下例中，设置客户组 1。

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

在下例中，设置客户组 1 的权限。

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

3. 执行 **showldapssl** 命令确认组名和权限。

下面是确认管理员组的示例。

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

下面是确认操作员组的示例。

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

下面是确认客户组的示例。

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

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

管理员组具有 `platadm`、`useradm` 和 `auditadm` 权限。这些权限无法更改。操作员组同样具有 `platop` 和 `auditop` 权限。这些权限无法更改。

设置超时

1. 执行 `showldapssl` 命令查看超时时间。

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 4
logdetail: none
```

2. 执行 `setldapssl` 命令以设置超时时间。
在以下示例中，超时时间被设置为 10 秒。

```
XSCF> setldapssl timeout 10
```

3. 执行 `showldapssl` 命令确认超时时间。

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: none
```

启用或禁用 LDAP over SSL 验证和验证诊断信息的日志

1. 执行 `showldapssl` 命令以查看日志详细程度。

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: none
```

2. 执行 **setldapssl** 命令以设置日志详细程度。
在以下的示例中，启用日志并将日志详细程度设置为 **trace**。

```
XSCF> setldapssl logdetail trace
```

在下例中，禁用日志。

```
XSCF> setldapssl logdetail none
```

3. 执行 **showldapssl** 命令并确认日志详细程度。
以下示例中，将日志详细程度设置为 **trace**。

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

查看诊断信息日志和清除日志文件

1. 执行 **showldapssl** 命令以查看日志详细程度。

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

2. 执行 **showldapssl** 命令查看诊断信息。
在以下的示例中，实时查看诊断信息。

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

3. 执行 **setldapssl** 命令清除诊断信息的日志文件。

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

重置 LDAP over SSL 设置到默认状态

1. 执行 **showldapssl** 命令以查看 LDAP over SSL 的设置状态。

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

2. 执行 **setldapssl** 命令将 LDAP over SSL 设置恢复到默认状态。

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

3. 执行 **showldapssl** 命令，确认 LDAP over SSL 设置恢复到其默认值。

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

使用 LDAP over SSL 用户帐户登录

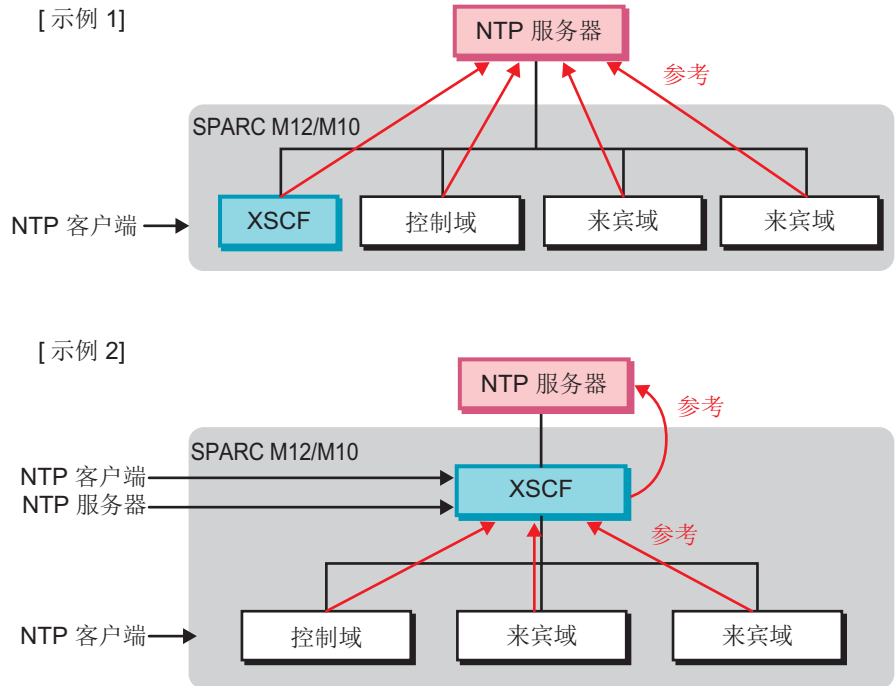
完成每项设置后，确认是否可使用 LDAP over SSL 用户账户登录。

3.6 设置 XSCF 时间/日期

本节介绍如何设置系统的时间。系统将 XSCF 时钟用作所有物理分区的基准时钟。也可以将 XSCF 配置为 NTP 服务器或 NTP 客户端运行。如果未将 XSCF 配置为 NTP 客户端，则 SPARC M12/M10 的每个机箱内置的实时时钟 (RTC) 将用于 XSCF 时间。如需此时更改 XSCF 时间，使用 **setdate** 命令。

图 3-1 显示了与该系统的时间有关的运行方案的一些示例。在示例 1 中，XSCF 和逻辑域作为 NTP 客户端运行。在示例 2 中，XSCF 作为 NTP 客户端和 NTP 服务器运行。

图 3-1 与时间有关的运行方案的示例



注 - 要求客户确定 NTP 服务器操作方案。有关 NTP 的详情，请参见 NTP 相关手册。

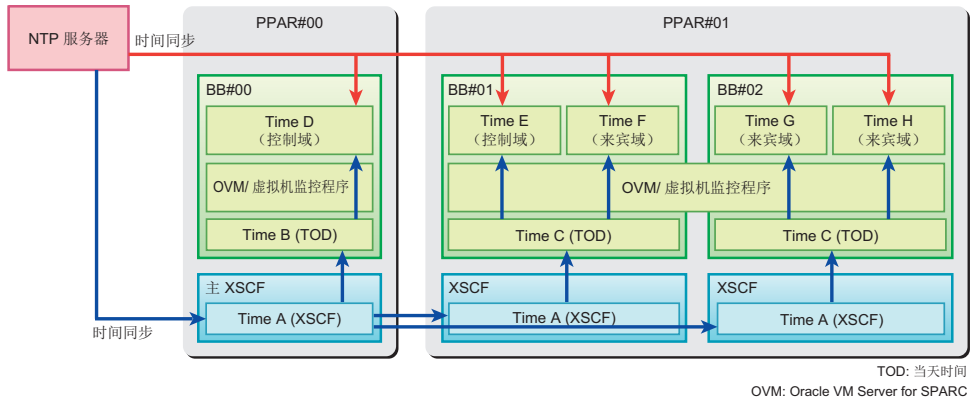
3.6.1 了解 XSCF 时间和物理分区时间之间的关系

XSCF 保持 XSCF 和物理分区之间的时间差。这样可以防止逻辑域和 XSCF 之间的时间差变化，即使物理分区被重置。即使在 XSCF 固件上执行 `setdate` 命令更改 XSCF 的时间，物理分区和 XSCF 之间的时间差也会保持。

XSCF 时间和物理分区时间采用以下方式管理。

- 当物理分区的电源开启时，XSCF 和物理分区之间的时间差信息将添加至 XSCF 时间，此数值被设置为物理分区硬件时间 (TOD)。
- Oracle Solaris 启动时，将基于物理分区硬件时间 (TOD) 设置逻辑域时间。

图 3-2 设置 XSCF 和逻辑域的时间



注 - 在物理分区初始配置之外，请勿使用 `resetdateoffset` 命令，因为该命令影响上述提到的时间控制。仅在物理分区初始配置时才使用 `resetdateoffset` 命令。
关于物理分区初始配置时 `resetdateoffset` 命令的使用，请参见所使用服务器的《安装指南》。

3.6.2 逻辑域的时间管理策略

您可为逻辑域设置各自的时间管理策略。因此逻辑域可以用多种方式管理时间。以下介绍域时间管理策略。

- 逻辑域启动的时间基于 XSCF 时间设置。
- 逻辑域可以被配置为外部 NTP 服务器的 NTP 客户端。在此情况下，逻辑域初始时间基于 XSCF 时间被设置后，与 NTP 服务器同步。
- 逻辑域可以被配置为当做 NTP 服务器的 XSCF 的 NTP 客户端。在此情况下，逻辑域启动的时间与 XSCF 时间同步。
- 使用 Oracle Solaris 的 `date` 命令在逻辑域上配置时间设置后，逻辑域和物理分区之间的时间差在重新启动后会保持。

注 - 如需使用 NTP 同步时间，请为同一个物理分区中的逻辑域指定相同 NTP 服务器。有关如何指定域中 NTP 服务器的详情，请参见《Oracle Solaris Administration: Network Services》(Oracle Solaris 10) 或《Introduction to Oracle Solaris 11 Network Services》(Oracle Solaris 11)。

3.6.3 查看与时间有关的设置项目和命令

表 3-18 列出了与时间有关的设置项目和对应的 XSCF shell 命令。

表 3-18 与时间有关的设置项目

设置项目	必须或可选设置	相关命令
时区	可选	settimezone(8), showtimezone(8)
夏令时	可选	settimezone(8), showtimezone(8)
系统时间	必须	setdate(8), showdate(8)
NTP 服务器	可选	setad(8), showad(8)
DNS 轮循	可选	setad(8), showad(8)
首选, 层次	可选	setad(8), showad(8)
本地时钟	可选	setad(8), showad(8)

3.6.4 设置时区

如需查看设置的时区, 执行 `showtimezone` 命令并指定 `-c tz` 选项。如需设置时区, 请使用 `settimezone` 命令。通过指定 `settimezone` 命令的 `-a` 选项, 您可列出可以设置的标准时区。请使用具有 `platadm` 或 `fieldeng` 权限的用户账户执行 `settimezone` 命令。

标准配置中配置的时区符合 POSIX 标准。标准时区列表可能会每年修改。

1. 执行 **showtimezone** 命令以查看时区。

```
XSCF> showtimezone -c tz
America/Chicago
```

2. 执行 **settimezone** 命令以设置 XSCF 时区。
在以下示例中, 指定 `-c settz` 和 `-a` 选项以查看时区列表。

```
XSCF> settimezone -c settz -a
Africa/Abidjan
Africa/Accra
:
Asia/Thimphu
Asia/Tokyo
Asia/Ujung_Pandang
:
Europe/Lisbon
Europe/Ljubljana
Europe/London
:
```

以下是设置亚洲/东京作为时区。

```
XSCF> settimezone -c settz -s Asia/Tokyo
Asia/Tokyo
```

3. 执行 **showtimezone** 命令，并确认设置。

注 -XSCF 所支持的时区（地区/地理名称）可能变更为支持最新的时区信息。

如果预先设置的时区在系统上变得不可用，XSCF 将通过从不可用的时区切换到协调通用时间 (UTC) 来操作。

如果设置的时区变更为采用 UTC 操作，执行 **settimezone-c settz-a** 命令可查看可指定的时区。

如果时区列表中未包括您预先设置的时区，请重置时区。

3.6.5 设置夏令时

如需检查或设置夏令时信息，使用 **showtimezone** 和 **settimezone** 命令。

1. 执行 **showtimezone** 命令以查看时区。

下面是查看时区的示例。

```
XSCF> showtimezone -c tz
Asia/Tokyo
```

以下是查看设置夏令时信息的示例。在以下的示例中，时区是 JST，和 GMT 的偏差是 +9 小时，夏令时名称是 JDT，夏令时早 1 小时，并且期间是从 3 月的最后一个星期日的 2:00 (JST) 到 10 月的最后一个星期日的 2:00 (JDT)。

```
XSCF> showtimezone -c dst -m custom
JST-9JDT,M3.5.0,M10.5.0
```

2. 执行 **settimezone** 命令为 XSCF 设置夏令时信息。

在以下的示例中设置如下的夏令时信息：时区缩写是 JST，和 GMT 的偏差是 +9 小时，夏令时名称是 JDT，和 GMT 夏令时的偏差是 +10 小时，并且期间是从 4 月的第一个星期日的 0:00 (JST) 到 9 月的第一个星期日的 0:00 (JDT)。

```
XSCF> settimezone -c adddst -b JST -o GMT-9 -d JDT -p GMT-10 -f
M4.1.0/00:00:00 -t M9.1.0/00:00:00
JST-9JDT-10,M4.1.0/00:00:00,M9.1.0/00:00:00
```

以下是删除当前设置的夏令时信息的示例。

```
XSCF> settimezone -c deldst -b JST -o GMT-9
```

如需应用通过 **-c adddst** 或 **-c deldst** 选项更改的夏令时信息，请注销后再次登录。

3. 执行 **showtimezone** 命令，并确认设置。

3.6.6 设置系统时间

为 XSCF 时钟的日期和时间设置本地时间或协调世界时 (UTC)。时间设置后, XSCF 重新启动。

如需确认 XSCF 时钟的日期和时间, 请使用 `showdate` 命令。使用 `setdate` 命令设置 XSCF 时钟的日期和时间。请使用具有 `platadm` 或 `fieldeng` 权限的用户账户执行 `setdate` 命令。

注 - 在初始安装时设置系统时间。

1. 执行 `showdate` 命令以显示 XSCF 时间。
以下示例以本地时间显示当前的时间。

```
XSCF> showdate
Mon Jan 23 14:53:00 JST 2012
```

在以下示例中, 指定 `-u` 选项用于查看 UTC 中的当前时间。

```
XSCF> showdate -u
Mon Jan 23 05:56:15 UTC 2012
```

2. 执行 `setdate` 命令以设置时间。
以下是将当前时间指定为本地时间 2012 年 1 月 27 日 16:59:00 的示例。

```
XSCF> setdate -s 012716592012.00
Fri Jan 27 16:59:00 JST 2012
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2012
```

以下是将当前时间指定为 UTC 的 2012 年 1 月 27 日 07:59:00 的示例。

```
XSCF> setdate -u -s 012707592012.00
Fri Jan 27 07:59:00 UTC 2012
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2012
```

设置时间后, XSCF 将重新启动。此时, XSCF 会话被断开。重新连接到 XSCF, 重新登录。

注 - 如果输入电源关闭并进行维护作业, 请务必在输入电源开启后使用 `showdate` 命令确认 XSCF 时间。如果与当前时间不符, 使用 `setdate` 命令设置到当前时间。

3.6.7 同步控制域时间和 XSCF 时间

本节介绍使用 Oracle Solaris 的 `date` 命令设置控制域时间后，同步控制域时间和 XSCF 时间的如下两种方法：

- 将 XSCF 设置为控制域的 NTP 服务器
- 为控制域和 XSCF 设置相同的 NTP 服务器

将 XSCF 设置为控制域的 NTP 服务器

1. 将 **XSCF** 设置为 **NTP** 服务器。
有关详情，请参见 "3.6.8 将 XSCF 指定为 NTP 服务器"。
2. 指定目标物理分区的 ID 并执行 **console** 命令切换到目标物理分区的控制域控制台。

```
XSCF> console -p xx
```

3. 将 **XSCF** 指定为控制域的 **NTP** 服务器。
有关 Oracle Solaris 的 NTP 服务器设置的详情，请参见《Oracle Solaris Administration: Network Services》(Oracle Solaris 10) 或《Introduction to Oracle Solaris 11 Network Services》(Oracle Solaris 11)。
4. 重新启动控制域。
5. 执行 **Oracle Solaris** 的 **date** 命令查看控制域时间。
6. 在物理分区的控制域控制台上，按 **#** 或其他退出命令以返回 **XSCF shell**。
7. 执行 **showdate** 命令以查看 **XSCF** 时间并确认目标物理分区控制域的时间与 **XSCF** 时间相同。

为控制域和 XSCF 指定相同的 NTP 服务器

1. 将 **XSCF** 配置为 **NTP** 客户端。
有关详情，请参见 "3.6.9 将 XSCF 指定为 NTP 客户端"。
2. 向 **XSCF** 注册外部 **NTP** 服务器。
有关 XSCF 的 NTP 服务器设置的详细信息，请参见 "3.6.10 配置由 XSCF 使用的 NTP 服务器"。
3. 指定目标物理分区的 ID 并执行 **console** 命令切换到目标物理分区的控制域控制台。

```
XSCF> console -p xx
```

4. 为控制域指定和 **XSCF** 相同的外部 **NTP** 服务器。
有关 Oracle Solaris 的 NTP 服务器设置的详情，请参见《Oracle Solaris Administration: Network Services》(Oracle Solaris 10) 或《Introduction to Oracle Solaris 11 Network Services》(Oracle Solaris 11)。
5. 重新启动控制域。

6. 执行 **Oracle Solaris** 的 **date** 命令查看控制域时间。
7. 在物理分区的控制域控制台上，按 **#** 或其他退出命令以返回 **XSCF shell**。
8. 执行 **showdate** 命令以查看 **XSCF** 时间并确认目标物理分区控制域的时间与 **XSCF** 时间相同。

注 - 如果您为来宾域、XSCF 和控制域指定相同的 NTP 服务器，您可以将所有域的时间与 XSCF 同步。

3.6.8 将 XSCF 指定为 NTP 服务器

将 XSCF 配置为向其他客户端提供服务的 NTP 服务器。默认状态下，XSCF 不是向其他客户端提供服务的 NTP 服务器。

使用 **showntp** 命令检查 XSCF 网络的 NTP 信息。如需将 XSCF 作为 NTP 服务器使用并提供 NTP 服务，请使用 **setntp** 命令并指定 **-s server** 选项。请使用具有 **platadm** 权限的用户账户执行 **setntp** 命令。

1. 执行 **showntp** 命令以显示 **XSCF** 的 NTP 服务状态。

```
XSCF> showntp -a
client : disable
server : disable
```

2. 执行 **setntp** 命令将 **XSCF** 配置成为 NTP 服务器并向其他客户端提供服务。
在以下示例中，指定 **-s server** 和 **-c enable** 选项，以便将 XSCF 配置成为 NTP 服务器并提供 NTP 服务。

```
XSCF> setntp -s server -c enable
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. 执行 **rebootxscf** 命令重新启动 **XSCF**。

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

此时，XSCF 会话被断开。重新连接到 XSCF，重新登录。

4. 执行 **showntp** 命令并确认 **XSCF** 已配置为 NTP 服务器。

```
XSCF> showntp -a
client : disable
server : enable
```

3.6.9 将 XSCF 指定为 NTP 客户端

如需把 XSCF 当做 NTP 服务器使用，将 XSCF 配置为 NTP 客户端。默认情况下，XSCF 没有被配置为从 NTP 服务器获得时间的 NTP 客户端。如需将 XSCF 配置成为 NTP 服务器，请使用 `setntp` 命令并指定 `-s client` 选项。

1. 执行 `showntp` 命令查看作为 NTP 客户端的 XSCF 状态。

```
XSCF> showntp -a
client : disable
server : enable
```

2. 执行 `setntp` 命令以将 XSCF 配置 NTP 客户端。

```
XSCF> setntp -s client -c enable
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. 执行 `rebootxscf` 命令重新启动 XSCF。

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

此时，XSCF 会话被断开。重新连接到 XSCF，重新登录。

4. 执行 `showntp` 命令并确认 XSCF 已被配置为 NTP 客户端。

```
XSCF> showntp -a
client : enable
server : enable
```

注 - 如果 XSCF 和 NTP 服务器之间的时间差达到 1000 秒（约 17 分钟）或以上，客户端 XSCF 的 `ntp` 守护程序将停止。因此，与 NTP 服务器时间同步将变得不可能。若需确认 `ntp` 守护程序是否停止，请执行 `showntp -l` 命令。如果出现 "NTP is unavailable."，则守护程序停止。如需重新启动 `ntp` 守护程序，请执行 `rebootxscf` 命令，重新启动 XSCF。

- 当 `ntp` 守护程序停止时

```
XSCF> showntp -l
XSCF> NTP is unavailable.
```

- 当 `ntp` 守护程序正在运行时

```
XSCF> showntp -l
remote          refid          st t when poll reach delay  offset jitter
=====
```

```
*192.168.10.10 10.0.20.20 4 u 805 1024 377 19.429 0.083 0.917
127.127.1.0 .LOCL. 5 1 7 64 377 0.000 0.000 0.008
XSCF>
```

3.6.10 配置由 XSCF 使用的 NTP 服务器

最多可以注册 3 个 NTP 服务器用于从上级 NTP 服务器获取 XSCF 时间。如需注册 NTP 服务器，请使用 `setntp` 命令并指定 `-c add` 选项。

此时，XSCF 必须被配置为 NTP 客户端。有关如何将 XSCF 配置为 NTP 客户端的详细信息，请参见“3.6.9 将 XSCF 指定为 NTP 客户端”。

注册 NTP 服务器后，现存的设置被指定的 NTP 服务器删除或覆盖。如需使用主机名指定 NTP 服务器，服务器名称必须能够用 DNS 服务器进行解析。

1. 执行 `showntp` 命令以查看 XSCF 网络使用的 NTP 服务器。

```
XSCF> showntp -a
client : disable
server : enable

server ntp1.example.com prefer
server ntp2.example.com
```

2. 执行 `showntp` 命令以检查同步和查看状态。

```
XSCF> showntp -l
remote          refid          st t when poll reach delay offset jitter
=====
*192.168.0.27 192.168.1.56 2 u 27 64 377 12.929 -2.756 1.993
+192.168.0.57 192.168.1.86 2 u 32 64 377 13.030 2.184 94.421
127.127.1.0 .LOCL. 5 1 44 64 377 0.000 0.000 0.008
```

3. 执行 `setntp` 命令以添加 NTP 服务器。

以下是添加如下 3 个 IP 地址作为 XSCF 的上级 NTP 服务器的示例：192.168.1.2、130.34.11.111 和 130.34.11.117。

```
XSCF> setntp -c add 192.168.1.2 130.34.11.111 130.34.11.117
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

以下是添加如下 2 个主机名作为 XSCF 的上级 NTP 服务器的示例：ntp1.red.com 和 ntp2.blue.com。

```
XSCF> setntp -c add ntp1.red.com ntp2.blue.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

4. 执行 `setntp` 命令删除 XSCF 的 NTP 服务器。

下面是删除 ntp2.example.com（XSCF 的 NTP 服务器）的示例。

```
XSCF> setntp -c del ntp2.example.com  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

5. 执行 **rebootxscf** 命令重新启动 XSCF 以反映所做的设置。

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

此时，XSCF 会话被断开。重新连接到 XSCF，重新登录。

6. 执行 **showntp** 命令并确认 NTP 服务器。

```
XSCF> showntp -a  
client : enable  
server : disable  
  
server ntp1.red.com prefer  
server ntp2.blue.com
```

3.6.11 配置 NTP 服务器的 DNS 轮循

如果您已经使用主机名注册 NTP 服务器，可使用该主机名进行 DNS 轮循。如需使用 DNS 轮循，请使用 **setntp** 命令并指定 **-c pool** 选项。在此之前，您需要配置的 NTP 服务器必须向 XSCF 注册。有关如何注册 NTP 服务器的详细信息，请参见 ["3.6.10 配置由 XSCF 使用的 NTP 服务器"](#)。

1. 执行 **showntp** 命令以显示 DNS 轮循的设置。

```
XSCF> showntp -a  
client : enable  
server : disable  
  
server ntp1.example.com prefer  
server ntp2.example.com
```

2. 执行 **setntp** 命令以配置 DNS 轮循。
以下是表示 NTP 服务器启用 DNS 轮循的示例。

```
XSCF> setntp -c pool ntp2.example.com  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

以下是表示 NTP 服务器禁用 DNS 轮循的示例。

```
XSCF> setntp -c server ntp2.example.com  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```


3. 执行 **rebootxscf** 命令重新启动 XSCF 以反映所做的设置。

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

此时，XSCF 会话被断开。重新连接到 XSCF，重新登录。

4. 执行 **showntp** 命令以显示 DNS 轮循的设置。
以下是表示 ntp2.example.com 启用 DNS 轮循的示例。

```
XSCF> showntp -a  
client : enable  
server : disable  
  
server ntp1.example.com prefer  
pool ntp2.example.com
```

3.6.12 指定/取消 NTP 服务器首选

如果配置了多个 NTP 服务器，在同步 NTP 时，指定 **-m prefer=on**，可将优先权授予首先使用 **setntp** 命令注册的 NTP 服务器。从此时间点以后，启用 DNS 轮循的已注册的服务器将被从同步排除。默认情况下，优先选项设置为 "on (启用)"。

1. 执行 **showntp** 命令以查看首选设置。

```
XSCF> showntp -m  
prefer : on  
localaddr : 0
```

2. 执行 **setntp** 命令设置首选。
下面是指定 NTP 服务器首选的示例。

```
XSCF> setntp -m prefer=on  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

下面是取消 NTP 服务器首选的示例。

```
XSCF> setntp -m prefer=off  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. 执行 **rebootxscf** 命令重新启动 XSCF 以反映所做的设置。

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

此时，XSCF 会话被断开。重新连接到 XSCF，重新登录。

4. 执行 **showntp** 命令并确认首选设置。
以下是取消首选指定的示例。

```
XSCF> showntp -m
prefer : off
localaddr : 0
```

以下是没有指定首选的示例。

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.red.com
server ntp2.blue.com
```

3.6.13 设置 XSCF 层次值

如需设置 XSCF 层次值，使用 **setntp** 命令并指定 **-c stratum** 选项。stratum 值可设置在 1 到 15 之间。默认值为 5。

1. 执行 **showntp** 命令查看为 XSCF 网络设置的 **stratum** 值。

```
XSCF> showntp -s
stratum : 5
```

2. 执行 **setntp** 命令以更改层次值。
下面是将 7 设置为 XSCF 网络中使用的 stratum 值的示例。

```
XSCF> setntp -c stratum -i 7
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. 执行 **rebootxscf** 命令重新启动 XSCF 以反映所做的设置。

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

此时，会话被断开。在新界面重新连接，重新登录。

4. 执行 **showntp** 命令并确认 **stratum** 值。

```
XSCF> showntp -s
stratum : 7
```

3.6.14 更改 XSCF 本地时钟的时钟地址

设置 XSCF 自身的本地时钟地址。您可以将本地时钟地址的最低有效字节指定为 0 到 3 之间的值。本地时钟的默认时钟地址为 127.127.1.0。

1. 执行 **showntp** 命令查看 XSCF 自身本地时钟的时钟地址。

```
XSCF> showntp -m
prefer : on
localaddr : 0

XSCF> showntp -l
remote          refid          st t when poll reach  delay  offset  jitter
=====
*192.168.0.27  192.168.1.56    2 u  27   64   377 12.929 -2.756  1.993
+192.168.0.57  192.168.1.86    2 u  32   64   377 13.030  2.184  94.421
127.127.1.0    .LOCL.          5 l  44   64   377  0.000  0.000  0.008
```

2. 执行 **setntp** 命令以更改 XSCF 自身的本地时钟的时钟地址。
下面是将 1 设置为时钟地址的最低有效字节的示例。

```
XSCF> setntp -m localaddr=1
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. 执行 **rebootxscf** 命令重新启动 XSCF 以反映所做的设置。

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

此时，XSCF 会话被断开。重新连接到 XSCF，重新登录。

4. 执行 **showntp** 命令查看 XSCF 本地时钟的时钟地址。

```
XSCF> showntp -m
prefer : on
localaddr : 1

XSCF> showntp -l
remote          refid          st t when poll reach  delay  offset  jitter
=====
*192.168.0.27  192.168.1.56    2 u  27   64   377 12.929 -2.756  1.993
+192.168.0.57  192.168.1.86    2 u  32   64   377 13.030  2.184  94.421
127.127.1.1    .LOCL.          5 l  44   64   377  0.000  0.000  0.008
```

NTP 服务器引用本地时钟时的注意事项

假设 XSCF 引用的 NTP 服务器引用服务器本身的系统时间（本地时钟），并且“127.127.1.0”是已设置的本地时钟地址。此时，XSCF 可能无法进行时间同步。

XSCF 自身的本地时钟地址被固定在 "127.127.1.0"。当 XSCF 引用的 NTP 服务器的本地时钟的地址被设置为 "127.127.1.0" 时，时钟源 (refid) 的地址与 XSCF 自身的本地时钟地址相同。此类 NTP 服务器不进行 XSCF 时间同步。

执行 `showntp -l` 命令使您能够查看配置在 XSCF 的各 NTP 服务器的时钟源的地址以及 XSCF 自身的本地时钟的地址。

```
XSCF> showntp -l
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
192.168.1.2	LOCAL(0)	3	u	10	1024	377	0.000	0.000	0.000
*127.127.1.0	.LOCAL.	5	l	28	64	377	0.000	0.000	0.008

输出的两个 NTP 服务器中，第一个服务器 (192.168.1.2) 是使用 `setntp` 命令配置的 NTP 服务器。由于本 NTP 服务器的 `refid` 是 LOCAL(0)，地址 "127.127.1.0" 的本地时钟被配置为 NTP 服务器的时钟源。第二个服务器的时钟源是 XSCF 自身的本地时钟。XSCF 自身的本地时钟地址被固定在 "127.127.1.0"。因为 NTP 服务器 (192.168.1.2) 不进行 XSCF 时间同步，所以 XSCF 会与其本地时钟进行时间同步。

为了通过采取以下任何一项措施防止此类问题，您可使用 `setntp` 命令与配置的 NTP 服务器进行正确地时间同步。

- 更改为 XSCF 配置的 NTP 服务器所引用的时钟源。
使用 `showntp -l` 命令检查为 XSCF 配置的 NTP 服务器的时钟源。在上面的输出中，对于其 `refid` 是 LOCAL(0) 的 NTP 服务器，引用地址为 "127.127.1.0" 的本地时钟。因此应进行更改，使服务器引用另一个时钟源。在更改 NTP 服务器的时钟源前，确认更改不会影响其它的 NTP 客户端。
- 更改 NTP 服务器本地时钟的地址。
将 XSCF 引用的 NTP 服务器本地时钟的地址变更为 "127.127.1.1"、"127.127.1.2" 或 "127.127.1.3"。修改 Oracle Solaris 的 `/etc/inet/ntp.conf`。如需应用更改，请重新启动 `ntp` 守护程序。在更改 NTP 服务器的本地时钟地址前，确认更改不会影响其它的 NTP 客户端。
- 更改 NTP 服务器的 `stratum` 值。
将 XSCF 引用的 NTP 服务器的 `stratum` 值变更为 1。`stratum` 值是 1 的 NTP 服务器是最重要的时钟源并且没有 `refid`。因此，其地址永远不会与 XSCF 自身的本地时钟地址相同。在更改 NTP 服务器的 `stratum` 值前，确认更改不会影响其它的 NTP 客户端。
- 更改 XSCF 自身的本地时钟的地址。
使用 `setntp -m localaddr=value` 命令变更 XSCF 自身的本地时钟的地址。指定本地时钟地址的最低字节为 "127.127.1.x"。您可以指定 0 到 3 之间的一个数字值。如果为 `value` 指定的值在 1 和 3 之间，引用本地时钟的 NTP 服务器地址不再与 XSCF 内部本地时钟地址相符。因此，即使引用本地时钟的服务器也可以被配置为 XSCF 的 NTP 服务器。

3.7 配置用于登录 XSCF 的 SSH/Telnet 服务

本节介绍如何配置 SSH 服务和 Telnet 服务。如需使用 XSCF shell 终端和指定物理分区的控制域控制台，请使用 SSH 或 Telnet。启用/禁用 SSH 和 Telnet，设置 SSH 主机密钥和为已登录用户设置自动超时时间。另外也向 XSCF 注册 SSH 用户公钥。

SSH 和 Telnet 可以同时启用。但是，使用 Telnet 服务不能被认为是安全的通信方式。我们建议启用 SSH 服务时，禁用 Telnet 服务。

SSH 客户端

本系统可在如下客户端软件使用 SSH 功能：

- Oracle Solaris Secure Shell
- OpenSSH
- PuTTY
- UTF-8 TeraTerm Pro with TTSSH2

有关使用的软件术语，请参见各自的软件手册。

端口号

SSH 端口号是 22，Telnet 端口号是 23。

用户公钥

如需通过 XSCF-LAN 连接使用 SSH 用户密钥时，为客户端 PC 上的已注册 XSCF 用户帐户创建一个用户密钥和用户公钥，并在 XSCF 注册用户公钥。

如需通过指定用户名查看、注册或删除 SSH 用户公钥，需要 useradm 用户权限。

注 - UTF-8 TeraTerm Pro with TTSSH2 4.66 或更高版本不支持 2048-bit DSA 的用户公钥。

控制台

SPARC M12/M10 系统可以与物理分区的可写 (RW) 或只引用 (RO) 控制域控制台一起使用。您可在每个物理分区使用 1 个 RW 控制台。使用 console 命令使用控制域控制台。有关控制台的详细信息，请参见“第2章 登录和注销 XSCF”。

3.7.1 检查与 SSH 和 Telnet 相关的设置项目和命令

表 3-19 列出了与 SSH 和 Telnet 相关的设置项目以及对应的 XSCF shell 命令。

表 3-19 与 SSH 和 Telnet 相关的设置项目

设置项目	必须或可选设置	相关命令
启用/禁用 SSH	可选	setssh(8), showssh(8)
生成一个主机密钥	可选	setssh(8), showssh(8)

表 3-19 与 SSH 和 Telnet 相关的设置项目 (续)

设置项目	必须或可选设置	相关命令
注册/删除用户公钥	可选	setssh(8), showssh(8)
启用/禁用 Telnet	可选	settelnet(8), showtelnet(8)
超时时间	可选	setautologout(8), showautologout(8)

3.7.2 启用/禁用 SSH 和 Telnet 服务

如需确认为 XSCF 网络设置的 SSH 服务和 Telnet 服务，请使用 `showssh` 和 `showtelnet` 命令。也可使用 `setssh` 和 `settelnet` 命令设置 SSH 服务或 Telnet 服务。使用 `setssh` 和 `settelnet` 命令启用/禁用 SSH 服务或 Telnet 服务时，执行命令后所做的设置立即得到应用。

1. 执行 `showssh` 命令查看 SSH 设置或执行 `showtelnet` 命令查看 Telnet 设置。
下面示例显示 SSH 服务设置。

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwhcBBb/UU0LN08S
ilUXE6j+av1xdY7AFqBflwGxLF+Tx5pTa6HuZ8o8yUBbdZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQ122G8pwibESrh5JmOhSxpLz13P26ksI8qPr+7B
xmjlR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPYP3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RE1U5Pyb8F16uq96L8Q
DMswFlICMzgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
W9pqa/WxC21Ja4RQVN3009kmVwAAAIaON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzFFj5XUzQBdabh5p5Rwz+lvriawFIZI9j2uhM/3HQdrvYSVBEDmJjaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2r1UoI6GICMr64F
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

下面示例显示 Telnet 服务设置。

```
XSCF> showtelnet
Telnet status: disabled
```

2. 执行 **setssh** 命令以配置 SSH 服务设置或执行 **settelnet** 命令以配置 Telnet 服务。
下面示例指定启用 SSH 服务。

```
XSCF> setssh -c enable
Continue? [y|n] :y
```

下面示例指定禁用 Telnet 服务。

```
XSCF> settelnet -c disable
Continue? [y|n] :y
```

3.7.3 设置 SSH 服务主机密钥

如需启用和开始使用 SSH 服务，应首先生成一个主机密钥。
在通过 XSCF-LAN 连接使用 SSH 服务时，记下指纹。将生成的主机公钥的文本数据复制到客户端指定目录内的文件。

1. 执行 **showssh** 命令查看主机密钥和指纹。
第一次启用 SSH 服务时，生成主机密钥。

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwhcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQ122G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUdQZQPYP3PuY2IG7QC4BQ1k
ewDnb1B8/JEqI+8pnfbWzmOWU37KHL19OEYNAV6v+WZT6RE1U5Pyb8F16uq96L8Q
DMswFlICMzgrn+ilJNstr6r8KDjfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
W9pqa/WxC21Ja4RQVN3009kmVwAAAIaON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzzFFj5XUzQBdabh5p5Rwz+lvriawFIZI9j2uhM/3HQdrvYSVBEJMjaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

2. 执行 **setssh** 命令生成主机密钥。
在以下的示例中，生成一个主机密钥并替换现有的主机密钥。

```
XSCF> setssh -c genhostkey
Host key already exists. The key will be updated. Continue? [y|n]
: y
```

3.7.4 注册/删除 SSH 服务的用户公钥

如需通过 XSCF-LAN 连接使用 SSH 服务用户密钥时，为客户端 PC 上的已注册 XSCF 用户帐户创建一个用户密钥和用户公钥，并在 XSCF 注册用户公钥。

1. 执行 **showssh** 命令查看用户公钥。

在以下示例中，指定 **-c pukey** 选项用于查看用户公钥。但是，因为没有注册用户密钥所有没有返回任何响应。

```
XSCF> showssh -c pubkey
```

2. 为客户端上的已注册 **XSCF** 用户帐户创建一个用户密钥和用户公钥。

有关如何创建用户密码和如何在客户端指定密码的详情，请参见使用的客户端软件手册。我们建议您设置密码。

3. 如需注册用户公钥，执行 **setssh** 命令并指定 **-c addpubkey** 选项，复制步骤 2 中创建的用户公钥并粘贴在窗口中。

按下 [Enter] 键后，按下 [Ctrl] 和 [D] 键完成注册。

以下是为用户 **efgh** 注册用户公钥的示例。

```
XSCF> setssh -c addpubkey -u efgh
Please input a public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIPKP0nBK4XJpCFoFbPXNUHDwlrTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
<按 [Ctrl] 和 [D] >
XSCF>
```

4. 执行 **showssh** 命令并确认用户公钥和用户公钥编号。

下面是注册编号为 1 的用户密钥的示例。

```
XSCF> showssh -c pubkey
Public key:
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIPKP0nBK4XJpCFoFbPXNUHDwlrTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

下次登录 XSCF shell 时，使用 XSCF 用户帐户从客户端 PC 建立 SSH 连接。确认您可使用用户密钥验证登录 XSCF shell。

5. 如需删除用户公钥，请执行 **setssh** 命令，指定用户公钥编号。

在下一个示例中，指定 **-c delpubkey** 选项和指定用户公钥编号 **-s** 选项，删除用户

公钥。

```
XSCF> setssh -c delpubkey -s 1  
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAIEAzFh95SohrDgpnN7zFCJCVNy+  
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNkoVLMYlJtBmUMPbGgGV  
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDwlrTD9icD5U/  
wRFGSRRxFI+Ub5oLRxN8+A8= efgH@example.com
```

6. 执行 **showssh** 命令并确认用户公钥已被删除。

```
XSCF> showssh -c pubkey
```

3.7.5 设置 SSH/Telnet 服务超时时间

1. 执行 **showautologout** 命令查看超时时间。

```
XSCF> showautologout  
30min
```

2. 执行 **setautologout** 命令以配置超时时间。
下面是设置超时时间为 255 分钟的示例。

```
XSCF> setautologout -s 255  
255min
```

设置的超时时间在下次登录时有效。

3.8 配置用于登录 XSCF 的 HTTPS 服务

本节介绍如何配置 HTTPS 服务。

为了使用 XSCF-LAN 连接的 XSCF Web 和使用 Web 浏览器窗口，对 HTTPS 服务设置进行配置。使用这里描述的设置来启用/禁用 HTTPS 和使用 HTTPS。这些系统中默认禁用 HTTPS。XSCF Web 控制台是一个安全控制台。

选择证书颁发机构

考虑客户的系统和 Web 浏览器环境，选择以下其中一个证书颁发机构：

- 外部证书颁发机构
- Intranet 中的证书颁发机构
- 自签名证书颁发机构

如果客户环境中既没有外部证书颁发机构也没有 Intranet 中的证书颁发机构，请使用

XSCF 自签名证书颁发机构。（请参见 "3.8.2 使用自签名证书颁发机构时的流程"。）
XSCF 的自签名证书颁发机构是 XSCF 配置的自签名证书颁发机构，不能用作其它系统的外部证书颁发机构。

自签名证书的有效期

自签名证书有如下固定的有效期：

- 服务器证书：10年

在 Web 服务器证书的有效期过期后，或 Web 服务器证书被更改时，请再次配置 HTTPS 服务设置。

可分辨名称 (DN)

如需创建 Web 服务器证书签名请求 (CSR)，指定以下可分辨名称 (DN)：

注 - 在 XSCF 自签名证书颁发机构中，用于 Web 服务器证书签名的自签名证书的密钥长度为 2048 位。密钥长度无法更改。

- 2 字母国家代码（如：US 或 JP）
- 地区
- 城市
- 组织（公司）名称、部门或科室名称
- 公用名（用户名、Web 服务器域名）
- 管理员电子邮件地址

除了国家代码，以上条目有多达64个字符。有关 DN 的详细信息，请参见 sethttps(8) 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

3.8.1 使用外部或 Intranet 中的证书颁发机构的流程

本节介绍使用外部证书颁发机构或 Intranet 中的证书颁发机构的设置流程。

1. 创建 **XSCF Web 服务器密钥**。
2. 在 **XSCF** 上创建 **Web 服务器证书签名请求 (CSR)**。
3. 请证书颁发机构给 **XSCF Web 服务器证书签名请求** 发布一个证书。
4. 将证书颁发机构签名的 **Web 服务器证书** 导入 **XSCF**。
5. 启用 **HTTPS**。

在上面步骤的 1 到 5，在 sethttps 命令中设置各自的选项。如果用 XSCF Web 进行设置，选择各自的设置项目。

在多个 XSCF 系统中，设置也自动应用到备用 XSCF。

3.8.2 使用自签名证书颁发机构时的流程

本节介绍使用自签名证书颁发机构时的设置流程。

如果既没有 Web 服务器密钥也没有自签名 Web 服务器证书，您可在 `sethttps` 命令中为自签名指定 "enable"，一次自动完成从步骤 1 到 4 的所有的设置。

如果有 Web 服务器密钥和自签名 Web 服务器证书时，执行下面的步骤 1 到 4。

1. 配置 **XSCF** 自签名证书颁发机构。
2. 生成 **XSCF Web** 服务器密钥。
3. 在 **XSCF** 上创建自签名 **Web** 服务器证书。
4. 启用 **HTTPS**。

在多个 XSCF 系统中，设置也自动应用到备用 XSCF。

3.8.3 检查与 HTTPS 有关的设置和命令

表 3-20 列出了与 HTTPS 有关的设置项目和对应的 XSCF shell 命令。

表 3-20 与 HTTPS 有关的设置项目

设置项目	必须或可选设置	相关命令
启用/禁用 HTTPS	可选	<code>sethttps(8)</code> , <code>showhttps(8)</code>
外部证书 - 在 XSCF 上创建 Web 服务器密钥 - 在 XSCF 上创建 Web 服务器 CSR 和请求颁发机构发行证书 - 将 Web 服务器证书导入 XSCF	可选	<code>sethttps(8)</code> , <code>showhttps(8)</code>
自签名证书 - 配置自签名证书颁发机构 - 创建 Web 服务器密钥 - 创建自签名 Web 服务器证书	可选	<code>sethttps(8)</code> , <code>showhttps(8)</code>

3.8.4 启用/禁用 HTTPS 服务

如需确认为 XSCF 网络设置的 HTTPS 服务器，请使用 `shownetwork` 命令。也可使用 `sethttps` 命令设置 HTTPS 服务。请使用具有 `platadm` 权限的用户账户执行 `sethttps` 命令。

1. 执行 `showhttps` 命令查看 **HTTPS** 服务设置。
下面是 HTTPS 服务设置的示例。

```
XSCF> showhttps
HTTPS status: enabled
Server key: installed in Apr 24 12:34:56 JST 2006
CA key: installed in Apr 24 12:00:34 JST 2006
CA cert: installed in Apr 24 12:00:34 JST 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIBwjCCASsCAQAwgYExCzAUBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTERMA8G
A1UEBxMIbG9jYWxpdkhkaFTATBgNVBAoTDG9yZ2FuaXphdGlvbjEPMA0GA1UECzMG
```

```
b3JnYW5pMQ8wDQYDVQQDEWZjb21tb24xZjAUBGkqhkiG9w0BCQEWB2VlLm1haWww
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5D57X/k42LcipTbWzV2GrxaVM
5GEyx3bdBW8/7WZhd3uiZ9+ANlvRAuw/Yy7I/pAD+NQJesBcBjuyj9x+IiJl9F
MrI5fR8pOIywV0dbMPCar09rrU45bVeZhTyi+uQOdWLoX/Dhq0fm2BpYuh9WukT5
pTEg+2dABg8UdHmNAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAuxljH3dyB6Xho
PgbuVIakDzIKEPipK9qQfC57YI43uRBGRubu0AHEcLVue5yTu6G5SxHTCq07tV5g
38UHSg5Kqy9QuWHWMri/hxm0kQ4gBpApjNb6F/B+ngBE3j/thGbEuvJb+0wbycvu
5jrhB/ZV9k8X/MbDOxSx/U5nF+Zuyw==
-----END CERTIFICATE REQUEST-----
```

2. 执行 `sethttps` 命令以配置 HTTPS。

下面示例启用 HTTPS 服务。

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

如果既没有 Web 服务器的密钥，也没有自签名的 Web 服务器证书，则指定 "enable" 的本命令自动配置自签名，生成 Web 服务器密钥，创建 Web 服务器证书，并允许 HTTPS 在同一时间完成此操作。

下面是禁用 HTTPS 服务的示例。

```
XSCF> sethttps -c disable
Continue? [y|n] : y
```

3.8.5 使用外部或 Intranet 中的证书颁发机构导入 Web 服务器证书

1. 执行 `sethttps` 命令生成 Web 服务器密钥。

以下是指定 `-c genserverkey` 生成 Web 服务器密钥的示例。

```
XSCF> sethttps -c genserverkey
Server key already exists. Do you still wish to update? [y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. 执行 `sethttps` 命令，指定 DN 以生成 CSR。

在以下的示例中，指定 `-c gencsr` 选项和 DN (JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com) 生成 CSR。

```
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example
development scfhost abc@example.com
```

3. 执行 `showhttps` 命令查看 CSR。将显示的 CSR (BEGIN 到 END) 复制并保存到一个文本文件。

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2006
CA key: installed in Jul 11 06:33:21 UTC 2006
CA cert: installed in Jul 11 06:33:21 UTC 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAoBgNVBAoTB0Z0VSk1UU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IImqKg==
-----END CERTIFICATE REQUEST-----
```

4. 将复制的 **CSR** 发送到证书颁发机构，请求它发布 **Web** 服务器证书。
5. 如需执行导入，执行 **sethttps** 命令并指定 **-c importca** 选项，复制步骤 4 中签名的 **Web** 服务器证书并粘贴在窗口中。
按 [Enter] 键进行导入，然后按 [Ctrl] 和 [D] 完成本步骤。

```
XSCF> sethttps -c importca
Please import a certificate:
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgTELMakGA1UEBhMCamox
:
R+OpXAVQvb2tjIn3k099dq+begECO4mwknW1t7QI7A1BkcW2/MkOolIRa6iP1Zwg
JoPmwAbrGyAvGUTdzUoyIH0j17dRQrVIRA==
-----END CERTIFICATE-----
<按 [Ctrl] 和 [D] >
```

6. 执行 **sethttps** 命令以启用 **HTTPS**。

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

7. 从客户端，使用指定的 **HTTPS** 访问 **XSCF Web**。确认屏幕的对话框上没有显示安全警告，并且证书正确无误。

3.8.6 配置自签名证书颁发机构并创建 Web 服务器证书

既没有 Web 服务器密钥也没有自签名 Web 服务器证书时

1. 执行 **sethttps** 命令并指定 **-c enable** 选项启动 **HTTP** 服务。

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

本命令自动配置自签名，生成 Web 服务器密钥，创建 Web 服务器证书和启用

HTTPS，一次完成本过程。

有 Web 服务器密钥和自签名 Web 服务器证书时

现有 Web 服务器密钥和证书将会覆盖。

1. 执行 **sethttps** 命令，指定 **DN** 以创建自签名 **Web** 服务器证书。
在以下的示例中，指定 **-c selfsign** 选项和 **DN** (**JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com**) 创建自签名 **Web** 服务器证书。

```
XSCF> sethttps -c selfsign JP Kanagawa Kawasaki Example
development scf-host abc@example.com
CA key and CA cert already exist. Do you still wish to update?
[y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. 执行 **showhttps** 命令并指定 **-t** 选项确认自签名 **Web** 服务器证书已创建。

```
XSCF> showhttps -t
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      cb:92:cc:ee:79:6c:d3:09
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=JP, ST=Kanagawa, O=Fujitsu, OU=Fujitsu, CN=XSCF
    Validity
      Not Before: May 24 07:15:17 2017 GMT
      Not After : May 22 07:15:17 2027 GMT
    Subject: C=JP, ST=Kanagawa, O=Fujitsu, OU=Fujitsu, CN=XSCF/
emailAddress=hoge@hoge
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:c7:5f:f1:61:ad:ba:4b:64:25:7e:49:ba:7a:6c:
        d4:5c:b1:8c:2d:15:9f:8a:2f:70:c8:cc:4a:3d:2c:
        bd:0a:b7:f8:1d:4a:12:93:ea:22:d5:be:85:69:d7:
        0b:31:a8:1a:ae:34:c6:f6:e8:a1:c8:cc:02:08:be:
        bc:2b:e9:34:8f:f2:ee:4a:93:26:a0:47:93:7e:b7:
        f8:3f:73:24:55:45:02:14:f7:c2:d8:56:f7:a1:cf:
        2f:2d:3e:d4:ff:05:1a:82:25:34:1f:f2:1a:83:91:
        a7:35:98:7d:2a:92:53:6b:19:75:91:86:b5:2e:ef:
        :
        :
```

3. 执行 **sethttps** 命令以启用 **HTTPS**。

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

在多个 XSCF 系统中，设置也自动应用到备用 XSCF。

3.9 配置 XSCF 网络

本节介绍如何配置系统的 XSCF 网络。

XSCF 网络设置包括 XSCF-LAN 和 SP 对 SP 通信协议 (SSCP) 等的 XSCF 网络接口设置、路由设置和与 DNS 相关的设置。

3.9.1 通过 XSCF 网络使用服务

连接到 XSCF 网络时，通过 XSCF shell 和 XSCF Web 界面可以使用各种服务器信息和服务。有关各服务器的详情，请参见以下各章节：

- 服务器操作、状态显示和配置更改（请参见 [第10章](#) 和 [第11章](#)。）
- NTP 服务（请参见 [3.6节](#)。）
- Telnet 服务（请参见 [3.7节](#)。）
- SSH 服务（请参见 [3.7节](#)。）
- HTTPS 服务（请参见 [3.8节](#)。）
- SMTP 服务（请参见 [10.2节](#)。）
- SNMP 服务（请参见 [10.3节](#)。）
- 远程维护服务（请参见《产品说明》。）
- LDAP 服务（请参见 [3.5.12节](#)。）
- Active Directory 服务（请参见 [3.5.13节](#)。）
- LDAP over SSL 服务（请参见 [3.5.14节](#)。）

3.9.2 了解 XSCF 网络接口

XSCF 以太网端口

每个 SPARC M12/M10 机箱和接线盒都有两个 XSCF 以太网端口。这些端口分别被命名为 XSCF-LAN#0 和 XSCF-LAN#1。

两个都使用 RJ-45 接口，支持 10Base-T/100Base-TX/1000Base-T。XSCF-LAN 端口是 LAN 连接端口，用于系统管理员使用 XSCF shell 或 XSCF Web 执行操作。操作包括查看服务器状态、操作域和查看控制台。

如需连接到 XSCF 网络，请指定以太网端口的 IP 地址。使用两个 LAN 路径，用户可以维护和管理服务器。

对于有多个 XSCF 的系统，从 XSCF 的 XSCF-LAN 端口不用于进行服务器维护/管理。仅当使用远程存储时，从 XSCF 的 XSCF-LAN 端口才连接到网络。有关远程存储器的详细信息，请参见 ["4.6 使用远程存储"](#)。

主 XSCF 和备用 XSCF 之间的接管 IP 地址

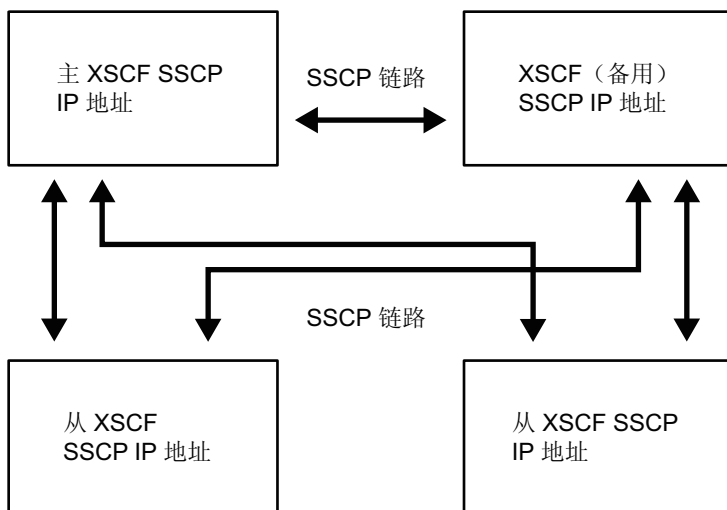
在配有多个 XSCF 的系统上，主 XSCF 和备用 XSCF 上的 XSCF-LAN#0 端口和 XSCF-LAN#1 端口可以分别分组，并可以为这些组设置一个接管 IP 地址（虚拟 IP 地址）。所以即使安装了主 XSCF 和备用 XSCF 的机柜被切换，用户也不需要关注主 XSCF 和备用 XSCF 的 IP 地址。继续使用接管 IP 地址，即使切换以后也能访问主 XSCF。

内部服务处理器通信协议 (SSCP)

在配有多个 XSCF 的系统上，配置了 XSCF 之间的网络。XSCF 之间的网络接口协议是指内部服务处理器通信协议 (SSCP) 或 SSCP 链路网络。通过其通讯路径，各 XSCF 相互连接，相互监控状态和交换系统信息。

图 3-3 显示了 4BB 配置（机箱直接互连）中使用 SPARC M12-2S 或 SPARC M10-4S 系统的 SSCP 链路网络。

图 3-3 SSCP 链路网络



配置 SSCP 链路时，使用各自的线缆将主 XSCF 连接到备用 XSCF，将主 XSCF 连接到各从 XSCF，将备用 XSCF 连接到各从 XSCF。在主 XSCF 和备用 XSCF 之间，XSCF DUAL 控制端口相互连接。将主 XSCF 或备用 XSCF 连接到各从 XSCF 的 SSCP 端口称为 XSCF BB 控制端口。各从 XSCF 之间不会相互连接。有关配置 SSCP 的线缆连接详情，请参见《Fujitsu SPARC M12-2S 安装指南》中的“第4章 设置模块化架构配置中的 SPARC M12-2S”或《Fujitsu M10-4S/SPARC M10-4S 安装指南》中的“第4章 配置模块化架构连接”。

SSCP IP 地址在出厂前已预先设置。如果您希望设置其他 IP 地址，需要在进行系统初始设置时即进行设置。有关 SSCP IP 地址的详细信息，请参见“3.9.5 了解使用 SSCP 设置的 IP 地址”。

3.9.3 XSCF 网络接口配置

本节介绍如下 XSCF 网络接口：

- 支持用户访问 XSCF (XSCF-LAN) 的系统控制网络
- XSCF 之间通信的链路网络 (SSCP) (在配有多个 XSCF 的系统上)

在仅由一个 SPARC M12/M10 组成的系统中，为了访问 XSCF，为 XSCF-LAN 设置了两个 IP 地址。XSCF-LAN 只能使用一个 LAN 端口。

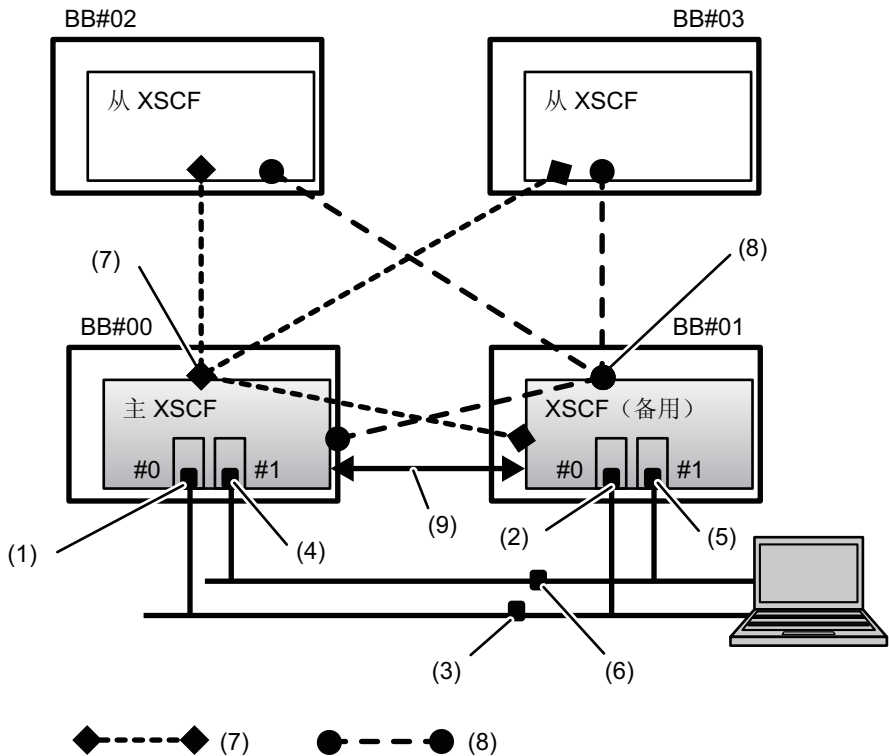
在由四个机箱组成的 SPARC M12-2S 系统或由直接连接的四个机箱组成的 SPARC M10-4S 系统的情况时，为 XSCF-LAN 设置四个 IP 地址，两个设置为接管 IP 地址，10 个为 SSCP 设置，共有 16 个 IP 地址。

在由 16 个机箱组成的 SPARC M12-2S 系统或由四个接线盒连接的 16 个机箱组成的 SPARC M10-4S 系统的情况时，为 XSCF-LAN 设置四个 IP 地址，两个设置为接管 IP 地址，44 个为 SSCP 设置，共有 50 个 IP 地址。

注 - 在多个 XSCF 系统中，在备用 XSCF 不能配置 XSCF。用于配置所有 XSCF 的命令只能在主 XSCF 执行。

图 3-4 显示了用于为 4BB 配置（机箱直接互连）中的 SPARC M12-2S 或 SPARC M10-4S 系统配置 XSCF 网络所必需的网络接口。

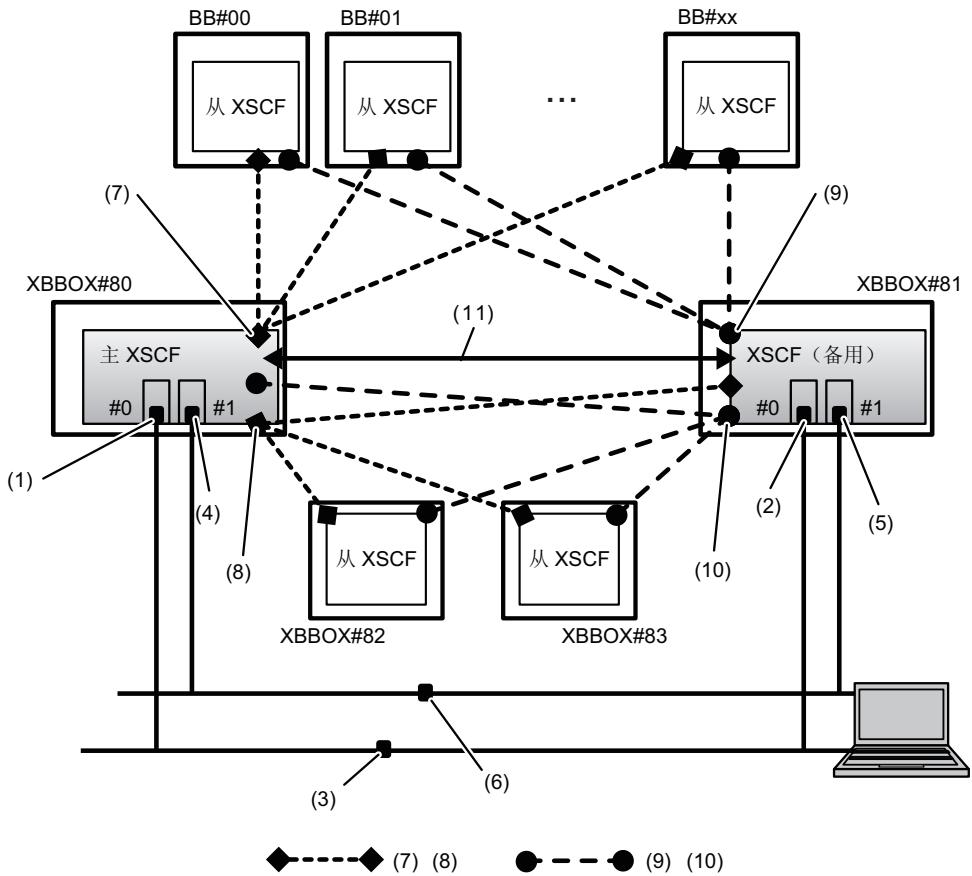
图 3-4 4BB 配置中的 XSCF 网络



编号	地址设置	编号	地址设置
1	XSCF-LAN#0 地址 (主 XSCF 侧)	6	内部-XSCF-LAN#1 接管 IP 地址
2	XSCF-LAN#0 地址 (备用 XSCF 侧)	7	SSCP 地址 (主 XSCF 和各 BB#xx 中的 XSCF) : 4 个地址
3	内部-XSCF-LAN#0 接管 IP 地址	8	SSCP 地址 (备用 XSCF 和各 BB#xx 中的 XSCF) : 4 个地址
4	XSCF-LAN#1 地址 (主 XSCF 侧)	9	用于复制的 SSCP 地址 (主 XSCF 和备用 XSCF) : 2 个地址
5	XSCF-LAN#1 地址 (备用 XSCF 侧)		

图 3-5 显示了用于为带有接线盒的 SPARC M12-2S 或 SPARC M10-4S 系统配置 XSCF 网络所必需的网络接口示例。

图 3-5 带有接线盒的系统配置中的 XSCF 网络



编号	地址设置	编号	地址设置
1	XSCF-LAN#0 地址（主 XSCF 侧）	7	SSCP 地址（主 XSCF 和各 BB#xx 中的 XSCF）：17 个地址
2	XSCF-LAN#0 地址（备用 XSCF 侧）	8	SSCP 地址（主 XSCF 和各 XBBOX#xx 中的 XSCF）：4 个地址
3	内部-XSCF-LAN#0 接管 IP 地址	9	SSCP 地址（备用 XSCF 和各 BB#xx 中的 XSCF）：17 个地址
4	XSCF-LAN#1 地址（主 XSCF 侧）	10	SSCP 地址（备用 XSCF 和各 XBBOX#xx 中的 XSCF）：4 个地址
5	XSCF-LAN#1 地址（备用 XSCF 侧）	11	用于复制的 SSCP 地址（主 XSCF 和备用 XSCF）：2 个地址
6	内部-XSCF-LAN#1 接管 IP 地址		

3.9.4 了解网络组子网

以下 XSCF 网络连接组中 IP 地址的网络地址必须设置为不同的地址：

- XSCF-LAN#0
- XSCF-LAN#1
- 主 XSCF 和各 BB 之间的 SSCP 链路
- 备用 XSCF 和各 BB 之间的 SSCP 链路
- 主 XSCF 和各 XBBOX XSCF 之间的 SSCP 链路
- 备用 XSCF 和各 XBBOX XSCF 之间的 SSCP 链路
- 主 XSCF 和备用 XSCF (DUAL) 之间的 SSCP 链路

在 4BB 配置（机箱直接互连）的 SPARC M12-2S 或 SPARC M10-4S 系统的情况时，需要三种类型的子网作为 SSCP 网络地址（SSCP 链路网络 ID 0-2）。图 3-4 中由编号 7、8 和 9 表示的 SSCP 链路必须配置不同的子网 IP 地址。

A 带接线盒的系统最多需要 5 种类型的子网。（各子网的 SSCP 链路网络 ID 从 0 到 4。）图 3-5 中由编号 7 至 11 表示的五种类型的 SSCP 链路必须配置不同的子网 IP 地址。

3.9.5 了解使用 SSCP 设置的 IP 地址

分类 SSCP 使用的 IP 地址，并设置在以下组中。这些组通过 SSCP 链路网络 ID 加以区别。每个 SSCP 端口至少需要设置两个 IP 地址。（请参见图 3-4 和图 3-5。）

- 主 XSCF 和各 BB 的 XSCF 构成的组 (图 3-4, No. 7, 图 3-5, No. 7)
- 备用 XSCF 和各 BB 的 XSCF 构成的组 (图 3-4, No. 8, 图 3-5, No. 9)
- 主 XSCF 和每个 XBBOX 的 XSCF 构成的组 (图 3-5, No. 8)
- 备用 XSCF 和每个 XBBOX 的 XSCF 构成的组 (图 3-5, No. 10)
- 主 XSCF 和备用 XSCF 构成的组 (图 3-4, No. 9, 图 3-5, No. 11)

具有一个 XSCF 的配置中的 SPARC M12-1/M12-2/M10-1/M10-4 系统无 SSCP 设置。

表 3-21 列出了为 4BB 配置（机箱直接互连）中的 SPARC M12-2S 或 SPARC M10-4S 设置的每个 SSCP IP 地址的位置、数量、ID 和默认 IP 地址值。执行 showsscp 命令检查当前设置的 IP 地址。

表 3-21 SSCP IP 地址（4BB 配置）

位置	数量	SSCP 链路 网络 ID	默认 IP 地址
<u>主 XSCF 和各 BB#xx 的 XSCF 之间的连接</u>	4	0	
BB#00（主）			169.254.1.1
BB#01			169.254.1.2
BB#02			169.254.1.3
BB#03			169.254.1.4
<u>备用 XSCF 和各 BB#xx 之间的连接</u>	4	1	
BB#00			169.254.1.9
BB#01（备用）			169.254.1.10
BB#02			169.254.1.11
BB#03			169.254.1.12
<u>主 XSCF 和备用 XSCF 之间的双重连接</u>	2	2	
BB#00（主）			169.254.1.17
BB#01（备用）			169.254.1.18
总数	10		

表 3-22 列出了为最大配置（16BB 和 4-XBBOX 配置）中的 SPARC M12-2S 或 SPARC M10-4S 设置的每个 SSCP IP 地址的位置、数量、ID 和默认 IP 地址值。

表 3-22 SSCP IP 地址（16-BB 和 4-XBBOX 配置）

位置	数量	SSCP 链路 网络 ID	默认 IP 地址
<u>主 XSCF 和各 BB#xx 的 XSCF 之间的连接</u>	17	0	
XBBOX#80（主）			169.254.1.1
从 BB#00 到 BB#15			169.254.1.2 到 169.254.1.17
<u>备用 XSCF 和各 BB#xx 的 XSCF 之间的连接</u>	17	1	
XBBOX#81（备用）			169.254.1.33
从 BB#00 到 BB#15			169.254.1.34 到 169.254.1.49
<u>主 XSCF 和各 XBBOX#xx 的 XSCF 之间的连接</u>	4	2	
XBBOX#80（主）			169.254.1.65
XBBOX#81			169.254.1.66
XBBOX#82			169.254.1.67
XBBOX#83			169.254.1.68
<u>备用 XSCF 和各 XBBOX#xx 的 XSCF 之间的连接</u>	4	3	
XBBOX#80			169.254.1.73
XBBOX#81（备用）			169.254.1.74
XBBOX#82			169.254.1.75
XBBOX#83			169.254.1.76
<u>主 XSCF 和备用 XSCF 之间的双重连接</u>	2	4	
XBBOX#80（主）			169.254.1.81
XBBOX#81（备用）			169.254.1.82
总数	44		

3.9.6 检查与 XSCF 网络相关的设置项目和命令

表 3-23 列出了与 XSCF 网络相关的设置项目以及对应的 XSCF shell 命令。

完成网络配置后，需要重新启动 XSCF。使用 `rebootxscf` 命令重新启动 XSCF。XSCF 重新启动会断开 XSCF 会话，因此再次登录 XSCF。

表 3-23 与 XSCF 网络相关的设置项目

设置项目	必须或可选设置	相关命令
XSCF 网络 IP 地址 - XSCF-LAN - 接管 IP 地址 - SSCP	必须	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
启用/禁用网络	可选	setnetwork(8), shownetwork(8)
网络掩码	必须	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
主机名/域名	可选	sethostname(8), showhostname(8)
添加/删除网络路由 - 目标 IP 地址 - 网关 - 网络掩码	必须	setroute(8), showroute(8)
添加/删除 DNS - 名称服务器 - 搜索路径	可选	setnameserver(8), shownameserver(8)
IP 数据包筛选规则	可选	setpacketfilters(8), showpacketfilters(8)
应用网络	必须	applynetwork(8)

3.9.7 配置 XSCF 网络的流程

本节介绍配置 XSCF 网络的步骤。以下各步骤中介绍了详细的方法。

1. 设置以太网 (XSCF-LAN) IP 地址 (物理 IP 地址)。

根据网络配置，可使用两个 XSCF-LAN 端口。

在配有一个 XSCF 的系统中，设置以下全部两个或其中一个 IP 地址：

- BB#00 的 XSCF-LAN#0 (主 XSCF)
- BB#00 的 XSCF-LAN#1 (主 XSCF)

在具有多个 XSCF 的系统中，首先设置主 XSCF 侧的各 XSCF-LAN IP 地址，然后设置备用 XSCF 的 XSCF-LAN IP 地址 (请参见 shownetwork(8)、setnetwork(8) 以及 3.9.8)。

为了在 XSCF 故障转移时能够连接到任意一个 XSCF，为 LAN 端口设置与各 XSCF 编号相同的网络地址。

必须为 XSCF-LAN#0 和 XSCF-LAN#1 的 IP 地址设置不同的网络地址。

2. 对于多个 XSCF 的系统，设置接管 IP 地址。(虚拟 IP 地址)。

在 XSCF 发生故障的情况下切换主和备用双方，接管 IP 地址的设置可以接管 IP 地址。用户始终可以通过访问接管 IP 地址连接到主 XSCF，不必考虑 XSCF 的切换。

在设置 XSCF-LAN#0 和 XSCF-LAN#1 的各自 IP 地址后，为 XSCF-LAN#0 和 XSCF-LAN#1 (它们为冗余配置) 的各自 LAN 端口设置一个接管 IP 地址 (请参见 shownetwork(8)、setnetwork(8) 和 3.9.9)。

3. 对于多个 **XSCF** 的系统，设置 **SSCP IP 地址**。
SSCP 用于多重 XSCF 之间通信的网络，因此需要设置 IP 地址。SSCP IP 地址的值在出厂时已预先设置（请参见 表 3-21 和 表 3-22）。
如果设置的 XSCF-LAN IP 地址与 SSCP 默认网络地址冲突，需要对 SSCP IP 地址进行重新设置。SSCP IP 地址在同一组时必须处于同一网络中，在组外时必须处于不同的网络。有关子网的详细信息，请参见 "3.9.4 了解网络组子网"。用户无法访问 SSCP 网络（请参见 showsscp(8)、setsscp(8) 和 3.9.10）。
4. 设置主机名、路由和 **DNS**。
在具有多个 XSCF 的系统中，首先在主 XSCF 侧设置主机名和路径，然后在备用 XSCF 侧对其进行设置（请参见 showhostname(8)、sethostname(8)、showroute(8)、setroute(8)、shownameserver(8)、setnameserver(8)、3.9.11、3.9.12 和 3.9.13）。
5. 设置 **IP 数据包筛选规则**。
为 XSCF-LAN 设置 IP 包筛选规则（请参见 showpacketfilters(8)、setpacketfilters(8) 和 3.9.14）。
有关将远程存储器连接到从 XSCF 的设置，请参见 "4.6.10 配置与远程存储一同使用的 XSCF-LAN"。
6. 应用网络设置。
若需完成网络配置，必须反映设置并重新启动 XSCF。XSCF 重新启动会断开 XSCF 会话，因此需再次登录（请参见 applynetwork(8)、rebootxscf(8) 和 3.9.15）。

注 - 如果在执行涉及所有 XSCF 的设置命令期间发生 XSCF 重新启动或故障转移，则可能无法成功完成配置。再次登录主 XSCF，并检查设置是否正确。如果不正确，请重新设置。

3.9.8 启用/禁用 XSCF 网络，并设置 XSCF-LAN IP 地址和网络掩码

如需确认为 XSCF 设置的网络接口信息，请使用 shownetwork 命令。如需配置网络接口，请在 XSCF 使用 setnetwork 命令。请使用具有 platadm 权限的用户账户执行 setnetwork 命令。

1. 执行 **shownetwork** 命令查看所有 **XSCF** 网络接口的信息。

```
XSCF> shownetwork -a
bb#00-lan#0
    Link encap:Ethernet HWaddr 00:00:00:12:34:56
    inet addr: 192.168.11.10 Bcast: 192.168.11.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
    TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:12241827 (11.3 MiB) TX bytes:1189769 (0.9 MiB)
    Base address:0x1000
lan#0   Link encap:Ethernet HWaddr 00:00:00:12:34:56
    inet addr:192.168.11.11 Bcast:192.168.11.255 Mask:255.255.255.0
```

```
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Base address:0xe000
bb#00-lan#1
:
```

2. 查看 **XSCF-LAN#0** 或 **XSCF-LAN#1** 信息。

以下是查看 BB#00（主 XSCF）的 XSCF-LAN#1 网络接口信息的示例。

```
XSCF> shownetwork bb#00-lan#1
bb#00-lan#1
Link encap:Ethernet HWaddr 00:00:00:12:34:57
inet addr:192.168.10.10 Bcast: 192.168.10.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20241827 (19.3 MiB) TX bytes:2089769 (1.9 MiB)
Base address:0x1000
```

3. 执行 **setnetwork** 命令，指定网络接口信息。

下面是将 IP 地址 192.168.1.10 和网络掩码 255.255.255.0 设置给 BB#00 的 XSCF-LAN#0，并启用 XSCF-LAN 的示例。

```
XSCF> setnetwork bb#00-lan#0 -m 255.255.255.0 192.168.1.10
```

下面是禁用 BB#00 的 XSCF-LAN#1 的示例。

```
XSCF> setnetwork bb#00-lan#1 -c down
```

下面是删除已设置的 BB#00 的 XSCF-LAN#1 的 IP 地址和网络掩码的示例。

```
XSCF> setnetwork -r bb#00-lan#1
You specified '-r' interface remove option.
So, we delete routing information that interface corresponds.
Continue? [y/n] :y
If you choose 'y'es, you must execute 'applynetwork' command for application.
Or you choose 'y'es, but you don't want to apply, you execute 'rebootxscf' for
reboot.
```

4. 执行 **applynetwork** 和 **rebootxscf** 命令，应用 XSCF 网络接口设置。

注 - 您可通过执行 **applynetwork** 和 **rebootxscf** 命令，应用接管 IP 地址、SSCP IP 地址、XSCF 主机名、XSCF 域名、XSCF 路由、XSCF 的 DNS 和其他所做的设置。

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname :hostname-0
```



```
bb#01 hostname      :hostname-1
DNS domain name    :example.com
nameserver         :10.23.4.3

interface          :bb#00-lan#0
status             :up
IP address         :10.24.144.214
netmask           :255.255.255.0
route              : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(略)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

XSCF 重新启动会断开 XSCF 会话，因此再次登录。

5. 执行 **shownetwork** 命令并确认 **XSCF** 网络接口信息。

3.9.9 设置接管 IP 地址

如需为主 XSCF 和备用 XSCF 设置接管 IP 地址（虚拟 IP 地址），请使用 **setnetwork** 命令。

1. 执行 **shownetwork** 命令查看所有 **XSCF** 网络接口的信息。

```
XSCF> shownetwork -a
```

2. 查看 **XSCF-LAN#0** 或 **XSCF-LAN#1** 接管 IP 地址的信息。
以下是查看 XSCF-LAN#0 接管 IP 地址信息的示例。

```
XSCF> shownetwork lan#0
lan#0 Link encap:Ethernet HWaddr 00:00:00:12:34:56
inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Base address:0xe000
```

3. 设置 **XSCF-LAN#0** 或 **XSCF-LAN#1** 的接管 IP 地址。
以下是为 XSCF-LAN#0 设置接管 IP 地址 192.168.11.10 和网络掩码 255.255.255.0 的示例。

```
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.11.10
```

4. 执行 **applynetwork** 和 **rebootxscf** 命令，应用 **XSCF** 网络接口设置。

注 - 您可通过执行 **applynetwork** 和 **rebootxscf** 命令，应用 SSCP IP 地址、XSCF 主机名、XSCF 域名、XSCF 路由、XSCF 的 DNS 和其他所做的设置。

```

XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname      :hostname-0
  bb#01 hostname      :hostname-1
  DNS domain name     :example.com
  nameserver          :10.23.4.3

  interface           :bb#00-lan#0
  status              :up
  IP address          :10.24.144.214
  netmask             :255.255.255.0
  route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(略)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y

```

XSCF 重新启动会断开 XSCF 会话，因此再次登录。

5. 执行 **shownetwork** 命令并确认 **XSCF** 网络接口信息。

3.9.10 设置 SSCP 的 IP 地址

如需确认分配给服务处理器间通信协议 (SSCP) 的 IP 地址，请使用 **showsscp** 命令。
setsscp 命令用于设置 SSCP IP 地址。请使用具有 **platadm** 或 **fieldeng** 权限的用户帐户
 执行 **setsscp** 命令。

1. 执行 **shownetwork** 命令查看所有 **XSCF** 网络接口的信息。

```

XSCF> shownetwork -a

```

2. 执行 **showsscp** 命令以显示 **SSCP** 地址信息。
 以下是查看 4BB 配置中的机柜直接互联的 SPARC M10-4S 系统上所有 SSCP 地址
 信息的示例。

```

XSCF> showsscp -a
SSCP network ID:0 address 169.254.1.0
SSCP network ID:0 netmask 255.255.255.248
Location Address
-----
bb#00-if#0 169.254.1.1
bb#01-if#0 169.254.1.2
bb#02-if#0 169.254.1.3
bb#03-if#0 169.254.1.4
SSCP network ID:1 address 169.254.1.8
SSCP network ID:1 netmask 255.255.255.248
Location Address
-----
bb#00-if#1 169.254.1.9
bb#01-if#1 169.254.1.10
bb#02-if#1 169.254.1.11

```

```

bb#03-if#1 169.254.1.12
SSCP network ID:2 address 169.254.1.16
SSCP network ID:2 netmask 255.255.255.252
Location Address
-----
bb#00-if#2 169.254.1.17
bb#01-if#2 169.254.1.18

```

以下是查看主 XSCF 的 BB#00 中的 SSCP 网络 ID 0 的设置信息的示例。

```

XSCF> showsscp -b 0 -N 0
SSCP network ID:0 address 169.254.1.0
SSCP network ID:0 netmask 255.255.255.248

Location Address
-----
bb#00-if#0 169.254.1.1

```

以下是查看备用 XSCF 侧的 SSCP 设置信息的示例。

```

XSCF> showsscp -b 1 -N 1
SSCP network ID:1 address 169.254.1.8
SSCP network ID:1 netmask 255.255.255.248

Location Address
-----
bb#01-if#1 169.254.1.10

```

以下是查看主 XSCF 和备用 XSCF 双重 SSCP 链路设置信息的示例。

```

XSCF> showsscp -N 2
SSCP network ID:2 address 169.254.1.16
SSCP network ID:2 netmask 255.255.255.252

Location Address
-----
bb#00-if#2 169.254.1.17
bb#01-if#2 169.254.1.18

```

3. 设置 SSCP 的 IP 地址（需要设置时）。
SSCP 网络中使用的 IP 地址是默认设置。但是，当 XSCF-LAN 的 IP 地址和 SSCP 默认 IP 地址的网络地址相同时，使用 `setsscp` 命令更改 SSCP 的 IP 地址。以下示例在交互模式下，设置 4BB 配置（其机柜直接相互连接）中 SPARC M12-2S 或 SPARC M10-4S 系统 SSCP 链路网络的 SSCP 地址和子网掩码。

```

XSCF> setsscp
How many BB[4] > 4
SSCP network ID:0 address [169.254.1.0 ] > 10.1.1.0
SSCP network ID:0 netmask [255.255.255.248] > 255.255.255.0
bb#00-if#0 address [10.1.1.1 ] >

```

```

bb#01-if#0 address [10.1.1.2 ] >
bb#02-if#0 address [10.1.1.3 ] >
bb#03-if#0 address [10.1.1.4 ] >

SSCP network ID:1 address [169.254.1.8 ] > 10.2.1.0
SSCP network ID:1 netmask [255.255.255.248] > 255.255.255.0
bb#00-if#1 address [10.2.1.1 ] >
bb#01-if#1 address [10.2.1.2 ] >
bb#02-if#1 address [10.2.1.3 ] >
bb#03-if#1 address [10.2.1.4 ] >

SSCP network ID:2 address [169.254.1.16 ] >
SSCP network ID:2 netmask [255.255.255.252] >
bb#00-if#2 address [169.254.1.17 ] >
bb#01-if#2 address [169.254.1.18 ] >

```

4. 执行 **applynetwork** 和 **rebootxscf** 命令，应用 IP 地址和网络掩码的设置。

注 - 您可通过执行 **applynetwork** 和 **rebootxscf** 命令，应用 XSCF 主机名、XSCF 域名、XSCF 路由、XSCF 的 DNS 和其他所做的设置。

```

XSCF> applynetwork
The following network settings will be applied:
  bb#00 hostname      :hostname-0
  bb#01 hostname      :hostname-1
  DNS domain name     :example.com
  nameserver          :10.23.4.3

  interface           :bb#00-lan#0
  status              :up
  IP address          :10.24.144.214
  netmask             :255.255.255.0
  route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(略)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y

```

XSCF 重新启动会断开 XSCF 会话，因此再次登录。

5. 执行 **showsscp** 命令并确认 **SSCP** 地址信息。

3.9.11 设置 XSCF 主机名和域名

如需确认为主 XSCF 和备用 XSCF 机柜设置的主机名，请使用 **showhostname** 命令。
如需设置为主 XSCF 和备用 XSCF 机柜设置的主机名和域名，请使用 **sethostname** 命令。
请使用具有 **platadm** 权限的用户账户执行 **sethostname** 命令。

1. 执行 **showhostname** 命令以显示主机名。

```
XSCF> showhostname -a
bb#00: scf-hostname0.example.com
bb#01: scf-hostname1.example.com
```

2. 执行 **sethostname** 命令以设置主机名。
下面是将主机名 scf0-hostname 设置给 BB#00 的示例。

```
XSCF> sethostname bb#00 scf0-hostname
```

以下示例将域名 company.com 设置给主 XSCF 和备用 XSCF。

```
XSCF> sethostname -d example.com
```

3. 执行 **sethostname** 命令，并执行 **applynetwork** 和 **rebootxscf** 命令以应用所设置的主机名和域名。

注 - 您可通过执行 **applynetwork** 和 **rebootxscf** 命令，应用 XSCF 路由、XSCF 的 DNS 和其他所做的设置。

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver          :10.23.4.3

interface           :bb#00-lan#0
status              :up
IP address          :10.24.144.214
netmask             :255.255.255.0
route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(略)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

XSCF 重新启动会断开 XSCF 会话，因此再次登录。

4. 执行 **showhostname** 命令并确认主机名和域名。

3.9.12 设置 XSCF 路由

本节介绍在多个 XSCF 系统中以子网为单位的路由数据示例。

- 配置了一个默认网关时

BB#00 的 XSCF		BB#01 的 XSCF
bb#00-lan#0 [192.168.11.10]	+-----+	bb#01-lan#0 [192.168.11.20]
bb#00-lan#1 [10.12.108.10]	+-----+	bb#01-lan#1 [10.12.108.20]

目标	网关	网络掩码	接口
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[默认]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[默认]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

注 - 在 XSCF 的各接口决定如何进行路由，随着安装位置的网络环境而变化。网络环境必须被配置为适应系统运行。

注 - 不能为接管 IP 地址设置路由。

■ 配置了两个默认网关时

BB#00 的 XSCF		BB#01 的 XSCF
bb#00-lan#0 [192.168.11.10]	+-----+	bb#01-lan#0 [192.168.11.20]
bb#00-lan#1 [10.12.108.10]	+-----+	bb#01-lan#1 [10.12.108.20]

目标	网关	网络掩码	接口
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[默认]	[192.168.11.1]	[0.0.0.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[默认]	[192.168.11.1]	[0.0.0.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[默认]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[默认]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

注 - 如果配置了两个默认网关，会自动选择其中一个网关。在该配置中，必须配置使两个默认网关都能正常运行的网络。

使用 `showroute` 命令检查 XSCF 网络的路由信息。此外，使用 `setroute` 命令设置路由信息。请使用具有 `platadm` 权限的用户帐户执行 `setroute` 命令。

操作步骤

1. 执行 `showroute` 命令以显示路由环境。

```
XSCF> showroute -a
Destination Gateway Netmask Flags Interface
192.168.11.0 * 255.255.255.0 U bb#00-lan#0
10.12.108.0 * 255.255.255.0 U bb#00-lan#1
default 10.12.108.1 0.0.0.0 UG bb#00-lan#1

Destination Gateway Netmask Interface
192.168.11.0 * 255.255.255.0 bb#01-lan#0
10.12.108.0 * 255.255.255.0 bb#01-lan#1
default 10.12.108.1 0.0.0.0 bb#01-lan#1
```

2. 执行 `setroute` 命令，指定网络接口路由环境。

以下是为 BB#00 的 XSCF-LAN#0 添加目标是 192.168.11.0，网络掩码是 255.255.255.0 的路由的示例。

```
XSCF> setroute -c add -n 192.168.11.0 -m 255.255.255.0 bb#00-lan#0
```

以下是为 BB#00 的 XSCF-LAN#1 添加默认网关是 10.12.108.1 的路由的示例。

```
XSCF> setroute -c add -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

下面是删除 BB#00 的 XSCF-LAN#0 目标是 192.168.11.0 的路由的示例。

```
XSCF> setroute -c del -n 192.168.11.0 bb#00-lan#0
```

以下是为 BB#00 的 XSCF-LAN#0 删除目标是 192.168.1.0，网络掩码是 255.255.255.0 的路由的示例。

```
XSCF> setroute -c del -n 192.168.1.0 -m 255.255.255.0 bb#00-lan#0
```

以下是为 BB#00 的 XSCF-LAN#1 删除默认网关是 10.12.108.1 的路由的示例。

```
XSCF> setroute -c del -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

3. 执行 `applynetwork` 和 `rebootxscf` 命令以应用使用 `setroute` 命令所做的设置。

注 - 您可以通过执行 `applynetwork` 和 `rebootxscf` 命令，应用 XSCF 的 DNS 和其他所做的设置。

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface           :bb#00-lan#0
status              :up
IP address           :10.24.144.214
netmask              :255.255.255.0
route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(略)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

XSCF 重新启动会断开 XSCF 会话，因此再次登录。

4. 执行 `showroute` 命令并确认路由设置。

3.9.13 设置 XSCF 的 DNS

使用 `shownameserver` 命令确认用于 XSCF 网络的名称服务器和搜索路径。也可使用 `setnameserver` 命令设置名称服务器和搜索路径。请使用具有 `platadm` 权限的用户账户执行 `setnameserver` 命令。

指定搜索路径时，您必须设置名称服务器。

1. 执行 `shownameserver` 命令查看名称服务器和搜索路径。

如果注册了多个名称服务器和搜索路径，在不同的行显示各自的信息。

下面是注册有三个名称服务器和一个搜索路径的示例。

```
XSCF> shownameserver
nameserver  10.0.0.2
nameserver  172.16.0.2
nameserver  192.168.0.2
search      sub.example.com
```

下面是没有名称服务器和没有搜索路径的示例。

```
XSCF> shownameserver
nameserver  ---
search      ---
```

2. 执行 `setnameserver` 命令，指定名称服务器和搜索路径。

以下是添加如下 3 个 IP 地址作为名称服务器的示例：10.0.0.2、172.16.0.2 和 192.168.0.2。


```
XSCF> setnameserver 10.0.0.2 172.16.0.2 192.168.0.2
```

以下是删除所有已设置名称服务器的示例。

```
XSCF> setnameserver -c del -a
```

以下是删除已注册 DNS 服务器的 3 次重复登录中的 2 次的示例。

```
XSCF> shownameserver  
nameserver 10.24.1.2  
nameserver 10.24.1.2  
nameserver 10.24.1.2  
XSCF> setnameserver -c del 10.24.1.2 10.24.1.2  
XSCF> shownameserver  
nameserver 10.24.1.2
```

下面是将一个域名 sub.example.com 添加为搜索路径的示例。

```
XSCF> setnameserver -c addsearch sub.example.com
```

以下是删除所有已设置搜索路径的示例。

```
XSCF> setnameserver -c delsearch -a
```

3. 执行 **applynetwork** 和 **rebootxscf** 命令以应用使用 **setnameserver** 命令配置的名称服务器和搜索路径设置。

```
XSCF> applynetwork  
The following network settings will be applied:  
bb#00 hostname      :hostname-0  
bb#01 hostname      :hostname-1  
DNS domain name     :example.com  
nameserver           :10.23.4.3  
  
interface           :bb#00-lan#0  
status              :up  
IP address          :10.24.144.214  
netmask             :255.255.255.0  
route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1  
(略)  
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y/n] :y
```

XSCF 重新启动会断开 XSCF 会话，因此再次登录。

4. 执行 **showroute** 命令并确认路由设置。

3.9.14 给 XSCF 网络设置 IP 数据包筛选规则

如需确认为 XSCF 网络设置的 IP 数据包筛选规则，请使用 `showpacketfilters` 命令。也可使用 `setpacketfilters` 命令设置 IP 数据包筛选规则。请使用具有 `platadm` 或 `fieldeng` 权限的用户账户执行 `setpacketfilters` 命令。您只能为输入数据包设置 XSCF 网络 IP 筛选规则。不能在输出数据包设置以上的规则。

1. 执行 `showpacketfilters` 命令查看 XSCF-LAN 的 IP 数据包筛选规则。
以下是给 XSCF 网络设置 IP 数据包筛选规则的示例。

```
XSCF> showpacketfilters -a
-i bb#00-lan#0 -j ACCEPT
-i bb#01-lan#1 -j ACCEPT
-s 173.16.0.0/255.255.0.0 -j ACCEPT
-s 205.168.148.100/255.255.255.255 -j ACCEPT
```

以下是应用 IP 数据包筛选规则的示例。

```
XSCF> showpacketfilters -l
pkts  bytes target      prot  in          source
124   102K ACCEPT  all    bb#00-lan#0 0.0.0.0/0.0.0.0
0     0  ACCEPT  all    bb#00-lan#1 0.0.0.0/0.0.0.0
0     0  ACCEPT  all    *           173.16.0.0/255.255.0.0
0     0  ACCEPT  all    *           205.168.148.100
```

以下是没有设置 IP 数据包筛选规则的示例。

```
XSCF> showpacketfilters -a
XSCF>
```

2. 执行 `setpacketfilters` 命令设置 IP 数据包筛选规则。
IP 数据包筛选规则的优先级取决于它们配置的时间先后顺序。
以下是允许数据包通过 IP 地址 192.168.100.0/255.255.255.0 的示例。

```
XSCF> setpacketfilters -y -c add -i bb#00-lan#0 -s
192.168.100.0/255.255.255.0 -j ACCEPT
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

以下是允许数据包通过 BB#00 的 XSCF-LAN#0 中的 IP 地址 192.168.100.0/255.255.255.0 的示例。

```
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
XSCF>
XSCF> setpacketfilters -y -c add -i bb#00-lan#0 -j DROP
```

```
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
-i bb#00-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
-i bb#00-lan#0 -j DROP
```

以下是删除从 10.10.10.10 断开通信设置的示例。

```
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
-s 10.10.10.10 -j DROP
XSCF>
XSCF> setpacketfilters -y -c del -s 10.10.10.10 -j DROP
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
```

以下是清除所有已设置的 IP 数据包筛选规则的示例。

```
XSCF> setpacketfilters -c clear
(none)
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

3.9.15 应用 XSCF 网络设置

使用 `setnetwork`、`setsscp`、`sethostname`、`setroute` 和 `setnameserver` 命令完成设置后，应用网络设置。

1. 执行 **applynetwork** 命令。
显示网络设置，确认应用。

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface            :bb#00-lan#0
status               :up
IP address           :10.24.144.214
netmask              :255.255.255.0
```

```

route                : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1

interface            :bb#00-lan#1
status               :down
IP address           :
netmask              :
route                :

interface            :bb#01-lan#0
status               :up
IP address           :10.24.144.215
netmask              :255.255.255.0
route                : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1

interface            :bb#01-lan#1
status               :down
IP address           :
netmask              :
route                :

interface            :lan#0
status               :down
IP address           :
netmask              :

interface            :lan#1
status               :down
IP address           :
netmask              :

SSCP network ID:0 netmask :255.255.255.248

interface            :bb#00-if#0
IP address           :192.168.1.1

interface            :bb#01-if#0
IP address           :192.168.1.2

interface            :bb#02-if#0
IP address           :192.168.1.3

interface            :bb#03-if#0
IP address           :192.168.1.4

SSCP network ID:1 netmask :255.255.255.248

interface            :bb#00-if#1
IP address           :192.168.1.10

interface            :bb#01-if#1
IP address           :192.168.1.9

interface            :bb#02-if#1
IP address           :192.168.1.11

```

```
interface                :bb#03-if#1
IP address                :192.168.1.12

SSCP network ID:2 netmask :255.255.255.252

interface                :bb#00-if#2
IP address                :192.168.1.17

interface                :bb#01-if#2
IP address                :192.168.1.18

Continue? [y|n] : y
```

2. 执行 **rebootxscf** 命令以重新启动 **XSCF** 和完成设置。

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

此时，会话被断开。在新界面重新连接，重新登录。

3. 执行 **shownetwork**、**showsscp**、**showhostname**、**showroute** 和 **shownameserver** 命令查看网络设置，并确认新的网络信息。
4. 执行 **nslookup** 命令并确认主机名称信息。
下面是主机名 **scf0-hostname** 信息的示例。

```
XSCF> nslookup scf0-hostname
Server: server.example.com
Address: 192.168.1.3

Name: scf0-hostname.example.com
Address: 192.168.10.10
```

3.9.16 检查 XSCF 网络连接状态

如需检查网络设备的响应，请使用 **ping** 命令。也可使用 **traceroute** 命令确认网络路由。

1. 执行 **shownetwork** 命令以查看网络连接状态。

```
XSCF> shownetwork -i
Active Internet connections (without servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 xx.xx.xx.xx:telnet xxxx:1617 ESTABLISHED
```

2. 执行 **ping** 命令以检查网络设备的响应。
下面是向主机名 **scf0-hostname** 三次发送一个数据包的示例。

```
XSCF> ping -c 3 scf0-hostname
PING scf0-hostname (XX.XX.XX.XX): 56 data bytes
64 bytes from XX.XX.XX.XX: icmp_seq=0 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=64 time=0.1 ms

--- scf0-hostname ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

3. 执行 **tracert** 命令以检查到网络设备的网络路径。
以下是到名为 `server.example.com` 的主机的网络路径的示例。

```
XSCF> traceroute server.example.com
traceroute to server.example.com (XX.XX.XX.XX), 30 hops max, 40
byte packets
 1 XX.XX.XX.1 (XX.XX.XX.1) 1.792 ms 1.673 ms 1.549 ms
 2 XX.XX.XX.2 (XX.XX.XX.2) 2.235 ms 2.249 ms 2.367 ms
 3 XX.XX.XX.3 (XX.XX.XX.3) 2.199 ms 2.228 ms 2.361 ms
 4 XX.XX.XX.4 (XX.XX.XX.4) 2.516 ms 2.229 ms 2.357 ms
 5 XX.XX.XX.5 (XX.XX.XX.5) 2.546 ms 2.347 ms 2.272 ms
 6 server.example.com (XX.XX.XX.XX) 2.172 ms 2.313 ms 2.36 ms
```

3.10 配置审核以强化 XSCF 安全

本节介绍为了使用审核如何配置 XSCF。

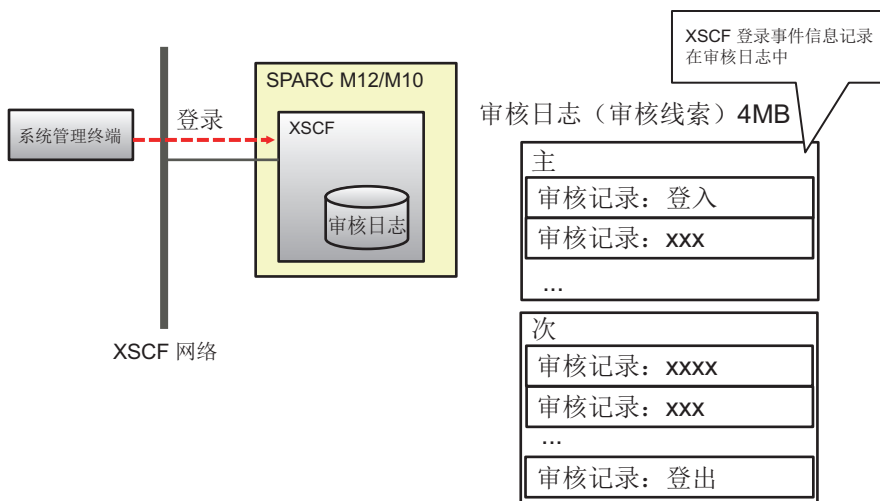
审核设置用于审核用户的网络操作并保存详细的访问记录，访问记录记录了谁在何时登录到 XSCF，并执行了哪些操作。在本系统中审核设置默认启用。审核设置主要设置审核是启用还是禁用，以及如何管理审核策略和审核日志（审核线索）。

3.10.1 审核

SPARC M12/M10 系统可以记录可能与安全性相关的所有 XSCF 事件，如用户登录和注销、用户权限的更改以及包括系统启动和停止的所有操作。审核配置完成后，审核开始，单一事件的信息、发生原因、发生日期以及其他相关信息记录为审核记录。系统有一个审核日志（审核线索），它是审核记录的集合。系统管理员可以参考审核日志，检查是否有可疑或不正常的操作，或确定做了特定事件的人员。

图 3-6 对登录事件信息如何记录到审核日志中进行了简要介绍。

图 3-6 记录到审核日志



3.10.2 了解审核术语

表 3-24 列出了与 XSCF 审核设置相关的术语。

表 3-24 与审核有关的术语

术语	说明
审核	审核是一种审核系统访问的功能。也称审核。
审核事件	审核事件是与安全有关的可被审核的系统行为。 通过数值或名称可以指定多个审核事件。 (如: AEV_LOGIN_SSH、LOGIN_SSH、0 和全部)
审核类别	审核类别是相关审核事件的分组。 (如: 登录审核类别的审核事件: SSH 登录、Telnet 登录、HTTPS 登录和注销) 可以指定多个审核类别。 (如: CS_AUDIT、AUDIT、2 和全部)
审核记录	一条审核记录是识别一个审核事件的信息。它包括事件信息、事件时间和其它相关信息。 审核记录存储在审核文件中。
审核日志	审核日志是存储多个审核记录的日志文件。 审核日志有两个区: 主要和次要。
审核线索	审核线索也被称为审核日志。 用户使用 <code>viewaudit</code> 命令来分析审核日志中各审核记录的内容。
审核策略	审核策略可设置通过指定审核事件、审核类别或用户而产生的各种类型的审核记录。 也可指定其他设置, 如审核日志达到满容量时所使用的电子邮件通知的设置。

表 3-24 与审核有关的术语 (续)

术语	说明
审核标记	审核标记是审核记录的一个字段。审核标记含有审核事件属性的描述，例如用户或权限。

3.10.3 管理审核

执行审核之前，系统管理员可确定用于审核的审核类别、审核事件或用户。系统管理员也可确定以哪一级审核日志使用级别来产生警告，以及容量已满时采取什么操作。将这些确定称为审核策略，审核之前在 XSCF 上进行配置。系统管理员可根据审核策略查看所收集的审核日志中的各审核记录，确认审核信息是否存在任何异常或可疑的访问。

下面详述用于审核的审核事件、审核策略、审核记录以及审核日志。

审核事件

审核事件是与安全有关的可被审核的系统操作。审核事件说明如下。

- XSCF 配置变更，如 IP 地址变更
- 物理分区相关的设置变更、操作和状态显示
- 任何验证的使用
- 用户安全属性的变更，如密码和用户权限等
- 审核记录信息的读取（包括失败的尝试）
- 审核策略变更
- 超过审核日志容量阈值时需要发送的电子邮件的目的地的变更
- 系统管理员对审核日志的变更。
- 时间变更

审核策略

审核策略确定如何执行审核功能。可以配置以下审核功能：

- 是否启用/禁用审核功能
- 需要进行审核的事件类型
- 事件审核员
- 超过审核日志容量阈值时产生警告的审核日志容量阈值和需要发送的电子邮件的目的地
- 当审核日志达到满容量时执行的操作（使用此设置的默认值。）

注 - 如果需要使用电子邮件报告超出了审核日志容量阈值，需使用 `setsmtp` 命令配置 SMTP 服务器。

审核记录和审核日志

审核记录都保存在 XSCF4 中的 4-MB 审核日志中。审核日志以二进制格式保存，但可以 XML 格式导出。

审核日志有两个区：主要和次要。当这些区域已满，并且又生成了一个新审核记录时，该记录将不被保存，而是被放弃（丢弃）。

为了防止新审核记录被丢弃，系统管理员将在审核日志达到满容量之前，删除次要区域的数据。删除次要区域数据后，主要区域变为新的次要区域，并创建新的主要区域。当产生一个新的审核记录时，该记录将被写入新的主要区域。

注 - "count"（默认）被设置为当审核日志达到满容量时执行的操作。使用此设置，当审核日志达到满容量时，新的审核记录会被放弃（丢弃），所丢弃记录的数量被统计（丢弃统计）。

注 - 如果指定 "suspend"，可能会发生由于错误而导致的降级或 XSCF 可能重新启动。指定为默认的 "count"，作为写入审核日志的策略。也需要注意：在 XCP 2250 和更高版本中，指定为 "suspend" 会导致与指定为 "count" 时的动作相同。

使用审核策略来设置文件容量的阈值（例如 50%、75% 或 80%），以便在审核日志达到满容量之前出现警告。出现此警告后，系统管理员可手动存档审核日志并删除审核记录，以保证足够的新存储空间。或者，他/她可禁用审核功能。删除两个审核日志区域的较旧文件。如果连续执行两次此删除操作，审核日志的所有数据都将被删除。

注 - 对于具有多个 SPARC M12-2S/M10-4S 系统的配置中的 XSCF 审核，需要查阅主和备用 XSCF 上的审核日志。有关详情，请参见 "3.10.10 管理备用 XSCF 的审核日志"。

3.10.4 检查与审核有关的设置项目和命令

表 3-25 列出了与审核有关的设置项目和对应的 XSCF shell 命令。

表 3-25 与审核有关的设置项目

设置项目	必须或可选设置	相关命令
启用/禁用审核	可选	setaudit(8), showaudit(8)
存档审核日志 (*1)、删除数据	可选	setaudit(8), showaudit(8)
审核策略	可选	setaudit(8), showaudit(8)
- 指定针对指定的用户启用/禁用，或指定应用全局策略		setsmtmp(8), showsmtmp(8)
- 启用/禁用审核类别		
- 启用/禁用审核事件		
- 启用/禁用针对所有用户的审核（全局策略）		
- 审核日志量的警告阈值 (%)		
- 审核日志量达到阈值时使用的目标电子邮件地址		
- 当审核日志达到满容量时挂起写入/丢弃数据 (*2)		

表 3-25 与审核有关的设置项目 (续)

设置项目	必须或可选设置	相关命令
显示审核日志	可选	viewaudit(8)
<ul style="list-style-type: none"> - 在指定时间之后的记录 - 在指定时间之前的记录 - 在指定时间范围内的记录 - 在特定日期的记录（本地时间特定日期 24 小时） - 审核类别 - 审核事件 - 审核会话 ID - 用户权限 - 返回值（成功、失败或无） - 用户（名称或数字 UID 值） 		
<p>按照如下所述指定格式显示审核线索：</p> <ul style="list-style-type: none"> - 一行接一行输出数据 - 指定分隔符（默认：逗号） - 抑制从 UID 到用户名的转换和从 IP 地址到主机名的转换 - 以 XML 格式输出数据 		

*1 当前不支持审核日志存档。

*2 当审核日志达到满容量时，目前仅支持丢弃审核记录的默认审核策略“count”。请勿指定“suspend”。

3.10.5 审核流程

图 3-7 显示了配置审核设置和显示审核日志的流程。

图 3-7 审核设置和日志显示流程

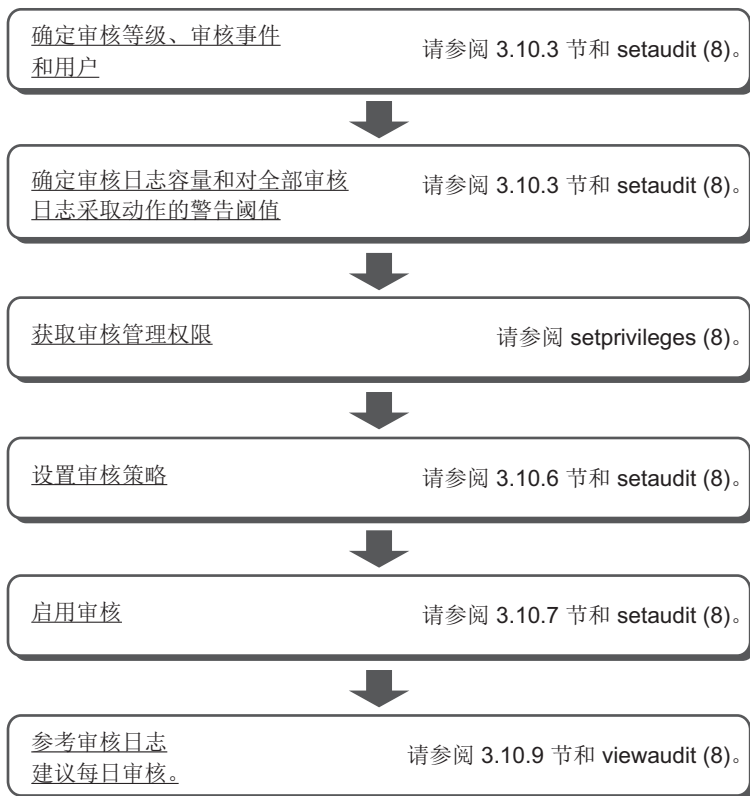
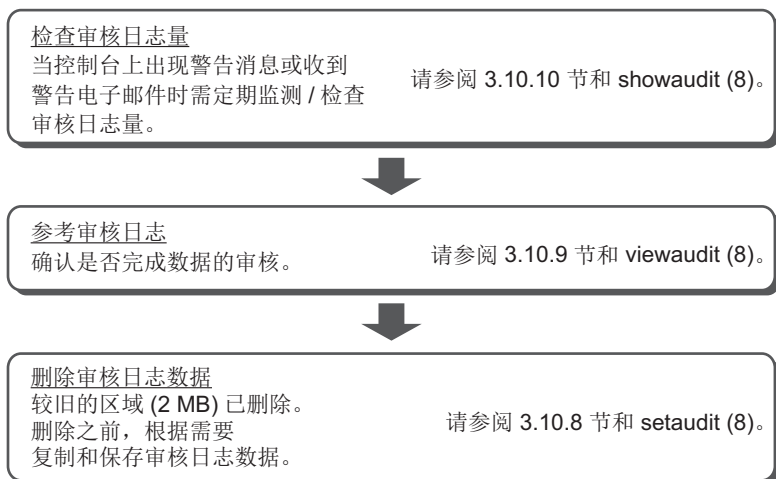


图 3-8 显示了删除审核日志数据的流程。

图 3-8 删除审核日志数据



3.10.6 显示/设置审核策略

1. 执行 **showaudit** 命令以查看审核策略设置。

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:        13713 (bytes)
Audit space free:        4180591 (bytes)
Records dropped:         0
Policy on full trail:    count
User global policy:      enabled
Mail:
Thresholds:              80% 100%
User policy:
Events:
    AEV_AUDIT_START      enabled
    AEV_AUDIT_STOP       enabled
```

2. 执行 **setaudit** 命令以设置审核策略。
在以下的示例中，指定三个用户（yyyyy、uuuuu 和 nnnnn），启用审核类别的 AUDIT 和 LOGIN，启用审核事件的版本，并禁用用户的全局策略。

```
XSCF> setaudit -a yyyyy,uuuuu,nnnnn=enable -c
ACS_AUDIT,ACS_LOGIN=enable -e AEV_version=enable -g disable
```

在以下的示例中，指定警告传输的目的地电子邮件地址、审核线索量达到满容量时删除新的审核记录并统计删除的记录，以及文件总量警告阈值（50%、75% 和 90%）。

```
XSCF> setaudit -m yyyy@example.com -p count -t 50,75,90
```

3. 执行 **showaudit** 命令，并确认设置。

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:        13713 (bytes)
Audit space free:        4180591 (bytes)
Records dropped:         0
Policy on full trail:    count
User global policy:      enabled
Mail:                    yyyy@example.com
Thresholds:              50% 75% 90%
User policy:
Events:
    AEV_AUDIT_START      enabled
    AEV_AUDIT_STOP       enabled
    :
    AEV_LOGIN_BUI        enabled
```

```
AEV_LOGIN_CONSOLE      enabled
AEV_LOGIN_SSH          enabled
AEV_LOGIN_TELNET       enabled
AEV_LOGOUT             enabled
AEV_AUTHENTICATE       enabled
:
AEV_version            enabled
:
```

通过指定 `-p count`，当审核日志达到满容量时，新的审核记录数据会被放弃（丢弃），所丢弃记录的次数被统计（丢弃统计）。

注 - 当审核日志达到满容量时，目前仅支持丢弃审核记录的默认审核策略 "count"。因此，请勿指定 "suspend"。

如果审核日志量超过了阈值，控制台上将出现警告消息。如果指定了警告目的地的电子邮件地址，也采用安全的格式发送警告。

下面是警告消息的示例。

```
WARNING: audit trail is 91% full
```

3.10.7 启用/禁用审核

如需确认审核的当前状态，请使用 `showaudit` 命令。也可使用 `setaudit` 命令设置审核项目。请使用具有 `auditadm` 权限的用户账户执行 `setaudit` 命令。

默认情况下审核启用。当审核被禁用时停止向审核日志写入。当审核启用时恢复向审核线索写入。在重启后的过程中在被启用前审核被禁用。

1. 执行 `showaudit` 命令查看审核设置。

下面是查看当前系统审核整个状态的示例。

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:        13713 (bytes)
Audit space free:        4180591 (bytes)
Records dropped:         0
Policy on full trail:    count
User global policy:      enabled
Mail:
Thresholds:              80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
    AEV_AUDIT_STOP enabled
:
```

2. 执行 `setaudit` 命令以设置启用/禁用。

下面是指定启用审核数据写入的示例。

```
XSCF> setaudit enable
```

下面是指定禁用审核数据写入的示例。

```
XSCF> setaudit disable
```

3.10.8 删除审核日志数据

在下列情况下，审核日志数据可以通过执行 `setaudit` 命令删除：当超过审核日志容量阈值时、当控制台上显示警告消息或警告邮件到达时、或当审核日志达到满容量时。

1. 执行 `showaudit` 命令查看审核设置和审核日志量。

以下是完全查看系统中当前审核状态的示例。

此示例表明审核日志量是 3.5 MB，已超过 80% 的警告级别的容量阈值。

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:        3670016 (bytes)
Audit space free:       524288 (bytes)
Records dropped:         0
Policy on full trail:    count
User global policy:      enabled
Mail:
Thresholds:              80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
    AEV_AUDIT_STOP  enabled
:
```

2. 执行 `setaudit` 命令删除审核日志数据。

较旧的 2-MB 区域（次要）被删除。

```
XSCF> setaudit delete
```

注 - 删除审核日志数据之前，使用 `viewaudit` 命令检查数据的审核是否已经完成。

3. 执行 `showaudit` 命令以检查 `setaudit` 命令的执行结果。

下面的示例表明审核日志的较旧的区域被删除，并创建约 2 MB 的可用容量。

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:        2097152 (bytes)
```

```
Audit space free:      2097152 (bytes)
Records dropped:      0
Policy on full trail: count
User global policy:  enabled
Mail:
Thresholds:          80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
    AEV_AUDIT_STOP  enabled
:
```

注 - 删除次要区域数据后，主要区域变为次要区域，并创建新的主要区域。系统然后认可新的次要区域量为 2 MB，不管该区域的实际剩余量。因此，即使已经删除审核日志数据，当使用 `showaudit` 命令查看审核日志量时，2 MB 始终显示为使用中。

如果连续执行两次此删除操作，审核日志中的所有信息都将被删除。即使在这种情况下，使用 `showaudit` 命令查看显示的审核日志量中，2 MB 也显示为使用中。

3.10.9 查看审核日志

使用 `viewaudit` 命令查看审核日志。请使用具有 `auditadm` 或 `auditop` 权限的用户账户执行 `viewaudit` 命令。

1. 执行 `viewaudit` 命令以查看审核线索。

```
XSCF> viewaudit
file,1,2015-06-29 13:42:59.128 +09:00,20150629044259.
0000000000.localhost
header,20,1,audit - start,localhost.localdomain,2015-06-29 13:
42:59.131 +09:00
header,31,1,login - console,localhost.localdomain,2015-06-29
13:45:03.755
+09:00subject,1,default,normal,console
header,60,1,command - showpasswordpolicy,localhost.localdomain,
2015-06-29
13:45:33.653 +09:00
subject,1,default,normal,console
command,showpasswordpolicy
platform access,granted
return,0
:
```

有关如何查阅审核记录的详细信息，请参见“[第12章 检查日志和信息](#)”。

3.10.10 管理备用 XSCF 的审核日志

主/备用 XSCF 的审核数据保存到主/备用 XSCF 中的审核日志区域。可以从各个 XSCF 使用 `viewaudit` 命令查看审核日志。然而，仅主 XSCF 可以用来显示审核的状态或删除审核日志数据。因此，如需管理备用 XSCF 的审核日志，需将 XSCF 从备用切换到主。

下面介绍如何管理保存到备用 XSCF 的审核日志。

查看审核日志

从备用 XSCF 执行 `viewaudit(8)` 命令。有关查看方法的详情，请参见 "[3.10.9 查看审核日志](#)"。

删除审核日志数据

1. 执行 `switchscf(8)` 命令以在主 XSCF 和备用 XSCF 之间切换。
2. 执行 `showaudit(8)` 命令检查先前备用 XSCF 的审核日志量。
3. 执行 `setaudit(8)` 命令删除审核日志数据。
有关删除数据的详细信息，请参见 "[3.10.8 删除审核日志数据](#)"。
4. 执行 `showaudit(8)` 命令确认审核日志是否存在可用空间。
5. 再次执行 `switchscf(8)` 命令以在主 XSCF 和备用 XSCF 之间切换。

按照使用型号配置系统

本章将介绍配置适合于系统使用的重点是电源控制和驱动器连接的项目。

- 设置/确认系统海拔高度
- 控制系统启动
- 启用/禁用双回路供电
- 降低功耗
- 连接 DVD 驱动器
- 使用远程存储

4.1 设置/确认系统海拔高度

本节介绍如何设置和确认系统海拔高度。

SPARC M12/M10 系统根据安装位置的海拔高度和温度控制系统内冷却风扇的速度。因此，在初始系统安装时，需要设置海拔高度。

注 - 在初始安装期间设置系统海拔高度。如果需要更改设置值，请再次设置。

有关以下步骤中执行的 XSCF 命令的详细信息，请参见其手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

4.1.1 设置系统海拔高度

要设置系统海拔高度，请使用 XSCF 固件 `setaltitude` 命令。
请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。

```
XSCF> setaltitude -s altitude=value
```

用 `value` 指定服务器所安装位置的海拔高度（米）。您可从 0 开始指定，增量为 100。

注 - 设置系统海拔高度后，您需要重新启动 XSCF 才能应用该设置，因此需执行 `rebootxscf` 命令。

操作步骤

1. 执行 `setaltitude` 命令以设置海拔高度设置。
下面是将海拔高度配置 1,000 米的示例。

```
XSCF> setaltitude -s altitude=1000
1000m
```

2. 执行 `rebootxscf` 命令重新启动 XSCF 以反映所做的设置。

注 - 当继续进行其他设置时，您可以在所有设置完成后再执行此任务。

```
XSCF> rebootxscf -a
```

4.1.2 检查系统的海拔高度设置

使用 XSCF 固件的 `showaltitude` 命令可检查当前设置的系统的海拔高度。请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。

```
XSCF> showaltitude
```

此命令显示当前设置的系统海拔高度（以米为单位）。

操作步骤

1. 执行 `showaltitude` 命令以显示海拔高度。
下面是设置海拔高度为 1,000 米的示例。

```
XSCF> showaltitude
1000m
```

4.2 控制系统启动

本节介绍可控制系统启动的预热时间和启动等待时间。

预热时间和启动等待时间适用于以下目的。

- 可以保持系统不启动，直到外设上电。可以保持系统不启动，直到其预热完毕。此外，可以为每个物理分区设置不同的运行时间。设置了功耗的上限值时，同时上电可能导致功耗超过此限制。因此需为每个物理分区设置不同的时间。（请参见 "4.2.1 设置/确认预热时间"。）
- 您可以在数据中心的空调已调节温度后再启动系统。（请参见 "4.2.2 设置/确认启动等待时间"。）

4.2.1 设置/确认预热时间

设置预热时间后，服务器电源开启并且开始开启电源的处理，OpenBoot PROM 在预热时间结束后开始启动。

设置预热时间

要设置预热时间，请使用 XSCF 固件 `setpowerupdelay` 命令。请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。

```
XSCF> setpowerupdelay {-a|-p ppar-id} -c warmup -s time
```

如果目标是所有的物理分区，指定 `-a`。如果目标是一个物理分区，指定 `-p`。

对于 `time`，指定以分钟为单位的预热时间。您可以指定 0 到 255 间的一个整数。默认值为 0。

注 - 如果您通过在操作面板按 POWER 开关开启电源，设置的预热时间无效。

操作步骤

1. 执行 `setpowerupdelay` 命令以设置预热时间。
下面是将物理分区 0 的预热时间配置为 5 分钟的示例。

```
XSCF> setpowerupdelay -p 0 -c warmup -s 5
```

如果在系统运行时设置预热时间，则设置的时间会在系统下次启动时有效。

确认预热时间

要确认预热时间，请使用 XSCF 固件 `showpowerupdelay` 命令。请使用具有 `platadm`、`plato` 或 `fieldeng` 权限的用户账户执行此命令。另外，对于目标物理分区，具有 `pparadm`、`pparmgr` 或 `pparop` 权限的用户帐户也能执行此操作。

```
XSCF> showpowerupdelay
```

在 `showpowerupdelay` 命令的输出结果中以分钟为单位显示当前设置的预热时间 "warmup time"。以分钟为单位显示当前设置的启动等待时间 "wait time"。

操作步骤

1. 执行 **showpowerupdelay** 命令显示预热时间。
下面是设置预热时间为 10 分钟的示例。

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

4.2.2 设置/确认启动等待时间

设置了启动等待时间后，系统在服务器开启并且在设置的时间结束后启动。

设置启动等待时间

要设置启动等待时间，请使用 XSCF 固件 **setpowerupdelay** 命令。
请使用拥有 **platadm** 或 **fieldeng** 权限的用户账户执行此命令。

```
XSCF> setpowerupdelay -c wait -s time
```

对于 **time**，请指定以分钟为单位的启动等待时间。您可以指定 0 到 255 间的一个整数。
默认值为 0。

注 - 如果您通过在操作面板按 POWER 开关开启电源，设置的启动等待时间无效。

操作步骤

1. 执行 **setpowerupdelay** 命令设置启动等待时间。
下面是设置启动等待时间为 5 分钟的示例。

```
XSCF> setpowerupdelay -c wait -s 5
```

如果在系统运行时设置启动等待时间，则设置的时间会在系统下次启动时有效。

确认启动等待时间

要确认启动等待时间，请使用 XSCF 固件 **showpowerupdelay** 命令。
请使用具有 **platadm**、**platop** 或 **fieldeng** 权限的用户账户执行此命令。另外，对于目标物理分区，具有 **pparadm**、**pparmgr** 或 **pparop** 权限的用户帐户也能执行此操作。

```
XSCF> showpowerupdelay
```

在 **showpowerupdelay** 命令的输出结果中以分钟为单位显示当前设置的预热时间 "warmup time"。以分钟为单位显示当前设置的启动等待时间 "wait time"。

操作步骤

1. 执行 **showpowerupdelay** 命令显示启动等待时间。
下面是设置启动等待时间为 20 分钟的示例。

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

4.3 启用/禁用双回路供电

SPARC M12-2/M12-2S 上安装了四个电源单元。对于双电源系统，每个系统都有两个电源单元。

例如，PSU#0/PSU#1 用于电源系统 0，PSU#2/PSU#3 用于电源系统 1
启用/禁用双回路供电时，PSU 状态和系统操作如 [表 4-1](#) 中所示。

表 4-1 SPARC M12-2/M12-2S 启用系统操作的双回路供电设置和电源单元 (PSU) 状态

双回路供电设置	PSU 状态	系统运行
禁用	2 个或更多个运行的 PSU	可运行
	不超过 1 个运行的 PSU	不可运行
启用	至少 1 个电源系统上 2 个运行的 PSU	可运行
	两个电源系统上不超过 1 个运行的 PSU	不可运行

SPARC M10 和 SPARC M12-1 上安装了两个电源单元 (PSU)。由于 PSU 是冗余配置，只要至少有一个 PSU 正在运行，系统就可以运行。因此，即使启用/禁用双回路供电功能，也不影响系统运行。

4.3.1 启用双回路供电

要启用双回路供电，需使用 XSCF 固件的 **setdualpowerfeed** 命令。

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s enable
```

要对系统中的所有机柜启用双回路供电，请指定 **-a**。

要只对系统中的特定机柜启用双回路供电，请指定 **-b bb_id**。对于 **bb_id**，请指定机柜的 BB-ID。根据系统配置，可指定 0 到 15 或 80 到 83 间的整数。

操作步骤

1. 执行 **setdualpowerfeed** 命令启用双回路供电。
下面是为 BB-ID 1 启用双回路供电的示例。

```
XSCF> setdualpowerfeed -b 1 -s enable
BB#01:disable -> enable
NOTE: Dual power feed will be enabled the next time the platform is powered on.
```

4.3.2 禁用双回路供电

要禁用双回路供电，请使用 XSCF 固件的 **setdualpowerfeed** 命令。

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s disable
```

要对系统中的所有机柜启用双回路供电，请指定 **-a**。
要只对系统中的特定机柜启用双回路供电，请指定 **-b bb_id**。对于 **bb_id**，请指定机柜的 BB-ID。根据系统配置，可指定 0 到 15 或 80 到 83 间的整数。

操作步骤

1. 执行 **setdualpowerfeed** 命令禁用双回路供电。
下面是处理所有机柜的示例。

```
XSCF> setdualpowerfeed -a -s disable
BB#00:enable -> disable
BB#01:enable -> disable
NOTE: Dual power feed will be change the next time the platform is powered on.
```

4.3.3 确认双回路供电设置

要确认双回路供电设置，请使用 XSCF 固件的 **showdualpowerfeed** 命令。

```
XSCF> showdualpowerfeed
```

根据情况输出以下几种信息。

- 启用双回路供电时

```
BB#00: Dual power feed is enabled.
```

- 禁用双回路供电时

```
BB#00: Dual power feed is disabled.
```

- 双回路供电状态从启用变为禁用时

```
BB#00:enable -> disable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

- 双回路供电状态从禁用变为启用时

```
BB#00:disable -> enable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

操作步骤

1. 执行 **showdualpowerfeed** 命令确认双回路供电。
下面是 BB-ID 0和 BB-ID 1 组成的系统状态从禁用变为启用的示例。

```
XSCF> showdualpowerfeed  
BB#00:disable -> enable  
BB#01:disable -> enable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

4.4 降低功耗

本节介绍用于降低 SPARC M12/M10 功耗的各种精制的功能。

4.4.1 设置功耗上限

在 SPARC M12/M10 中，您可以设置功耗上限和超过上限时所执行的操作。

要设置功耗上限，请使用 XSCF 固件的 **setpowercapping** 命令。

请使用拥有 **platadm** 或 **fieldeng** 权限的用户账户执行此命令。执行此命令后，设置会立即应用到 XSCF。

```
XSCF> setpowercapping -s option=value [[-s option=value]...]
```

您可用 **option** 和 **value**，设置以下项目。

- 启用/禁用功率上限功能 (**activate_state**)
指定启用或禁用。默认禁用。
- 设置功耗上限
使用如下方法之一指定。

- 瓦特数 (powerlimit_w) 指定 0 到 999999 之间的一个值。
- 百分比 (powerlimit_p) 指定到 0 到100 之间的一个值。
- 超过上限时允许的时间延长 (timelimit)

时间延时（以秒为单位）指定到 10 到 99999 之间的一个值。您还可通过指定以下值设置时间延长：

 - default: 30 秒
 - none: 无延长时间
- 违反时的操作 (violation_actions)

指定超过功耗上限和时间延长时采取的措施。指定以下其中一个操作。默认值为 none。

 - none

输出信息。
 - shutdown

输出一条信息并关闭物理分区，直到功耗低于功耗上限。按照 PPAR-ID 降序对物理分区执行关闭。
 - poff

输出一条信息并强制关闭物理分区，直到功耗低于功耗上限。按照 PPAR-ID 降序强制关闭物理分区。

注 - 如果功耗上限的设定是基于运行中的平均功耗，则 SPARC M12/M10 系统启动时在开机过程中、自诊断测试等产生的浪涌电流可能成为问题。使用 XSCF 的 `setpowerupdelay` 命令错开多个物理分区开启时间，消除冲击电流以避免这个问题。

注 - 因为客户的操作造成服务器负荷增加时，功耗可能急剧增加。造成功耗可能长时间超过指定功耗上限。因此，对您的业务启动系统操作之前，需将 `violation_actions` 的值设置为“none”（默认值），避免影响系统连续运行。接下来，在客户侧执行环境测试后，确保功耗上限 (`powerlimit_w`, `powerlimit_p`) 不能过低，超出上限的延长时间 (`timelimit`) 不能过短。然后，设置 `violation_actions` 的值。

有关 `setpowercapping` 命令的详细信息，请参见 `setpowercapping(8)` 命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

操作步骤

1. 执行 `showenvironment power` 命令检查系统功耗信息。
使用 [Peak Permitted] 和 [Actual AC power consumption] 的值设置功耗上限。

```
XSCF> showenvironment power
Power Supply Maximum      :5000W
Installed Hardware Minimum:1268W
Peak Permitted            :2322W
BB#00
    Permitted AC power consumption:5000W
    Actual AC power consumption  :1719W
```

各项目如下：

- 电源最大值：整个系统电源单元 (PSU) 的最大功耗
- Installed Hardware Minimum: 用 `setpowercapping` 能够设置的最小值
- Peak Permitted: 假定峰值参考值
- 许可交流功耗：PSU 的最大功耗 (*1)
- 实际交流功耗：机箱中的实际功耗值

*1 在 SPARC M12 中，显示“可用交流功耗”。也显示 PSU 的额定功耗。

2. 执行 `setpowercapping` 命令。

下面是将功耗上限设置为 1,800 W 和将超过上限时的时间延长设置为 90 秒的示例。

```
XSCF> setpowercapping -s powerlimit_w=1800 -s timelimit=90
activate_state      : enabled -> -
powerlimit          : 2322w -> 1800w
timelimit           : 30 -> 90
violation_actions   : none -> -
The specified options will be changed.
Continue? [y|n]     : y
configured.
activate_state      : enabled
powerlimit          : 1800w
timelimit           : 90
violation_actions   : none
```

3. 启用功耗限制。

```
XSCF> setpowercapping -s activate_state=enabled
activate_state      : disabled -> enabled
powerlimit          : 1800w -> -
timelimit           : 90 -> -
violation_actions   : none -> -
The specified options will be changed.
Continue? [y|n]     : y
configured.
activate_state      : enabled
powerlimit          : 1800w
timelimit           : 90
violation_actions   : none
```

4.4.2 处理因电源异常造成的温度/负荷异常

检测到由温度异常、功率异常或一些其他问题引起的负荷时，SPARC M12/M10 中所精制的一项功能可以降低 CPU 频率以继续运行。对 SPARC M12/M10 上的每个 CPU 都可以控制此功能。当温度或电源异常造成的负荷问题解决以后，CPU 频率自动回到初始值。

4.4.3 降低未使用的或低利用率硬件的功耗

在 SPARC M12/M10 中，您可以设置每个物理分区的运行，降低未使用或低利用率硬件的功耗（省电操作）。

当降低功耗的设置起作用时，目标硬件将根据其利用率以省电级别运行。因此，低利用率硬件的供电被减少，随着利用率上升，对硬件的供电增加。

在 SPARC M12 中，通过使用 Solaris Power Aware Dispatcher，也可以降低功耗，几乎不影响 CPU 处理性能。

有关使用 Solaris Power Aware Dispatcher 降低功耗而对 XCP 固件和 Oracle Solaris 的软件要求，请参见最新版本的《Fujitsu SPARC M12 产品说明》。

如需设置硬件的上述省电运行，请使用 XSCF 固件的 `setpparmode` 命令。请使用拥有 `platadm` 或 `pparadm` 权限的用户帐户执行此命令。

■ SPARC M12

如需为 SPARC M12 设置省电操作，请使用 `-m powermgmt_policy` 选项。

```
XSCF> setpparmode -p ppar_id -m powermgmt_policy={elastic|performance|disabled}
```

使用 `powermgmt_policy` 选项，您可以启用（`elastic` 或 `performance`）或禁用（`disabled`）省电操作。默认禁用。命令执行后，此设置立即生效。

各个选项设置值的含义如下所示。

- elastic

启用 CPU 和内存的省电运行。根据 CPU 和内存的当前利用率级别，变更系统电源使用状况。此选项可以降低系统功耗。

- performance

启用 CPU 的省电运行。此选项可以省电，而不会对性能产生太大影响，因为系统中未使用的、空闲的 CPU 以较慢的速度运行，或者可能已进入睡眠状态。

- disabled（默认值）

禁用 CPU 和内存的省电运行。系统中的所有 CPU 和内存将以最高性能持续运行。

注 - 通过指定 `elastic` 选项启用省电操作时，可以降低功耗，但 CPU 性能可能会降级。指定 `performance` 值可降低功耗，几乎不会影响 CPU 处理性能。

如果固件从低于 XCP3040 的版本更新到 XCP3040 或更高版本，则使用 Solaris Power Aware Dispatcher 的 Power Aware Dispatcher 功能（PAD 功能）被禁用（`off`）。

对 `powermgmt_policy` 选项指定 `performance` 时，您需要将 PAD 功能更改为启用（`on`）。

当您对 `powermgmt_policy` 选项指定 `disabled` 或 `elastic` 时，PAD 功能设置为 `on` 还是设置为 `off` 在省电操作中无差异。

如需变更 PAD 功能的设置，需使用 `-m pad` 选项。

```
XSCF> setpparmode -p ppar_id -m pad={off|on}
```

使用 `pad` 选项，您可以启用 (on) 或禁用 (off) PAD 功能。默认启动 (on)。各个选项设置值的含义如下所示。

- on (默认值)
启用 PAD 功能。
- off
禁用 PAD 功能。
将此选项设置为 off 时，`powermgmt_policy` 选项必须设置为 `disabled` 或 `elastic`。

PAD 功能的设置需在 PPAR 停止时进行。

当 PAD 功能的设置从 `disabled` 状态变为 `enabled` 状态或反之之时，逻辑域的配置信息在 PPAR 启动后将恢复为出厂默认值。在这种情况下，逻辑域需要重新配置。提前将配置信息保存在 XML 文件中。

■ SPARC M10

如需为 SPARC M10 设置省电操作，请使用 `-m elastic` 选项。

```
XSCF> setpparmode -p ppar_id -m elastic={on|off}
```

但具有弹性，您可以启用 (on) 或禁用 (off) 省电运行。默认禁用 (off)。命令执行后，此设置立即生效。

各个选项设置值的含义如下所示。

- on
启用 CPU 和内存的省电运行。根据 CPU 和内存的当前利用率级别，变更系统电源使用状况。此选项可以降低系统功耗。
- off (默认值)
禁用 CPU 和内存的省电运行。系统中的所有 CPU 和内存将以最高性能持续运行。

注 - 启用省电操作时，可以降低功耗，但 CPU 性能可能会降级。

有关 `setpparmode` 命令的详细信息，请参见 `setpparmode(8)` 命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

操作步骤

■ SPARC M12

注 -

- 禁用 PAD 功能时，您将无法将省电运行的设置变更为 `performance`。启用 PAD 功能 (on) 后，可将该设置变更为 `performance`。
 - 当将省电运行设置为 `performance` 时，您将无法禁用 PAD 功能 (off)。将省电运行设置为 `disabled` 或 `elastic` 后，可禁用该功能。
-

以下是将省电运行设置为 `performance` 的示例。

1. 执行 `showpparmode` 命令确认省电运行和 PAD 功能的设置。以下示例表明：禁用了省电运行，启用了 PAD 功能。

```

XSCF> showpparmode -p 0
Host-ID                :90060027
Diagnostic Level       :min
Message Level         :normal
Alive Check           :on
Watchdog Reaction     :reset
Break Signal          :on
Autoboot(Guest Domain):on
Power Aware Dispatcher:on
Power Management Policy:disabled
IOreconfigure         :false
CPU Mode              :-
PPAR DR(Current)      :-
PPAR DR(Next)         :off

```

2. 执行 **setpparmode** 命令设置省电操作为 **performance**。

```

XSCF> setpparmode -p 0 -m powermgmt_policy=performance
Diagnostic Level       :min          -> -
Message Level         :normal       -> -
Alive Check           :on           -> -
Watchdog Reaction     :reset        -> -
Break Signal          :on           -> -
Autoboot(Guest Domain):on          -> -
Power Aware Dispatcher:on          -> -
Power Management Policy:disabled    -> performance
IOreconfigure         :false        -> -
CPU Mode              :-
PPAR DR               :off          -> -
The specified modes will be changed.
Continue? [y/n] :y
configured.
Diagnostic Level       :min
Message Level         :normal
Alive Check           :on (alive check:available)
Watchdog Reaction     :reset (watchdog reaction:reset)
Break Signal          :on (break signal:non-send)
Autoboot(Guest Domain):on
Power Aware Dispatcher:on
Power Management Policy:performance
IOreconfigure         :false
CPU Mode              :-
PPAR DR               :off

```

3. 执行 **showpparmode** 命令，并确认设置。

```

XSCF> showpparmode -p 0
Host-ID                :90060027
Diagnostic Level       :min
Message Level         :normal
Alive Check           :on
Watchdog Reaction     :reset

```

```

Break Signal           :on
Autoboot(Guest Domain) :on
Power Aware Dispatcher :on
Power Management Policy :performance
IOreconfigure         :false
CPU Mode               :-
PPAR DR(Current)      :-
PPAR DR(Next)         :off

```

■ 对于 SPARC M10

以下是启用省电运行的示例。

1. 执行 **showpparmode** 命令查看未使用的或低利用率硬件的省电运行是否启用/禁用。

```

XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level       :min
Message Level         :normal
Alive Check           :on
Watchdog Reaction     :reset
Break Signal          :on
Autoboot(Guest Domain) :on
Elastic Mode          :off
IOreconfigure         :true
CPU Mode              :auto
PPAR DR(Current)      :-
PPAR DR(Next)         :off
Ethernet Address       :00:0b:5d:e2:01:0c

```

2. 执行 **setpparmode** 命令以启用省电运行。

```

XSCF> setpparmode -p 0 -m elastic=on
Diagnostic Level       :min      -> -
Message Level         :normal   -> -
Alive Check           :on       -> -
Watchdog Reaction     :reset    -> -
Break Signal          :on       -> -
Autoboot(Guest Domain) :on     -> -
Elastic Mode          :off      -> on
IOreconfigure         :true     -> -
CPU Mode              :auto     -> -
PPAR DR               :off      -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level       :min
Message Level         :normal
Alive Check           :on (alive check:available)
Watchdog Reaction     :reset (watchdog reaction:reset)
Break Signal          :on (break signal:non-send)
Autoboot(Guest Domain) :on
Elastic Mode          :on

```

IOreconfigure	:true
CPU Mode	:auto
PPAR DR	:off

3. 执行 **showpparmode** 命令，并确认设置。

```
XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level       :min
Message Level          :normal
Alive Check            :on
Watchdog Reaction     :reset
Break Signal           :on
Autoboot (Guest Domain) :on
Elastic Mode          :on
IOreconfigure         :true
CPU Mode               :auto
PPAR DR (Current)     :-
PPAR DR (Next)        :off
Ethernet Address       :00:0b:5d:e2:01:0c
```

4.5 连接 DVD 驱动器

SPARC M12/M10 没有内置 DVD 驱动器。如需从 DVD 驱动器安装 Oracle Solaris 和业务应用程序，请使用以下任一方式连接的 DVD 驱动器：

- 连接到 USB 端口的外部 DVD 驱动器
- 安装在连接到 XSCF-LAN 的终端上的 DVD 驱动器

本节将介绍连接到 USB 端口的外部 DVD 驱动器。如需使用安装在终端上的 DVD 驱动器，请参见 ["4.6 使用远程存储"](#)。

4.5.1 使用外部 DVD 驱动器

SPARC M12/M10 机箱已经在前面和后面都配有 USB 端口。如需使用外部 DVD 驱动器，请将其连接到其中的一个 USB 端口。使用专用的 AC 适配器给所连接的外部 DVD 驱动器供电。

图 4-1 可连接到 DVD 驱动器的 USB 端口 (SPARC M12-1)

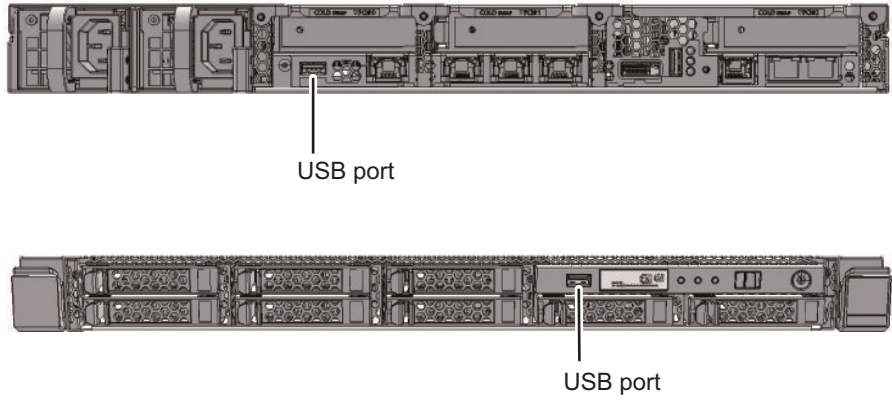


图 4-2 可连接到 DVD 驱动器的 USB 端口 (SPARC M12-2)

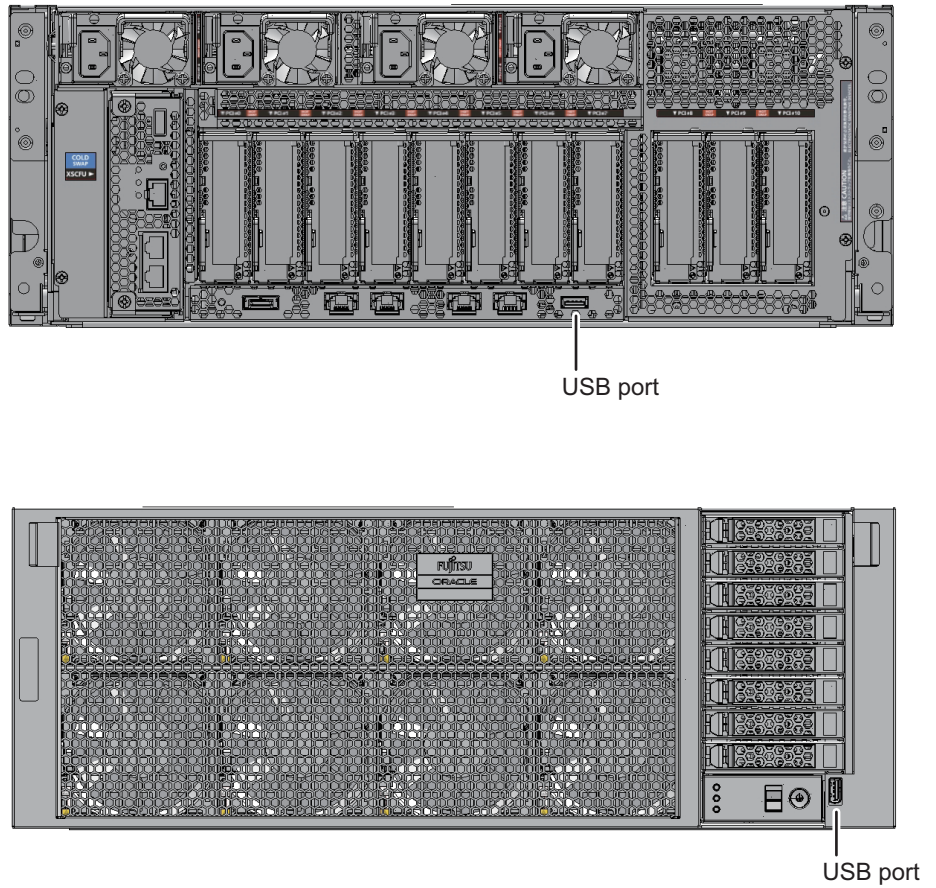


图 4-3 可连接到 DVD 驱动器的 USB 端口 (SPARC M12-2S)

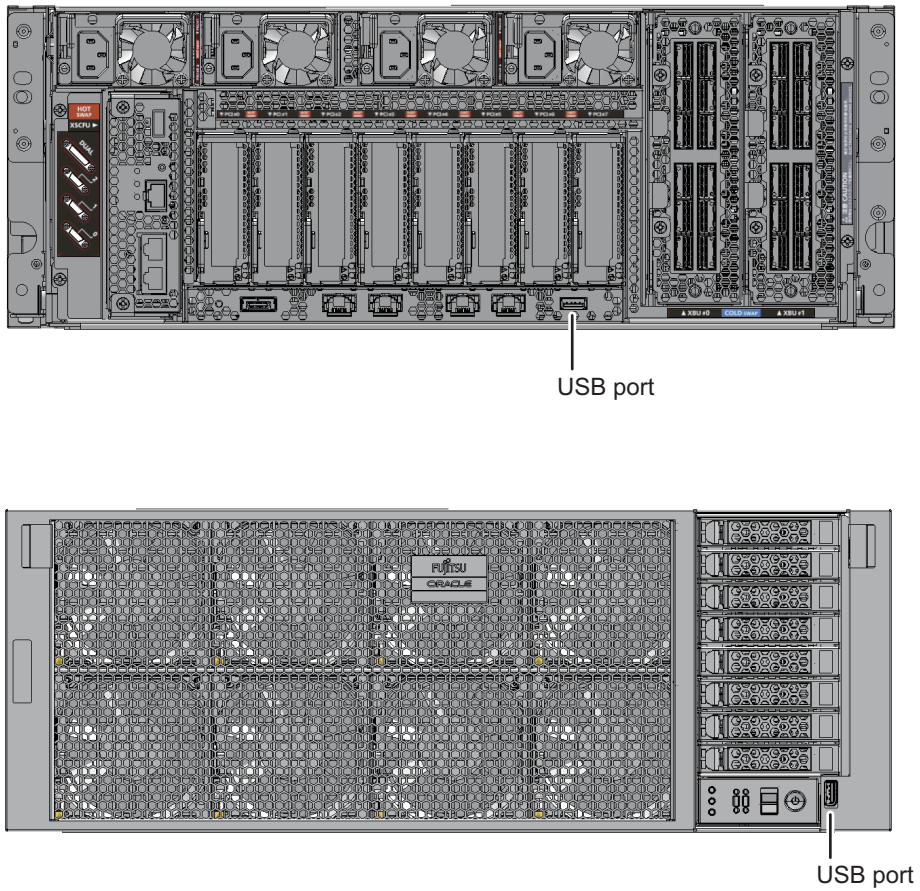


图 4-4 可连接到 DVD 驱动器的 USB 端口 (SPARC M10-1)

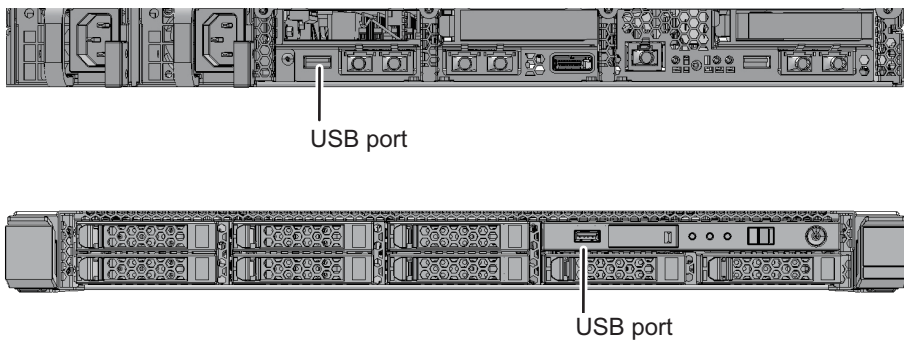
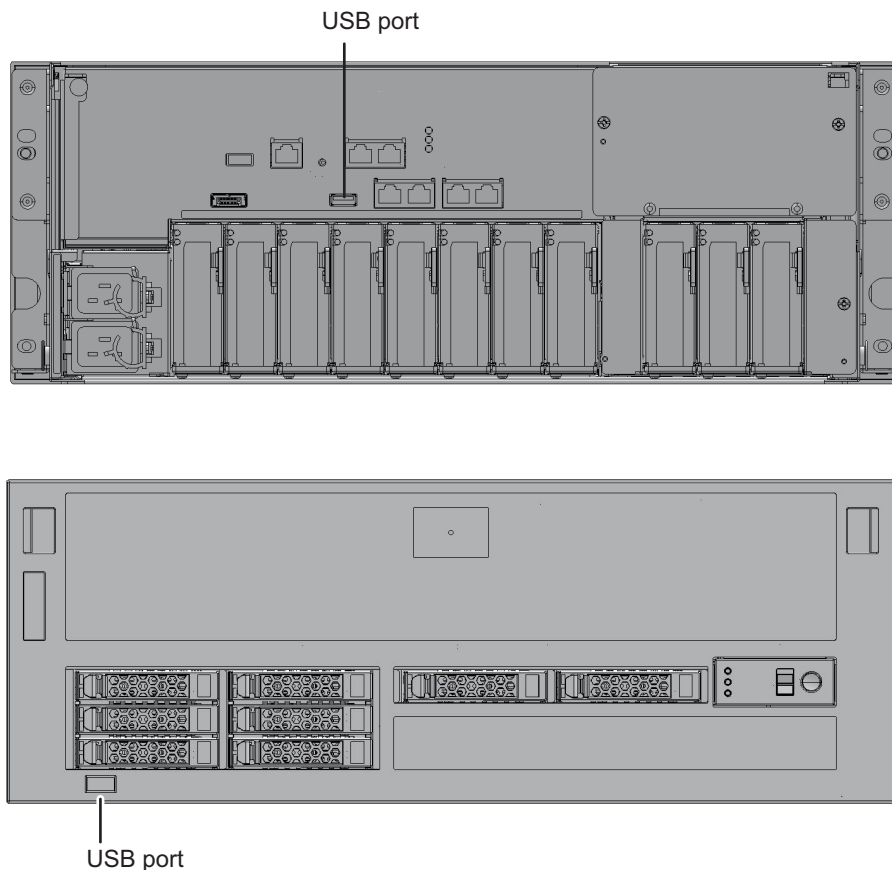


图 4-5 可连接到 DVD 驱动器的 USB 端口 (SPARC M10-4/M10-4S)



4.5.2 使用外部 DVD 驱动器安装 Oracle Solaris

从 CD/DVD-ROM 驱动器上安装 Oracle Solaris on OpenBoot PROM 时，请指定适用于您正在使用的 SPARC M12/M10 型号的设备路径。有关每种型号的设备路径的详细信息，请参见“附录 A SPARC M12/M10 系统设备路径列表”。有关 DVD 驱动器别名的详情，请参见“附录 J DVD 驱动器别名列表”。

以下是指定设备路径和安装 Oracle Solaris 的步骤。

1. 将 **USB DVD 驱动器** 连接到机柜前面或后面的 **USB 端口**。
如果连接了多个 DVD 驱动器，断开其他的 DVD 驱动器，只保留一个用于安装的驱动器。
2. **OpenBoot PROM 提示 ok 提示符**后，执行 **show-disks** 命令并确认设备路径。
 - 在 SPARC M12-1 的前面板上连接 USB DVD 驱动器的示例

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- 在 SPARC M12-1 的后面板上连接 USB DVD 驱动器 (USB3.0) 的示例

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- 在 SPARC M12-1 的后面板上连接 USB DVD 驱动器 (USB2.0/1.1) 的示例

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- 在 SPARC M12-2/M12-2S 的前面板上连接 USB DVD 驱动器的示例
安装两个 CPU 时

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- 在 SPARC M12-2/M12-2S 的后面板上连接 USB DVD 驱动器 (USB3.0) 的示例

注 - 如果使用了 USB3.0, 则其按 USB2.0 工作。

安装两个 CPU 时

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
```

```
Enter Selection, q to quit: q
```

- 在 SPARC M12-2/M12-2S 的后面板上连接 USB DVD 驱动器 (USB2.0/1.1) 的示例
安装两个 CPU 时

```
{0} ok show-disks  
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk  
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk  
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk  
d) /iscsi-hba/disk  
q) NO SELECTION  
Enter Selection, q to quit: q
```

- 在 SPARC M10-1 的前面板上连接 USB DVD 驱动器的示例

```
{0} ok show-disks  
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk  
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk  
c) /iscsi-hba/disk  
q) NO SELECTION  
Enter Selection, q to quit: q
```

- 在 SPARC M10-1 的后面板上连接 USB DVD 驱动器的示例

```
{0} ok show-disks  
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk  
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk  
c) /iscsi-hba/disk  
q) NO SELECTION  
Enter Selection, q to quit: q
```

- 在 SPARC M10-4/M10-4S 的前面板上连接 USB DVD 驱动器的示例

```
{0} ok show-disks  
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk  
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk  
c) /iscsi-hba/disk  
q) NO SELECTION  
Enter Selection, q to quit: q
```

- 在 SPARC M10-4/M10-4S 的后面板上连接 USB DVD 驱动器的示例

```
{0} ok show-disks  
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk  
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk  
c) /iscsi-hba/disk  
q) NO SELECTION  
Enter Selection, q to quit: q
```

3. 指定步骤 2 的 a) 中显示的设备路径, 执行 **boot** 命令并安装 **Oracle Solaris**。

- 指定连接在 SPARC M12-1 前面板上的 USB DVD 驱动器的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk
```

- 指定连接在 SPARC M12-1 后面板上的 USB DVD 驱动器 (USB3.0) 的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk
```

- 指定连接在 SPARC M12-1 后面板上的 USB DVD 驱动器 (USB2.0/1.1) 的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk
```

- 安装两个 CPU 时指定连接在 SPARC M12-2/M12-2S 前面板上的 USB DVD 驱动器的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
```

- 安装两个 CPU 时指定连接在 SPARC M12-2/M12-2S 后面板上的 USB DVD 驱动器 (USB3.0) 的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk
```

- 安装两个 CPU 时指定连接在 SPARC M12-2/M12-2S 后面板上的 USB DVD 驱动器 (USB2.0/1.1) 的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk
```

- 指定连接在 SPARC M10-1 前面板上的 USB DVD 驱动器的示例

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk
```

- 指定连接在 SPARC M10-1 后面板上的 USB DVD 驱动器的示例

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
```

- 指定连接在 SPARC M10-4/M10-4S 前面板上的 USB DVD 驱动器的示例

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk
```

- 指定连接在 SPARC M10-4/M10-4S 后面板上的 USB DVD 驱动器的示例

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk
```

注 - 根据使用的 CD/DVD 类型，"/cdrom@x" 可能被 "/storage@x" 替代。

注 - 假设只有前面板上的 USB DVD 驱动器与 SPARC M10-4/M10-4S 连接，您对后面板上的 USB DVD 驱动器指定了驱动器路径来执行 boot 命令。即使指定的设备路径不正确，启动也从连接到前面板的 USB DVD 执行。当执行启动命令时，请务必确认指定的设备是否正确。

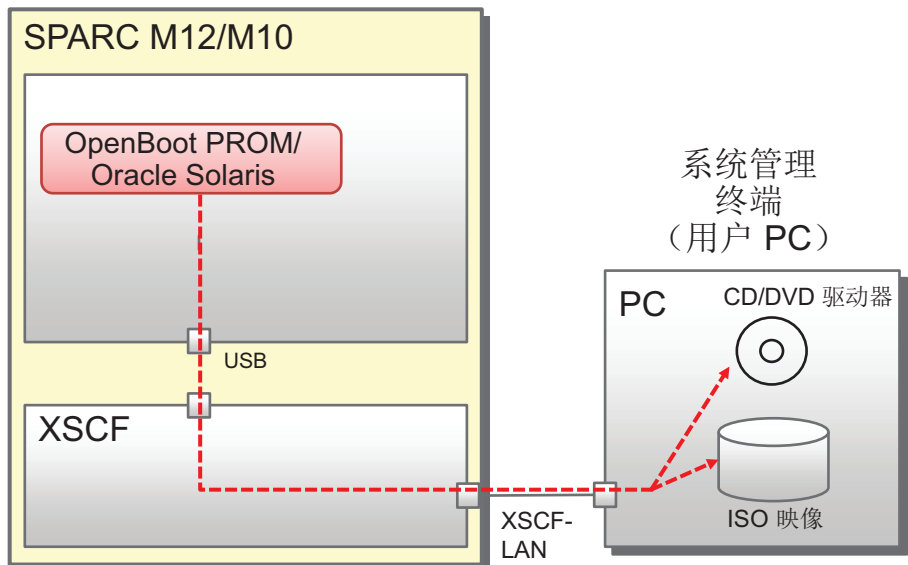
4.6 使用远程存储

本节将介绍可访问终端中安装的存储器（介质）的远程存储。对于远程存储，需使用 XSCF 网络接口以太网 (XSCF-LAN)。

4.6.1 远程存储是什么？

远程存储是通过 XSCF-LAN 访问系统管理终端或用户 PC 等终端中的存储器的功能。远程存储仅支持从存储器读取到 SPARC M12/M10。图 4-6 是一个概念图，显示了从 OpenBoot PROM 或 Oracle Solaris 如何使用远程存储功能来访问终端中的介质。

图 4-6 远程存储的概念图



远程存储启用从逻辑域到以下介质的连接：

- 插入到安装在/连接到终端的 CD/DVD 驱动器的介质
- 终端上的 ISO 映像

此外，如果满足以下所有的环境，您可以通过 XSCF 所需的设置使用远程存储：

- SPARC M12/M10 系统所需的环境
 - XSCF-LAN 网络可用。
 - HTTPS 服务启用，XSCF Web 可用。
- 终端所需的环境

Java Runtime Environment 软件可用。

有关 XSCF 网络设置的详情，请参见 ["3.9 配置 XSCF 网络"](#)。有关 XSCF Web 操作要求以及启用 XSCF HTTPS 服务的步骤的详细信息，请参见 ["3.8 配置用于登录 XSCF 的 HTTPS 服务"](#)。另外，有关终端上 Java Runtime Environment 软件操作要求的详细信息，请参见 ["4.6.4 终端和浏览器的使用要求"](#)。

从 Oracle Solaris 所见

当使用远程存储从逻辑域可访问终端中的介质时，远程存储设备被识别为来自 OpenBoot PROM 和 Oracle Solaris 的 USB 设备，如下所示。

- Oracle Solaris 的示例

```
# cfgadm -al
Ap_Id Type Receptacle Occupant Condition
...
usb1/3 usb-storage connected configured ok
```

- OpenBoot PROM 的示例

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

有关如何连接介质的详情，请参见 ["4.6.12 使用远程存储时连接到介质"](#)。有关如何访问介质的详情，请参见 ["4.6.13 从 Oracle Solaris 使用远程存储"](#)。

4.6.2 远程存储网络配置

网络配置

远程存储使用 SPARC M12/M10 的 XSCF-LAN 网络实现对终端中介质的访问。

[图 4-7](#) 显示了使用远程存储时的网络配置，其中系统仅配置一个 SPARC M12/M10。

图 4-7 仅配置一个 SPARC M12/M10 的系统

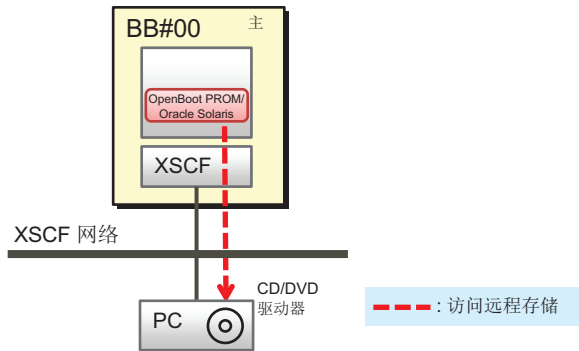
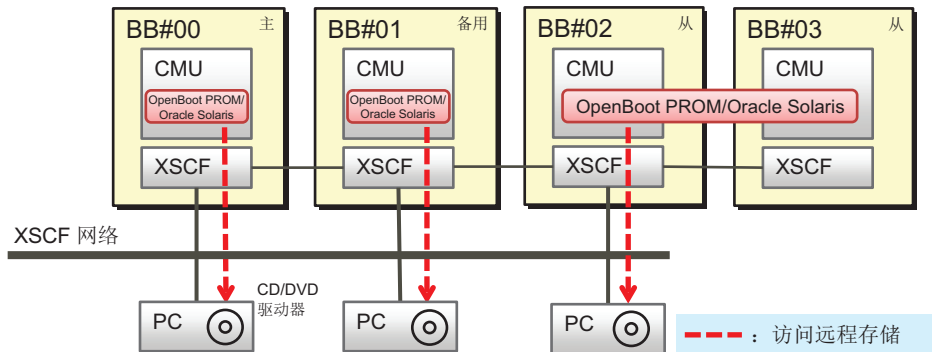


图 4-8 显示了在模块化架构配置（无接线盒）中的系统中使用远程存储时的网络配置。主 XSCF 和系统管理终端的 LAN、远程存储使用的 XSCF-LAN 以及终端的 LAN 连接在同一子网中。

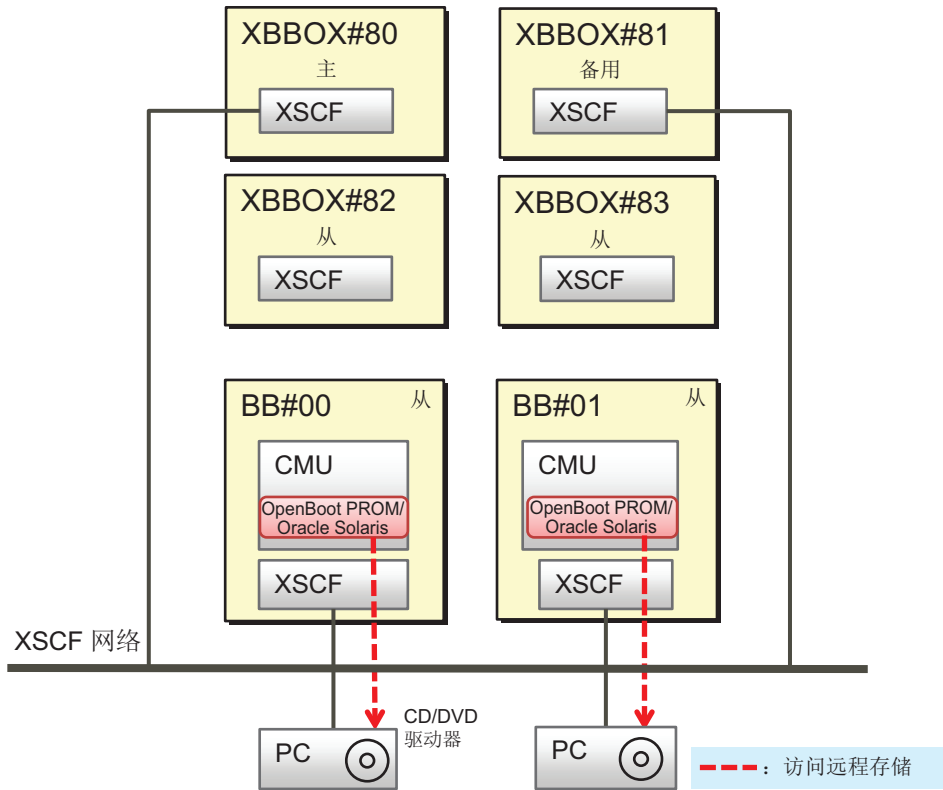
图 4-8 远程存储网络配置（无接线盒）



注 - 如果只有一台 PC，您甚至可以通过每次切换连接的 SPARC M12/M10 系统机箱来使用每个 SPARC M12/M10 的远程存储器。

图 4-9 显示了在模块化架构配置中的系统连接到接线盒的情况下，使用远程存储时的网络配置。使用远程存储时，请勿使用接线盒机箱的 XSCF-LAN 连接到介质。使用作为从机箱的 SPARC M12/M10 的 XSCF-LAN。在图 4-9 中，主 XSCF 和系统管理终端的 LAN、远程存储使用的 XSCF-LAN 以及终端的 LAN 连接在同一子网中。

图 4-9 远程存储网络配置（连接到接线盒时）



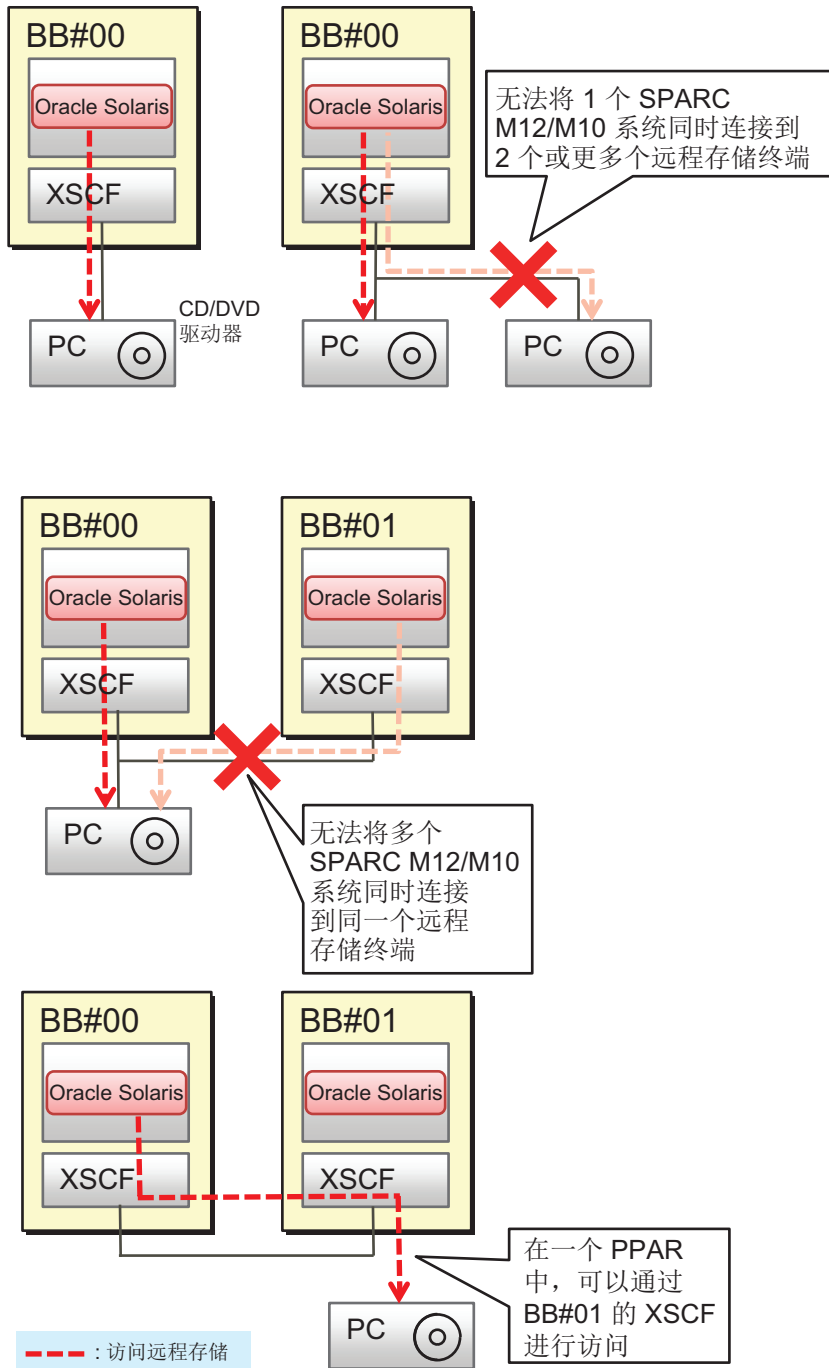
注 - 如果只有一台 PC，您甚至可以通过每次切换连接的 SPARC M12/M10 系统机箱来使用每个 SPARC M12/M10 的远程存储器。

SPARC M12/M10 与 PC 之间 1 对 1 连接的规则

如 图 4-10 所示，SPARC M12/M10 机箱以 1 对 1 连接到终端 (PC) 介质。同一个 SPARC M12/M10 机箱不能连接到两个或更多终端，多个 SPARC M12/M10 机箱不能同时连接到同一个终端。

对于从 BB#00 逻辑域经由 BB#01 的 XSCF 到终端中的介质的连接，需要注意的是，BB#00 和 BB#01 必须属于同一个物理分区。

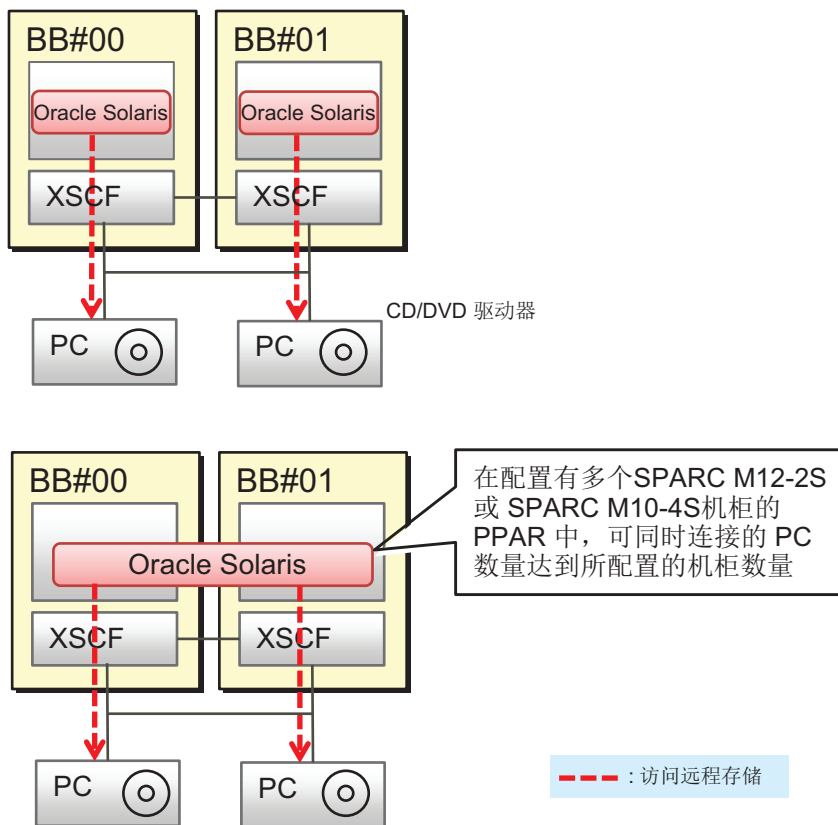
图 4-10 与 SPARC M12/M10 机箱连接的规则



如 图 4-11 中所示, 在具有多个 SPARC M12-2S 系统或多个 SPARC M10-4S 系统的系统配置中, 可以为每个 SPARC M12-2S/M10-4S 系统以 1 对 1 安装终端。所安装的这些终端中, 可同时连接多个终端。同样, 在具有多个 SPARC M12-2S 系统或多个

SPARC M10-4S 系统的物理分区配置中，可以同时连接与所配置机箱数量相同数量的终端。

图 4-11 多个 SPARC M12-2S 或 SPARC M10-4S 系统同时连接的形式



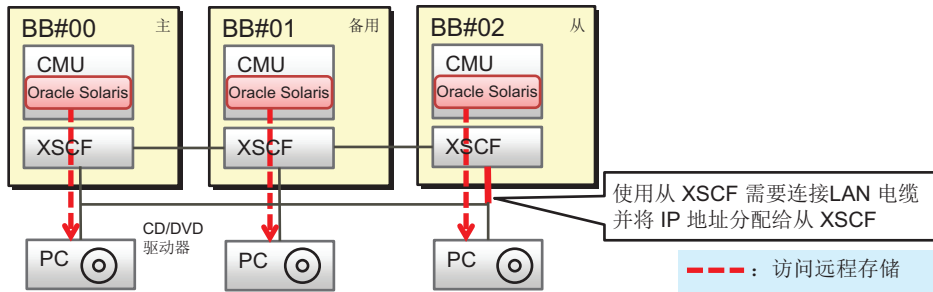
通过从 XSCF 连接

如 图 4-12 所示，SPARC M12/M10 的远程存储器甚至可以通过从 XSCF 进行连接。

注 - 从 XSCF 的 XSCF-LAN 仅可用于远程存储。其无法用于 Telnet、SSH、XSCF Web 和 SNMP 的服务。

注 - 从接线盒的 XSCF-LAN 无法用于远程存储。

图 4-12 通过从 XSCF 连接到远程存储



注 - 如果只有一台 PC，您甚至可以通过每次切换连接的 SPARC M12/M10 系统机箱来使用每个 SPARC M12/M10 的远程存储器。

开始配置远程存储之前

使用 XSCF Web 开始配置远程存储之前，您需要完成主/备用 XSCF 的网络设置。这是因为在配置主/备用 XSCF 网络时必须重新启动 XSCF。此外，如需启用 HTTPS 服务以便可以使用 XSCF Web，主 XSCF 的网络设置和 HTTPS 服务设置必须已经完成。

对于通过从 XSCF 的连接，您需要连接 XSCF-LAN 线缆并提前设置 XSCF-LAN IP 地址。另外，对于从 XSCF 的网络设置，请从 XSCF Web 或 XSCF shell 配置远程存储，而不是使用 `setnetwork` 命令或 XSCF Web 上的 [Network] 菜单。

如果连接了接线盒，则连接到接线盒的 SPARC M12/M10（从机箱）的 XSCF-LAN IP 地址必须进行设置以防止接线盒的 XSCF-LAN 用于远程存储。

表 4-2 列出了通过主/备用 XSCF 使用远程存储和通过从 XSCF 使用远程存储之间的 XSCF 网络设置差异。

表 4-2 使用远程存储的 XSCF 网络设置的差异

XSCF	XSCF-LAN 网络设置
主/备用 XSCF 的 SPARC M12/M10 机箱	XSCF Web 的 [Network]（网络）页面 或者， <code>setnetwork</code> 、 <code>setroute</code> 和 <code>applynetwork</code> 命令 注 - 需要重新启动 XSCF。
从 XSCF 的 SPARC M12/M10 机箱	XSCF Web 的 [Remote Storage]（远程存储） 页面 或者， <code>setremotestorage</code> 和 <code>showremotestorage</code> 命令 注 - 不需要重新启动 XSCF。

注 - 如果路由设置中未设置网关，则终端和 XSCF-LAN 必须连接在同一个子网中。

在具有多个 SPARC M12-2S 系统或多个 SPARC M10-4S 系统的系统配置中，物理 IP 地址用作 XSCF-LAN IP 地址，以便使用远程存储访问终端中的介质。不使用接管的 IP 地址（虚拟地址）。

有关 XSCF 网络设置的详情，请参见 "4.6.10 配置与远程存储一同使用的 XSCF-LAN"。

4.6.3 使用远程存储的方法

两种类型的画面可用于使用远程存储的设置和操作：一个是 XSCF Web 控制台，另一个是终端上的 [XSCF Remote Storage Server]（XSCF 远程存储服务器）。

图 4-13 显示了 XSCF Web 的 [Remote Storage] 页面。在此页面上，您可以配置远程存储。当您点击 [Launch]（启动）按钮时，用于选择/启动介质的 XSCF Remote Storage Server（XSCF 远程存储服务器）从终端上的 Java Runtime Environment 软件启动。然后，[XSCF Remote Storage Server] 画面打开，如 图 4-14 所示。在 XSCF 远程存储服务器运行时，介质可以连接/停止多次。

图 4-13 XSCF Web 的 [Remote Storage]（远程存储）页面

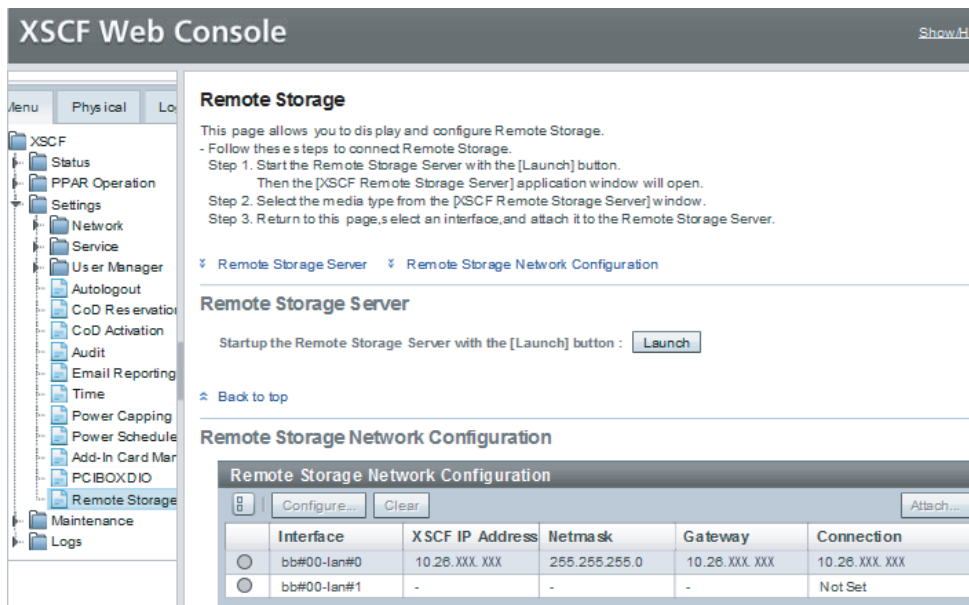
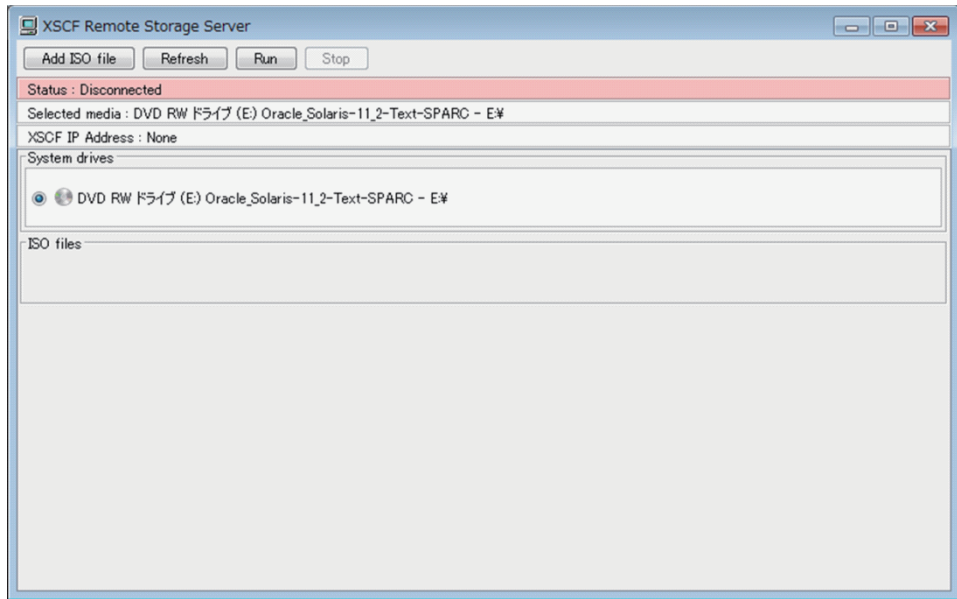


图 4-14 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面



4.6.4 终端和浏览器的使用要求

本节将介绍使用远程存储的必要使用要求以及各种设置。

终端和浏览器的使用要求

表 4-3 列出了支持远程存储的终端上 Windows 操作系统的使用要求。

表 4-3 终端的使用要求

类型	使用要求
Windows 操作系统	Windows 7、Windows 8、Windows 8.1 或 Windows 10

终端上所安装的 Java Runtime Environment 的版本必须与 XSCF Web 使用的浏览器的版本相对应。表 4-4 列出了 Java Runtime Environment 和浏览器的组合。

表 4-4 Java Runtime Environment 和 XSCF Web 使用的浏览器的组合

浏览器	Java Runtime Environment
Microsoft Internet Explorer 8 或 9, 32 位版本	Java Runtime Environment 8, 32 位版本
Microsoft Internet Explorer 8 或 9, 64 位版本	Java Runtime Environment 8, 64 位版本
Microsoft Internet Explorer 10 或 11	Java Runtime Environment 8, 32 位版本
Mozilla Firefox 10.0 至 ESR 52, 32 位版本	Java Runtime Environment 8, 32 位版本

有关终端操作系统的详细信息、最新支持的 Java Runtime Environment 的版本以及 XSCF Web 支持的浏览器，请参见您的服务器的最新《产品说明》。

Windows 操作系统环境变量 TMP 的目录设置

操作 XSCF Remote Storage Server (XSCF 远程存储服务器) 可生成用于维护和控制的以下三个文件。该文件在终端上的 Windows 操作系统环境变量 TMP 中设置的文件夹中生成。如果设置的文件夹中未生成这些文件，则 XSCF Remote Storage Server (XSCF 远程存储服务器) 启动失败，禁用远程存储。

- 跟踪文件 (Remote_Storage_Trace.txt, 最大 512 KB)
- 上一代的压缩跟踪文件 (Remote_Storage_Trace_1.txt.zip, 最大容量 512 KB)
- 监控多个启动的锁定文件 (RemoteStorageLockFile 0B)

当使用远程存储时，请确保确认以下内容。

- Windows 操作系统环境变量 TMP 中设置的目录。
- 所设置目录的访问权限不是管理员权限。

在 Windows 操作系统中，下面的文件夹是环境变量 TMP 的默认设置。

```
%USERPROFILE%\AppData\Local\Temp
```

当远程存储以默认设置使用时，XSCF Remote Storage Server (XSCF 远程存储服务器) 启动时在以下文件夹中生成文件。我们建议使用默认设置。

```
C:\Users\UserName\AppData\Local\Temp\Remote_Storage\
```

终端上使用的端口和权限

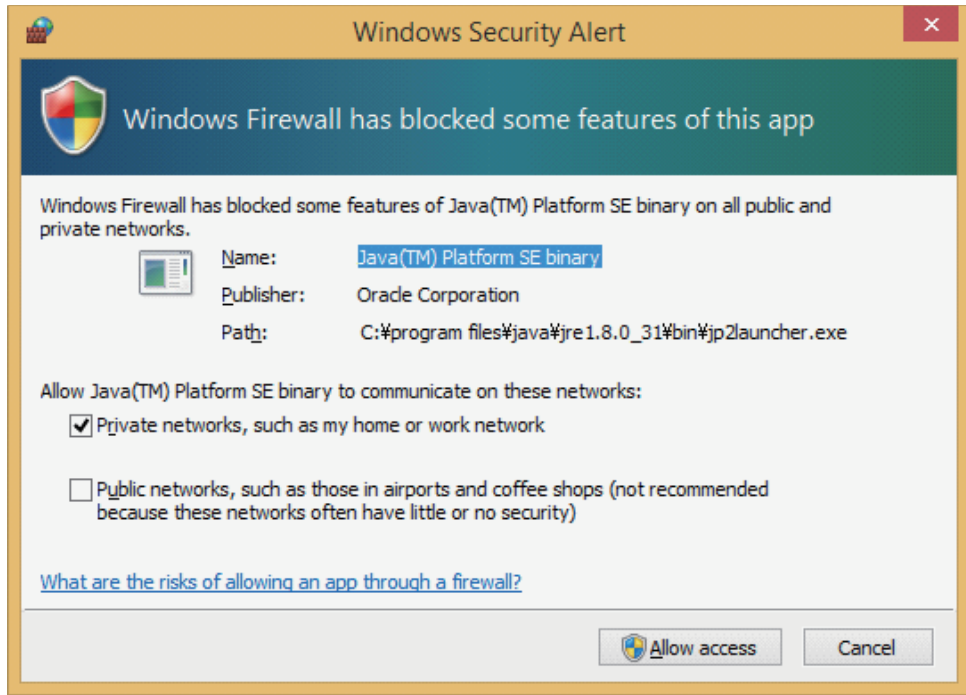
终端使用 tcp/3260 端口进行 XSCF Remote Storage Server (XSCF 远程存储服务器) 和 XSCF 之间的双向通讯。

因此，请在终端上进行以下设置。

- 在 Windows 操作系统中，允许连接到端口 3260。
- 在使用的防病毒软件中，允许连接到端口 3260。
- 使用 Windows 防火墙时，允许 Java Platform SE 的二进制程序。

使用远程存储时，单击 XSCF Web 中的 [Launch] 按钮将输出显示在图 4-15 的警告消息。在这种情况下，执行以下步骤。

图 4-15 使用 Windows 防火墙时的警告消息



1. 单击 **[Allow access]** 按钮。

这将“Java Platform SE binary”添加到控制面板中 Windows 防火墙的许可程序中。

启动 Java 并允许加载项

如果 Java 安装在终端上，请执行下列步骤启用 XSCF Web 使用的网络浏览器中的 Java，并允许加载项。

对于 **Internet Explorer**

1. 选择 **[工具] - [Internet 选项] - [程序] 选项卡 - [管理加载项]**。
2. 启用 **"Java Plug-in XX.XX.X"**。
3. 在 **Internet Explorer 8.0** 中，当使用远程存储时，选择 **XSCF Web** 中的 **[Remote Storage]**（远程存储）菜单将打开一个页面并触发消息的输出。该消息会询问是否允许安装 **Java Runtime Environment** 加载项来运行。在此消息画面上进行选择，允许加载项。

对于 **Firefox**

1. 从 **[Firefox]** 菜单，选择 **[Add-ons] - [Plugins]**。
2. 选择 **"Java(TM) Platform"**，然后设置 **[Ask to Activate]** 或 **[Always Activate]**。
3. 使用远程存储期间点击 **XSCF Web** 中的 **[Launch]**（启动）按钮将触发消息的输出。该消息会询问是否允许插件运行。选择 **[允许]**。
4. 再次显示消息询问是否允许插件运行。选择 **[Allow Now]** 或 **[Allow and**

Remember], 然后点击 **[OK]** 按钮。

终端注意事项

当使用连接到远程桌面的 PC 上的 XSCF Remote Storage Server (XSCF 远程存储服务器) 时, 您无法访问插入到 CD/DVD 驱动器的介质。指定一个 ISO 文件。

4.6.5 Oracle Solaris 的设置

如需使用远程存储, 需启用 Oracle Solaris 中的可移动介质管理服务。启用可移动介质管理服务后, 当在终端中连接介质时, Oracle Solaris 会自动安装可移动介质。

- 对于 Oracle Solaris 11 或更高版本
可移动介质管理服务: `svc:/system/hal:default`
`svc:/system/filesystem/rmvolmgr:default`
`svc:/system/dbus:default`
- 对于 Oracle Solaris 10
volfs 服务: `svc:/system/filesystem/volfs:default`

关于启用可移动介质管理服务的步骤, 请参见《External USB-DVD Drive User Manual》中的 "2.How to connect/disconnect a USB-DVD drive"。

4.6.6 远程存储软件的版本

表 4-5 列出了远程存储操作的软件版本。远程存储不支持未包含在表 4-5 中的任何版本。有关 XCP、Oracle Solaris 和基本 SRU/ 补丁的详细信息, 请参见服务器的最新《产品说明》。

表 4-5 远程存储操作所需的 XCP、Oracle Solaris 和必需的 SRU/ 补丁

XCP	Oracle Solaris	必需 SRU (*1) 必需补丁 (*2)
2260 或更高版本	Oracle Solaris 11.2 或更高版本	无
	Oracle Solaris 11.1	SRU 2.5 或更高版本 (*3)
	Oracle Solaris 10 1/13	无

*1 用于 Oracle Solaris 11

*2 用于 Oracle Solaris 10

*3 如果将远程存储作为虚拟磁盘分配给来宾域, 则需要将此应用到服务域。

4.6.7 远程存储设备的路径和别名

有关 SPARC M12/M10 型号的设备路径的详细信息，请参见“附录 A SPARC M12/M10 系统设备路径列表”。有关 DVD 驱动器别名的详情，请参见“附录 J DVD 驱动器别名列表”。

4.6.8 远程存储注意事项

使用远程存储注意事项

关于使用远程存储，请注意以下几点。

- 在物理分区的电源开启/关闭处理未完成之前，请勿执行操作来连接或停止远程存储。
- 如果网络设置中未设置默认网关，则 XSCF Web 的 [Remote Storage]（远程存储）页面上的远程存储网络配置表以及执行 `showremotestorage` 命令时网关都将显示 "-"。
- 如果使用远程存储连接到终端上的 ISO 映像，则请勿将 ISO 映像和包含该 ISO 映像的文件夹的属性设置为只读 (R)。如果设置为只读 (R) 属性，介质将无法启动（运行）。
- 使用远程存储过程中不支持通过终端操作弹出或切换介质。如果该操作访问远程存储器，会出现访问错误。
通过终端操作弹出介质是指不使用 Oracle Solaris 的 `eject` 命令而弹出介质。假定进行以下操作：
 - 按下终端的 CD/DVD 驱动器上的弹出按钮，弹出介质
 - 在终端上操作 Windows 弹出介质如需弹出介质，请执行“4.6.14 从介质断开/结束远程存储”中的步骤结束远程存储，然后弹出介质。
如需切换介质，请执行“4.6.13 从 Oracle Solaris 使用远程存储”中“切换介质”的步骤。
- 如果在远程存储使用期间点击 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面上的 [Stop]（停止）按钮并访问远程存储，会出现访问错误。
如果在使用远程存储期间单击了 [Stop] 按钮，请执行“4.6.14 从介质断开/结束远程存储”中的步骤结束远程存储。如需再次使用远程存储，请执行“4.6.12 使用远程存储时连接到介质”中的步骤。
- 请勿使用 `deleteboard` 命令断开连接远程存储器的 SPARC M12/M10。
- 如需在使用远程存储期间执行重新启动 XSCF 或主和备用 XSCF 之间切换的任何操作（包括固件升级等），则必须断开远程存储器。请参考“4.6.14 从介质断开/结束远程存储”断开连接。
如果没有断开，则可能导致域控制台输出错误消息或警告消息以及 XSCF 登记错误日志。
- 尝试通过 VPN 或其他应用地址转换的网络来连接远程存储器失败，并显示错误消

息 "iscsiadm: no records found!"。

请勿通过 VPN 或其他应用地址转换的网络来连接远程存储器。如果终端中存在多个网络连接，某些情况下无法连接远程存储器。

在这种情况下，在连接之前，禁用终端上除了用于连接 XSCF-LAN 的网络设备之外的网络设备。

使用 CD（光盘）作为远程存储介质的注意事项

当使用 CD（光盘）作为远程存储介质时，需使用采用光盘一次性 (DAO) 方法写入的 CD。如果所使用的介质不是采用光盘一次性 (DAO) 方法写入的 CD，当读取介质时，OpenBoot PROM 或 sd 驱动程序可能出现错误。

4.6.9 使用远程存储的流程

本节介绍使用远程存储的流程。通常情况下，使用远程存储时，使用 XSCF Web。

使用远程存储之前

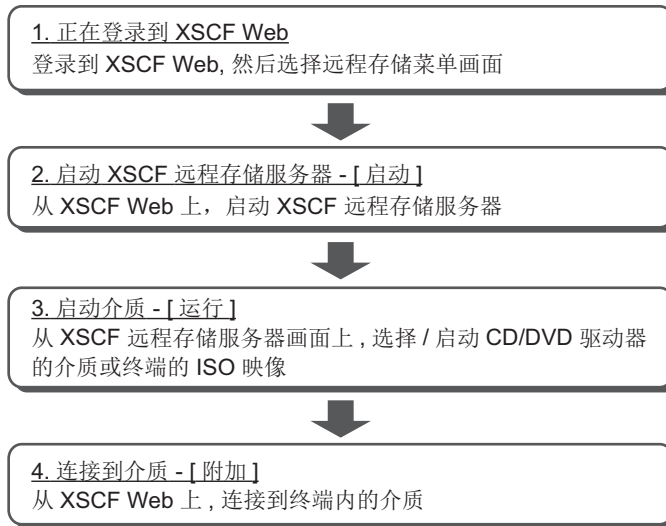
为了使用远程存储，需要进行以下提前准备工作。

- 参考 "4.6.2 远程存储网络配置" 和 "4.6.10 配置与远程存储一同使用的 XSCF-LAN"，进行主/备用 XSCF 的 XSCF 网络设置。使用 XSCF Web 必须进行主 XSCF 的网络设置。
 - 参考 "3.8 配置用于登录 XSCF 的 HTTPS 服务"，启用 HTTPS 服务。
 - 满足 "4.6.4 终端和浏览器的使用要求" 中的要求。
 - 参考 "4.6.5 Oracle Solaris 的设置"，进行 Oracle Solaris 所需的设置。
- 完成上述准备工作后，执行基本操作。

基本操作流程

如需使用远程存储，需从系统管理终端使用 XSCF Web 执行 图 4-16 中所示的四个基本操作。

图 4-16 基本远程存储操作



下面将概述四个基本操作。

1. **登录到 XSCF Web**
使用远程存储首先要登录到 XSCF Web。选择远程存储菜单，然后打开配置远程存储的网页。
2. **启动 XSCF Remote Storage Server (XSCF 远程存储服务器) - [Launch] (启动)**
从 XSCF Web 上，启动 XSCF Remote Storage Server (XSCF 远程存储服务器) (启动)。启动 XSCF Remote Storage Server (XSCF 远程存储服务器) 将打开 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面，可进行选择/启动系统管理终端上的介质。从此画面上，选择/启动介质并显示介质的状态。

注 - 您仅可从 XSCF Web 启动 XSCF Remote Storage Server (XSCF 远程存储服务器)。XSCF shell 的任何命令均无法启动 XSCF Remote Storage Server (XSCF 远程存储服务器)。

3. **启动介质 - [Run] (运行)**
显示 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面后，选择终端的 CD/DVD 驱动器或 ISO 映像启动介质。此操作允许使用该终端的远程存储使用的网络端口，并设置 XSCF 连接的等待状态。
4. **连接到介质 - [Attach] (连接)**
从 XSCF Web 或 XSCF shell 连接到终端的目标介质。此时，需指定 XSCF-LAN 接口和终端的 IP 地址。这些操作能够从 OpenBoot PROM 和 Oracle Solaris 使用目标介质。
此时，当通过从 XSCF 访问介质时，您可以从 XSCF Web 和 XSCF shell 进行 XSCF 网络设置。此时不需要重新启动 XSCF。
您可以使用 `setremotestorage` 命令或 `showremotestorage` 命令连接到介质，这两者都是 XSCF 命令。有关各命令的详细信息，请参见该命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

有关各设置的详细信息，请参见 "4.6.12 使用远程存储时连接到介质"。

4.6.10 配置与远程存储一同使用的 XSCF-LAN

本节介绍与远程存储一同使用的 XSCF-LAN 的设置。

为了使用远程存储，必须配置 XSCF-LAN 接口网络。确定使用主、备用或从 XSCF 的 XSCF-LAN#0 或 XSCF-LAN#1 两者之一后，配置 XSCF 网络。

配置主/备用 XSCF 使用 XSCF Web

使用 XSCF Web 配置远程存储之前，您必须已经完成主/备用 XSCF 网络设置。这将启用 XSCF Web，其需要启用 HTTPS 服务。这些设置需要重新启动 XSCF。

使用 `setnetwork` 命令或 XSCF Web 的 [Network]（网络）页面进行 XSCF 网络设置。使用 `setremotestorage` 命令或 XSCF Web 的 [Remote Storage]（远程存储）页面无法进行这些设置。

有关主/备用 XSCF 网络设置和 HTTPS 服务设置的详细信息，请参见 "3.9 配置 XSCF 网络" 和 "3.8 配置用于登录 XSCF 的 HTTPS 服务"。

使用主/备用 XSCF

当通过所有主/备用机箱的 XSCF-LAN 使用远程存储器时，如果 "配置主/备用 XSCF 使用 XSCF Web" 中的设置已经完成，则无需配置 XSCF 网络。

注 - 如果使用主/备用 XSCF，当使用远程存储访问终端中的介质时，物理 IP 地址将用作 XSCF-LAN IP 地址。不使用接管的 IP 地址（虚拟地址）。

使用从 XSCF

通过从 XSCF 使用远程存储之前，需要已经完成主 XSCF 网络设置。配置远程存储之前或在配置的同时，您可以进行从 XSCF 网络设置。

使用 `setremotestorage` 命令或 XSCF Web 的 [Remote Storage]（远程存储）页面进行 XSCF 网络设置。使用 `setnetwork` 命令或 XSCF Web 的 [Network]（网络）页面无法进行这些设置。

而且，在连接到接线盒的系统中，通过作为 SPARC M12/M10 的从 XSCF 使用远程存储。因此，必须配置从 XSCF 网络。

使用 XSCF Web 进行从 XSCF 网络设置的步骤如下所述。有关使用 XSCF shell 设置的详情，请参见 `setremotestorage` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

1. 连接从 **XSCF (XSCF-LAN#0 或 XSCF-LAN#1)** 的 **XSCF LAN** 线缆。
2. 执行 `sethttps` 命令启用 HTTPS 服务。
3. 在主 **XSCF** 上登录到 **XSCF Web**。
4. 选择 **[Menu]**（菜单）- **[Settings]**（设置）- **[Remote Storage]**（远程存储）。

5. 从远程存储网络配置表中的 **Interface**（接口），选择从 **XSCF** 的 **XSCF-LAN#0** 或 **XSCF-LAN#1**。然后，点击 **[Configure]**（配置）按钮。
6. 在所显示的画面上设置 **IP** 地址、子网掩码和网关，然后点击 **[OK]** 按钮。
7. 参考远程存储网络配置表，确认所有这组数据正确。
从 XSCF 的网络设置不需要重新启动 XSCF。

4.6.11 XSCF Remote Storage Server（XSCF 远程存储服务器）的状态

本节将介绍在 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面顶部的 Status（状态）显示。

来自 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面和 XSCF Web 的远程存储操作将刷新 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面顶部的 Status（状态）显示。您可使用 Status（状态）的数据，查看 XSCF 和终端中介质之间的连接状态。

表 4-6 列出了从远程存储操作的 [XSCF Remote Storage Server] 画面上的状态转换。

表 4-6 远程存储操作 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面上的 Status（状态）变化

操作	状态
连接	
XSCF Remote Storage Server（XSCF 远程存储服务器）启动后立即 （在 XSCF Web 上点击 [Launch]（启动）按钮）	已断开
在 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面选择目标介质	已断开
在 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面点击 [Run]（运行）	等待来自 XSCF 的连接
在 XSCF Web 上点击 [Attach]（连接）按钮	已连接
断开	
通过点击 [Attach]（连接）按钮连接	已连接
在 XSCF Web 上点击 [Detach]（分离）按钮	等待来自 XSCF 的连接
在 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面点击 [Stop]（停止）	已断开
弹出	
通过点击 [Attach]（连接）按钮连接	已连接
从 Oracle Solaris 执行弹出	已弹出
在 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面点击 [Run]（运行）	等待来自 XSCF 的连接
点击上述 [Run]（运行）按钮几秒钟后	已连接

表 4-7 列出了显示在 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面顶部的 Status (状态) 的含义。

表 4-7 XSCF Remote Storage Server (XSCF 远程存储服务器) Status (状态) 的含义

状态	含义
已断开	终端中的介质已经从 XSCF 断开。
等待来自 XSCF 的连接	终端中的介质可连接并正在等待来自 XSCF 的连接。
已连接	终端中的介质已连接到 XSCF。
已弹出	从 Oracle Solaris 已执行 eject 命令。

4.6.12 使用远程存储时连接到介质

本节将介绍使用远程存储时连接到终端中介质的操作。请注意，仅允许只读的介质。不允许写入。

将分成以下三种情况进行说明：

- 物理分区停止
- 控制域在 ok 提示符下
- 控制域上正在运行 Oracle Solaris

在上述三种情况下，连接到介质的基本操作均相同。然而，介质连接后，控制域的操作将不同。上述情况的基本操作与 "物理分区停止" 的内容相同。

注 - 如需在来宾域使用远程存储，需分配资源 (ldm add-vdisk)。

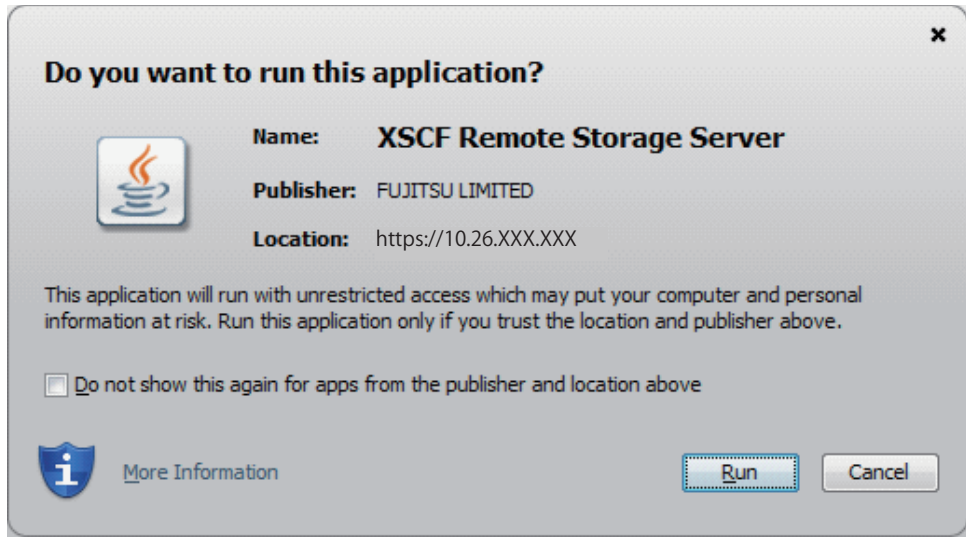
注 - 当使用远程存储时，我们的建议是，在物理分区或控制域启动或停止过程期间，不执行连接到介质的任何操作。这可以防止物理分区和控制域启动和停止过程中的较长处理时间。根据不同的时机，如果物理分区或控制域启动过程中连接介质，OpenBoot PROM 可能无法识别目标介质。因此，控制域将需要被再次复位。

以下步骤假定 "4.6.9 使用远程存储的流程" 中 "使用远程存储之前" 中的操作已完成。

物理分区停止

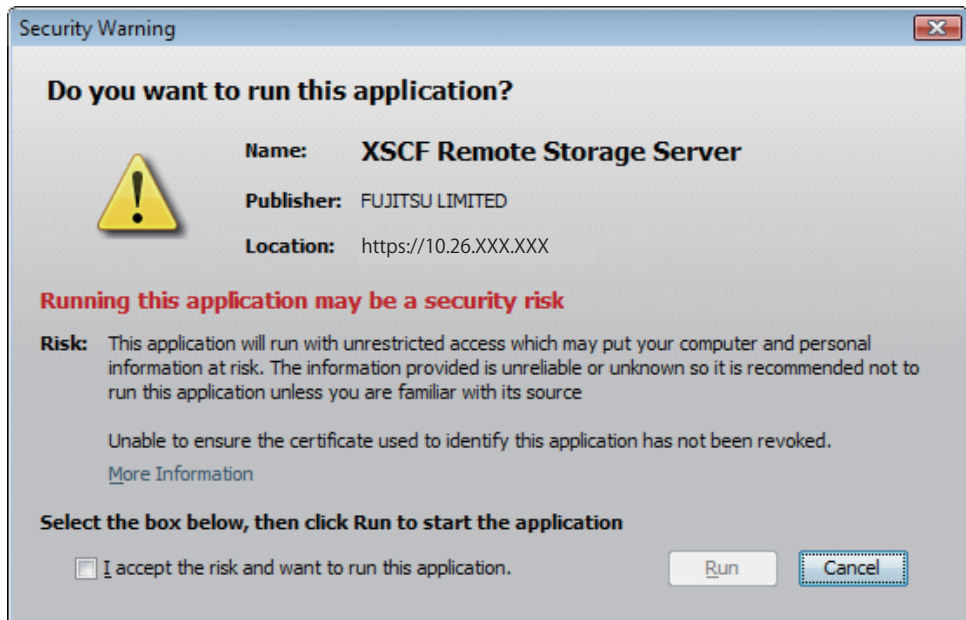
1. 从系统管理终端登录到 XSCF Web。
2. 选择 [Menu] (菜单) - [Settings] (设置) - [Remote Storage] (远程存储)。
3. 点击 Remote Storage Server (远程存储服务器) 上的 [Launch] (启动) 按钮。
图 4-17 画面出现。点击该画面上的 [Run] (运行) 按钮，显示 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面。

图 4-17 点击 [Launch]（启动）按钮时的消息



如果无法确认 XSCF 远程存储服务器的签名证书的有效性，则会输出如图 4-18 中所示的安全警告。勾选 [I accept the risk and want to run this application]（我接受风险并希望运行此应用程序）复选框，然后单击 [Run]（运行）按钮。

图 4-18 安全警告消息



如果使用 Windows 防火墙，将输出“图 4-15 使用 Windows 防火墙时的警告消息”中显示的警告消息。按照“4.6.4 终端和浏览器的使用要求”中“终端上使用的端口和权限”中的步骤进行操作。

4. 选择显示在 **[XSCF Remote Storage Server]** (XSCF 远程存储服务器) 画面上的 **CD/DVD 驱动器** 的介质或 **ISO 映像**。

如果画面上没有显示介质, 则可能没有介质插入该终端的 CD/DVD 驱动器, 或可能没有添加 ISO 映像。如果没有介质插入 CD/DVD 驱动器, 请插入介质, 然后点击画面顶部的 **[Refresh]** (刷新) 按钮。或者, 点击 **[Add ISO file]** (添加 ISO 文件) 按钮, 显示 ISO 映像列表。从显示的列表中选择目标介质。

[XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面顶部的 **Status** (状态)、**Selected media** (选定的介质) 和 **XSCF IP Address** (XSCF IP 地址) 中的每一行, 均刷新, 如下所示。有关 **Status** (状态) 的含义, 请参见“4.6.11 XSCF Remote Storage Server (XSCF 远程存储服务器) 的状态”。

Status (状态)	已断开
Selected media (选定的介质)	选定介质的路径
XSCP IP Address (XSCF IP 地址)	无

5. 点击 **[XSCF Remote Storage Server]** (XSCF 远程存储服务器) 画面上的 **[Run]** (运行) 按钮。

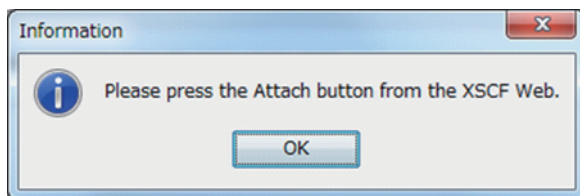
此操作允许通过远程存储来使用终端的网络端口。选定的目标介质等待来自 XSCF 的连接。

[XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面顶部的 **Status** (状态)、**Selected media** (选定的介质) 和 **XSCF IP Address** (XSCF IP 地址) 中的每一行, 均刷新, 如下所示。

Status (状态)	等待来自 XSCF 的连接
Selected media (选定的介质)	选定介质的路径
XSCP IP Address (XSCF IP 地址)	无

执行时, 此操作将显示用于从 XSCF Web 执行 "Attach" (连接) 操作的 **[Information]** (信息) 画面, 如 **图 4-19** 所示。点击 **[OK]** 按钮可返回 XSCF Web 控制台。

图 4-19 **[Information]** (信息) 画面



6. 从 **XSCF Web** 的远程存储网络配置表的 **Interface** (接口) 栏中, 选择将要连接到目标介质的 **XSCF-LAN** 接口。

如果未配置 XSCF-LAN 接口网络, 请参见“4.6.10 配置与远程存储一同使用的 XSCF-LAN”。然后, 配置该网络。

7. 点击 **[Attach]** (连接) 按钮连接到介质。

将出现指定终端 IP 地址的画面。确认 IP 地址正确后, 单击 **[OK]** 按钮。

远程存储网络配置表中的 **Connection** (连接) 将显示终端的 IP 地址。以这种方式, 连接了 XSCF 和目标介质。

[XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面顶部的 **Status** (状态)、**Selected media** (选定的介质) 和 **XSCF IP Address** (XSCF IP 地址) 中的每一行, 均刷新, 如下所示。

Status (状态) 已连接
Selected media (选定的介质) 选定介质的路径
XCP IP Address (XSCF IP 地址) 所连接 XSCF-LAN 的物理 IP 地址

8. 执行 **poweron** 命令来开启物理分区的电源。

注 - 如需将控制域停止在 ok 提示符处, 请使用 **setenv** 命令将 OpenBoot PROM 环境变量 **auto-boot?** 变更为 **false**。

[示例]

```
XSCF> setpparam -p 0 -s bootscript "setenv auto-boot? false"
```

9. 从 **Oracle Solaris** 执行 **cfgadm -al** 命令, 确认远程存储设备路径是否已添加。

```
# cfgadm -al
Ap_Id          Type          Receptacle    Occupant      Condition
...
usb1/3         usb-storage   connected     configured    ok
```

注 - 如果控制域中未使用远程存储, 则没有必要执行步骤 10 的操作。如需在来宾域使用远程存储, 需分配资源 (**ldm add-vdisk**)。

10. 如果目标介质尚未添加, 则使用 **Oracle Solaris** 的 **mount** 命令进行加载。

下面是检查目标介质安装状态的示例。由于远程存储设备没有自动安装, 因此将要安装目标介质。

有关 **mount** 命令的详情, 请参见您所使用版本的《Oracle Solaris Reference Manual》。

注 - 有关启用可移动介质管理服务的步骤, 请参见 "4.6.5 Oracle Solaris 的设置"。

```
# df
/                (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices         (/devices        ):          0 blocks 0 files
...
# mount -F hsfs /dev/dsk/c4t0d0s2 /media/xxxxx
```

/dev/dsk/c4t0d0s2 指定了远程存储的设备路径名。

有关 **mount** 命令的详情, 请参见您所使用版本的《Oracle Solaris Reference Manual》。

现在, 您可以从目标介质安装软件、读取文件并进行其他操作。请注意, 您无法写入目标介质。

注 - 如果控制域处于 ok 提示符下, 则执行 **show-disks** 命令, 并确认远程存储设备路径是否已添加。

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

控制域在 ok 提示符下

1. 执行 "物理分区停止" 中的步骤 1 到 7。
2. 从 **XSCF Shell** 执行 **console** 命令切换到处于 **ok** 提示符下的控制域控制台。
下面的示例显示了切换到的物理分区#0 的控制域控制台。

```
XSCF> console -p 0
```

3. 执行 **reset-all** 命令重置处于 **ok** 提示符下的控制域。

```
{0} ok reset-all
```

注 - 如需当控制域再次停止在 **ok** 提示符下时重置控制域，需使用 **setenv** 命令将 **OpenBoot PROM** 环境变量 **auto-boot?** 的值变更为 **false**。

4. 在已重置的控制域的 **ok** 提示符下，执行 **show-disks** 命令，并确认远程存储设备路径是否已添加。

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

您可以从目标介质设置远程存储设备的别名、安装 Oracle Solaris 和执行其他操作。

控制域上正在运行 Oracle Solaris

1. 执行 "物理分区停止" 中的步骤 1 到 7。
2. 从 **XSCF Shell** 执行 **console** 命令切换到 **Oracle Solaris** 正在运行的控制域控制台。
下面的示例显示了切换到的物理分区#0 的控制域控制台。

```
XSCF> console -p 0
```

3. 从 **Oracle Solaris** 执行 **df** 命令或 **cfgadm -al** 命令，确认远程存储设备路径是否已添加。

注 - 如果可移动介质管理服务是 **enabled**（设置为启用），当 XSCF 连接到远程存储时，远程存储设备将被自动安装。有关启用可移动介质管理服务的步骤，请参见 "4.6.5 Oracle Solaris 的设置"。

下面的示例执行 **df** 命令，并表明远程存储设备上的 **/media** 已自动安装。

```
# df
/                (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices         (/devices           ):          0 blocks 0 files
...
/media/DISC-LABEL(/dev/dsk/c4t0d0s2 ):          0 blocks 0 files
```

下面的示例执行 **cfgadm** 命令，并表明类型为 **usb-storage** 的远程存储设备 (**usb1/3**) 已添加。

```
# cfgadm
Ap_Id           Type           Receptacle      Occupant        Condition
...
usb1/3          usb-storage    connected       configured      ok
```

注 - 如果控制域中未使用远程存储，则没有必要执行步骤 4 的操作。如需在来宾域使用远程存储，需分配资源 (**ldm add-vdisk**)。

4. 如果远程存储设备尚未安装，需使用 **mount** 命令进行安装。
下面的示例表明远程存储设备尚未自动安装，因此将要被安装。

```
# df
/                (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices         (/devices           ):          0 blocks 0 files
...
# mount -F hsfs /dev/dsk/c4t0d0s2 /media/xxxxx
```

/dev/dsk/c4t0d0s2 指定了远程存储的设备路径名。

有关 **mount** 命令的详情，请参见您所使用版本的《Oracle Solaris Reference Manual》。

现在，您可以从目标介质安装软件、读取文件并进行其他操作。请注意，您无法写入目标介质。

4.6.13 从 Oracle Solaris 使用远程存储

本节将介绍使用远程存储的示例。

下面两个示例的介绍涉及到 SPARC M10-1:

- 安装 Oracle Solaris
- 切换介质

安装 Oracle Solaris

如下文所述，本例在 SPARC M10-1 控制域安装了 Oracle Solaris。

1. 从 **XSCF Shell** 执行 **console** 命令切换到处于 **ok** 提示符下的控制域控制台。
下面的示例显示了切换到物理分区#0 的控制域控制台。

```
XSCF> console -p 0
```

2. 从 **CD/DVD 驱动器** 中的目标介质安装 **Oracle Solaris**。
下面的示例显示了查看当前设置的设备别名和所查看设备别名的规格。如果省略了别名编号，从存储中使用较小的 LSB 编号。

```
{0} ok devalias  
{0} ok boot rcdrom
```

下面是显示指定设备路径的示例。

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3/disk@0
```

注 - 有关 SPARC M12/M10 型号的设备路径的详细信息，请参见“附录 A SPARC M12/M10 系统设备路径列表”。有关驱动器别名的详情，请参见“附录 J DVD 驱动器别名列表”。

切换介质

这里所介绍的步骤从 Oracle Solaris 执行 **eject** 命令切换远程存储使用的 CD/DVD 驱动器的介质或 ISO 映像。

注 - 如需切换介质，需从 Oracle Solaris 执行 **eject** 命令。远程存储不支持使用终端的 CD/DVD 驱动器上的弹出按钮切换介质。如果使用弹出按钮切换介质，则可能不识别数据大小的变化，并可能发出警告消息。在这种情况下，首先执行 **eject** 命令。然后，您需要再次点击 XSCF Remote Storage Server（XSCF 远程存储服务器）中的 [Run]（运行）按钮。

1. 从 **XSCF Shell** 执行 **console** 命令切换到 **Oracle Solaris** 正在运行的控制域控制台。
下面的示例显示了切换到物理分区#0 的控制域控制台。

```
XSCF> console -p 0
```

2. 使用 **eject** 命令移除目标介质。
使用 **eject** 命令，通过指定的选项，您可以显示设备名称和昵称的对应列表。下面

的示例显示了使用 Oracle Solaris 11 时，在 eject 命令中指定了 -l 选项。

```
# eject -l  
/dev/dsk/c4t0d0s2      cdrom, cdrom0, cd, cd0, DISC-LABEL, /media/DISC-LABEL
```

下面的示例显示在远程存储设备上指定的 /media。

```
# eject /media/DISC-LABEL
```

执行时，此操作将显示 XSCF 远程存储服务器的 [Information]（信息）画面，如图 4-20 所示。点击 [OK] 按钮可返回 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面。

图 4-20 [Information]（信息）画面



[XSCF Remote Storage Server]（XSCF 远程存储服务器）画面顶部的 Status（状态）、Selected media（选定的介质）和 XSCF IP Address（XSCF IP 地址）中的每一行，均刷新，如下所示。有关 Status（状态）的含义，请参见“4.6.11 XSCF Remote Storage Server（XSCF 远程存储服务器）的状态”。

Status（状态） 已弹出
Selected media（选定的介质） 无
XCP IP Address（XSCF IP 地址） 无

注 - 有关每个 SPARC M12/M10 型号的设备路径和设备别名的详细信息，请分别参见“附录 A SPARC M12/M10 系统设备路径列表”和“附录 J DVD 驱动器别名列表”。

3. 切换 CD/DVD 驱动器中的介质，或重新选择 ISO 映像。
4. 点击 [XSCF Remote Storage Server]（XSCF 远程存储服务器）画面上的 [Refresh]（刷新）按钮，然后选择 CD/DVD 驱动器。
点击 [Refresh]（刷新）按钮将刷新画面上的系统驱动器信息。当再次选择了 CD/DVD 驱动器时，将刷新画面上选定的介质信息。

[XSCF Remote Storage Server]（XSCF 远程存储服务器）画面顶部的 Status（状态）、Selected media（选定的介质）和 XSCF IP Address（XSCF IP 地址）中的每一行，均刷新，如下所示。

Status（状态） 已弹出
Selected media（选定的介质） 选定介质的路径

XSCP IP Address (XSCF IP 地址) 无

5. 点击 **[XSCF Remote Storage Server]** (XSCF 远程存储服务器) 画面上的 **[Run]** (运行) 按钮。

此操作允许通过远程存储来使用终端的目标介质。

[XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面顶部的 **Status** (状态)、**Selected media** (选定的介质) 和 **XSCF IP Address** (XSCF IP 地址) 中的每一行, 均刷新, 如下所示。

Status (状态)	已连接
Selected media (选定的介质)	选定介质的路径
XSCP IP Address (XSCF IP 地址)	所指定 XSCF-LAN 的物理 IP 地址

注 - 如需切换 ok 提示符下的介质, 需执行以下步骤。

1. 执行 "4.6.14 从介质断开/结束远程存储" 中 "物理分区停止" 中的步骤 1 到 6。然后, 执行 "控制域在 ok 提示符下" 中的步骤 2 到 4。
 2. 切换 CD/DVD 驱动器中的介质, 或重新选择 ISO 映像。
 3. 执行 "4.6.12 使用远程存储时连接到介质" 中 "物理分区停止" 中的步骤 4 到 7。然后, 执行 "控制域在 ok 提示符下" 中的步骤 2 到 4。
-

4.6.14 从介质断开/结束远程存储

本节将介绍从所使用终端中的介质断开以及结束远程存储的操作。

将分成以下三种情况进行说明:

- 物理分区停止
- 控制域在 ok 提示符下
- 控制域上正在运行 Oracle Solaris

在上述三种情况下, 从介质断开/结束远程存储的基本操作均相同。然而, 介质断开/远程存储结束之前和之后, 控制域的操作将不同。上述情况的基本操作与 "物理分区停止" 内容相同。

物理分区停止

1. **XSCF Remote Storage Server** (XSCF 远程存储服务器) 正在运行。确认画面顶部的 **Status** (状态)、**Selected media** (选定的介质) 和 **XSCF IP Address** (XSCF IP 地址) 的每一行的状态如下。

Status (状态)	已连接
Selected media (选定的介质)	选定介质的路径
XSCP IP Address (XSCF IP 地址)	所指定 XSCF-LAN 的物理 IP 地址

2. 从系统管理终端登录到 **XSCF Web**。
3. 选择 **[Menu]** (菜单) - **[Settings]** (设置) - **[Remote Storage]** (远程存储)。
4. 从远程存储网络配置表中的 **Interface** (接口) 栏, 选择用于断开终端的目标介质的 **XSCF-LAN** 接口。
5. 点击 **[Detach]** (分离) 按钮。
远程存储网络配置表中的 **Connection** (连接) 将显示 "Available" (可用)。此操作从目标介质断开 XSCF。当 XSCF Remote Storage Server (XSCF 远程存储服务

器)正在运行时,您可以通过点击 [Attach] (连接)按钮重新连接介质。

[XSCF Remote Storage Server] (XSCF 远程存储服务器)画面顶部的 Status (状态)、Selected media (选定的介质)和 XSCF IP Address (XSCF IP 地址)中的每一行,均刷新,如下所示。

```
Status (状态)          等待来自 XSCF 的连接
Selected media (选定的介质)  选定介质的路径
XCP IP Address (XSCF IP 地址)  无
```

6. 如需断开目标介质,需点击 [XSCF Remote Storage Server] (XSCF 远程存储服务器)画面上的 [Stop] (停止)按钮。

出现确认消息。点击 [OK] 按钮。

此操作将断开目标介质。然而,即使执行了此操作之后,仍然可以使用远程存储所用终端的网络端口。再次点击 [Run] (运行)按钮将导致目标介质等待来自 XSCF 的连接。

[XSCF Remote Storage Server] (XSCF 远程存储服务器)画面顶部的 Status (状态)、Selected media (选定的介质)和 XSCF IP Address (XSCF IP 地址)中的每一行,均刷新,如下所示。

```
Status (状态)          已断开
Selected media (选定的介质)  选定介质的路径
XCP IP Address (XSCF IP 地址)  无
```

7. 如需结束远程存储,需点击 [XSCF Remote Storage Server] (XSCF 远程存储服务器)画面右上角的 [x]。

画面关闭并结束远程存储。

控制域在 ok 提示符下

1. 执行 "物理分区停止" 中的步骤 1 到 7。
2. 从 XSCF Shell 执行 **console** 命令切换到处于 ok 提示符下的控制域控制台。下面的示例显示了切换到物理分区#0 的控制域控制台。

```
XSCF> console -p 0
```

3. 执行 **reset-all** 命令重置处于 ok 提示符下的控制域。

```
{0} ok reset-all
```

注 - 如需当控制域再次停止在 ok 提示符下时重置控制域,需使用 **setenv** 命令将 OpenBoot PROM 环境变量 **auto-boot?** 的值变更为 **false**。

4. 在已重置的控制域的 ok 提示符下,执行 **show-disks** 命令,并确认远程存储设备路径是否已删除。


```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

控制域上正在运行 Oracle Solaris

1. 从 **XSCF Shell** 执行 **console** 命令切换到 **Oracle Solaris** 正在运行的控制域控制台。
下面的示例显示了切换到的物理分区#0 的控制域控制台。

```
XSCF> console -p 0
```

2. 确认 **Oracle Solaris** 未正在访问目标介质。如果有必要，卸载远程存储设备。
下面是卸载远程存储设备的示例。

```
# cd /
# umount /media/xxxxx
```

3. 停止可移动介质管理服务。
下面是执行 **svcadm** 命令停止可移动介质管理服务的示例。
- 对于 Oracle Solaris 11 或更高版本

```
# svcadm disable hal
```

- Oracle Solaris 10 的情形

```
# svcadm disable volfs
```

注 - 如需在来宾域使用远程存储，需停止该来宾域的可移动介质管理服务。

4. 从 **Oracle Solaris** 执行 **cfgadm -c unconfigure** 命令，停止特定路径上的远程存储设备。
下面的示例执行 **cfgadm** 命令，并表明 **usb1/3** 是一个远程存储设备。

```
# cfgadm
Ap_Id          Type          Receptacle      Occupant        Condition
...
usb1/3         usb-storage   connected       configured      ok
```

下面的示例执行 **cfgadm -c unconfigure** 命令，并表明远程存储设备被停止。

注 - 如果远程存储 (vdisk) 的资源已经分配给来宾域，则断开该资源 (ldm remove-vdisk)，然后从控制域执行 `cfgadm -c unconfigure`。

```
# cfgadm -c unconfigure usb1/3
```

以下示例执行 `cfgadm` 命令并检查是否停止了 `usb1/3`。

```
# cfgadm
Ap_Id          Type          Receptacle      Occupant         Condition
...
usb1/3         usb-storage   connected       unconfigured     ok
```

5. 执行 **"物理分区停止"** 中的步骤 1 到 7。
6. 从 **Oracle Solaris** 执行 `df` 命令或 `cfgadm` 命令，确认远程存储设备路径是否已删除。

下面的示例执行 `df` 命令，并表明远程存储设备上的 `/media` 已删除。

```
# df
/              (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices      (/devices          ):          0 blocks 0 files
...
```

下面的示例执行 `cfgadm` 命令，并表明远程存储设备 (`usb1/3`) 被停止。

```
# cfgadm
Ap_Id          Type          Receptacle      Occupant         Condition
...
usb1/3         unkown        empty           unconfigured     ok
```

4.6.15 其他注意事项和操作

本节将介绍在使用远程存储时需要注意的事项和操作方法。

使用远程存储时发生错误的注意事项

从 `ok` 提示符或 Oracle Solaris 使用远程存储可能会发生异常事件，如 XSCF 重新启动、主/备用 XSCF 切换、XSCF-LAN 断开连接以及终端停止。域控制台上将输出错误结果或警告消息，并且 XSCF 上登记错误日志。

下面的示例显示了从 `ok` 提示符下安装 Oracle Solaris 后的错误消息的输出。

```
{0} ok boot rcdrom
Boot device: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@
3/disk@0,0:a File and args:
|
read failed
FCode aborted.
$boot failed
The file just loaded does not appear to be executable.
```

如果在 Oracle Solaris 上访问远程存储出现错误，则将检测到从 sd 驱动程序的错误并输出警告信息。下面的示例显示了由 sd 驱动程序输出的警告消息。

```
WARNING: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0 (sd5):
Error for Command: read(10)                Error Level: Retryable
Requested Block: 39665                      Error Block: 39665
Vendor: Fujitsu                             Serial Number:
Sense Key: Media_Error
ASC: 0x11 (unrecovered read error), ASCQ: 0x0, FRU: 0x0
```

```
WARNING: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0 (sd5):
SCSI transport failed: reason 'timeout': giving up
```

从所发生的错误恢复后，您可以通过执行 XSCF 和终端的各自操作恢复远程存储连接。请参见“使用远程存储过程中发生错误时的恢复操作”。

使用远程存储过程中发生错误时的恢复操作

本节介绍了使用远程存储过程中发生错误时的恢复操作。

1. 从系统管理终端登录到 **XSCF Web**。
2. 选择 **[Menu]**（菜单） - **[Settings]**（设置） - **[Remote Storage]**（远程存储）。
3. 检查远程存储网络配置表中的 **Connection**（连接）。
 - 如果显示 IP 地址，则执行步骤 4 及以后的操作。
 - 如果显示 "Available"（可用），则执行步骤 6 及以后的操作。
 - 如果显示 "Unavailable"（不可用），则 XSCF 重新启动正在进行中。进入 "Available"（可用）状态后，则执行步骤 6 及以后的操作。
4. 从远程存储网络配置表的 **Interface**（接口）栏中，选择将要连接到目标介质的 **XSCF-LAN** 接口。
5. 点击 **[Detach]**（分离）按钮。
6. 查看 **[XSCF Remote Storage Server]**（XSCF 远程存储服务器）画面上的 **Status**（状态）。

如果显示 "Waiting for connection from XSCF"（等待来自 XSCF 的连接），则执行步骤 8 及以后的操作。

如果显示 "Connected"（已连接），则点击 **[Stop]**（停止）按钮。出现确认消息。点击 **[OK]** 按钮。

注 - 如果已经显示 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面, 则没有必要在 XSCF Web 中 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面上执行 Launch (启动) 操作。

注 - 如果远程存储网络配置表中的 Connection (连接) 是 "Available" (可用), 则 "Connected" (已连接) 将显示在 [XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面上。因此, 点击 [Stop] (停止) 按钮可将 Status (状态) 变更为 "Disconnected" (已断开)。

- 再次点击 **[XSCF Remote Storage Server]** (XSCF 远程存储服务器) 画面上的 **[Run]** (运行) 按钮。
目标介质等待来自 XSCF 的连接。
- 从 **XSCF Web** 的远程存储网络配置表的 **Interface** (接口) 栏中, 选择将要连接到目标介质的 **XSCF-LAN** 接口。
- 点击 **[Attach]** (连接) 按钮。
此时, 将出现指定终端 IP 地址的画面。确认 IP 地址是否正确, 然后点击 [OK] 按钮。

远程存储网络配置表中的 Connection (连接) 将显示终端的 IP 地址。此操作将 XSCF 连接到目标介质。

[XSCF Remote Storage Server] (XSCF 远程存储服务器) 画面顶部的 Status (状态)、Selected media (选定的介质) 和 XSCF IP Address (XSCF IP 地址) 中的每一行, 均刷新, 如下所示。

Status (状态)	已连接
Selected media (选定的介质)	选定介质的路径
XSCP IP Address (XSCF IP 地址)	所连接 XSCF-LAN 的物理 IP 地址

- 当 **Oracle Solaris** 正在运行时, 使用远程存储登录到域。然后, 执行 **cfgadm** 命令和 **df** 命令, 并确认远程存储可使用。在 **ok** 提示符下, 执行 **show-disks** 命令, 并确认远程存储设备路径是否已添加。

下面的示例在 Oracle Solaris 上执行 **cfgadm** 命令。

```
# cfgadm
Ap_Id           Type           Receptacle      Occupant         Condition
...
usb1/3         usb-storage   connected       configured       ok
```

下面的示例在 **ok** 提示符执行 **show-disks** 命令。

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...

Enter Selection, q to quit:
```

CPU 激活

必须激活 CPU 内核才能在 SPARC M12/M10 中使用 CPU 内核资源。本章概括介绍如何管理 CPU 内核。您可以在 SPARC M12/M10 中动态添加或移除工作 CPU 内核，以便更好满足工作负荷要求。

- CPU 激活的基本概念
- CPU 激活密钥
- 添加 CPU 内核资源
- 删除 CPU 内核资源
- 移动 CPU 内核资源
- 查看 CPU 激活信息
- 保存/恢复 CPU 激活密钥
- CPU 激活异常的故障排除
- CPU 激活的重要注意事项

5.1 CPU 激活的基本概念

您可以动态扩展或缩减 SPARC M12/M10 中的 CPU 内核资源，而无需中断系统运行，满足您的工作负荷要求。本功能可灵活使用 CPU 内核资源，从而可以在必要时根据需要增加 CPU 内核资源，同时降低初始服务器成本。

CPU 的成本占以前的服务器的大部分投资，因为以芯片单元购买 CPU 内核资源。此外，软件的成本直接与内核的总数有关，因为很多软件的许可证基于系统内核的数量。

在 SPARC M12/M10 中，CPU 激活功能允许您以比一个 CPU 芯片更细的粒度购买 CPU 内核。

注 - SPARC M12/M10 需要最少数量激活的 CPU 内核即可运行。此外，SPARC M12/M10 CPU 激活在购买时可从存储器和 I/O（PCI Express 插槽、板载设备和端口以及内部存储器）中拆开 CPU 内核。即使指定的 CPU 芯片中没有激活的内核，内存和 I/O 仍可使用。您可不受激活 CPU 内核数量的影响，独立使用 DIMM 槽、PCI Express 槽、板载设备和端口。

如需启用 CPU 内核，您需要购买 CPU 激活，即使用 CPU 内核的权利。当您购买 CPU 激活时，您可以获得使 CPU 内核资源可用的 CPU 激活密钥。各服务器 CPU 激活的购买单位如下。

表 5-1 CPU 激活购买单位

服务器	最小所需内核数	购买单位
SPARC M12-1	1 个内核	1 个内核 (1 套)
SPARC M12-2	2 个内核	1 个内核 (1 套)
SPARC M12-2S	2 个内核	1 个内核 (1 套)
SPARC M10-1	2 个内核	2 个内核 (1 套)
SPARC M10-4	4 个内核	2 个内核 (1 套)
SPARC M10-4S	4 个内核	2 个内核 (1 套)

初始服务器安装之前，CPU 激活密钥已在工厂注册到 XSCF。不但在初始服务器安装期间，而且即使在应用于生产的系统正在运行时也可以激活额外的 CPU 激活密钥。将 CPU 激活密钥注册到 XSCF 后，需要将 CPU 内核资源分配给物理分区。某些类型软件的许可证编号和形式根据所使用的 CPU 内核的数量而有所不同。添加需要使用的 CPU 内核时，请确认软件的许可条款。

注 - 在 SPARC M12/SPARC M10 中，一个 CPU 内核具有多个线程。Oracle Solaris 将每个硬件线程识别为一个虚拟 CPU (vCPU)。

在 SPARC M12 中，使用一组 CPU 激活来激活一个 CPU 内核，可使八个虚拟 CPU 可用于 Oracle Solaris。

在 SPARC M10 中，使用一组 CPU 激活来激活两个 CPU 内核，可使四个虚拟 CPU 可用于 Oracle Solaris。

CPU 激活密钥可以在同一型号的单元之间移动。可以删除注册在服务器上的 CPU 激活密钥并在其他服务器上注册。

可以按照如下所示移动 CPU 激活：

- SPARC M12-1 ==> SPARC M12-1
- SPARC M12-2 ==> SPARC M12-2
- SPARC M12-2S ==> SPARC M12-2S
- SPARC M10-1 ==> SPARC M10-1
- SPARC M10-4 ==> SPARC M10-4
- SPARC M10-4S ==> SPARC M10-4S

CPU 激活不能在上述之外的型号之间移动：

5.2 CPU 激活密钥

可以通过购买 CPU 激活获得 CPU 激活密钥。密钥在 CD-ROM 上。每个 CPU 激活密钥包含一组代表加密的 CPU 激活信息字符串。

CD-ROM 包含如下内容:

/readme_ja.txt : 日语自述文件
/readme_en.txt : 英语自述文件
/Activation_key/ : 包含激活文件的目录
/Activation_key/\$KEY_FILES (多个文件)
: 每个文件包含 1 组 CPU 激活。
/Activation_key/\$CONSOLIDATED_KEY_FILES
: 一个文件包含来自每个 \$KEY_FILES 的所有 CPU 激活密钥信息。
/Certificate/Certificate.pdf
: 硬件激活证书

\$KEY_FILES 和 \$CONSOLIDATED_KEY_FILES 是具有如下格式文件名的纯文本文件:

\$KEY_FILES : AK11111_01_001.txt
\$CONSOLIDATED_KEY_FILES
: AK11111_01.txt

以下示例显示 SPARC M10 中一组 CPU 激活密钥 (2 个内核) 上的激活文件的内容。

```
Product: SPARC M10-1  
SequenceNumber: 1234567890123456  
Cpu: noExpiration 2  
Text-Signature-SHA256-RSA2048:  
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA.....
```

每组 CPU 激活密钥包含多行信息。每行由项目名和值组成, 之间用分隔符 ":" 连接。以下是示例。在这个示例中, 项目名是 "Cpu", 值是 "noExpiration 2"。请注意 1 组密钥包含两个 CPU 激活。

```
Cpu: noExpiration 2
```

表 5-2 CPU 激活密钥项目和可能的值

项目	值
Product	SPARC M12-2、SPARC M12-2S、SPARC M10-1、SPARC M10-4 或 SPARC M10-4S
SequenceNumber	1 到 16 位数的数字值
Cpu	CPU 容量 (单位: 内核) noExpiration + 最多 4 位数的数字值
Text-Signature-xxxxxx-xxxxxx	Signature

CPU 激活密钥数据存储在 XSCF 上。密钥信息也自动备份到 PSU 底板单元 (PSUBP)。如果 XSCF 故障并被更换，密钥信息从 PSUBP 恢复到新换的 XSCF 上。

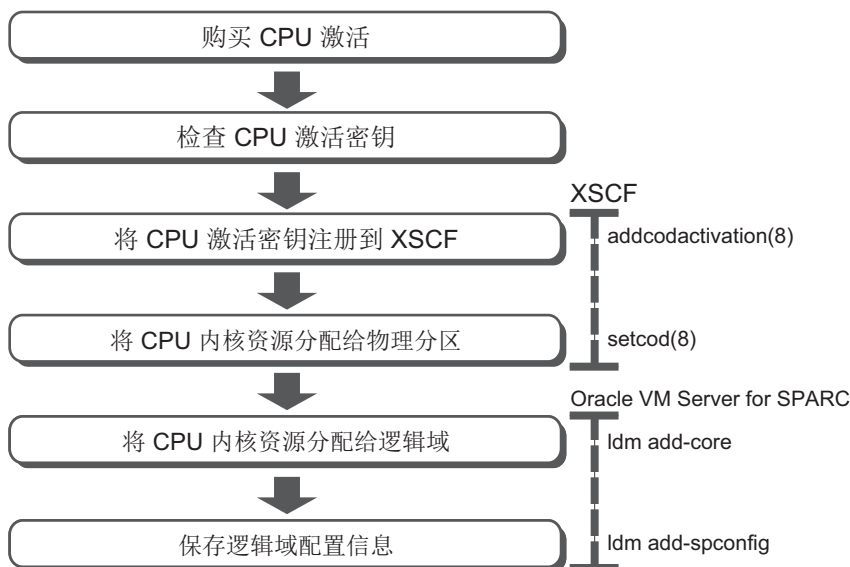
5.3 添加 CPU 内核资源

本节介绍在购买 CPU 激活后如何将 CPU 内核资源添加到物理分区和逻辑域。

5.3.1 将 CPU 内核添加到物理分区和逻辑域的工作流程

图 5-1 显示了从购买 CPU 激活到开始使用添加到物理分区和逻辑域的 CPU 内核资源的步骤。

图 5-1 将 CPU 内核添加到逻辑域的工作流程



5.3.2 购买添加的 CPU 激活

当 SPARC M12/M10 的负荷增加时，确认是否可以添加 CPU 内核资源。您可以在 XSCF shell 上使用 `showcodusage` 命令来查看物理分区中正在使用的内核的数量，所安装的 CPU 内核的数量以及分配给物理分区的 CPU 激活的数量。如果为物理分区设置的 CPU 激活数量小于所安装的 CPU 内核的数量，则可以添加 CPU 内核资源。有关详情，请参见“5.6.4 查看已激活 CPU 内核资源的使用状况”。如需购买添加的 CPU 激活，请联络当地的销售代表。如需支持所需的负载，您可以暂时使用 CPU 内核，直到 CPU 激活交付。有关详情，请参见“附录 K CPU 激活临时许可证”。

5.3.3 检查 CPU 激活密钥

在获得订购的 CPU 激活后，请确认每个收到的 CPU 激活密钥文件中的“产品”字段与您的型号名称相匹配。否则，CPU 激活密钥将无法注册。

5.3.4 登录 CPU 激活密钥

如需将 CPU 激活密钥注册到 XSCF，需在 XSCF shell 或 XSCF Web 上使用 `addcodactivation` 命令。本节介绍使用 XSCF shell 的步骤。为了执行这个命令，您需要具有 `platadm` 权限的用户账户。

```
XSCF> addcodactivation key-signature
```

指定接收的 CPU 激活密钥作为密钥签名。如需这样操作，需或者指定带 `-F` 选项的 USB 介质，或者复制并粘贴 CPU 激活密钥的内容。以下命令句法说明如何指定 USB 介质。

```
XSCF> addcodactivation -F file:///media/usb_msd/filename
```

如需注册存储在 CD-ROM 上的所有 CPU 激活密钥，需为文件名指定 `$CONSOLIDATED_KEY_FILES`。

注 - 在 XCP 2041 之前的版本中，无法指定 `$CONSOLIDATED_KEY_FILES`。

操作步骤

1. 用具有 `platadm` 权限的用户帐户登录 XSCF。
有关详情，请参见“2.2 登录 XSCF Shell”。
2. 执行 `addcodactivation` 命令将 CPU 激活密钥注册到 XSCF。
为了输入 CPU 激活密钥，需在执行 `addcodactivation` 命令时指定激活密钥的内容。复制并粘贴激活密钥的所有内容，或通过指定 `-F` 选项从文件中读取。
输入 `"y"`，确认信息。
下面是将 CPU 激活密钥添加到 SPARC M10-1 的示例。

```
XSCF> addcodactivation "Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048: U1VOVyxTUEFSQy1FbnRlcnByaXN1AA....."
Above Key will be added, Continue?[y|n]: y
XSCF>
```

3. 执行 `showcodactivation` 命令确认 CPU 激活密钥已被正确添加到 XSCF。

使用指定的 `-r` 选项，该命令显示添加的 CPU 激活密钥。

以下是 `showcodactivation` 命令输出结果的示例。

```
XSCF> showcodactivation -r
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyXTUEFSQy1FbnRlcnByaXNlAA.....
```

此时，对于在 Oracle Solaris 上的使用，CPU 内核资源尚未准备就绪。

如需使 CPU 内核资源准备就绪，需转到“[5.3.5 分配 CPU 内核资源到物理分区](#)”将其分配给物理分区。

4. 执行 `exit` 命令从 XSCF shell 注销。

如您在 XSCF shell 没有更多的任务，请从 XSCF 注销。

注 - 如果 CPU 激活密钥信息因意外操作而损坏，XSCF 可能需要 CPU 激活密钥。为了能够恢复，确保安全保管 CPU 激活密钥。

注 - 不允许将同一个 CPU 激活密钥添加到多个 SPARC M12/M10 单元。

5.3.5 分配 CPU 内核资源到物理分区

如需将 CPU 内核资源分配给物理分区，请从 XSCF shell 交互式操作执行 `setcod` 命令。您需要具有执行此命令的 `platadm` 权限。

```
XSCF> setcod [-p ppar_id] -s cpu
PROC Permits installed: XX cores
PROC Permits assigned for PPAR 0 (X MAX)
  [Permanent Xcores]
Permanent [X]: permits
PROC Permits assigned for PPAR 1 (X MAX)
  [Permanent Xcores]
Permanent [X]: permits
: 略
```

对于 `-p ppar_id`，指定分配 CPU 内核资源的物理分区 ID。如果 `permits` 操作数未被指定，该命令将启动一个交互式会话分配 CPU 内核资源。

如果所使用的 XSCF 固件的版本为 XCP 2260 或更高版本，您也可以执行以下命令。

`permits` 值为允许使用的 CPU 内核指定 CPU 激活的数量。

可以以一个 CUP 内核为单位指定 CPU 激活。

```
XSCF> setcod [[-q] -{y|n}] -p ppar_id -s cpu -c {set|add|del} permits
```

注 - 我们不建议使用以下面的方式指定的 `setcod` 命令。

```
XSCF> setcod -p ppar_id -s cpu permits
```

当 XCP 固件是 XCP 2260 或更高版本时，如需执行 `setcod` 命令，需指定 `-c` 选项或使用交互式操作。对于 XCP 2250 或更早版本，也需使用交互式操作。

原因如下。

- 在命令执行时，关于以所进行的设置实现变更，无确认消息 ([y/n]) 输出。
 - 当 CPU 激活分配给正在运行的物理分区的数量已经减少时，不输出警告消息。CPU 激活数量的任何不足，如由于许可被错误指定均可能导致系统停止。
-

可以使用 `setcod` 命令指定使用 `addcodactivation` 命令注册的最多 CPU 激活数量。

操作步骤

1. 用具有 `platadm` 权限的用户帐户登录 XSCF。
有关详情，请参见 ["2.2 登录 XSCF Shell"](#)。
2. 用 `setcod` 命令将 CPU 内核资源分配到物理分区。

注 - 如需使用 `-c set` 或不使用 `-c` 选项，则请勿在 `permits` 操作数中指定需要添加或删除的唯一数量。相反，指定当前设定的数量加上所添加分配的数量，或指定当前设定的数量减去已删除分配的数量。如果由于意外仅指定了需要添加/删除的数量，CPU 激活的数量可能降低，这可能导致系统停止。

以下是将四个 CPU 内核资源分配到物理分区 1 的示例。

```
XSCF> setcod -p 1 -s cpu -c set 4
PROC Permits assigned for PPAR 1 : 0 -> 4

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

以下是 CPU 内核资源被交互分配到物理分区的示例。

```
XSCF> setcod -s cpu
PROC Permits installed: 5 cores
PROC Permits assigned for PPAR 0 (5 MAX) [Permanent 2cores]
  Permanent [2]:1
PROC Permits assigned for PPAR 1 (4 MAX) [Permanent 0cores]
  Permanent [0]:4
PROC Permits assigned for PPAR 2 (0 MAX) [Permanent 0cores]
  Permanent [0]:
PROC Permits assigned for PPAR 3 (0 MAX) [Permanent 0cores]
  Permanent [0]:
PROC Permits assigned for PPAR 4 (0 MAX) [Permanent 0cores]
  Permanent [0]:
PROC Permits assigned for PPAR 5 (0 MAX) [Permanent 0cores]
```

```
Permanent [0]:
PROC Permits assigned for PPAR 6 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 7 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 8 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 9 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 10 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 11 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 12 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 13 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 14 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 15 (0 MAX) [Permanent 0cores]
Permanent [0]:
```

以下示例将两个 CPU 内核资源添加到物理分区 0。

```
XSCF> showcod -p 0
PROC Permits assigned for PPAR 0: 10
XSCF> setcod -p 0 -s cpu -c add 2
PROC Permits assigned for PPAR 0 : 10 -> 12

PROC Permits assigned for PPAR will be changed.
Continue? [y/n] :y

Completed.
XSCF> showcod -p 0
PROC Permits assigned for PPAR 0: 12
```

注 - 指定 **setcod -p 0 -s cpu -c set 12** 时，该命令得到相同的结果。

注 - XCP 2250 或更早版本的 XSCF 固件不支持 **-c add**、**-c delete** 和 **-c set** 选项。按如下所示指定 **setcod** 命令选项可交互式添加和删除分配。

```
XSCF> setcod -s cpu
```

3. 执行 **exit** 命令从 **XSCF shell** 注销。
如您在 **XSCF shell** 没有更多的任务，请从 **XSCF** 注销。

5.3.6 将 CPU 内核添加到逻辑域

如需将 CPU 内核分配给逻辑域，需使用 **add-core** 或 **set-core**，这两个命令均是

Oracle VM Server for SPARC 的 `ldm` 子命令。
有关详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的“第3章 域配置的操作”。

5.3.7 保存逻辑域配置信息

如需保存逻辑域配置信息，请执行 Oracle VM Server for SPARC 的 `ldm` 命令并指定子命令 `add-spconfig`。

```
primary# ldm add-spconfig config_name
```

对于 `config_name`，请指定用于在 XSCF 中保存逻辑域配置信息的文件名。

注 - `add-spconfig` 子命令不能重写已存在文件的配置信息。为 `config_name` 指定已存在文件的文件名之前，您需使用 `remove-spconfig` 子命令删除已存在文件。

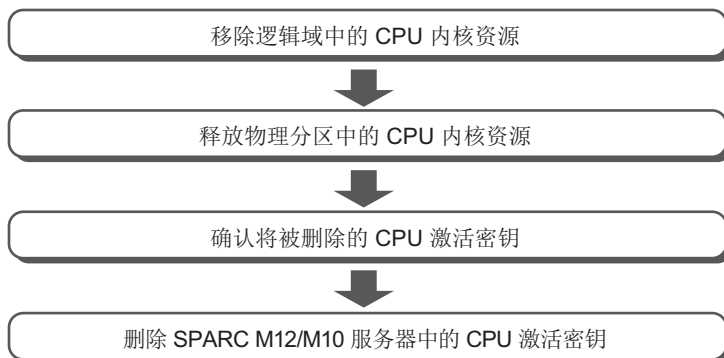
5.4 删除 CPU 内核资源

本节介绍如何从 SPARC M12/M10 中删除 CPU 激活。通常不需要删除 CPU 激活。将 CPU 激活移到另一台服务器时，需要将其从 SPARC M12/M10 中删除。有关移动步骤，请参见“5.5 移动 CPU 内核资源”。

5.4.1 删除 CPU 激活的工作流程

图 5-2 显示了删除 CPU 激活的步骤。

图 5-2 删除 CPU 激活的工作流程



5.4.2 移除逻辑域中的 CPU 内核

如需从逻辑域移除 CPU 内核，需使用 `remove-core` 或 `set-core`，这两个命令均是 Oracle VM Server for SPARC 的 `ldm` 子命令。
有关详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的“第3章 域配置的操作”。

5.4.3 释放物理分区中的 CPU 内核资源

如需从物理分区释放 CPU 内核资源，请使用 XSCF shell 的 `setcod` 命令。您可通过指定少于当前设置的 CPU 激活数量来释放 CPU 内核资源。

从 XSCF shell 以交互式操作的方式执行 `setcod` 命令。您需要具有执行此命令的 `platadm` 权限。

```
XSCF> setcod [-p ppar_id] -s cpu
```

如果所使用的 XSCF 固件的版本为 XCP 2260 或更高版本，您也可以执行以下命令。
`permits` 值为允许使用的 CPU 内核指定 CPU 激活的数量。
可以以一个 CUP 内核为单位指定 CPU 激活。

```
XSCF> setcod [[-q] -{y|n}] -p ppar_id -s cpu -c {set|add|del} permits
```

有关详情，请参见“5.3.5 分配 CPU 内核资源到物理分区”。

5.4.4 检查将被删除的 CPU 激活密钥

如需识别将被删除的 CPU 激活密钥，请使用 XSCF shell 的 `showcodactivation` 命令。
您可选择任何 CPU 激活密钥。
输入 `showcodactivation` 命令，您可列出带索引的 CPU 激活密钥。

```
XSCF> showcodactivation
Index   Description Count
-----
1 PROC          2
2 PROC          2
```

然后，找到决定删除的 CPU 激活密钥的索引号。接着使用 `showcodactivation` 命令确认由索引识别的 CPU 激活密钥信息。
例如，如果您将删除 `index=1` 的 CPU 激活密钥。输入以下命令，识别如下将被删除的 CPU 激活密钥。

```
XSCF> showcodactivation -r -i 1
*Index1
Product: SPARC M10-1
```

```
SequenceNumber: 116
Cpu noExpiration 2
Text-Signature-SHA256-RSA2048:
SBxYBSmB32E1ctOidgWV09nGFnWKNtCJ5N3WSlowbRUY1VVySvjncfOrDNteFLzo
.
.
1TSgrjnee9FyEYITT+ddJQ==
```

如需记录将被删除的 CPU 激活密钥信息，您需复制和粘贴密钥的全部内容或将它们记录后用于保存。

5.4.5 删除 CPU 激活密钥

如需从 SPARC M12/M10 的 XSCF 中删除 CPU 激活密钥，需在 XSCF shell 上使用 `deletecodactivation` 命令。
您需要具有执行此命令的 `platadm` 权限。

```
XSCF> deletecodactivation -i key-index
```

指定将被删除的 CPU 激活密钥的索引号。
`deletecodactivation` 命令不允许您以这样的方式（通过 `setcod` 命令数量变得小于为 PPAR 设置的 CPU 激活总数）删除 CPU 激活密钥。
提前减少为 PPAR 设置的 CPU 激活数量。

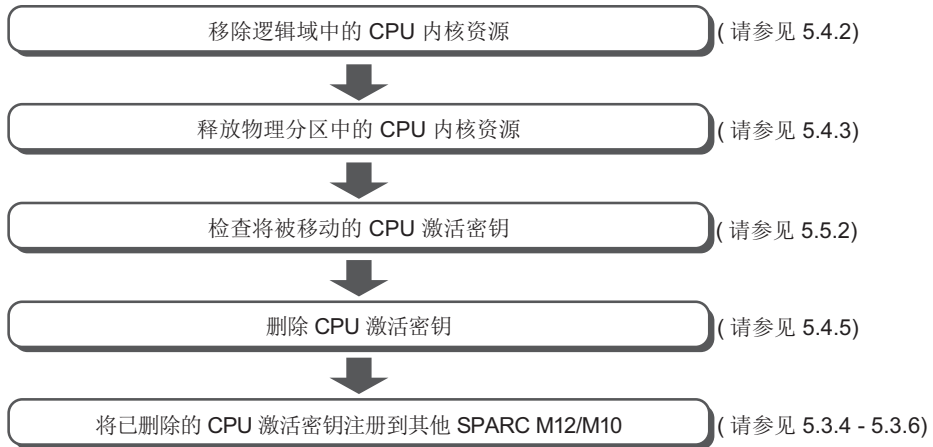
5.5 移动 CPU 内核资源

使用多个 SPARC M12/M10 单元时，仅能在相同型号之间移动 CPU 激活。

5.5.1 CPU 激活移动工作流程

图 5-3 显示了移动 CPU 激活的步骤。

图 5-3 CPU 激活移动工作流程



注 - 如果 SPARC M12/M10 系统出现故障，则可将故障 SPARC M12/M10 系统上的 CPU 激活密钥注册在其他 SPARC M12/M10 系统上。您不需要从故障系统中删除密钥。

5.5.2 检查将被移动的 CPU 激活密钥

如需识别将被移动的 CPU 激活密钥，请使用 XSCF shell 的 `showcodactivation` 命令。您可以选择任何 CPU 激活密钥，查看其信息。

输入 `showcodactivation` 命令，您可列出带索引的 CPU 激活密钥。

```
XSCF> showcodactivation
Index   Description Count
-----
      1  PROC           2
      2  PROC           2
```

然后，找到决定移动的 CPU 激活密钥的索引号。

接着使用 `showcodactivation` 命令确认由索引识别的 CPU 激活密钥信息。例如，如果您将移动 `index=1` 的 CPU 激活密钥。然后，输入以下命令，识别如下将被移动的 CPU 激活密钥的信息。

```
XSCF> showcodactivation -r -i 1
*Index1
Product: SPARC M10-1
SequenceNumber: 116
Cpu noExpiration 2
Text-Signature-SHA256-RSA2048:
SBxYBSmB32E1ctOidgWV09nGFnWKNtCJ5N3WSlowbRUY1VVySvjncfOrDNteFLzo
```



```
.  
.  
1TSgrjnee9FyEYITT+ddJQ==
```

接下来，通过复制从产品阵容开始的此密钥的整个内容，然后粘贴该内容或通过编写内容，精确地将同一密钥添加到同一型号的另一个 M12/M10。

5.6 查看 CPU 激活信息

5.6.1 查看 CPU 激活注册和设置信息

如需显示 SPARC M12/M10 中注册和设置的 CPU 激活信息，请在 XSCF shell 上使用 `showcod` 命令。您需要具有执行此命令的 `platadm` 或 `platop` 权限。另外，对于目标物理分区，具有 `pparadm`、`pparmgr` 或 `pparop` 权限的用户帐户也能执行此操作。

```
XSCF> showcod [-p ppar_id]
```

对于 `-p ppar_id` 选项，指定查看信息的物理分区 ID。如果此选项未被指定，此命令查看可访问物理分区的信息。

执行 `showcod` 命令后，显示如下的信息。

- 系统中注册的 CPU 激活的数量
- 为物理分区设置的 CPU 激活的数量

操作步骤

1. 用具有 **appropriate user** 权限的用户帐户登录 **XSCF**。
有关详情，请参见“[2.2 登录 XSCF Shell](#)”。
2. 执行 **showcod** 命令查看 **CPU 激活资源** 信息。
下面的示例显示所有 CPU 激活的详细信息。

```
XSCF> showcod -v -s cpu  
PROC Permits installed : 8 cores  
PROC Permits assigned for PPAR 0: 4 [Permanent 4cores]  
:  
PROC Permits assigned for PPAR 15: 0 [Permanent 0cores]
```

3. 执行 **exit** 命令从 **XSCF shell** 注销。
如果您在 XSCF shell 没有更多的任务，请从 XSCF 注销。

5.6.2 检查 COD 日志

如需查看例如添加/删除 CPU 激活密钥的事件日志，使用 XSCF shell 的 `showcodactivationhistory` 命令。

为了执行这个命令，您需要具有 `platadm`、`platop` 或 `fieldeng` 权限。

```
XSCF> showcodactivationhistory [target_url]
```

将输出结果文件名指定为 `target_url`。

操作步骤

1. 用具有 `platadm`、`platop`、或 `fieldeng` 权限的用户帐户登录 XSCF。
有关详情，请参见“2.2 登录 XSCF Shell”。
2. 执行 `showcodactivationhistory` 命令查看 CPU 激活密钥 COD 日志。

```
XSCF> showcodactivationhistory
11/30/2012 01:42:41PM PST: Report Generated SPARC M10-1 SN: 843a996d
10/02/2012 02:08:49PM PST: Activation history initialized: PROC 0
cores
10/15/2012 01:36:13PM PST: Capacity added: PROC 2 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 2 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 2 cores
11/07/2012 01:46:23PM PST: Capacity deleted: PROC 2 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 2 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 2 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 2 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 2 cores
11/30/2011 01:42:41PM PST: Summary: PROC 8 cores
Signature: 9138HVZQ0zFJh8EoRy7i1A
```

3. 执行 `exit` 命令从 XSCF shell 注销。
如您在 XSCF shell 没有更多的任务，请从 XSCF 注销。

5.6.3 查看 CPU 激活密钥信息

如需显示系统中注册的 CPU 激活密钥信息，请在 XSCF shell 上使用 `showcodactivation` 命令。您需要具有执行此命令的 `platadm` 或 `platop` 权限。无需指定任何选项，输入 `showcodactivation` 命令，您可列出带索引的 CPU 激活密钥。

```
XSCF> showcodactivation [-r] [-v] [-y key-index] [-M]
```

指定 CPU 激活密钥的索引号查看信息。

您可以通过指定 `-i` 和 `-r` 选项并执行 `showcodactivation` 命令查看以原始数据格式指定

索引的 CPU 激活密钥。
如需一次查看一个屏幕，请指定 -M 选项。

操作步骤

1. 用具有 **platadm** 或 **platop** 权限的用户帐户登录 **XSCF**。
有关详情，请参见 "2.2 登录 XSCF Shell"。
2. 无需指定任何选项，执行 **showcodactivation** 命令可列出带索引的 **CPU** 激活密钥。

```
XSCF> showcodactivation
Index   Description Count
-----
1       PROC          2
2       PROC          2
```

3. 执行 **showcodactivation** 命令显示系统中 **CPU** 激活密钥的信息。
下面是查看原始数据格式索引号 2 的 CPU 激活密钥信息的示例。

```
XSCF> showcodactivation -r -i 2
*Index2
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA.....
```

4. 执行 **exit** 命令从 **XSCF shell** 注销。
如果您在 XSCF shell 没有更多的任务，请从 XSCF 注销。

5.6.4 查看已激活 CPU 内核资源的使用状况

CPU 内核资源使用状况包括如下项目：

- 使用中的 CPU 内核资源
- 已安装的 CPU 内核的数量
- 为物理分区设置的 CPU 激活的数量
- 任何 CPU 激活的违规信息

如需查看 CPU 内核资源的使用状况，请使用 XSCF shell 的 **showcodusage** 命令。为了执行这个命令，您需要具有 **platadm**、**platop** 或 **fieldeng** 权限。另外，对于目标物理分区，具有 **pparadm**、**pparmgr** 或 **pparop** 权限的用户帐户也能执行此操作。

```
XSCF> showcodusage [-v] [-M] [-p {resource|ppar|all}]
```

如需一次查看一个屏幕，请指定 -M 选项。

如需查看所有物理分区的 CPU 内核资源使用状况，请使用 `-p all` 选项。
如需查看每个物理分区的 CPU 内核资源使用状况，请使用 `-p ppar` 选项。
如需查看每个 CPU 内核资源的 CPU 内核资源使用状况，请使用 `-p resource` 选项。

操作步骤

1. 用具有 **appropriate user** 权限的用户帐户登录 **XSCF**。
有关详情，请参见 ["2.2 登录 XSCF Shell"](#)。

2. 执行 **showcodusage** 命令查看 CPU 激活信息。
以下是查看 CPU 激活信息的示例。

此示例表明该系统已安装 16 个 CPU 内核资源，已注册 4 个 CPU 激活，4 个 CPU 内核资源正在使用中，当前未在使用的 CPU 激活的数量是 0。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          4          16          4 OK: 0 cores available

Note:
  Please confirm the value of the "In Use" by the ldm command of
  Oracle VM Server for SPARC.

  The XSCF may take up to 20 minutes to reflect the "In Use" of
  logical domains.
```

注 - 由 `showcodusage` 命令显示的 "In Use" 的值可能不是最新的，具体取决于 XSCF 更新的时间。"In Use" 值升级到最新的数据可能需要 20 分钟。如果 "In Use" 值和您的期待不符，重新执行 `showcodusage` 命令并确认。

3. 执行 **exit** 命令从 **XSCF shell** 注销。
如您在 XSCF shell 没有更多的任务，请从 XSCF 注销。

5.7 保存/恢复 CPU 激活密钥

某些场合，操作员可能误操作将 CPU 激活密钥删除。
为了在发生这类意外时能够及时恢复，建议您保存 CPU 激活密钥。
本节介绍如何保存和恢复 CPU 激活密钥。

5.7.1 保存 CPU 激活密钥

要将 CPU 激活密钥保存到系统中，请使用 XSCF shell 的 `dumpcodactivation` 命令。
为了执行这个命令，您需要具有 `platadm`、`platop` 或 `fieldeng` 权限的用户账户。

为 CPU 激活密钥指定储存的 URL 地址。
以下命令句法说明如何指定 USB 介质。

```
XSCF> dumpcodactivation file:///media/usb_msd/filename
```

此命令将所有的 CPU 激活密钥储存在 XSCF。
CPU 激活密钥默认储存在纯文本文件中。
如果指定了 `-e` 选项，该命令加密并保存 CPU 激活密钥。

5.7.2 恢复 CPU 激活密钥

要将 CPU 内核激活密钥恢复到系统中，请使用 XSCF shell 的 `restorecodactivation` 命令。

为了执行这个命令，您需要具有 `platadm`、`platop` 或 `fieldeng` 权限的用户账户。

指定使用 `restorecodactivation` 命令储存 CPU 激活密钥的 URL 地址。
以下命令句法说明如何指定 USB 介质。

```
XSCF> restorecodactivation file:///media/usb_msd/filename
```

执行此命令之前，需要关闭所有物理分区。
此命令恢复所有储存在 URL 的 CPU 激活密钥。

5.8 CPU 激活异常的故障排除

5.8.1 使用中的 CPU 内核数量超过了已激活的 CPU 内核数量

如果使用中的 CPU 内核数量超过已激活的 CPU 内核数量，下面的错误将被登记在 OVM 服务日志 (`/var/svc/log/ldoms-ldmd:default.log`) 中。

示例：

```
CPU permits-violation detection. executing permits-violation clearance
```

如果出现这种服务日志登记，需要采取停止使用 CPU 内核等措施。

如果问题仍未解决，超过已激活 CPU 内核数量的 CPU 内核将被自动从逻辑域删除。
此 CPU 内核的删除应用于所有的逻辑域。如果 CPU 内核删除仍然无法满足已激活 CPU 内核的数量条件，系统将停止逻辑域。

5.8.2 工作中的 CPU 内核数量因为故障下降到 CPU 激活的数量

如果工作 CPU 内核的数量由于故障而下降到低于 CPU 激活的数量，物理分区中的任何未分配的 CPU 内核资源会动态添加到逻辑域，以满足添加到逻辑域的 CPU 内核的数量。

故障的 CPU 内核将从逻辑域中删除。

在这种情况下，工作中的 CPU 内核数量不会超过 CPU 激活的数量。因此，本功能使您不必预备（购买）新的 CPU 激活。

本功能被称为故障 CPU 的自动替换。默认情况下此功能启用。

有关详情，请参见“10.7 设置故障 CPU 内核的自动更换”和 Oracle VM Server for SPARC 的 `ldm` 命令。

5.9 CPU 激活的重要注意事项

本节介绍关于 CPU 激活的如下注意事项：

- 动态添加/移除 CPU 内核
- 实时迁移
- 在模块化架构配置中添加/移除 SPARC M12-2S/M10-4S
- 保存逻辑域配置信息

动态添加/移除 CPU 内核

您可使用 `ldm` 命令或通过故障 CPU 的自动替换动态添加或移除 CPU 内核。

在 Oracle VM Server for SPARC 的帮助下，能够通过逻辑的动态配置功能实现。

但是，在使用特定的配置而不是动态配置功能时，添加/移除 CPU 内核必须重启逻辑域。这种情形发生在 CPU 内核被作为物理资源分配时。

有关详情，请参阅您所使用版本的《Oracle VM Server for SPARC Administration Guide》中的“Assigning Physical Resources to Domains”。

注 - SPARC M12/M10 具有以下两种动态重新配置 (DR)：

- 动态（重新）将 CPU 内核/内存资源分配给工作逻辑域的 DR 功能。Oracle VM Server for SPARC 软件支持此功能。
 - 动态（重新）将模块化架构（也就是一个 SPARC M12-2S 或 SPARC M10-4S）分配给工作物理分区的 DR 功能。Oracle VM Server for SPARC 软件和 XSCF 固件支持此功能。
-

实时迁移

作为来宾域迁移目的地的物理分区应具有足够已激活的未分配给物理域的 CPU 内核资源。如果未使用的已激活的 CPU 激活数不足，则可能需要添加 CPU 激活。即使在同一型号的 SPARC M12/M10 之间进行实时迁移，也可能需要将 CPU 激活添加到目的地。这是因为不可能在两个系统之间移动 CPU 激活（即使它们事实上是一个系统）。

有关实时迁移的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的 "第7章 迁移来宾域"。

在模块化架构配置中添加/移除 SPARC M12-2S/M10-4S

在模块化架构配置中添加 SPARC M12-2S/M10-4S 时，请检查 CPU 激活数量是否足够，并根据需要进行添加。

保存逻辑域配置信息

如果您更改了逻辑域的配置，执行 `ldm add-spconfig` 命令保存逻辑域信息。

例如，假设您通过实时迁移将逻辑域移动到另一个系统中，并减少了源系统上的 CPU 激活的数量。在这种情况下，需在完成实时迁移后，使用 `ldm add-spconfig` 命令保存逻辑域配置信息。

如果您没有保存逻辑域配置信息，下次物理分区启动时该域将使用前次的配置信息启动。在这种情况下，CPU 激活的数量可能不足，这样启动可能失败。

注 - 即使在其配置中仅有控制域的系统，当使用 Oracle Solaris 的 `ldm` 命令更改资源配置时也需保存逻辑域配置信息。

启动/停止系统

本章介绍了 SPARC M12/M10 系统的启动流程和停止流程及其操作步骤。

- 启动系统
- 停止系统
- 重新启动系统
- 禁止在开机时启动 Oracle Solaris

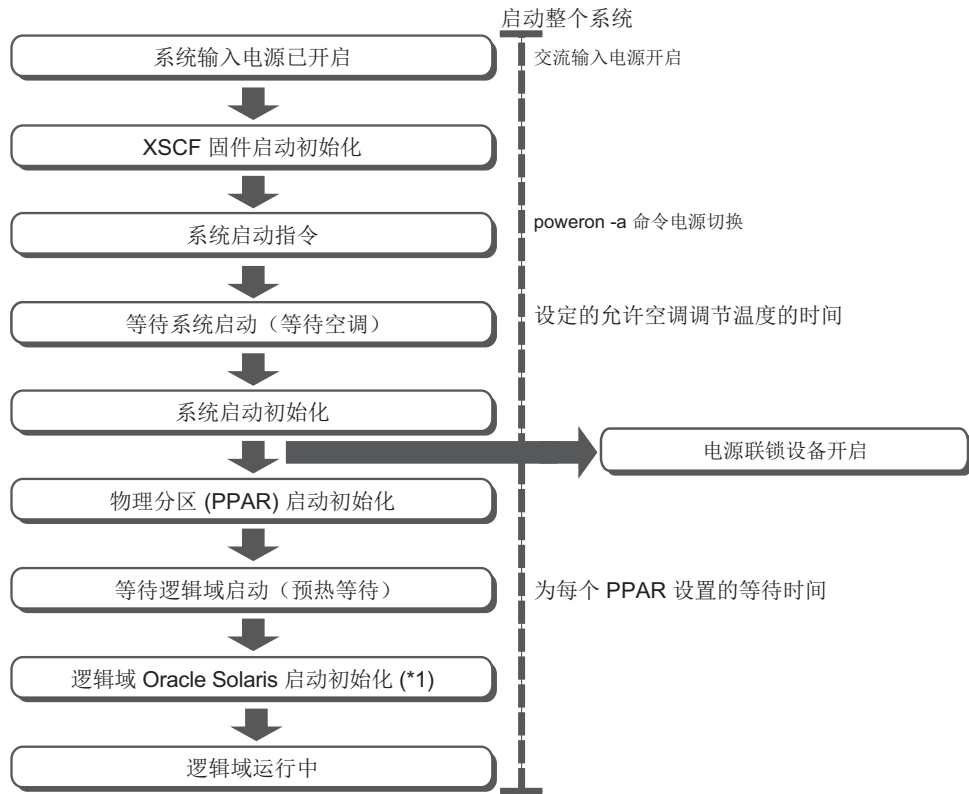
6.1 启动系统

本节介绍系统启动流程和操作步骤。

6.1.1 从输入电源开启到系统启动的流程

本节介绍从开机到逻辑域启动的流程。

图 6-1 从输入电源开启到系统启动的流程



*1 如需禁止启动 Oracle Solaris，请参见 "6.4 禁止在开机时启动 Oracle Solaris"。

下面列出了两种指定系统启动的方法。使用两种方法之一在配置主 XSCF 的机柜执行操作。

- 使用操作面板上的电源开关。
- 使用 XSCF 固件的 `poweron` 命令。

6.1.2 使用电源开关

按配置有主 XSCF 的机柜操作面板上的电源开关。按电源开关后，将开始按照正确的顺序给系统中所有的物理分区供电。之后，每个物理分区内的所有逻辑域以相应的顺序启动。

注 - 只有配置了主 XSCF 的机柜的电源开关有此功能。其他机柜的电源开关不能开启系统电源。

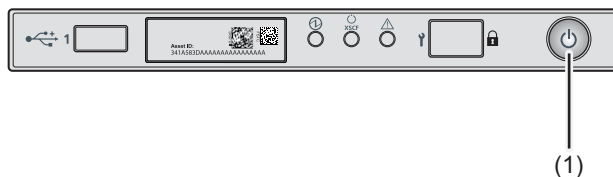
注 - 如果 XSCF 固件的 `setpparparam` 命令已经限制了控制域的自动重置，被限制的控制域不启动。此外，如果 `setpparmode` 命令限制了物理分区和逻辑域的自动重置，被限制的逻辑域不启动。有关 `setpparparam` 和 `setpparmode` 命令的详细信息，请参见 `setpparparam(8)` 和 `setpparmode(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF

根据型号配置主 XSCF 的机柜不同。

- SPARC M12-1
SPARC M12-1 上的电源开关
- SPARC M12-2
SPARC M12-2 上的电源开关
- SPARC M12-2S（无接线盒）
SPARC M12-2S BB#00 或 BB#01（MASTER LED 亮的机柜）上的电源开关
- SPARC M12-2S（带接线盒）
电源开关位于接线盒 XBBOX#80 或 XBBOX#81（MASTER LED 指示灯亮起的机柜）上
- SPARC M10-1
SPARC M10-1 上的电源开关
- SPARC M10-4
SPARC M10-4 上的电源开关
- SPARC M10-4S（无接线盒）
SPARC M10-4S BB#00 或 BB#01（MASTER LED 亮的机柜）上的电源开关
- SPARC M10-4S（带接线盒）
电源开关位于接线盒 XBBOX#80 或 XBBOX#81（MASTER LED 指示灯亮起的机柜）上

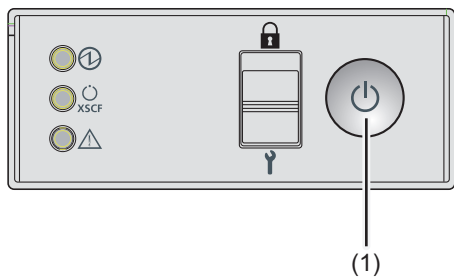
有关操作面板上的开关和 LED 指示灯的详情，请参见服务器的《Service Manual》。

图 6-2 操作面板 (SPARC M12-1/M10-1)



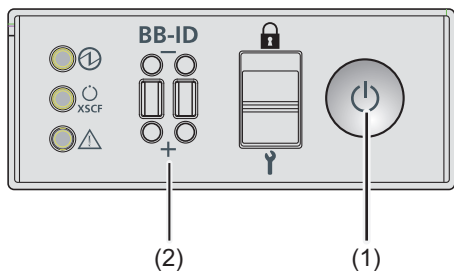
编号	组件
1	电源开关

图 6-3 操作面板 (SPARC M12-2/M10-4)



编号	组件
1	电源开关

图 6-4 操作面板 (SPARC M12-2S/M10-4S 接线盒)



编号	组件
1	电源开关
2	BB-ID 开关

操作步骤

1. 按配置有主 **XSCF** 的机柜操作面板上的电源开关。
系统所有的物理分区启动。之后，每个物理分区内的所有逻辑域启动。

6.1.3 使用 poweron 命令

请使用 XSCF 固件 poweron 命令启动整个系统。
请使用拥有 platadm 或 fieldeng 权限的用户账户执行此命令。

```
XSCF> poweron -a
```

如需启动整个系统，请执行 `poweron` 命令并指定 `-a` 选项。执行此命令后输出一个确认信息。输入 "y"。

执行此命令后，系统中的所有物理分区按照正确的顺序开机。之后，每个物理分区内的所有逻辑域以相应的顺序启动。

注 - 如果 XSCF 固件的 `setpparparam` 命令已经限制了控制域的自动重置，被限制的控制域不启动。此外，如果 `setpparmode` 命令限制了物理分区和逻辑域的自动重置，被限制的逻辑域不启动。有关 `setpparparam` 和 `setpparmode` 命令的详细信息，请参见 `setpparparam(8)` 和 `setpparmode(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

操作步骤

1. 执行 `poweron -a` 命令给整个系统上电。输入 "y"，确认信息。

```
XSCF> poweron -a
PPAR-IDs to power on:00,01,02,03
Continue? [y|n] :y
00 :Powering on
01 :Powering on
02 :Powering on
03 :Powering on

*Note*
  This command only issues the instruction to power-on.
  The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

系统所有的物理分区上电。之后，每个物理分区内的所有逻辑域启动。

2. 执行 `showpparstatus` 命令，并确认系统所有物理分区电源已开启。

```
XSCF> showpparstatus -a
PPAR-ID      PPAR Status
00           Running
01           Running
02           Running
03           Running
```

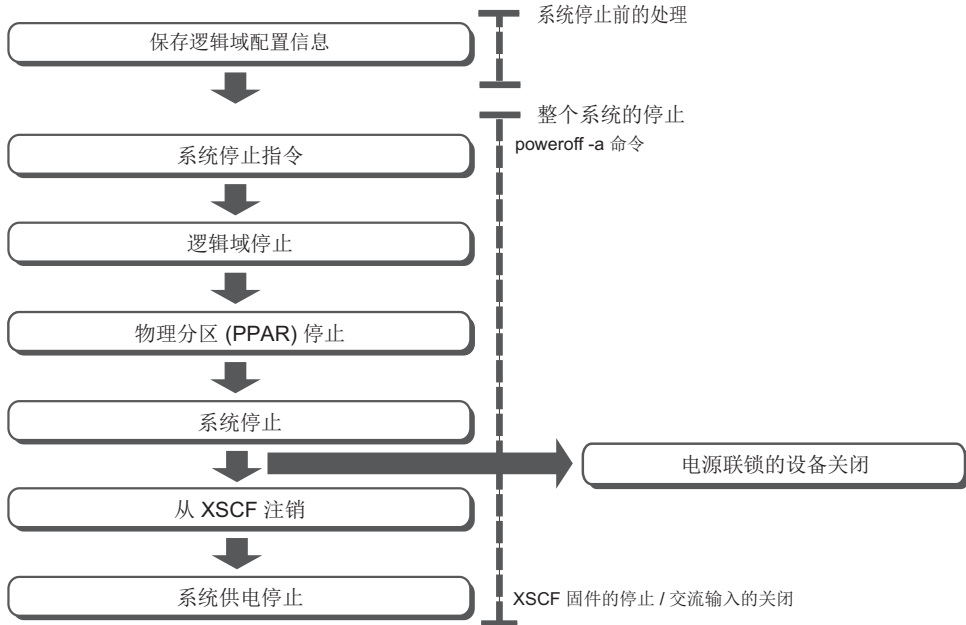
6.2 停止系统

本节介绍系统停止流程和操作步骤。

6.2.1 从系统停止到输入电源关闭的流程

本节介绍从停止系统到关闭输入电源的流程。

图 6-5 从系统停止指令到输入电源关闭的流程



如需停止系统电源，需要关闭目标物理分区中的所有逻辑域。逻辑域的关闭按指定的顺序进行，控制域以外的域先关闭，控制域必须最后关闭。

SPARC M12/M10 系统支持一种称为按顺序关闭的技术，它以适当的顺序关闭逻辑域，然后停止物理分区，因此用户不需要注意逻辑域的关闭。

使用按顺序关闭时，提前为逻辑域定义编号，该编号代表要关闭组的顺序。运用这项技术，定义的顺序存储在 XSCF 中，即使在 XSCF 管理下关闭顺序也能得到保证。

如果 non-active 来宾域包含在已定义的按顺序关闭的组中，则约需 10 分钟方可将该组关闭完毕。

有关按顺序关闭的详细信息，请参见“8.7 按顺序关闭逻辑域”。

6.2.2 系统停止之前保存逻辑域配置信息

对于逻辑域配置，请在控制域中执行 Oracle VM Server for SPARC 的 `ldm add-sponconfig` 命令，使得在停止物理分区之前将最新配置信息保存在 XSCF 中。

有关详情，请参见“10.11.1 保存/显示逻辑域配置信息”。

如果在停止物理分区之前未在 XSCF 中保存最新配置信息，则可能会发生以下问题。

- 变更逻辑域配置后，如果将物理分区在没有保存逻辑域配置信息的情况下停止，然后将其重新启动，则其将以变更之前的逻辑域配置启动。

- 即使在变更逻辑域配置后在 XSCF 中保存了最新配置信息，如果自上次保存逻辑域配置以来已经过去了很长时间，则将物理分区停止然后将其重新启动时，逻辑域的时间可能会发生偏离。

6.2.3 停止整个系统

请使用 XSCF 固件 `poweroff` 命令停止整个系统。
请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。

注 - 在锁定模式，主 XSCF 机柜操作面板上的电源开关不能用于关闭电源。有关锁定模式的详情，请参见“第13章 切换到锁定/维护模式”。

```
XSCF> poweroff -a
```

如需停止整个系统，请执行 `poweroff` 命令并指定 `-a` 选项。执行此命令后输出一个确认信息。输入 `"y"`。

执行命令后，每个物理分区中的逻辑域按规定的规则关闭。然后，物理分区自身的电源关闭。

操作步骤

1. 执行 `poweroff -a` 命令以关闭整个系统的电源。输入 `"y"`，确认信息。

```
XSCF> poweroff -a
PPAR-IDs to power off:00,01,02,03
Continue? [y|n] :y
00 : Powering off
01 : Powering off
02 : Powering off
03 : Powering off

*Note*
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

每个物理分区的所有逻辑域关闭，之后所有物理分区关闭电源。

2. 执行 `showpparstatus` 命令，并确认系统所有物理分区电源已关闭。

```
XSCF> showpparstatus -a
PPAR-ID          PPAR Status
00                Powered Off
01                Powered Off
02                Powered Off
03                Powered Off
```

6.3 重新启动系统

本节介绍如何重新启动系统。

使用 XSCF 固件的 `rebootxscf` 命令重新启动 XSCF。
请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。

配置以下 XSCF 项目后，XSCF 重新启动将启用以下设置：

- 将配置的 XSCF 网络应用到 XSCF (`applynetwork`)
- 系统海拔高度 (`setaltitude`)
- NTP 相关设置 (`setntp`)

```
XSCF> rebootxscf -a | -b bb_id | -s
```

如需重新启动系统中的所有 XSCF，需指定 `-a`。如需重新启动指定的 SPARC M12-2S/M10-4S 的 XSCF，需指定 `-b bb_id`。`-a` 和 `-b` 选项只能在主 XSCF 上执行。如需重新启动当前正在工作的 XSCF，需指定 `-s`。

重新启动 XSCF 会断开与 XSCF 的 SSH、Telnet 和其他的连接。请重新建立连接。

注 - 如果由 XSCF 固件的 `setdate` 命令重新启动 XSCF 已经被取消，则即使由 `rebootxscf` 命令重新启动 XSCF 也不会应用此设置。您需要再次执行 `setdate` 命令。

操作步骤

1. 执行 `rebootxscf` 命令重新启动 XSCF。输入 "y"，确认信息。
以下示例重新启动所有 XSCF。

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] : y
```

6.4 禁止在开机时启动 Oracle Solaris

本节介绍如何禁止在 SPARC M12/M10 开机时启动 Oracle Solaris。

注 - 在 SPARC M12/M10 中，即使将操作面板模式设置为 "Service"，也不能禁止启动 Oracle Solaris。

在 SPARC M12/M10 中禁止开机时启动 Oracle Solaris 的方法如下所述。

- 禁止在控制域中启动 Oracle Solaris
执行以下其中一种操作。此操作后，Oracle Solaris 停止在 OpenBoot PROM。
 - 使用 XSCF 固件的 `setpparam` 命令将 OpenBoot PROM 环境变量 `auto-boot?` 的值设置为 `false`。

- [示例] XSCF> **setpparparam -p 0 -s bootscript "setenv auto-boot? false"**
- 使用 Oracle Solaris 的 `eeeprom` 命令将 OpenBoot PROM 环境变量 `auto-boot?` 的值设置为 `false`。

有关 `setpparparam` 命令的详细信息，请参见 `setpparparam(8)` 命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

有关使用 XSCF 固件变更 OpenBoot PROM 环境变量的详细信息，请参见 "8.9.1 XSCF 固件可设置 OpenBoot PROM 环境变量"。

- 禁止在来宾域中启动 Oracle Solaris
使用 XSCF 固件的 `setpparmode` 命令设置 `guestboot=off`。

[示例] XSCF> **setpparmode -p 0 -m guestboot=off**

有关 `setpparmode` 命令的详细信息，请参见 `setpparmode(8)` 命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

控制物理分区

本章介绍控制物理分区需要的项目。

- 配置物理分区
- 设置物理分区运行模式
- 开启物理分区
- 关闭物理分区
- 更改物理分区的配置

7.1 配置物理分区

本节概括介绍物理分区配置。

如需配置 SPARC M12-2S 或 SPARC M10-4S 系统，需通过组合同一型号的服务器中的一个或多个模块化架构来配置物理分区 (PPAR)。配置物理分区称为分区，将得到的配置对象称为物理分区 (PPAR)。

在 SPARC M12-2S/M10-4S 中，最多可配置 16 个物理分区。

请注意，由于 SPARC M12-2/M10-1/M10-4 型号是单个机箱型，因此只能配置一个物理分区。

在 XSCF 固件中，配置物理分区时，一个模块化架构被视为一个系统板 (PSB)。

使用 XSCF 固件 `addboard` 命令配置物理分区。有关详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的 "第3章 域配置的操作"。

7.2 设置物理分区运行模式

本节概括介绍物理分区运行模式。

在 SPARC M12/M10 中，可以为每个物理分区设置以下运行模式：

- 自我诊断的诊断级别
- 自我诊断的控制台消息详细程度

- 实时检查（在 XSCF 和管理程序之间进行监控）
- 主机监视程序（在管理程序和控制域之间进行监控）超时情况下的操作
- 中断信号限制
- 来宾域自动启动
- 节能运行
- I/O 总线重新配置
- PPAR DR 功能
- CPU 运行模式

通过设置运行模式可启用对指定物理分区的控制。使其在运行或维护时不接收不必要的信号。

使用 XSCF 固件 `setpparmode` 命令设置物理分区运行模式。有关详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的“第3章 域配置的操作”。

注 - 控制域的自动启动由 `setpparparam` 命令设置。有关详情，请参见“8.9.1 XSCF 固件可设置 OpenBoot PROM 环境变量”。

7.2.1 搭载在物理分区上的 CPU 和 CPU 运行模式

在 SPARC M10-4S 中，您可以将系统配置为既有搭载 SPARC64 X+ 处理器的 SPARC M10-4S 的物理分区，又有搭载 SPARC64 X 处理器的 SPARC M10-4S 的物理分区。当使用 XSCF 固件 `setpparmode` 命令设置了 CPU 运行模式并且物理分区指定了 CPU 运行模式的类型时，下次激活 Oracle Solaris 时，系统自动判断应该使用 SPARC64X+ 处理器功能还是 SPARC64X 处理器功能进行操作。

CPU 操作的类型

以下有两种 CPU 操作类型：

- 使用 SPARC64 X+ 功能操作
物理分区上的所有 CPU 都使用增强功能的 SPARC64 X+ 处理器进行操作。
仅当使用 `setpparmode` 命令将 CPU 运行模式 (`cpumode`) 设置为“auto”，并且物理分区上的所有 CPU 都配置有 SPARC64 X+ 处理器时，这才适用。
- 使用 SPARC64 X 功能操作
物理分区上的所有 CPU 都使用 SPARC64 X 处理器的功能进行操作。
使用 `setpparmode` 命令将 CPU 运行模式设置为“compatible”时，所有搭载在物理分区上的任何类型的 CPU 使用 SPARC64 X 处理器功能操作。
使用 `setpparmode` 命令将 CPU 运行模式设置为“auto”时，如果将 SPARC64 X 处理器搭载到物理分区，所有 CPU 使用 SPARC64 X 处理器功能操作。

注 - 有关支持 CPU 运行模式设置的 XCP 固件和 Oracle Solaris 的版本，请参见最新 XCP 版本（XCP 2210 或更高版本）的《Fujitsu M10/SPARC M10 系统产品说明》。

物理分区的 CPU 配置和运行模式

如 图 7-1 中的 PPAR#2 所示，您可以将一个物理分区配置为在 SPARC M10-4S 系统中同时具有 SPARC64 X+ 处理器和 SPARC64 X 处理器。

图 7-1 安装在 SPARC M10-4S 系统上的处理器和物理分区的配置示例

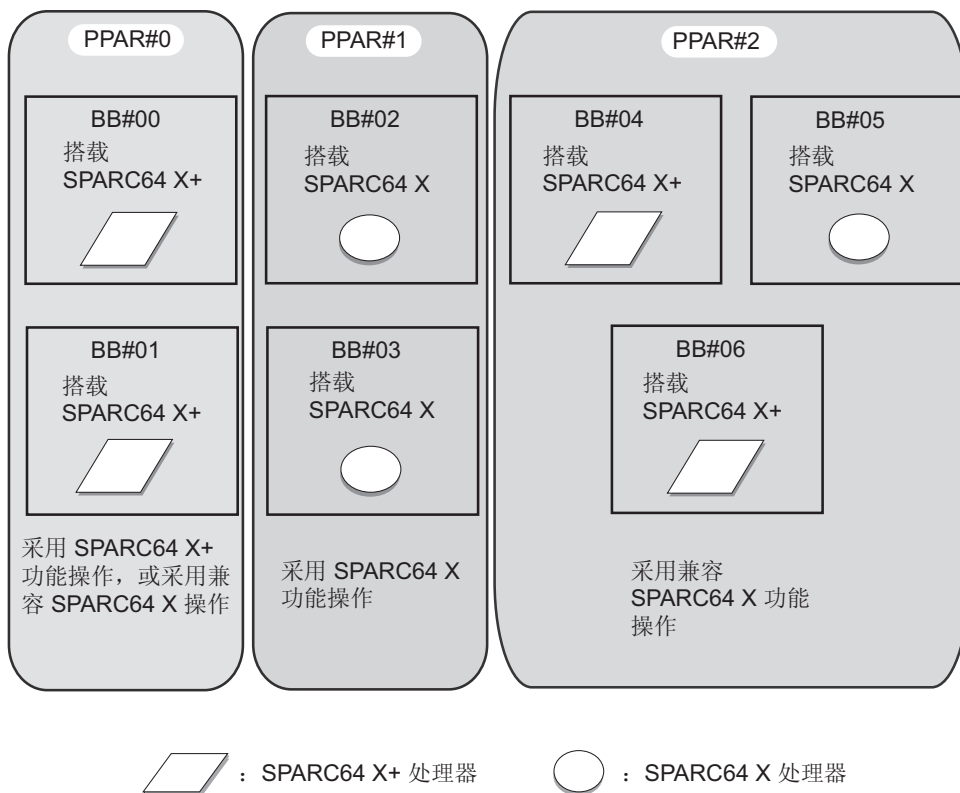


表 7-1 列出了物理分区的 CPU 配置、CPU 运行模式设置值和 Oracle Solaris 上的 CPU 操作类型。

表 7-1 物理分区的 CPU 配置和运行模式

PPAR 的 CPU 配置	setpparmode 命令的 CPU 运行模式 (CPU Mode) 设置值	Oracle Solaris CPU 操作类型
SPARC64 X+	auto	使用 SPARC64 X+ 功能操作
SPARC64 X+	compatible	使用兼容 SPARC64 X 操作
SPARC64 X+/X	"auto" 或 "compatible"	SPARC64 X+ 在 SPARC64 X 兼容模式下操作 SPARC64 X 使用 SPARC64 X 功能操作
SPARC64 X	"auto" 或 "compatible"	使用 SPARC64 X 功能操作

有关 PPAR DR 操作时物理分区的 CPU 配置以及 Oracle Solaris 上的 CPU 操作类型的详细信息，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的 "2.6 使用 SPARC64 X+ 处理器时的注意事项"。

检查应用 CPU 的操作类型

如需检查当前应用 CPU 的运行类型，请执行 Oracle Solaris 的 `prtdiag` 或 `psrinfo` 命令。当物理分区 CPU 使用 SPARC64 X+ 功能操作时，在 System Processor Mode 行显示 "SPARC64-X+"。与之对应，当物理分区 CPU 使用 SPARC64 X 功能正在运行时，在 System Processor Mode 行显示 "SPARC64-X"。

1. 在目标物理分区上，执行带 `-pv` 选项的 Oracle Solaris 的 `prtdiag` 或 `psrinfo` 命令，检查当前应用的 CPU 操作类型。

此例应用于使用 SPARC64 X+ 功能进行操作的情况。

以下是 `prtdiag` 命令执行结果的示例。

```
primary# prtdiag
System Configuration: Oracle Corporation sun4v SPARC M10-4S
Memory size: 391168 Megabytes

===== Virtual CPUs =====

CPU ID Frequency Implementation      Status
-----
0      3700 MHz  SPARC64-X+                          on-line
```

以下是 `psrinfo -pv` 命令执行结果的示例。

```
primary# psrinfo -pv
The physical processor has 12 cores and 24 virtual processors (0-23)
The core has 2 virtual processors (0 1)
The core has 2 virtual processors (2 3)
The core has 2 virtual processors (4 5)
The core has 2 virtual processors (6 7)
The core has 2 virtual processors (8 9)
The core has 2 virtual processors (10 11)
The core has 2 virtual processors (12 13)
The core has 2 virtual processors (14 15)
The core has 2 virtual processors (16 17)
The core has 2 virtual processors (18 19)
The core has 2 virtual processors (20 21)
The core has 2 virtual processors (22 23)
SPARC64-X+ (chipid 0, clock 3700 MHz)
```

检查 CPU 运行模式的设置状态

使用 XSCF 固件的 `showpparmode` 命令检查 CPU 运行模式的设置状态。请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。对于目标物理分区，具有 `pparadm` 权限的用户帐户也能执行此操作。

注 - 使用 `showpparmode` 命令，可查看用 `setpparmode` 命令设置的最新信息。有些场合对当前应用的 CPU 操作类型没有回应。这是因为用 `setpparmode` 命令设置的信息在物理分区重新

启动后才能查看。例如，如果将 CPU 运行模式设置为 "auto"，使用 `setpparmode` 命令为使用 SPARC64 X+ 功能操作的物理分区将 CPU 运行模式设置为 "compatible"，使用 `showpparmode` 命令时的输出结果将是 "compatible"。但是，物理分区重新启动后将使用 SPARC64 X+ 功能操作。

```
XSCF> showpparmode -p ppar_id
```

`ppar_id` 用于指定物理分区的 PPAR ID。您可以指定 0 到 15 间的一个数字值。

1. 在目标物理分区，执行 XSCF 固件的 `showpparmode` 命令，检查使用 `setpparmode` 命令设置的 CPU 运行模式。
此例用于检查 PPAR-ID 00。

```
XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level       :min
Message Level          :normal
Alive Check            :on
Watchdog Reaction      :reset
Break Signal           :on
Autoboot (Guest Domain) :on
Elastic Mode           :off
IOreconfigure          :true
CPU Mode               :auto
PPAR DR (Current)      :off
PPAR DR (Next)         :off
```

更改 CPU 运行模式

`setpparmode` 命令的默认 CPU 运行模式是 "auto"。设置为 "auto" 时，无论何时启动物理分区，系统根据搭载在物理分区的 CPU 类型自动选择 Oracle Solaris 的 CPU 操作类型。

使用 `setpparmode` 命令将 CPU 运行模式由 "auto" 设置为 "compatible" 时，不论搭载的 CPU 类型，下次物理分区启动时 CPU 使用 SPARC64 X 功能操作。

如需更改 CPU 运行模式，请使用 XSCF 固件的 `setpparmode` 命令。请使用拥有 `platadm` 权限的用户账户执行此命令。对于目标物理分区，具有 `pparadm` 权限的用户帐户也能执行此操作。

```
XSCF> setpparmode -p ppar_id -m cpumode=mode
```

`ppar_id` 用于指定物理分区的 PPAR ID。您可以指定 0 到 15 间的一个数字值。`mode` 用于指定 CPU 运行模式。当 CPU 使用 SPARC64 X+ 功能操作时您可指定为 "auto"，当 CPU 使用 SPARC64 X 功能操作时您可指定为 "compatible"。默认值为 "auto"。

注 - 更改 CPU 运行模式必须关闭目标物理分区的电源。

1. 执行 `poweroff` 命令以关闭目标物理分区。
以下是关闭 PPAR-ID 00 的示例。

```

XSCF> poweroff -p 0
PPAR-IDs to power off:00
Continue? [y|n] :y
00 : Powering off

*Note*
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showpparprogress".
XSCF>

```

2. 执行 **showpparmode** 命令确认当前的 CPU 运行模式设置 (CPU mode)。
 以下是将 CPU 运行模式设置为 "auto" 的示例。

```

XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level       :min
Message Level         :normal
Alive Check           :on
Watchdog Reaction     :reset
Break Signal          :on
Autoboot(Guest Domain):on
Elastic Mode          :off
IOreconfigure         :true
CPU Mode              :compatible
PPAR DR(Current)     :off
PPAR DR(Next)        :off

```

3. 执行 **setpparmode** 命令更改 CPU 运行模式。
 以下是将 CPU 运行模式由 "auto" 更改为 "compatible" 的示例。

```

XSCF> setpparmode -p 0 -m cpumode=compatible
Diagnostic Level       :max      -> -
Message Level         :normal   -> -
Alive Check           :on       -> -
Watchdog Reaction     :reset    -> -
Break Signal          :on       -> -
Autoboot(Guest Domain):on     -> -
Elastic Mode          :off      -> -
IOreconfigure         :true     -> -
CPU Mode              :auto     -> compatible
PPAR DR               :off      -> -
The specified modes will be changed.
Continue? [y|n] :y
configured.
Diagnostic Level       :max
Message Level         :normal
Alive Check           :on (alive check:available)
Watchdog Reaction     :reset (watchdog reaction:reset)
Break Signal          :on (break signal:non-send)
Autoboot(Guest Domain):on
Elastic Mode          :on
IOreconfigure         :false

```



```
CPU Mode           :compatible
PPAR DR            :off
```

4. 执行 **showpparmode** 命令确认当前的 CPU 运行模式设置 (CPU mode)。以下是将 CPU 运行模式设置为 "compatible" 的示例。

```
XSCF> showpparmode -p 0
Host-ID           :0f010f10
Diagnostic Level  :min
Message Level     :normal
Alive Check       :on
Watchdog Reaction :reset
Break Signal      :on
Autoboot (Guest Domain) :on
Elastic Mode      :off
IOreconfigure    :true
CPU Mode          :compatible
PPAR DR (Current) :off
PPAR DR (Next)   :off
```

5. 执行 **poweron** 命令开启目标物理分区的电源。以下是开启 PPAR-ID 00 的示例。

```
XSCF> poweron -p 0
PPAR-IDs to power on:00
Continue? [y|n] :y
00 :Powering on

*Note*
  This command only issues the instruction to power-on.
  The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

7.2.2 检查恢复供电/设置自动上电时电源的操作

本节将介绍如何检查和设置停电后自动恢复供电时以下操作是否自动完成：物理分区的上电和逻辑域的 Oracle Solaris 的启动。

检查恢复供电时电源的操作

使用 **showpowerschedule** 命令检查恢复供电时物理分区是否可以自动上电。使用 **showpparparam** 命令或 **showpparmode** 命令检查逻辑域上的 Oracle Solaris 在恢复供电时是否可以自动启动。对于这些命令，输出结果为默认值意味着恢复供电时物理分区上电，逻辑域上的 Oracle Solaris 启动。

操作步骤

1. 执行 **showpowerschedule** 命令，检查恢复供电时物理分区的电源操作。

```
XSCF> showpowerschedule -a -m state
PPAR-ID schedule member recover mode
-----
0         disable  -      on
1         enable   1      auto
```

如果 [recover mode] 为 "on"（默认），或如果 [schedule] 为 "enable" 并且 [recover mode] 为 "auto"，则恢复供电时物理分区将自动上电。

[schedule] 有以下含义。

- disable: 禁用已计划的电源操作。（默认）
- enable: 启用已计划的电源操作。

[recover mode] 有以下含义。

- on: 恢复供电时将电源恢复到与停电之前相同的状态。
如果停电之前电源接通，则电源将开启。（默认）
- off: 恢复供电时不开启电源。
- auto: 恢复供电时在已计划的电源运行期间开启电源。

2. 执行 **showpparparam** 命令，检查控制域的自动启动设置。
以下是查看 PPAR-ID 0 的控制域的 OpenBoot PROM 环境变量 [auto-boot?] 的设置值的示例。
设置为 "true"（默认），因此恢复供电时，Oracle Solaris 自动启动。

```
XSCF> showpparparam -p 0 -c auto-boot
auto-boot? :true
```

3. 执行 **showpparmode** 命令，检查来宾域的自动启动。
以下是查看 PPAR-ID 0 的来宾域的自动启动设置 [Autoboot(Guest Domain)] 的设置值的示例。设置为 "on"（默认），因此恢复供电时，Oracle Solaris 自动启动。

```
XSCF> showpparmode -p 0
Host-ID                :9007002b
Diagnostic Level       :min
Message Level          :normal
Alive Check            :on
Watchdog Reaction      :reset
Break Signal           :on
Autoboot(Guest Domain) :on
Elastic Mode           :off
IOreconfigure          :false
CPU Mode               :auto
PPAR DR(Current)       :-
PPAR DR(Next)         :off
```

设置恢复供电时自动上电

使用 `setpowerschedule` 命令，设置恢复供电时物理分区的电源操作。使用 `setpparparam` 或 `setpparmode` 命令，设置逻辑域的自动启动。设置物理分区的电源操作可启用恢复供电时物理分区自动上电。启用逻辑域的自动启动功能可启用恢复供电时 Oracle Solaris 自动启动。

1. 执行 `setpowerschedule` 命令，设置恢复供电时物理分区的电源操作。
两种设置如下。
 - 将电源恢复到与停电前相同的状态（默认）

```
XSCF> setpowerschedule -p ppar_id -c recover=on
```

- 按照电源恢复时预期的电源操作

当物理分区电源计划已经由 `addpowerschedule` 命令设置时使用此设置。在由电源计划覆盖的给定的时间，恢复供电时物理分区上电，与停电时物理分区电源的状态无关。

```
XSCF> setpowerschedule -p ppar_id -c control=enable
XSCF> setpowerschedule -p ppar_id -c recover=auto
```

2. 执行 `setpparparam` 命令设置 **OpenBoot PROM** 环境变量，防止控制域停止在 **ok** 提示符处。

```
XSCF> setpparparam -p ppar_id -s bootscript "setenv auto-boot? true"
```

3. 如需自动启动物理分区的来宾域，需执行 `setpparmode` 命令。

```
XSCF> setpparmode -y -p ppar_id -m guestboot=on
```

如需在恢复供电时自动启动某个域，您需要在该域进入活动状态以后，在控制域上使用 `ldm add-spconfig` 命令保存逻辑域配置信息。有关详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》。
当模式开关设置为 "Service" 时，无论上述如何设置，均抑制恢复供电时接通电源的功能。

有关 `setpowerschedule`、`addpowerschedule`、`setpparparam` 和 `setpparmode` 命令的详细信息，请参见各命令的 `man` 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

7.3 开启物理分区

请使用 XSCF 固件 `poweron` 命令分别开启物理分区。

请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。另外，对于目标物理分区，具有 `pparadm` 或 `pparmgr` 权限的用户帐户也能执行此操作。

```
XSCF> poweron -p ppar_id
```

要指定一个物理分区，请指定 `-p ppar_id` 选项。您可为 `ppar_id` 指定一个从 0 到 15 的数值，是即将启动的物理分区的 PPAR-ID。
执行此命令后输出一个确认信息。输入 "y"。

注 - SPARC M12-2/M10-1/M10-4 只有一个物理分区，因此只能为其 PPAR-ID 指定 0。

执行此命令后，指定的物理分区开启。之后，物理分区内的所有逻辑域启动。首先，控制域启动，之后其它域启动（无特定的顺序）。

注 - 如果 XSCF 固件的 `setpparparam` 命令已经限制了控制域的自动重置，被限制的控制域不启动。此外，如果 `setpparmode` 命令限制了物理分区和逻辑域的自动重置，被限制的逻辑域不启动。有关 `setpparparam` 和 `setpparmode` 命令的详细信息，请参见 `setpparparam(8)` 和 `setpparmode(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

操作步骤

1. 执行 `poweron` 命令以开启指定物理分区。
以下是开启 PPAR-ID 00 的示例。

```
XSCF> poweron -p 0  
PPAR-IDs to power on:00  
Continue? [y|n] :y  
00 :Powering on
```

Note

This command only issues the instruction to power-on.
The result of the instruction can be checked by the "showpparprogress".
XSCF>

PPAR-ID 00 的物理分区已开启。物理分区中的所有逻辑域启动。

2. 执行 `showpparprogress` 命令，并确认物理分区电源已开启。

```
XSCF> showpparprogress -p 0  
PPAR Power On Preprocessing PPAR#0 [ 1/12]  
PPAR Power On                PPAR#0 [ 2/12]  
XBBOX Reset                   PPAR#0 [ 3/12]  
PSU On                        PPAR#0 [ 4/12]  
CMU Reset Start               PPAR#0 [ 5/12]  
XB Reset 1                    PPAR#0 [ 6/12]  
XB Reset 2                    PPAR#0 [ 7/12]  
XB Reset 3                    PPAR#0 [ 8/12]  
CPU Reset 1                   PPAR#0 [ 9/12]  
CPU Reset 2                   PPAR#0 [10/12]
```

```
Reset released          PPAR#0 [11/12]
CPU Start                PPAR#0 [12/12]
The sequence of power control is completed.
XSCF>
```

7.4 关闭物理分区

对于逻辑域配置，请在控制域中执行 Oracle VM Server for SPARC 的 `ldm add-sponfig` 命令，使得在关闭物理分区之前将最新配置信息保存在 XSCF 中。有关详情，请参见 ["6.2.2 系统停止之前保存逻辑域配置信息"](#) 和 ["10.11.1 保存/显示逻辑域配置信息"](#)。

请使用 XSCF 固件 `poweroff` 命令分别停止物理分区。

请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。另外，对于目标物理分区，具有 `pparadm` 或 `pparmgr` 权限的用户帐户也能执行此操作。

```
XSCF> poweroff -p ppar_id
```

要指定一个物理分区，请指定 `-p ppar_id`。您可为 `ppar_id` 指定一个从 0 到 15 的数值，是将要关闭的物理分区的 PPAR-ID。设置值根据系统配置变化。

执行此命令后输出一个确认信息。输入 "y"。

执行命令后，每个物理分区中的逻辑域按规定的规则关闭。然后，物理分区电源关闭。

操作步骤

1. 执行 `poweroff` 命令以关闭指定物理分区。
以下是关闭 PPAR-ID 00 的示例。

```
XSCF> poweroff -p 0
PPAR-IDs to power off:00
Continue? [y|n] :y
00 : Powering off

*Note*
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

物理分区 PPAR-ID 00 的所有逻辑域关闭，之后所有物理分区关闭。

2. 执行 `showpparprogress` 命令，并确认指定的物理分区的电源开启/关闭状态。

```
XSCF> showpparprogress -p 0
PPAR Power Off          PPAR#0 [ 1/ 3]
CPU Stop                PPAR#0 [ 2/ 3]
PSU Off                 PPAR#0 [ 3/ 3]
```

```
The sequence of power control is completed.  
XSCF>
```

7.5 更改物理分区的配置

本节概括介绍物理分区配置的更改。

配置 SPARC M12/M10 系统中的物理分区后，可以通过添加或删除物理系统板 (PSB) 来更改物理分区的配置。

如需更改物理分区的配置，请使用 XSCF 固件的 `addboard` 或 `deleteboard` 命令。有关详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的 "第3章 域配置的操作"。

控制逻辑域

本章介绍逻辑域的控制以及如何控制逻辑域。

- 配置逻辑域
- 配置 Oracle Solaris 内核区
- 从 XSCF Shell 切换到控制域控制台
- 从控制域控制台返回 XSCF Shell
- 启动逻辑域
- 关闭逻辑域
- 按顺序关闭逻辑域
- 检查 CPU 激活信息
- 设置控制域的 OpenBoot PROM 环境变量
- 域控制台日志功能
- 更改逻辑域的配置
- 设置逻辑域时间
- 收集管理程序转储文件
- 管理与 CPU 插槽相关联的逻辑域资源
- 设置物理分区动态重新配置策略
- 设置逻辑域的最大页面大小

8.1 配置逻辑域

逻辑域是 Oracle VM Server for SPARC 提供的虚拟硬件环境。您可将一个平台分割为一个以上的虚拟硬件环境（逻辑域），Oracle Solaris 可以在每个逻辑域中独立运行。一个 SPARC M12/M10 可以配置多个逻辑域，从而集成多个服务器，并提高系统可用性。除此以外，CPU、内存、I/O 设备和平台上搭载的其它硬件资源可灵活地分配给逻辑域，从而提高资源利用率。

在 SPARC M12/M10 系统中，物理分区配置后，逻辑域被配置为物理分区 (PPAR) 中的独立系统环境（虚拟平台）。

8.2 配置 Oracle Solaris 内核区

Oracle Solaris 内核区是 Oracle Solaris 11.2 及更高版本提供的功能。一个可以作为独立于全局区域的操作系统 (OS) 运行的区域。Oracle Solaris 内核区与非全局区域不同，通过不依赖于全局区域的单独内核运行。这将增强操作系统和应用程序的独立性，并提高安全性。

关于配置 Oracle Solaris 内核区的步骤详情，请参见所使用版本的《Creating and Using Oracle Solaris Kernel Zones》。此外，关于内核区已知问题，请参见所使用版本的《Oracle Solaris Release Notes》中的“Kernel Zone Issues”。

8.2.1 Oracle Solaris 内核区的硬件和软件要求

下述显示了 XCP 和 Oracle Solaris 的版本以及执行 Oracle Solaris 内核区域所必需的 SRU。

- SPARC M12 XCP 3021 或更高版本，Oracle Solaris 11.2 SRU11.2.4.6.0 或更高版本
- SPARC M10 XCP 2230 或更高版本，Oracle Solaris 11.2 SRU11.2.4.6.0 或更高版本

下述显示了 XCP 和 Oracle Solaris 的版本以及执行 Oracle Solaris 内核区域热/实时迁移所必需的 SRU。

- SPARC M12 XCP 3021 或更高版本，Oracle Solaris 11.3 或更高版本
- SPARC M10 XCP 2280 或更高版本，Oracle Solaris 11.3 或更高版本

Oracle Solaris 内核区可以在逻辑域上运行。然而，在一个逻辑域上同时可运行的 Oracle Solaris 内核区的数量受限制。SPARC M12 系统的限制为 512 个，SPARC M10 系统的限制为 256 个。

8.2.2 Oracle Solaris 内核区上的 CPU 管理

当 Oracle Solaris 内核区配置在 SPARC M10 上时，我们建议执行带有 `dedicated-cpu property` 选项的 `zonecfg` 命令，以内核为单位将专用 CPU 分配给 Oracle Solaris 内核区。这可以最大限度地提高 CPU 的性能。

有关 `zonecfg` 命令的详情，请参见《Oracle Solaris Reference Manuals》。

8.2.3 Oracle Solaris 内核区注意事项

- 如果 Oracle Solaris 内核区正运行在物理分区的任何域上，您将无法执行物理分区动态重新配置 (PPAR DR)。请停止 Oracle Solaris 内核区，然后执行物理分区的动态重新配置。
- 在内核区正在来宾域上使用时，如果执行实时迁移或 PPAR DR (`deleteboard` 命

令), 在引导内核区之前需重新启动来宾域。

- 在 SPARC M12 和 SPARC M10 系统之间设置了 `cpu_arch=sparc64-class1` 的 Oracle Solaris 内核区域执行热/实时迁移之前, 请执行以下操作。

1.将以下行添加到安装了 Oracle Solaris 11.3 或更高版本的迁移目标内核区域上的 `/etc/system` 中。

```
set enable_lghz_stick = 1
set uhrt_enable=0x0
```

2.重新启动添加了上述行的内核区域。

- 在 SPARC M10 系统与 SPARC M10 以外的系统之间或 SPARC M10 系统之间执行 Oracle Solaris 内核区域的热/实时迁移之前, 请执行以下操作。

需要执行操作的逻辑域/Oracle Solaris 内核区域如下。

- 安装有运行在迁移目的地/源的 SPARC M10 上的 Oracle Solaris 11.3 或更高版本的所有逻辑域和 Oracle Solaris 内核区域
- 安装有 Oracle Solaris 11.3 或更高版本从 SPARC M10 以外的系统迁移来的 Oracle Solaris 内核区域

1.将以下行添加到符合上述条件的逻辑域/内核区域的 `/etc/system` 文件中。

```
set uhrt_enable = 0x0
```

2.重新启动添加了上述行的逻辑域/内核区域。

8.3 从 XSCF Shell 切换到控制域控制台

从 XSCF 终端登录 XSCF shell 后, 执行 `console` 命令以便使用控制域控制台。使用一个命令将 XSCF shell 切换到控制域控制台的功能被称为 XSCF 控制台重定向功能。在 SPARC M12/M10 系统中, XSCF 与 SPARC M12/M10 机箱具有直接串行连接。用户执行 `console` 命令时, XSCF 自动选择有效控制域的路径并切换到控制域控制台。

8.3.1 如何从 XSCF shell 切换到目标控制域控制台

当 PC 或工作站已建立了 XSCF-LAN 或串行连接时, 您只能在一个窗口画面上操作 XSCF shell 和控制域控制台。本节介绍切换的步骤。

1. 在 **XSCF shell** 终端上执行 **console** 命令以切换到控制域控制台。
下面是指定物理分区 0 的示例。

```
XSCF> console -p 0
```

2. 确认已切换到控制域控制台窗口画面。

```
#
```

每个物理分区只能连接一个 RW 控制台。当用户具有对物理分区的 `platadm` 或 `pparadms` 权限并强制连接另一个 RW 控制台时，当前连接的 RW 控制台会断开。

8.3.2 适当情况下连接到控制域控制台

当目标物理分区电源关闭时，不能切换到控制域控制台。
本节介绍如何开启物理分区并连接到控制域控制台。

1. 在 **XSCF shell** 终端上，指定物理分区并执行 `poweron` 命令以开启物理分区。
2. 参考 ["2.2 登录 XSCF Shell"](#)，设置并登录到其他 **XSCF shell** 终端，以在其他窗口中显示控制域控制台。
3. 执行 `console` 命令。
4. 确认已切换到指定的控制域控制台。

8.4 从控制域控制台返回 XSCF Shell

完成对控制域控制台的操作后，您可以按下相关的按键返回 XSCF shell。

8.4.1 如何从控制域控制台切换到 XSCF shell

本节介绍如何将控制域控制台切换回 XSCF shell。

1. 如需从控制域控制台返回到 **XSCF shell**，请按 **[Enter]** 键，再按 **[#]** 键（转义符的默认值）和 **[.]**（句点）键。
要设置一个不同于默认值的转义符，请指定相关的选项并执行 `console` 命令。处理默认值，转义符只在当前会话中有效。以下是转义符变为 `[!]` 的示例。

```
XSCF> console -p 0 -s "|"  
Console contents may be logged.  
Connect to DomainID 0?[y|n] :y
```

有关转义符的类型，请参见 `console(8)` 命令的 `man` 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

2. 确认 **XSCF shell** 提示符 (**XSCF>**) 出现在终端上。

8.4.2 从控制域控制台注销

如果从域控制台返回 XSCF shell 而不注销该域，您会被自动从域中注销。如果退出 XSCF shell 而不注销该域，您会被自动从域中注销。此时，结束信号会发送到从域控制台启动的后台程序。

如需了解域控制台未被使用时会话超时时间设置的详情，请参见 Oracle Solaris 参考手册中关于 `ttymon` 的说明。

8.5 启动逻辑域

使用 Oracle VM Server for SPARC 的 `ldm start-domain` 命令分别启动逻辑域。此操作只能由 `root` 用户或具有 `ldomadm` 权限的用户执行。

```
primary# ldm start-domain ldom
```

对于 `ldom`，指定将要启动逻辑域的名称。

有关 `ldm` 命令的详情，请参见您所使用版本的《Oracle VM Server for SPARC Reference Manual》。

操作步骤

1. 从 **XSCF** 控制台切换到目标逻辑域所属的控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 ["8.3 从 XSCF Shell 切换到控制域控制台"](#)。
如果您已经切换到目标控制域控制台，请转到下一步。
2. 执行 `ldm list-domain` 命令，查看域启动状态。
下面是查看 `primary`、`ldom1`、`ldom2` 和 `ldom3` 逻辑域状态的示例。

```
primary# ldm list-domain
NAME          STATE      FLAGS    CONS    VCPU  MEMORY  UTIL  UPTIME
primary      active    -n-cv-   SP       8     4G      3.1%  1d 36m
ldom1        active    -n----   5001    24    2G      34%   1m
ldom2        bound     -n----   5002    16    1G
ldom3        active    -n----   5003    16    4G      17%   17h 48m
```

3. 执行 `ldm start-domain` 命令启动指定的域。
下面是启动 `ldom2` 的示例。

```
primary# ldm start-domain ldom2
```

4. 执行 `ldm list-domain` 命令，查看域启动状态。
下面是查看 `primary`、`ldom1`、`ldom2` 和 `ldom3` 逻辑域状态的示例。

```
primary# ldm list-domain
NAME          STATE      FLAGS   CONS   VCPU  MEMORY  UTIL  UPTIME
primary       active    -n-cv-  SP     8     4G      3.1%  1d 36m
ldom1         active    -n----  5001   24    2G      34%   1m
ldom2         active    -n----  5002   16    1G      34%   17h 48m
ldom3         active    -n----  5003   16    4G      17%   17h 48m
```

您可以看到逻辑域 ldom2 已成功启动。

8.6 关闭逻辑域

使用 Oracle VM Server for SPARC 的 `ldm stop-domain` 命令分别关闭逻辑域。此操作只能由 root 用户或具有 ldomadm 权限的用户执行。

```
primary# ldm stop-domain ldom
```

对于 ldom，指定将要关闭逻辑域的名称。
有关 ldm 命令的详情，请参见您所使用版本的《Oracle VM Server for SPARC Reference Manual》。

操作步骤

1. 从 **XSCF** 控制台切换到目标逻辑域所属物理分区控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 ["8.3 从 XSCF Shell 切换到控制域控制台"](#)。
如果您已经切换到目标控制域控制台，请转到下一步。
2. 执行 **ldm list-domain** 命令，查看域启动状态。
下面是查看 primary、ldom1、ldom2 和 ldom3 逻辑域状态的示例。

```
primary# ldm list-domain
NAME          STATE      FLAGS   CONS   VCPU  MEMORY  UTIL  UPTIME
primary       active    -n-cv-  SP     8     4G      3.1%  1d 36m
ldom1         active    -n----  5001   24    2G      34%   1m
ldom2         active    -n----  5002   16    1G      34%   17h 48m
ldom3         active    -n----  5003   16    4G 1    7%    17h 48m
```

3. 执行 **ldm stop-domain** 命令关闭指定的域。
下面是关闭 ldom2 的示例。

```
primary# ldm stop-domain ldom2
```

4. 执行 **ldm list-domain** 命令，查看域启动状态。
下面是查看 primary、ldom1、ldom2 和 ldom3 逻辑域状态的示例。

```
primary# ldm list-domain
NAME          STATE      FLAGS    CONS    VCPU    MEMORY  UTIL  UPTIME
primary       active    -n-cv-   SP      8       4G      3.1%  1d 36m
ldom1         active    -n----- 5001    24      2G      34%   1m
ldom2         bound     ------ 5002    16      1G
ldom3         active    -n----- 5003    16      4G 1    7%    17h 48m
```

域关闭后，状态会变为资源绑定状态 (bound)。

8.7 按顺序关闭逻辑域

在 SPARC M12/M10 系统中，可以从 XSCF 执行所有逻辑域的按顺序关闭。有关如何启动按顺序关闭的详细信息，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

使用 `ldm` 命令，您可以通过设置逻辑域的关闭组编号来修改关闭顺序。按照其关闭组编号降序对逻辑域进行关闭。也就是，编号最高的域最先关闭。编号最低的域最后关闭。如果多个域共享优先级，则关闭顺序是同时的，除非有主从关系。此时，从域在主域前关闭。

有关如何设置主域和从域的详细信息，请参见《Oracle VM Server for SPARC 3.4 Administration Guide》。

有效值为 1 到 15。控制域的关闭组编号为 0，不能更改。其它任何域的默认值为 15。

```
# ldm set-domain shutdown-group=8 secondary
```

假设所有其它来宾域具有默认关闭组编号。那么，在按顺序关闭期间，将首先关闭所有来宾域，然后关闭 `secondary` 域，最后关闭控制域。

例如，命名为 “secondary” 的域不是默认关闭组编号。

注 - 当逻辑域处于 `inactive`、`bound` 和 `active` 状态时，您可以设置 `shutdown-group` 属性。您也可以在新创建逻辑域时设置属性。但是，XSCF 必须先识别新属性值后，更新的关闭顺序属性才会生效。

为了让 XSCF 识别设定的属性值，将每个域设置到 `bound` 或 `active` 状态，然后使用 `ldm add-spconfig` 命令保存逻辑域配置信息。之后，重新开启服务器以使 XSCF 识别新配置。

8.7.1 域表 (ldomTable)

`ldomShutdownGroup` 属性被添加到 `ldomTable`。`ldomTable` 用于表示系统中的每个域，并且可从 Oracle VM Server for SPARC MIB 获取信息。

表 8-1 域表 (ldomTable)

名称	数据类型	访问	说明
ldomShutdownGroup	整数	只读	来宾域的关闭组编号。 在 SPARC M12/M10 系统中，当 XSCF 启动按顺序关闭时，域将以关闭组号的降序关闭（从 15 到 0 的顺序）。默认值为 15。

8.7.2 域信息 (ldom_info) 资源

shutdown-group 属性被添加到 ldom_info 资源中的选项属性。

```
<Envelope>
  <References/>
  <Content xsi:type="ovf:VirtualSystem_Type" id="primary">
    <Section xsi:type="ovf:ResourceAllocationSection_type">
      <Item>
        <rasd:OtherResourceType>ldom_info</rasd:OtherResourceType>
        :
        :
        <gprop:GenericProperty key="shutdown-group">0</gprop:GenericProperty>
        :
        :
      </Item>
    </Section>
  </Content>
</Envelope>
```

ldom_info 资源始终包含在<Content>部分中。ldom_info 资源中的以下属性为可选属性。

- shutdown-group

此属性表示在按顺序关闭期间所使用的关闭优先级。以关闭组降序（从 15 到 0）将关闭请求发送给域。控制域的关闭组始终为 0。其它域的关闭组有效值为 1 到 15。

有关 ldom_info 资源其他属性的详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》。

8.8 检查 CPU 激活信息

使用 ldm 命令可显示 CPU 激活列表。有关 CPU 激活的详情，请参见“第5章 CPU 激活”。

1. 执行以下的子命令查看 CPU 激活信息列表。

```
# ldm list-permits
```

执行 `ldm list-permit` 命令时，将显示以下信息。

表 8-2 `list-permits` 命令显示的内容

项目	说明
PERMITS	显示已分配到物理分区的 CPU 激活的数量。
IN USE	显示逻辑域中使用的 CPU 激活的数量。
REST	显示逻辑域中未使用的 CPU 激活的数量。

在以下示例中，PERMITS 列显示已将 15 个 CPU 激活（权限数）分配给物理分区。IN USE 栏显示当前正在使用的所有许可中的 14 个 CPU 内核。REST 栏显示还有一个 CPU 内核可供使用。

```
#ldm list-permits
CPU CORE
PERMITS (PERMANENT)  IN USE      REST
15                    (15)      14        1
```

有关查看域资源其他列表的详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》。

8.9 设置控制域的 OpenBoot PROM 环境变量

本节介绍在控制域可设置的 OpenBoot PROM 环境变量中，XSCF 固件可设置的项目。

关于 OpenBoot PROM 和 OpenBoot PROM 环境变量的详细信息，请参见 Oracle Solaris 的参考手册中 `eeprom` 的说明以及 Oracle 公司的《OpenBoot 4.x Command Reference Manual》。

有关 SPARC M12/M10 系统特定的 OpenBoot PROM 命令和 OpenBoot PROM 环境变量的信息详情，请参见“附录 H [OpenBoot PROM 环境变量和命令](#)”。

8.9.1 XSCF 固件可设置 OpenBoot PROM 环境变量

控制域可设置的 OpenBoot PROM 环境变量中，XSCF 固件可设置以下环境变量。

表 8-3 在 XSCF 设置的控制域的 OpenBoot PROM 环境变量

OpenBoot PROM 环境变量	说明	设置方法
<code>auto-boot?</code>	开机时自动启动控制域（默认值为 <code>true</code> ）。启动脚本启动已设置此变量的物理分区前，配置 XSCF 固件使 OS 不自动启动（在 <code>{0}ok</code> 停止）。	

表 8-3 在 XSCF 设置的控制域的 OpenBoot PROM 环境变量 (续)

OpenBoot PROM 环境变量	说明	设置方法
input-device	设置控制域控制台的输入设备（默认值是 virtual-console）。 如果 OpenBoot PROM 无法启动，使用 XSCF 固件更新 OpenBoot PROM 环境变量并且启动 OpenBoot PROM。	启动脚本
output-device	设置控制域控制台的输出设备（默认值是 virtual-console）。 如果 OpenBoot PROM 无法启动，使用 XSCF 固件更新 OpenBoot PROM 环境变量并且启动 OpenBoot PROM。	启动脚本
use-nvramrc?	设置控制域启动时是否执行 nvramrc 的内容（默认值是 false）。 如果 OpenBoot PROM 无法启动，使用 XSCF 固件更新 OpenBoot PROM 环境变量并且启动 OpenBoot PROM。	use-nvramrc 操作数
security-mode	设置固件的安全模式（默认是 none）。 如果 OpenBoot PROM 无法启动，使用 XSCF 固件更新 OpenBoot PROM 环境变量并且启动 OpenBoot PROM。	security-mode 操作数

以下是根据每种类型，使用 setpparparam 命令对上述 OpenBoot PROM 环境变量进行设置的方法。

- 设置启动脚本中的环境变量
auto-boot?、input-device 和 output-device 的 OpenBoot PROM 环境变量由 setpparparam 命令的启动脚本设置。启动脚本是 OpenBoot PROM 启动时执行的一系列 OpenBoot PROM 命令。使用 setpparparam 命令的 -s bootscrip 选项进行设置。使用 setpparparam 命令设置的启动脚本只用于控制域启动时。启动后脚本的内容被清除。在启动脚本中，您可以设置多个 OpenBoot PROM 由 254 个字符组成的命令。如果启动脚本设置不正确，或者您想删除启动脚本，在 -s bootscrip 后指定 -r 选项。
- 使用 setpparparam 命令的操作数设置环境变量
使用 setpparparam 命令的操作数设置 OpenBoot PROM 环境变量 user-nvramrc? 和 security-mode。这些环境变量不能在启动脚本中设置。

8.9.2 设置控制域的 OpenBoot PROM 环境变量

使用 XSCF 固件 setpparparam 命令设置控制域的 OpenBoot PROM 环境变量。请使用拥有 platadm 或 fieldeng 权限的用户账户执行此命令。对于目标物理分区，具有 pparadm 权限的用户帐户也能执行此操作。

配置启动脚本

```
XSCF> setpparparam -p ppar_id -s bootscrip value
```


用 `ppar_id` 设置其环境变量存储在启动脚本中的物理分区。根据系统配置，可指定 0 到 15 的整数。

如需更改 OpenBoot PROM 环境变量，设置要存储在启动脚本中的 OpenBoot PROM 设置值。通过加双引号 ("") 指定一个值。

将 `use-nvramrc?` 设置为 `false`

```
XSCF> setpparparam -p ppar_id use-nvramrc
```

用 `ppar_id` 设置储存环境变量的物理分区。根据系统配置，可指定 0 到 15 的整数。

将 `security-mode` 设置为 `none`

```
XSCF> setpparparam -p ppar_id security-mode
```

用 `ppar_id` 设置储存环境变量的物理分区。根据系统配置，可指定 0 到 15 的整数。

操作步骤

1. 设置控制域的 **OpenBoot PROM** 环境变量。

以下是为 PPAR-ID 0 控制域启用 `auto-boot` 的示例。

```
XSCF> setpparparam -p 0 -s bootscript "setenv auto-boot? true"
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable bootscript will be changed.
Continue? [y|n]: y
```

以下是为 PPAR-ID 0 将 OpenBoot PROM 环境变量 `use-nvramrc?` 设置为 `false` 的示例。

```
XSCF> setpparparam -p 0 use-nvramrc
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable use-nvramrc will be set to false.
Continue? [y|n]: y
```

以下是为 PPAR-ID 0 将 OpenBoot PROM 环境变量 `security-mode` 设置为 `none` 的示例。

```
XSCF> setpparparam -p 0 security-mode
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable security-mode will be set to none.
Continue? [y|n]: y
```

8.9.3 查看控制域的 OpenBoot PROM 环境变量

使用 XSCF 固件 `showpparparam` 命令查看由 `setpparparam` 命令设置的控制域的 OpenBoot PROM 环境变量。

请使用具有 `useradm`、`platadm`、`platop` 或 `fieldeng` 权限的用户账户执行此命令。对于目标物理分区，您也可使用具有 `pparadm`、`pparmgr` 或 `pparop` 权限的用户帐户执行此操作。

```
XSCF> showpparparam -p ppar_id
```

用 `-ppar_id` 设置将要查看的环境变量的物理分区。根据系统配置，可指定 0 到 15 的整数。

操作步骤

1. 查看控制域的 **OpenBoot PROM** 环境变量和启动脚本。
以下是查看 PPAR-ID 0 控制域环境变量的示例。

```
XSCF> showpparparam -p 0
use-nvramrc           :false
security-mode         :none
bootscript            :
setenv auto-boot?    true
```

以下是查看为控制域 PPAR-ID 0 设置的 OpenBoot PROM 环境变量 `auto-boot?` 当前设置的示例。

```
XSCF> showpparparam -p 0 -c auto-boot
auto-boot?           :true
```

8.9.4 初始化控制域的 OpenBoot PROM 环境变量

使用 XSCF 固件 `setpparparam` 命令清除控制域 OpenBoot PROM 环境变量并且返回到出厂状态。

请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。对于目标物理分区，具有 `pparadm` 权限的用户帐户也能执行此操作。

```
XSCF> setpparparam -p ppar_id set-defaults
```

用 `ppar_id` 设置初始化环境变量的物理分区。根据系统配置，可指定 0 到 15 的整数。

操作步骤

1. 清除控制域的 **OpenBoot PROM** 环境变量。
在以下的示例中，PPAR-ID 0 控制域的 OpenBoot PROM 环境变量被清除，并恢

复到出厂状态。

```
XSCF> setpparparam -p 0 set-defaults
PPAR-ID of PPARs that will be affected:0
All OpenBoot PROM variables will be reset to original default
values.
Continue? [y|n]: y
```

8.10 域控制台日志功能

在逻辑域环境中，控制域的控制台输出目的地是 XSCF。所有其他逻辑域的控制台输出目的地是启动虚拟控制台终端收集和分配单元 (vcc) 的服务域。

在 Oracle Solaris 11.1 及更高版本，服务域支持除了控制域之外的逻辑域的控制台日志功能。

日志数据被保存到一个名为 `/var/log/vntsd/domainname/console-log` 的文件，此文件位于提供虚拟控制台终端收集和分配单元的服务域。执行 `logadm` 命令时，控制台日志文件被转储。有关详细信息，请参见 `logadm` 命令的 `man` 页和 `logadm.conf` 文件。

Oracle VM Server for SPARC 软件允许您启用和禁用除控制域之外的每个逻辑域的控制台日志功能。默认情况下控制台日志功能启用。

8.10.1 禁用控制台日志功能的方法

1. 查看域的当前控制台设置。

```
# ldm list -o console domain
```

2. 禁用控制台日志功能。

```
# ldm set-vcons log=off domain
```

注 - 如需使用 `ldm set-vcons` 命令修改控制台日志功能设置，您需将域设置为 `unbind` 状态，即 `inactive` 状态。

注 - 您需对每个来宾域启用 (on) 或禁用 (off) 控制台日志功能。

8.10.2 启用控制台日志功能的方法

1. 查看域的当前控制台设置。

```
# ldm list -o console domain
```

2. 启用控制台日志功能。

```
# ldm set-vcons log=on domain
```

8.10.3 服务域要求

必须在 Oracle Solaris 11.1 或更新版本启动服务域，才能使用控制域日志功能。

注 - 您需对每个来宾域启用 (on) 或禁用 (off) 控制台日志功能。

8.10.4 虚拟控制台组表 (ldomVconsTable)

ldomVconsLog 属性作为 Oracle VM Server for SPARC MIB 信息已添加到 ldomVconsTable。ldomVconsTable 显示虚拟控制台服务的所有虚拟控制台组。

表 8-4 虚拟控制台组表 (ldomVconsTable)

名称	数据类型	访问	说明
ldomVconsLog	显示的字符串	只读	控制台日志记录状态。属性值是由 ldm set-vcons 命令指定的字符串 "on" 或 "off"。

注 - 当一个组包含多个域时，ldomVconsLog 属性将显示最近由 ldm set-vcons 命令修改的域的控制台日志状态。

8.10.5 控制台资源

enable-log 属性已作为 XML 接口添加到控制台资源。

```
<Envelope>
  <References/>
  <Content xsi:type="ovf:VirtualSystem_Type" id="ldg1">
    <Section xsi:type="ovf:VirtualHardwareSection_Type">
      <Item>
        <rasd:OtherResourceType>console</rasd:OtherResourceType>
          :
          :
        <gprop:GenericProperty key="enable-log">on</gprop:GenericProperty>
      </Item>
    </Section>
  </Content>
</Envelope>
```

```
</Item>
</Section>
</Content>
</Envelope>
```

控制台资源始终包含在<Content>部分中。可使用包含以下键值的标签。

- **enable-log**
此键值启用或禁用目标控制台的虚拟控制台日志记录。

有关控制台资源的其他属性的详细信息，请参见所用版本的《Oracle VM Server for SPARC Administration Guide》或《Oracle VM Server for SPARC Management Information Base User Guide》。

8.11 更改逻辑域的配置

您可为逻辑域灵活地分配 CPU、内存、I/O 设备和物理分区中其他的硬件资源。您也可以正在运行的逻辑域中动态重组 CPU 和内存，这样您就可以处理临时的负荷增加而不必停止业务。根据域的运行方式，您可以添加或删除资源，这样您就可以有效使用服务器上的硬件资源并且提高利用率。

此外，CPU 内核资源可以通过组合逻辑域配置变更和 CPU 激活动态添加到逻辑域。通过分配未使用的 CPU 内核资源，不必从其他域借用资源就可以处理需求扩充资源。

Oracle VM Server for SPARC 用于动态重新配置 CPU 和内存。

有关变更逻辑域配置的方法，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的“第3章 域配置的操作”。

8.12 设置逻辑域时间

本节介绍设置逻辑域时间的必要知识和设置指南。

SPARC M12/M10 系统管理以下时间。

- 保持在 XSCF 上的时间
XSCF 管理系统的标准时间。由主 XSCF 管理，所有的 XSCF 都被设置成相同的时间。即使输入电源关闭也会保持。
- 保持在物理分区上的时间
管理程序管理各物理分区的时间。
- 保持在逻辑域上的时间
各逻辑域管理的时间。各逻辑域可保持不同的时间。

有关 XSCF 时间和逻辑域时间之间关系的详细信息，请参见“3.6 设置 XSCF 时间/日期”。

8.13 收集管理程序转储文件

本节介绍如何为管理程序转储文件的收集进行设置。

8.13.1 管理程序转储基本知识

管理程序可能会由于硬件故障或软件错误而终止。管理程序中止时，在所有逻辑域被重置之后，只有控制域以特定出厂默认配置启动，以便收集管理程序转储，并将管理程序信息保存为转储文件。这被称为管理程序转储功能。

所收集的转储文件对于诊断问题来说可能是非常重要的信息。

注 - 如果启用管理程序转储，当使用指定了 `xir` 选项的 XSCF 固件 `reset` 命令重置物理分区时，仍然收集管理程序转储。有关物理分区重置的详情，请参见“[10.17 重启物理分区](#)”。

注 - 如需从特定出厂默认配置返回原始配置来收集管理程序转储，您需要重新启动物理分区。

在控制域中收集以下文件名的转储文件。最多可以收集八个文件。

- 存储目录：
 `/var/opt/SUNWldm`
- 文件名：
 `hvdump.x.gz`
 x: 自动分配 0 到 7 之间的整数。

下一节介绍管理程序转储功能的命令。

8.13.2 管理程序转储功能的命令

启用/禁用管理程序转储

使用 Oracle VM Server for SPARC 的 `ldm set-hvdump` 命令设置管理程序转储。

```
primary# ldm set-hvdump [hvdump=on|off] [hvdump-reboot=on|off]
```

`hvdump` 指定是否启用管理程序转储功能。如需启用，指定为 `on`。如需禁用，请指定 `off`。默认启动 (`on`)。

对于 `hvdump-reboot`，指定是否在转储文件收集后自动重新启动物理分区。如需重新启动物理分区，请指定 `on`。如不需重启，指定为 `off`。默认值为 `off`。如果该值设置为 `off`，则即使在收集转储文件之后，控制域仍处于特定出厂默认配置，以收集管理程序转储。

如果您通过 `ldm set-hvdump` 命令更改 `hvdump` 和 `hvdump-reboot` 设置，请使用 `ldm add-spconfig` 命令保存配置信息。

```
primary# ldm add-spconfig file
```

注 - 即使重新启动以特定出厂默认配置启动的控制域来收集管理程序转储，系统也不会返回原始配置。如需在原始配置中启动系统，您需要重新启动物理分区。执行 XSCF 的 `poweroff` 命令或 Oracle Solaris 的 `shutdown -i5` 命令后，执行 XSCF 的 `poweron` 命令重新启动系统。

注 - 即使 `hvdump-reboot` 设置为 `on`，如果因为已收集八个转储文件或磁盘空间不足而没有收集转储文件，则物理分区无法重新启动。在这种情况下，首先移动或删除收集的转储文件。然后，使用 `ldm start-hvdump` 命令收集转储文件。转储文件收集完成后，重新启动物理分区。

查看管理程序转储设置的内容

使用 `ldm list-hvdump` 命令查看管理程序转储的设置。

```
primary# ldm list-hvdump
```

执行 `ldm list-hvdump` 命令后，显示如下的信息。

表 8-5 执行 `ldm list-hvdump` 命令显示的信息

项目	说明
<code>hvdump</code>	是否已启用管理程序转储功能。如果启用， <code>on</code> 显示。如果禁用， <code>off</code> 显示。
<code>hvdump-reboot</code>	创建转储文件后系统是否重新启动。如果将被重启，显示 <code>on</code> 。如果不被重启，显示 <code>off</code> 。

注 - 如果转储文件收集没有正常结束，会显示 "Pending hvdump exists"（存在待处理的信息）信息。

操作步骤

1. 从 **XSCF** 控制台切换到目标控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 ["8.3 从 XSCF Shell 切换到控制域控制台"](#)。
如果您已经切换到控制域控制台或 XSCF，请转到下一步。
2. 设置管理程序转储功能。
下面是启用管理程序转储功能并指定控制域在收集转储文件后重新启动的示例。

```
primary# ldm set-hvdump hvdump=on hvdump-reboot=on
```

3. 查看管理程序转储功能的设置。
下面是管理程序转储功能已启用，并且在收集转储文件后重新启动的示例。

```
primary# ldm list-hvdump  
hvdump=on  
hvdump-reboot=on
```

4. 保存管理程序转储功能的设置。
以下是指定和保存名为 *config_name* 的示例。

```
primary# ldm add-spconfig config_name
```

8.13.3 使用管理程序转储时的注意事项

在使用管理程序转储功能时注意以下事项。

- 如果用于收集转储文件的目录是以下其中一个状态，即使在管理程序中发生错误时也不能收集转储文件：
 - 已经存在八个转储文件，或
 - /var/opt/SUNWldm 目录磁盘空间不足例行检查转储文件的数量和保存转储文件目录的磁盘空间，确保满足转储文件收集的要求。
- 如果由于上述原因无法收集转储文件，转储处理会停止。解决问题后，执行 `ldm start-hvdump` 命令收集转储文件。如果重新启动控制域而没有执行 `ldm start-hvdump` 命令，不但不会收集转储文件而且记录的管理程序信息也将丢失。即使 `hvdump-reboot` 设置为 `on`，如果未收集转储文件，则无法重新启动物理分区。在这种情况下，首先移动或删除收集的转储文件。然后，使用 `ldm start-hvdump` 命令收集转储文件。转储文件收集完成后，重新启动物理分区。
- 即使 `hvdump-reboot` 设置为 `on`，如果 OpenBoot PROM 环境变量 `auto-boot?` 是 `false`，处理将停止在 `ok` 提示符，而不重新启动 Oracle Solaris。
- 如果控制域以出厂默认配置无意中启动，则管理程序转储处理可能无法完成。这可能是由于控制域是以特定出厂默认配置启动以收集管理程序转储。执行 `ldm list-hvdump` 命令检查转储文件是否已被收集。以下是转储文件无法收集的示例。

```
primary# ldm list-hvdump  
hvdump=on  
hvdump-reboot=on  
Pending hvdump exists
```


8.14 管理与 CPU 插槽相关联的逻辑域资源

8.14.1 CPU 插槽约束条件概述

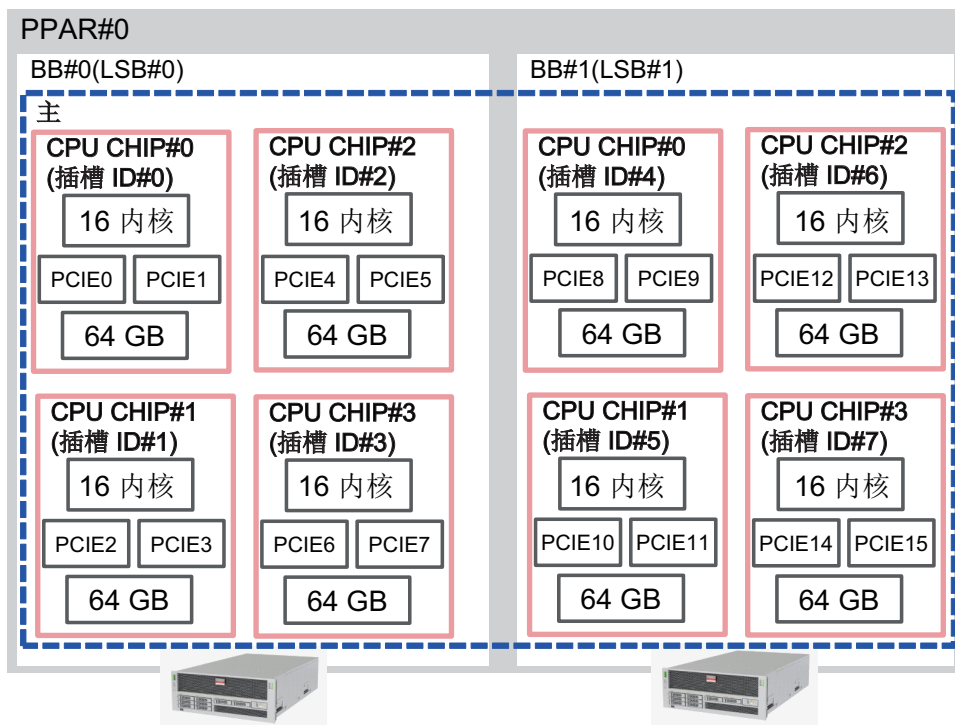
CPU 插槽约束条件可以使您以指定的 CPU 插槽 ID 创建和配置拥有有限的虚拟 CPU、内核或内存的逻辑域。由于 CPU 插槽 ID 与 LSB 编号和 CPU 位置编号相关联，您可以完全手动控制硬件资源，无需使用 CID 和 PA 等物理绑定。

CPU 插槽 ID 由 LSB 编号和 CPU 位置编号确定如下。

$$\text{CPU socket ID} = \text{LSB number} \times 4 + \text{CPU location number}$$

图 8-1 显示了配置有两个 SPARC M10-4S 单元（BB#0 和 BB#1）的物理分区中的物理资源。

图 8-1 物理分区中的资源



有关 LSB 编号和 CPU 位置编号的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的“2.4.1 逻辑域配置注意事项”。

您可以使用 CPU 插槽约束条件来执行类似下面的任务。

- 使用在指定的 CPU 芯片上启用的内存镜像创建可靠性高的域
- 在执行物理分区的动态重新配置 (PPAR DR) 之前，需提前分离要删除的 SPARC M12-2S 和 SPARC M10-4S 资源，以将停止正在执行 PPAR DR 的来宾域的时间最小化。
- 通过将虚拟 CPU 扩展到每个 CPU 芯片，或者通过将虚拟 CPU 合并到一个 CPU 芯片上来调整性能。
- 在也具有搭载 SPARC64 X/SPARC64 X+ 处理器的 SPARC M10-4S 的物理分区中仅使用 SPARC64 X+ 处理器配置逻辑域。

下面的命令是与 CPU 插槽约束条件相关的命令。有关各命令的详情，请参见您所使用版本的《Oracle VM Server for SPARC Reference Manual》。

- ldm list-socket
- ldm set-socket
- ldm grow-socket
- ldm shrink-socket

8.14.2 CPU 插槽约束条件的硬件和软件要求

SPARC M12/M10 平台支持此功能。但是，由于 SPARC M12-1/M10-1 仅有一个 CPU 配置，因此在此功能中没有任何意义。

如需在 SPARC M12/M10 上使用 CPU 插槽约束条件，系统必须满足以下要求。

- 运行 Oracle VM Server for SPARC 3.3 或更高版本
- 对于 SPARC M10，运行 XCP 固件的 XCP 2210 或更高版本
如需启用 CPU 插槽约束条件的 --remap 选项，必须使用 XCP 2260 或更高版本的 XCP 固件。
对于 SPARC M12，没有 XCP 固件要求。
- 使用 M12-2/M12-2S/M10-4/M10-4S

8.14.3 CPU 插槽约束条件的限制

CPU 插槽约束条件有以下限制。

- 如果一个域被迁移，CPU 插槽约束条件也以与物理分配指定 CID 或 PA 同样的方式被清除。
- 执行带 --restore-degraded 选项的 ldm set-socket 命令来恢复 CPU 插槽约束条件。
- 恢复模式忽略了故障 CPU 芯片的 CPU 插槽约束条件。
- ldm init-system -f 命令忽略了控制域的 CPU 插槽约束条件。
- 故障 CPU 的自动更换仅可在指定的插槽资源中起作用。如果在指定的插槽无可用的 CPU，发生故障的 CPU 将被隔离，但不被更换。

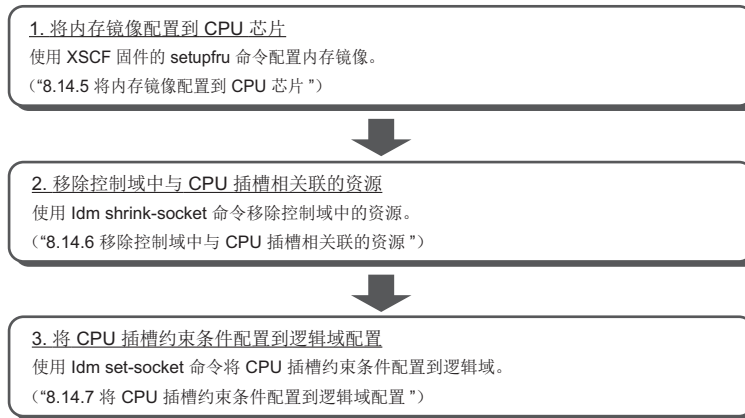
8.14.4 使用 CPU 插槽约束条件创建可靠性高的逻辑域

为了更好地理解 CPU 插槽的约束条件，本节介绍如何使用 CPU 插槽的约束条件创建

可靠性高的逻辑域。

图 8-2 显示了创建可靠性高的逻辑域的流程。

图 8-2 创建可靠性高的逻辑域的流程



后续第 8.14.5 到 8.14.7 节通过提供将 BB#1 中的 CPU 芯片 #0 的资源分配给具有两个 SPARC M10-4S 单元 (BB#0 和 BB#1) 配置的物理分区来创建逻辑域 ldom1 的示例介绍了该流程。

8.14.5 将内存镜像配置到 CPU 芯片

使用 XSCF 固件的 `setupfru` 命令配置内存镜像。有关如何设置内存镜像模式的详细信息，请参见“14.1 配置内存镜像”。有关 `setupfru` 命令的详细信息，请参见 `setupfru(8)` 命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

使用 `ldm list-socket` 命令显示每个 CPU 插槽的资源列表。

下面的示例表明，由于内存镜像模式被设置为 BB#1 中的 CPU 芯片 #0，与 CPU 插槽 #4 关联的内存的大小将减少一半。

```
# ldm list-socket
CONSTRAINTS

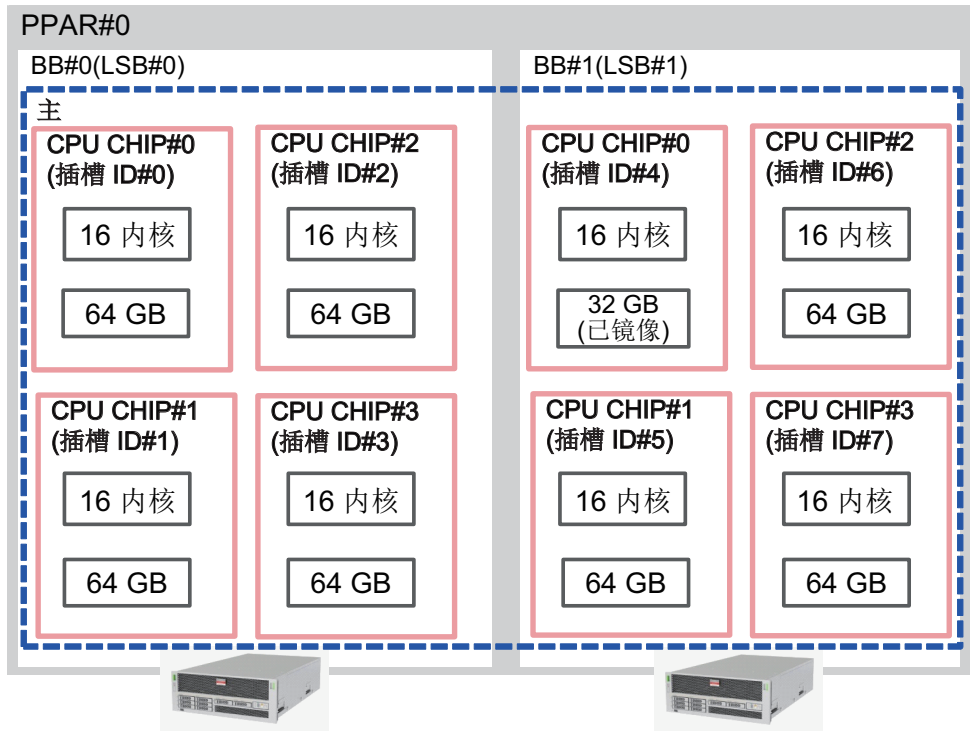
SOCKET
  TENANT      VCPUS  CORES  SOCKET_ID  GROUP
  primary     32     16     0           /BB0
  primary     32     16     1           /BB0
  primary     32     16     2           /BB0
  primary     32     16     3           /BB0
  primary     32     16     4           /BB1
  primary     32     16     5           /BB1
  primary     32     16     6           /BB1
  primary     32     16     7           /BB1
```

MEMORY				
PA	SIZE	SOCKET_ID	BOUND	
0x700000000000	64G	7	primary	
0x720000000000	64G	6	primary	
0x740000000000	64G	5	primary	
0x760050000000	31488M	4	primary	
0x780000000000	64G	3	primary	
0x7a0000000000	64G	2	primary	
0x7c0000000000	64G	1	primary	
0x7e0080000000	62G	0	primary	

IO				
NAME	TYPE	BUS	SOCKET_ID	BOUND
PCIE0	BUS	PCIE0	0	primary
PCIE1	BUS	PCIE1	0	primary
PCIE2	BUS	PCIE2	1	primary
PCIE3	BUS	PCIE3	1	primary
PCIE4	BUS	PCIE4	2	primary
PCIE5	BUS	PCIE5	2	primary
PCIE6	BUS	PCIE6	3	primary
PCIE7	BUS	PCIE7	3	primary
PCIE8	BUS	PCIE8	4	primary
PCIE9	BUS	PCIE9	4	primary
PCIE10	BUS	PCIE10	5	primary
PCIE11	BUS	PCIE11	5	primary
PCIE12	BUS	PCIE12	6	primary
PCIE13	BUS	PCIE13	6	primary
PCIE14	BUS	PCIE14	7	primary
PCIE15	BUS	PCIE15	7	primary

图 8-3 显示了物理分区中拥有配置有两个 SPARC M10-4S 单元 (BB#0 和 BB#1) 的物理分区中的所有资源的控制域。

图 8-3 物理分区中的 CPU 内核和内存



8.14.6 移除控制域中与 CPU 插槽相关联的资源

使用 `ldm shrink-socket` 命令移除控制域中 CPU 插槽 #4 的资源。
下面的示例显示了移除控制域中 CPU 插槽 #4 中的虚拟 CPU 和内存。

```
# ldm shrink-socket cores=16 socket_id=4 primary
# ldm shrink-socket memory=31488M socket_id=4 primary
```

注 - 如果资源忙，`ldm shrink-socket` 命令可能无法移除目标资源。如果发生此情况，请停止逻辑域，然后重试 `ldm shrink-socket` 命令。如果该域是控制域，需使用延迟重新配置，然后再试一次。

使用 `ldm list-socket` 命令列出每个 CPU 插槽的资源。可以确认，CPU 插槽#4 中的内存已经从控制域中移除。

```
# ldm list-socket
CONSTRAINTS

SOCKET
  TENANT      VCPUS  CORES  SOCKET_ID  GROUP
```

```

primary    32    16    0        /BB0
primary    32    16    1        /BB0
primary    32    16    2        /BB0
primary    32    16    3        /BB0
primary    32    16    5        /BB1
primary    32    16    6        /BB1
primary    32    16    7        /BB1

```

```

FREE      VCPUS  CORES  SOCKET_ID  GROUP
-----
32        16    4      /BB1

```

MEMORY

```

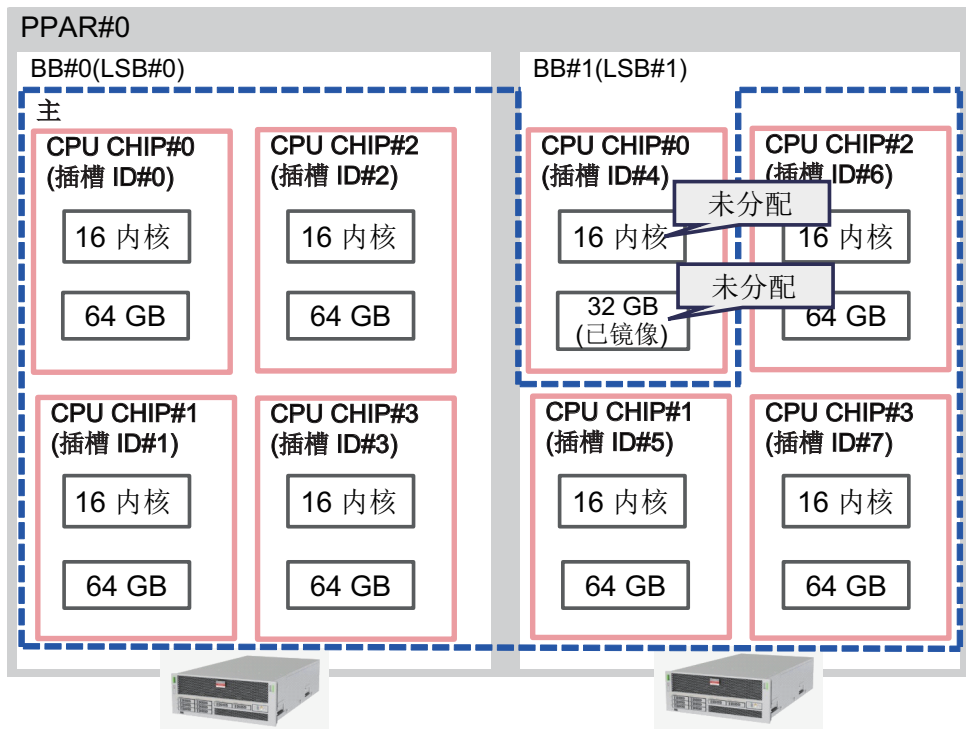
PA          SIZE      SOCKET_ID  BOUND
0x700000000000 64G        7          primary
0x720000000000 64G        6          primary
0x740000000000 64G        5          primary
0x760050000000 31488M     4          primary
0x780000000000 64G        3          primary
0x7a0000000000 64G        2          primary
0x7c0000000000 64G        1          primary
0x7e0080000000 62G        0          primary

```

--- 略 ---

图 8-4 显示了在配置有两个 SPARC M10-4S 单元（BB#0 和 BB#1）的物理分区中执行 ldm shrink-socket 命令后的物理分区配置。

图 8-4 执行 ldm shrink-socket 命令后的资源



8.14.7 将 CPU 插槽约束条件配置到逻辑域配置

下面的示例介绍了如何创建拥有 16 GB 镜像内存和与 CPU 插槽 #4 相关联的 8 个 CPU 内核的逻辑域 ldom1。

使用 `ldm add-domain` 命令创建逻辑域 ldom1。

```
primary# ldm add-domain ldom1
```

使用 `ldm set-socket` 命令约束 ldom1 以使用与 CPU 插槽#4 相关联的资源。

```
primary# ldm set-socket socket_id=4 ldom1
```

将 8 个 CPU 内核和 16-GB 内存分配给 ldom1。

```
primary# ldm set-core 8 ldom1
primary# ldm set-memory 16G ldom1
```

将资源绑定到 ldom1，并启动 ldom1。

```
primary# ldm bind-domain ldom1
primary# ldm start-domain ldom1
```

注 - 如需绑定并启动逻辑域，您应该准备虚拟控制台集中器、虚拟网络交换机和虚拟磁盘服务。有关各项的详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》。

使用 `ldm list-socket` 命令显示每个 CPU 插槽的资源列表。您可以确认只有那些与 CPU 插槽#4 相关联的资源被分配给 ldom1。

```
# ldm list-socket ldom1
CONSTRAINTS
  DOMAIN                SOCKET_ID    STATE
  ldom1                  4            active

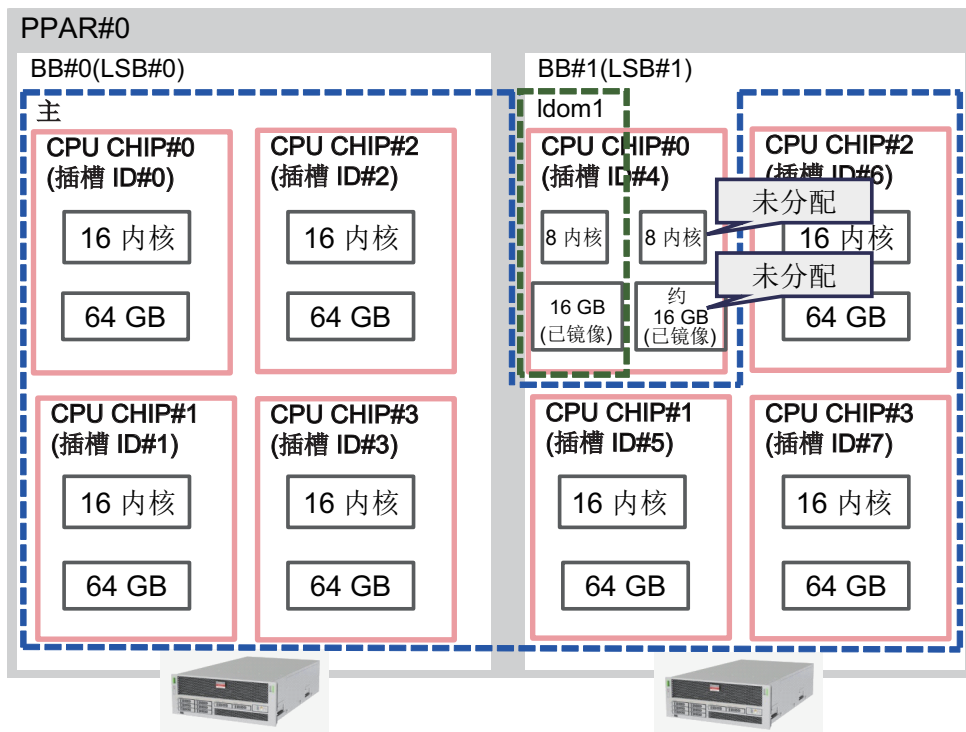
SOCKET
  TENANT                VCPUS    CORES    SOCKET_ID    GROUP
  ldom1                  16       8        4            /BB1

MEMORY
  PA                    SIZE      SOCKET_ID    BOUND
  0x760050000000       16G      4            ldom1

IO
```

图 8-5 显示了在配置有两个 SPARC M10-4S 单元（BB#0 和 BB#1）的物理分区中执行 `ldm set-socket` 命令后的物理分区配置。

图 8-5 执行 ldm set-socket 命令后的资源



8.15 设置物理分区动态重新配置策略

本节介绍如何设置物理分区的动态重新配置策略。

8.15.1 物理分区动态重新配置策略

Oracle VM Server for SPARC 3.4 或更高版本支持物理分区动态重新配置 (PPAR DR) 策略功能。对于 PPAR DR 策略，您可以变更使用 `deleteboard` 命令执行 PPAR DR 操作时 Oracle VM Server for SPARC 使用的资源减少策略。

资源减少策略设置为 `ldmd` 服务的 `ldmd/fj_ppar_dr_policy` 属性。可以设置的资源减少策略是 "auto"、"ratio" 或 "targeted"。

有关各资源减少策略的详细信息，请参见 "8.15.2 资源减少策略的详情"。

8.15.2 资源减少策略的详情

本节介绍各资源减少策略的详细信息。

fj_ppar_dr_policy = auto

此 PPAR DR 策略设置是用于自动使用最新策略的设置。Oracle VM Server for SPARC 3.4 系统设置为 "auto" 时，系统以与设置为 "ratio" 的方式相同的方式操作。"auto" 设置是默认策略。

fj_ppar_dr_policy = ratio

当物理分区中的所有逻辑域均正在运行 Oracle Solaris 11.3 或更高版本并且系统已经使用 XCP 2271 或更高版本时，此策略在 Oracle VM Server for SPARC 3.4 或更高版本的系统上有效。否则，系统以与设置为 "targeted" 的方式相同的方式操作。

假设在剩余模块化架构上的可用资源不足以将资源从需要删除的模块化架构（系统板）移动时，您将资源减少策略设置为 "ratio" 并执行 `deleteboard` 操作，并且由自动从现有的所有域中释放资源减少了资源。

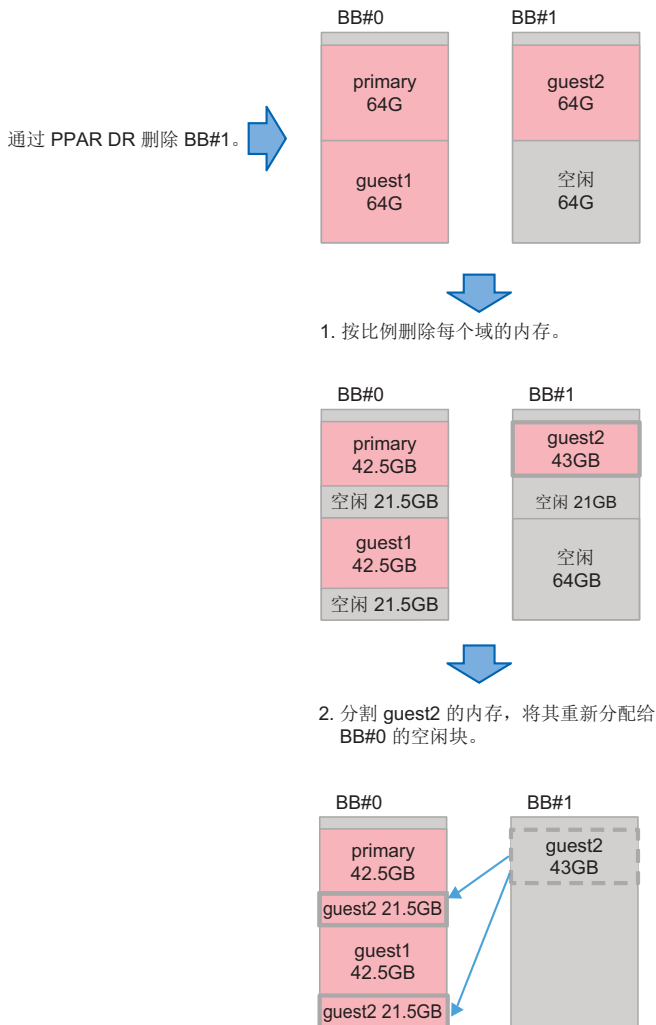
在这种情况下，将根据分配给现有域资源的比例自动释放资源。由于资源忙，或由于其他原因，并不总是知晓确切的减少比例。基于最大努力进行比例的减少。

此策略也支持内存块分割功能，会自动将大的内存块分割成小的内存块。内存块分割消除了对于使用 PPAR DR 移除的模块化架构中的每个重新定位的内存块的目的地模块化架构上具有足够的空闲连续内存区的要求。`deleteboard` 操作可分割域中的内存块以适应剩余模块化架构上的可用空闲区域。

由于资源正在使用或出于其他原因，如果无法从移动目的地模块化架构获取足够的可用资源，则 `deleteboard` 命令将失败，并显示错误消息。在这种情况下，从 `deleteboard` 命令引起的错误信息输出和 Oracle Solaris 信息中查明错误原因，并采取适当措施。有关 `deleteboard` 命令输出的错误消息的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的 "C.1.2 deleteboard"。虽然这样说，但是依据所发生的错误的详细信息，您可能需要关闭或重新启动物理分区。

图 8-6 中介绍将策略设置为 "ratio" 时内存删除的概念。

图 8-6 内存删除的概念（使用 `fj_ppar_dr_policy = ratio` 时）



`fj_ppar_dr_policy = targeted`

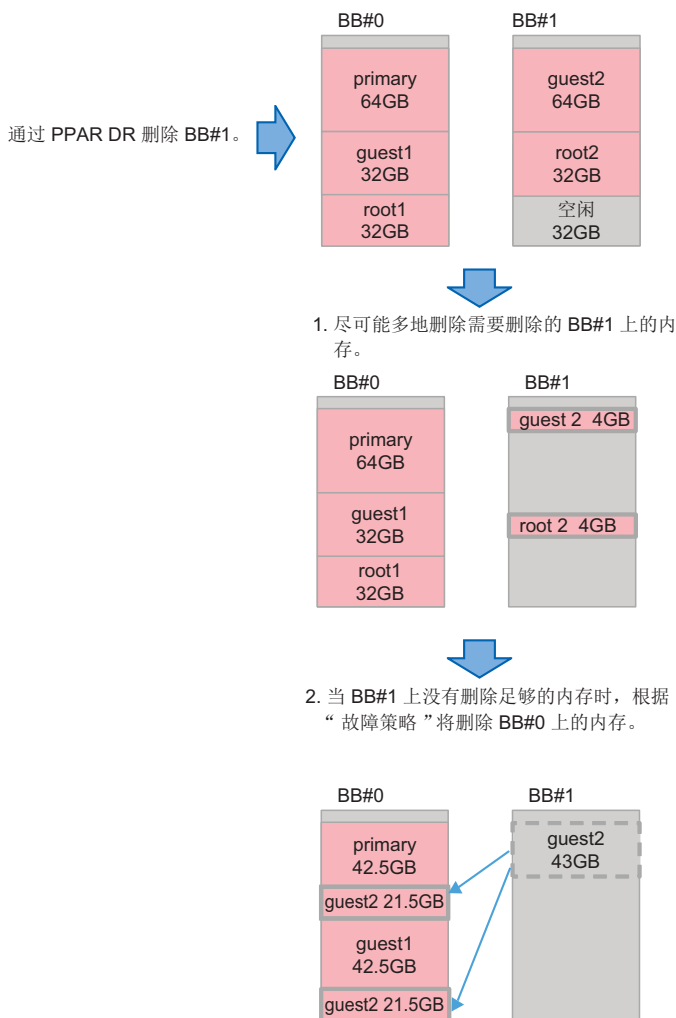
早于 Oracle VM Server for SPARC 3.4 的所有版本将使用 "Targeted" 策略。如果使用此策略可用资源不可用，则将从首先需要删除的模块化架构中具有 CPU/ 内存的各逻辑域释放资源。

如果即使在此删除操作之后，可用资源还不足，则从剩余模块化架构上具有 CPU/ 内存的各逻辑域释放资源。释放资源的逻辑域的顺序使用 "failure-policy" 所定义的顺序。此策略中的顺序为：默认逻辑域（未指定任何内容）、指定 `master` 的逻辑域、I/O 域、根域和控制域。相同作用的域之间的顺序按字母顺序排列。

有关 "failure-policy" 和 "master" 域的详情，请参见《Oracle VM Server for SPARC Administration Guide》中的“Configuring Domain Dependencies”。

如果无法在移动目的地系统板获得可用资源，`deleteboard` 命令会失败，并显示错误消息。在这种情况下，从 `deleteboard` 命令引起的错误信息输出和 Oracle Solaris 信息中查明错误原因，并采取适当措施。但是，依据所发生的错误的详细信息，可能需要关闭或重新启动物理分区。

图 8-7 内存删除的概念（使用 `fj_ppar_dr_policy = targeted` 时）



8.15.3 如何变更 PPAR DR 策略

在 Oracle VM Server for SPARC 3.4 或更高版本中，通过使用 `svccfg` 命令将 PPAR DR 策略设置为 `ldmd` 服务的 `fj_ppar_dr_policy` 属性来更改策略。有关可以设置的 PPAR DR 策略的详细信息，请参见“8.15.2 资源减少策略的详情”。

设置步骤如下。

1. 登录控制域。
2. 成为管理员。
有关详情，请参见《Securing Users and Processes in Oracle Solaris 11.3》。
3. 显示 `fj_ppar_dr_policy` 属性值。

```
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
```

4. 停止 **ldmd** 服务。

```
# svcadm disable ldmd
```

5. 变更 **fj_ppar_dr_policy** 属性值。

```
# svccfg -s ldmd setprop ldmd/fj_ppar_dr_policy=value
```

6. 刷新并重新启动 **ldmd** 服务。

```
# svcadm refresh ldmd  
# svcadm enable ldmd
```

以下示例表明了如何显示 **fj_ppar_dr_policy** 属性值以及如何将其从 "auto" 切换到 "targeted"。

```
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy  
ldmd/fj_ppar_dr_policy astring auto  
# svcadm disable ldmd  
# svccfg -s ldmd setprop ldmd/fj_ppar_dr_policy=targeted  
# svcadm refresh ldmd  
# svcadm enable ldmd  
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy  
ldmd/fj_ppar_dr_policy astring targeted
```

8.16 设置逻辑域的最大页面大小

本节介绍了如何设置逻辑域的最大页面大小以及执行此操作的效果。此设置适用于 Oracle VM Server for SPARC 3.5 或更高版本。

8.16.1 逻辑域的最大页面大小

SPARC M12 支持三种最大页面大小设置（256 MB、2 GB 和 16 GB）。有关如何查看最大页面大小的详情，请参见 ["8.16.5 查看逻辑域的最大页面大小"](#)。

SPARC M10 仅支持 256 MB 的最大页面大小，并且无法更改该设置。

8.16.2 较大的最大页面大小的优点

为最大页面大小设置了较大值时，逻辑域可以使用大页面。通常，当最大页面大小设置为 2 GB 或 16 GB（而不是 256 MB）时，使用大内存的应用程序通常运行得更快。

8.16.3 较大的最大页面大小的缺点

大于标准的最大页面大小的数值会对逻辑域实时迁移、逻辑域上 Oracle Solaris 内核区实时迁移以及使用 `deleteboard` 命令进行 PPAR DR 操作的成功率产生负面影响。我们建议将最大页面大小设置为 256 MB，以确保逻辑域和 Oracle Solaris 内核区实时迁移以及使用 `deleteboard` 命令进行 PPAR DR 操作的最高成功率。有关详情，请参见下述介绍。

实时迁移和使用 `deleteboard` 命令进行 PPAR DR 操作的成功率

实时迁移和使用 `deleteboard` 命令进行 PPAR DR 操作的成功率取决于目标处的内存使用状况。

逻辑域的内存队列限制为最大页面大小的倍数。如果目标处的空闲连续内存区的边界不是最大页面大小的倍数，则内存移动失败。

目标处内存使用状况和较大的最大页面大小影响的示例

图 8-8 显示了逻辑域的最大页面大小设置为 2 GB 时移动内存的示例。即使在目标处存在 2 GB 的空闲连续内存区，由于空闲连续内存区的边界不是最大页面大小的倍数，内存移动也会失败。

图 8-8 逻辑域的最大页面大小设置为 2 GB 时

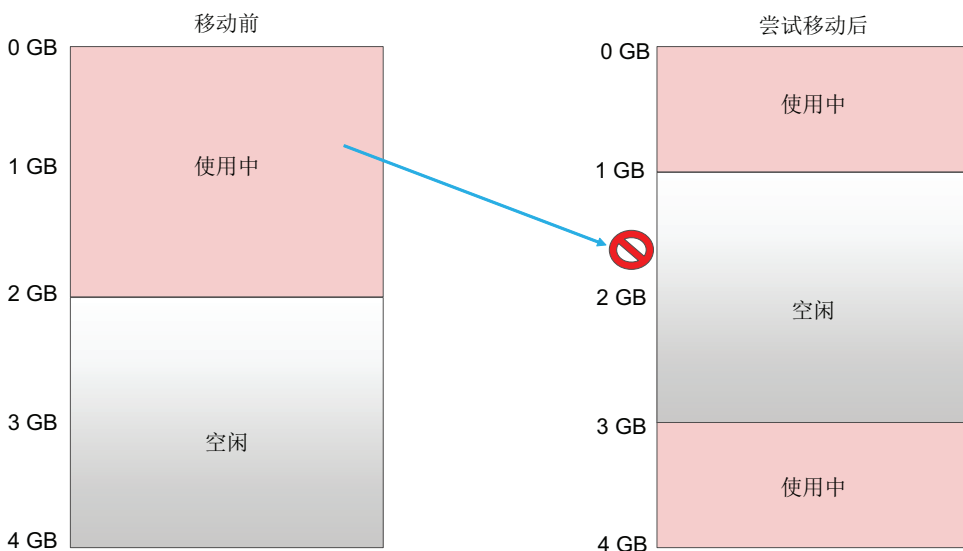
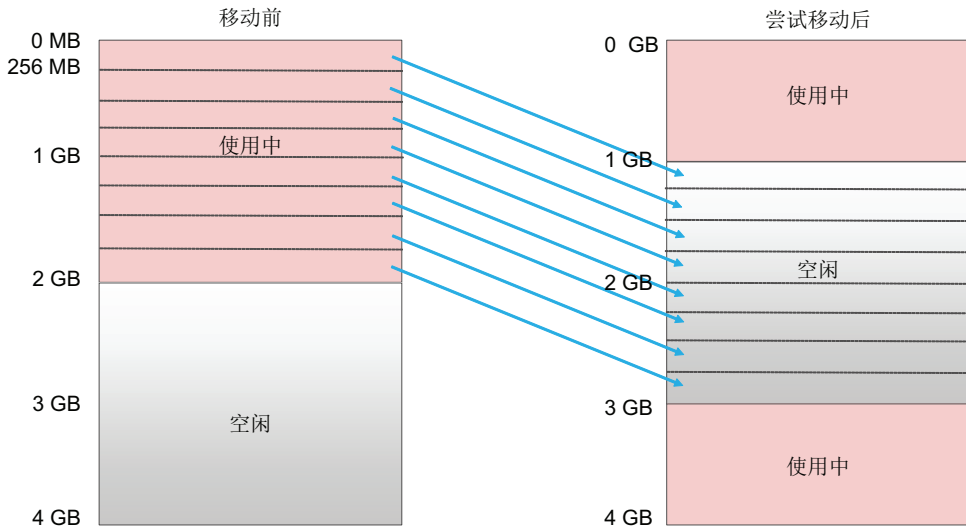


图 8-9 显示了逻辑域的最大页面大小设置为 256 MB 时移动内存的示例。由于目标处的

空闲内存区的边界可以设置为 256 MB 的倍数，内存移动成功。

图 8-9 逻辑域的最大页面大小设置为 256 MB 时



8.16.4 设置和变更逻辑域的最大页面大小

以下方法可用于设置逻辑域的最大页面大小。

- 设置 Idmd 服务的 `fj_dr_sw_limit_pagesize` 属性
- 使用 `ldm add-domain/ldm set-domain` 命令设置和变更 `fj-software-limit-pagesize`

设置 Idmd 服务的 `fj_dr_sw_limit_pagesize` 属性

您可以将 `fj_dr_sw_limit_pagesize` 属性值设置为 "true" 或 "false"。

- **`fj_dr_sw_limit_pagesize=false` [默认值]**
根据分配给逻辑域的内存大小和系统中支持的最大页面大小，对逻辑域的最大页面大小自动设置。
您可以使用 `ldm add-domain` 或 `ldm set-domain` 命令设置最大页面大小 (`fj-software-limit-pagesize`)。
- **`fj_dr_sw_limit_pagesize=true`**
对于新创建的逻辑域，将最大页面大小设置为 256 MB。
即使设置为 "true"，此属性也不会更改控制域和现有逻辑域的当前最大页面大小。

下面介绍了为 Idmd 服务设置 `fj_dr_sw_limit_pagesize` 属性的步骤。

1. 登录控制域。
2. 切换到管理员权限。
有关详情，请参见《Securing Users and Processes in Oracle Solaris 11.3》。
3. 显示 `fj_dr_sw_limit_pagesize` 属性值。

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
```

4. 停止 ldmd 服务。

```
primary# svcadm disable ldmd
```

5. 变更 fj_dr_sw_limit_pagesize 属性值。

```
primary# svccfg -s ldmd setprop ldmd/fj_dr_sw_limit_pagesize=value
```

6. 刷新并重新启动 ldmd 服务。

```
primary# svcadm refresh ldmd  
primary# svcadm enable ldmd
```

在以下示例中，将查看 fj_dr_sw_limit_pagesize 属性值，然后将其从“false”变更为“true”。

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize  
ldmd/fj_dr_sw_limit_pagesize boolean false  
primary# svcadm disable ldmd  
primary# svccfg -s ldmd setprop ldmd/fj_dr_sw_limit_pagesize=true  
primary# svcadm refresh ldmd  
primary# svcadm enable ldmd
```

在以下示例中，将 fj_dr_sw_limit_pagesize 属性值确认为“true”。

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize  
ldmd/fj_dr_sw_limit_pagesize boolean true
```

使用 ldm add-domain/ldm set-domain 命令设置和变更 fj-software-limit-pagesize

- 使用 **ldm add-domain** 命令设置 **fj-software-limit-pagesize**
可以使用 ldm add-domain 命令设置逻辑域的最大页面大小。
如果将 fj_dr_sw_limit_pagesize 属性设置为“true”，则最大页面大小被设置为 256 MB，并且无法更改。
有关 ldm 命令的详情，请参见《Oracle VM Server for SPARC 3.5 Reference Manual》。
以下示例将 256 MB 设置为 domainA（新创建的逻辑域）的最大页面大小。

```
primary# ldm add-domain fj-software-limit-pagesize=256MB domainA
```

- 使用 **ldm set-domain** 命令设置和变更 **fj-software-limit-pagesize**
可以使用 ldm set-domain 命令设置和变更逻辑域的最大页面大小。仅当逻辑域处

于延迟重新配置或非活动状态时，才可设置和变更最大页面大小。然而，如果将 `fj_dr_sw_limit_pagesize` 属性设置为"true"，则最大页面大小被设置为 256 MB，并且无法更改。有关 `ldm` 命令的详情，请参见《Oracle VM Server for SPARC 3.5 Reference Manual》。以下示例将 256 MB 设置为控制域的最大页面大小。

```
primary# ldm start-reconf primary
primary# ldm set-domain fj-software-limit-pagesize=256MB primary
primary# shutdown -y -i6 -g0
```

以下示例将 2 GB 设置为 domainB（逻辑域）的最大页面大小。

```
primary# ldm stop-domain domainB
primary# ldm unbind-domain domainB
primary# ldm set-domain fj-software-limit-pagesize=2GB domainB
primary# ldm bind-domain domainB
primary# ldm start-domain domainB
```

8.16.5 查看逻辑域的最大页面大小

可以使用 `ldm list-domain` 命令查看每个逻辑域的最大页面大小 (`fj-software-limit-pagesize`)。以下是 domainC 的最大页面大小是 2 GB 的示例。

```
primary# ldm list-domain -l domainC
NAME                STATE      FLAGS    CONS    VCPU    MEMORY    UTIL    NORM    UPTIME
domainC             active    -n----- 5003     8       6G        0.1%   0.0%   58m
SOFTSTATE
Solaris running
UUID
    xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
MAC
    xx:xx:xx:xx:xx:xx
HOSTID
    0xxxxxxxxx
CONTROL
    failure-policy=ignore
    extended-mapin-space=on
    cpu-arch=native
    rc-add-policy=
    shutdown-group=15
    perf-counters=
    boot-policy=warning
    effective-max-pagesize=256MB
    hardware-max-pagesize=16GB
    fj-software-limit-pagesize=2GB
```


管理系统日报

本章介绍了 SPARC M12/M10 系统管理中所需的日常工作。

备份 XSCF 设置信息

定期备份储存在主 XSCF 上的 XSCF 设置信息。因为包含主 XSCF 的现场可更换单元 (FRU) 损坏而实施现场可更换单元 (FRU) 更换后，从备份中恢复 XSCF 设置信息使系统操作保持在损坏之前的状态。

有关详情，请参见 ["10.10 保存/恢复 XSCF 设置信息"](#)。

备份逻辑域配置信息

定期对 Oracle VM Server for SPARC 所配置的逻辑域配置信息进行备份。从控制域为每一个逻辑域执行备份。按照如下 2 种方法储存逻辑域配置信息：

- 保存在 XSCF 中
- 保存为 XML 文件

更改域配置以后，确保备份最新的配置信息。建议在其它介质上保存备份文件的副本以备磁盘故障时使用。

有关详情，请参见 ["10.11 保存/恢复 XSCF 中的逻辑域配置信息"](#) 和 ["10.12 在 XML 文件中保存/恢复逻辑域配置信息"](#)。

备份 OpenBoot PROM 环境变量

定期记录并备份控制域中设置的 OpenBoot PROM 环境变量。

如果希望将逻辑域变更为出厂默认配置以从 XML 文件恢复逻辑域配置信息，则会初始化控制域中的 OpenBoot PROM 环境变量，并且无法执行 Oracle Solaris 启动。

为了防止发生这种情况，需在变更为出厂默认配置之前，将 OpenBoot PROM 环境变量记录并保存在控制域中。将逻辑域变更为出厂默认配置后，使用已保存的信息恢复控制域中的 OpenBoot PROM 环境变量。

有关详情，请参见 ["10.13 保存/恢复 OpenBoot PROM 环境变量"](#)。

备份内部磁盘驱动器

定期备份内部磁盘驱动器的数据。备份方法根据不同磁盘驱动器的配置有所不同。按照

驱动器的配置执行备份。

更新到最新的固件

SPARC M12/M10 系统管理的 XSCF 固件与 OpenBoot PROM、虚拟机监控程序和 POST 一起提供为 XCP 软件包。XCP 软件包的最新版本会定期发布新的附加功能，漏洞修复等。发布后请更新到 XCP 软件包的最新版本。

有关更新到最新固件的详细信息，请参见 "[第16章 更新 XCP 固件](#)"。

XCP 包中的新功能和变化在服务器的相应 XCP 版本的《产品说明》中进行简短介绍。请仔细阅读。

监控系统状态

XSCF 始终在监控系统操作。

您可以通过从 XSCF shell 或 XSCF Web 访问 XSCF 来掌握服务器的状态。

使用 XSCF SNMP 代理功能、故障信息通知功能以及各种消息和日志来监控系统故障和事件。

有关详细信息，请参见 "[10.2 通过电子邮件接收故障发生时的通知](#)"、"[10.3 使用 SNMP 代理监控/管理系统状态](#)" 和 "[第12章 检查日志和消息](#)"。

故障的预防和应对措施

本章介绍了事先配置的功能，应对 SPARC M12/M10 系统中可能发生的故障。此系统提供不同的功能来应对可能发生的故障。为了更早地找到和处理故障，用户必须做一定的准备，如指定系统监控、建立硬件冗余和保存数据。

本章介绍这些管理方法。

- 了解故障排除和相关功能
- 故障发生时通过电子邮件接收通知
- 通过 SNMP 代理监控/管理系统状态
- 监控系统
- 了解故障降级机制
- 查看发生故障的硬件资源
- 设置故障 CPU 内核的自动更换
- 设置恢复模式
- 建立冗余组件配置
- 保存/恢复 XSCF 设置信息
- 保存/恢复 XSCF 中的逻辑域配置信息
- 在 XML 文件中保存/恢复逻辑域配置信息
- 保存/恢复 OpenBoot PROM 环境变量
- 保存/恢复硬盘中的内容
- 重启逻辑域
- 在逻辑域中引起崩溃
- 重启物理分区
- 将服务器恢复为出厂默认状态
- 使用延迟转储收集崩溃转储文件

10.1 了解故障排除和相关功能

表 10-1 列出了用于应对可能发生故障的措施和功能。有关各项目的详情，请参见以下章节。

表 10-1 故障排除和功能

措施	功能	相关命令
尽早将故障信息发送给用户	<ul style="list-style-type: none">- 电子邮件通知- 远程维护服务	setsntp(8), showsntp(8), setemailreport(8), showemailreport(8) 请参见服务器的最新《产品说明》。
监控/管理故障和事件	<ul style="list-style-type: none">- 使用 SNMP 代理功能监控系统	setsnmp(8), showsnmp(8), setsnmpusm(8), showsnmpusm(8), setsnmpvacm(8), showsnmpvacm(8)
早期发现故障以确定服务器操作	<ul style="list-style-type: none">- 系统监控、检测信号、实时检查- 服务器操作控制	setpparmode(8), showpparmode(8), setpparparam(8), showpparparam(8)
阻止故障影响其它部分或采取配置冗余的措施	<ul style="list-style-type: none">- 故障降级- 冗余组件配置	showstatus(8), showhardconf(8)
保护当前设置数据并将其恢复到原来状态	<ul style="list-style-type: none">- 保存/恢复 XSCF 设置信息- 保存/恢复逻辑域设置信息- 保存/恢复硬盘	dumpconfig(8), restoreconfig(8), Oracle VM Server for SPARC 命令

注 - 如果 XSCF 失败，使用 XSCF 电子邮件通知功能、SNMP 陷阱或远程维护服务（ASR 功能、REMCS 等）时不发出任何通知。如需监控 XSCF 故障，请使用服务器监控软件。有关详情，请参见所使用服务器的相关管理软件使用手册。

10.2 故障发生时通过电子邮件接收通知

为预防系统中故障和事件的发生，可以对 XSCF 进行设置，使其通过电子邮件将故障或事件状态通知给用户。

强烈建议配置电子邮件通知。一旦设置了 XSCF 电子邮件通知，特定用户（例如具有 platadm 权限的系统管理员）即可立即收到服务器和物理分区故障的通知。

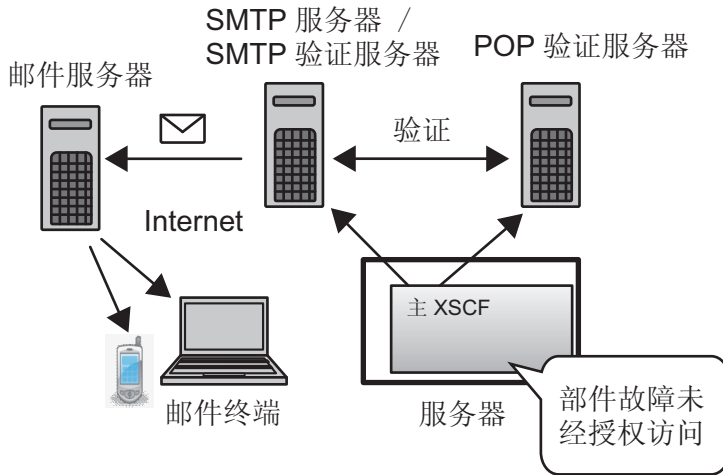
10.2.1 电子邮件通知功能的特点

电子邮件通知功能的特点如下。

- 使用电子邮件报告系统中 XSCF 所监控部件的故障
即使系统关闭或发生一系列无法重新启动的严重错误，也能发送电子邮件。
- 在电子邮件传输时启用 POP 验证功能和 SMTP 验证功能
为防止非法电子邮件传输，在通过 SMTP 服务器接受电子邮件传输之前，可以执行 POP 验证（POP 在 SMTP 前）或 SMTP 验证（SMTP-AUTH）。

图 10-1 概述了 XSCF 通过各服务器发送电子邮件的情况。

图 10-1 XSCF 电子邮件功能概要



10.2.2 故障通知详情

图 10-2 显示了通知电子邮件的示例。

图 10-2 部件故障时电子邮件的示例

```

Date: Mon, 02 Aug 2012 16:03:16 +0900
From: XSCF <root@host-name.example.com> _____ 1
To: mail-address@smtp.example.com _____ 2
Subject: Error: xxxxxxxxxxxx _____ 3

TYPE: Error, VER: XCP-32303030
MODE-SWITCH: -
SEVERITY: Alarm
EVENT-TIME: 08-02-2012 15:55:04 JST
CSN: CNL1126007
SERVER-ID: EM1U1S002
FRU: -
DIAGCODE: Code:0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
Msg: FAN shortage
    
```

-
- 1 邮件设置中设置的 "回复的电子邮件地址"
 - 2 邮件设置中设置的 "目标电子邮件地址"
 - 3 电子邮件标题
-

电子邮件示例显示以下项目。

表 10-2 故障时通知电子邮件的内容

项目	说明
TYPE	通知类型
VER	版本
MODE	模式开关状态
SEVERITY	错误级别
EVENT-TIME	故障发生的时间（显示本地时间）
CSN	机柜序列号
SERVER-ID	本系统的 ID
FRU	可能发生故障的部件
DIAGCODE	用于现场工程师和服务工程师进行故障处理。要求用户将此代码报告给现场工程师或服务工程师。该代码有助于早期解决问题。
Msg	描述问题概要的信息

10.2.3 检查与电子邮件通知相关的设置项目和命令

表 10-3 列出了与 XSCF 电子邮件通知相关的设置项目以及对应的 XSCF shell 命令。

表 10-3 与电子邮件通知相关的设置项目

设置项目	必须或可选设置	相关命令
SMTP 服务器 - 主机名 - 端口号 - 回复电子邮件地址	可选	setsmtp(8), showsmtp(8)
启用/禁用电子邮件通知功能	可选	setemailreport(8), showemailreport(8)
目标电子邮件地址	可选	setemailreport(8), showemailreport(8)
验证服务器 - POP 验证/SMTP 验证 - 主机名 - 用户 ID/密码	可选	setsmtp(8), showsmtp(8)

只指定一个 SMTP 服务器。如需使用主机名指定 SMTP 服务器，服务器名称必须能够用 DNS 服务器进行解析。

SMTP 服务器的默认端口号为 25。

到目标电子邮件地址的路径发生问题时，回复的电子邮件地址是用来发送故障的电子邮件地址。该路径的电子邮件服务器发送错误电子邮件。

10.2.4 电子邮件通知的设置流程

本节介绍 XSCF 电子邮件通知的设置流程。

1. 登录 **XSCF**。
2. 指定 **SMTP** 服务器的主机名或 IP 地址（见 **setsmtp(8)**）。
3. 选择 **POP** 或 **SMTP** 验证（见 **setsmtp(8)**）。
4. 指定回复电子邮件地址（**From** 指定）（见 **setsmtp(8)**）。
5. 指定系统管理员的目标电子邮件地址（见 **setemailreport(8)**）。
6. 启用 **XSCF** 电子邮件通知（见 **setemailreport(8)**）。
7. 发出测试电子邮件。

完成电子邮件设置后，测试电子邮件自动发出。发出的测试电子邮件送达系统管理员时设置完成。如果测试电子邮件未送达，错误电子邮件发送到回复电子邮件地址（**From** 指定），或者该错误被记录到错误日志。找到原因并解决问题之后，从步骤 1 开始重新执行。测试正常完成后，电子邮件通知功能即被启用。

10.2.5 设置 SMTP 服务器的主机名、端口号、回复电子邮件地址和验证方法

1. 执行 **showsmtp** 命令以显示 **SMTP** 服务器设置信息。

```
XSCF> showsmtp
Mail Server:
Port : 25
Authentication Mechanism: none
Reply address:
```

2. 执行 **setsmtp** 命令以设置 **SMTP** 服务器信息。
下面是指定主机名、端口号、回复电子邮件地址和 SMTP 验证的示例。

```
XSCF> setsmtp -s mailserver=192.1.4.5 -s port=25 -s
replyaddress=yyyy@example.com -s auth=smtp-auth -s user=usr001 -s
password=xxxxxxxx
```

下面是指定交互模式下的主机名、端口号、回复电子邮件地址和 POP 验证的示例。

```
XSCF> setsmtp
Mail Server [192.1.4.2]: 192.1.4.5
Port[25]:
Authentication Mechanism [none]:pop
POP Server [192.1.4.2]:
User Name []: usr001
Password []: xxxxxxxx
Reply Address [yyyy@example.com]:
```

3. 执行 **showsmtp** 命令并确认 **SMTP** 服务器设置信息。

```
XSCF> showsmtp
Mail Server: 192.1.4.5
Port: 25
Authentication Mechanism : pop
User Name: usr001
Password: *****
Reply Address: yyyy@example.com
```

10.2.6 设置通知的目标电子邮件地址和启用/禁用电子邮件通知功能

按 "10.2.5 设置 SMTP 服务器的主机名、端口号、回复电子邮件地址和验证方法" 中

所述，提前配置 SMTP 服务器。

设置 XSCF 电子邮件功能后，您可以发出测试电子邮件以确认设置。显示测试电子邮件发出的时间（本地时间显示）和电子邮件源的信息。此外，测试电子邮件标题包含字符 "Test Mail:"。

1. 执行 **showemailreport** 命令以显示电子邮件通知设置信息。

```
XSCF> showemailreport
E-Mail Reporting: disabled
```

2. 执行 **setemailreport** 命令以设置电子邮件通知信息。
以下是指定启用交互模式的电子邮件通知和目标电子邮件地址的示例。

```
XSCF> setemailreport
Enable E-Mail Reporting? [no]: yes
E-mail Recipient Address []: xxxxx@example.com
Do you want to send a test mail now [no]?: yes
... Sending test mail to 'xxxxx@example.com'
```

3. 执行 **showemailreport** 命令并确认电子邮件通知设置信息。

```
XSCF> showemailreport
E-Mail Reporting: enabled
E-Mail Recipient Address: xxxxx@example.com'
```

4. 确认可以收到带有 "Test Mail" 标题的测试电子邮件。

10.3 通过 SNMP 代理监控/管理系统状态

本节介绍如何监控系统故障和事件。

为 XSCF 设置了 SNMP 代理，服务器管理器即可监控/管理故障和事件。

10.3.1 SNMP 基本知识

简单网络管理协议 (SNMP) 是一个网络管理协议。

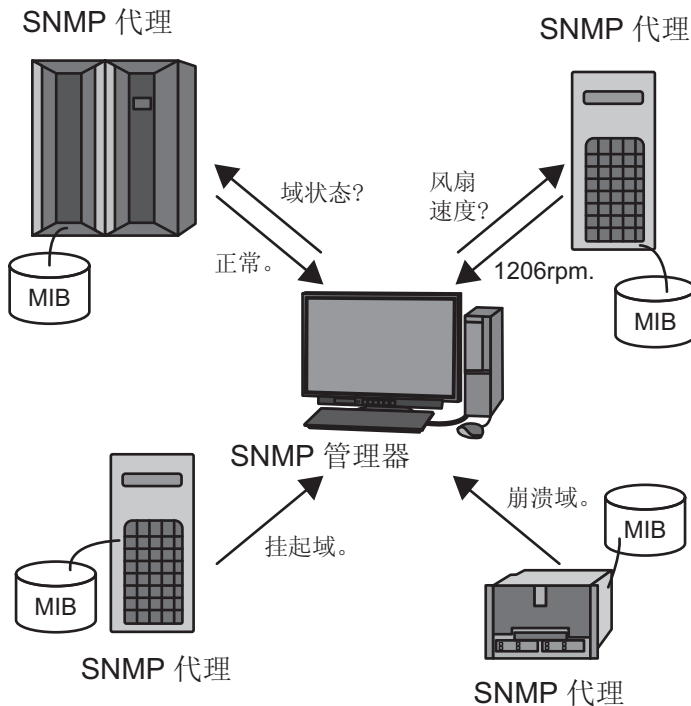
SNMP 被称为对测试和变更网桥、路由器、交换机和其它设备连接的 LAN 或 WAN 配置参数的查询、命令或响应协议。

目前提供以下版本：SNMPv1、SNMPv2c 和 SNMPv3。与 SNMPv1 和 SNMPv2c 相比，SNMPv3 增加了密码和验证功能。

SNMP 管理器集中管理网络上终端的操作和问题状态。SNMP 代理返回称为管理信息库的 (MIB) 的管理信息，来响应管理器请求。此外，代理可以使用称为 "陷阱" 的功能，针对特定的信息为管理器执行异步通知。

图 10-3 显示了使用 SNMP 的网络管理环境的示例。

图 10-3 网络管理环境的示例



SNMP 使用的默认端口号

SNMP 使用的默认端口号如下。

- SNMP 代理：端口 161
- 陷阱：端口 162

10.3.2 SNMP 相关术语

表 10-4 列出了 SNMP 相关术语。

表 10-4 SNMP 相关术语

术语	说明
USM	User-based Security Model (基于用户的安全模型) 的缩写。是由 SNMPv3 定义的基于用户的安全模型。

表 10-4 SNMP 相关术语 (续)

术语	说明
VACM	View-based Access Control Model (基于视图的访问控制模型) 的缩写。是由 SNMPv3 定义的基于视图访问控制模型。
组	属于 VACM 模型的用户集合。组为属于该组的所有用户定义了访问权限。
OID	Object Identifier (对象标识符) 的缩写。OID 是对象标识号码。对于 MIB 定义文件的对象, 用句点将整数连接起来表示的 MIB 数字地址。
视图 (MIB 视图)	视图是引用 MIB 定义文件的方法。视图是用 OID 和 OID 掩码定义的 MIB 的子目录树。可以将 MIB 访问控制视图分配给组。

10.3.3 MIB 定义文件基本知识

SNMP 代理功能包含称为 MIB 的管理信息。返回此 MIB 信息以响应管理器的请求。

标准 MIB

XSCF 支持被定义为 Internet 标准的 MIB-II (支持 SNMPv2 和 v3) 和 MIB-I (支持 SNMPv1), 主要管理以下信息:

- 与 XSCF-LAN 相关的基本信息 (管理员名称或类似)
- 与 XSCF-LAN 通信处理相关的信息
- 与 XSCF SNMP 代理操作相关的信息

有关 XSCF 支持的标准 MIB 的详细信息, 请参见 "附录 D XSCF MIB 信息"。

扩展 MIB

除标准 MIB 以外, 此系统支持以下扩展 MIB:

- XSCF 扩展 MIB: 针对 XSCF SNMP 代理的 MIB 扩展

此 MIB 主要管理以下信息:

- 与系统相关的基本信息 (序列号和类似)
- 与系统相关的不同类型的状态信息 (如: 上级 Oracle Solaris 的操作状态)
- 系统中的物理分区信息
- 系统中的部件故障信息
- 与系统功率值相关的信息

下面是 XSCF 扩展 MIB 的管理信息数据的示例。

```
scfMachineType OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION "System model name and model type name."
::= { scfInfo 1 }
scfNumberOfCpu OBJECT-TYPE
SYNTAX INTEGER
```

```
ACCESS read-only
STATUS mandatory
DESCRIPTION "Number of CPUs"
::= { scfInfo 2 }
scfSysSerial OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION "System serial number"
::= { scfInfo 3 }
```

有关 XSCF 支持的 XSCF 扩展 MIB 的详细信息，请参见“附录 D XSCF MIB 信息”。

安装扩展 MIB 定义文件

按照 ASN1 标准的解释定义 MIB 定义文件。

XSCF 扩展 MIB 定义文件定义管理信息，由 SNMP 管理器监控系统。如需监控服务器，请在 SNMP 管理器中安装 XSCF 扩展 SNMP 定义文件。

有关安装方法的详情，请参见您所使用的 SNMP 管理器的手册。关于获取扩展 MIB 定义文件的位置，请参见您的服务器的最新《产品说明》或固件下载网站上 MIB 定义文件相关的信息。

10.3.4 陷阱基本知识

如果启用 SNMP 代理功能，称为陷阱的通知将被发给 SNMP 管理器。XSCF 陷阱涵盖以下事件：

- 检测信号通知（XCP 2050 或更高版本）
- 发生 XSCF 故障转移
- 由于 PSB 和组件的添加、移除、更换等而导致的配置变化
- 系统部件中发生故障，或者通过更换系统中的故障部件排除了问题
- 物理分区状态因启动、崩溃和断电或其他状态发生改变
- 物理分区中并入或释放 BB (PSB)
- 管理程序终止
- 配置已更改，如：PCI 扩展单元部件的添加和删除
- PCI 扩展单元部件的 LED 状态已更改
- PCI 扩展单元部件中出现温度异常
- 模式开关更改
- 崩溃或发生其他逻辑域状态变化
- XSCF SNMP 代理功能启动（标准陷阱）
- 对 XSCF SNMP 代理进行的非法访问（标准陷阱）
- 在 SNMP 代理启动时管理对象配置发生改变时，发出冷启动陷阱（标准陷阱）

在系统中由 XSCF 监控的部件中，陷阱目标部件可通过故障位置和部件号进行识别。即使不能识别该部件，通过发出 XSCF 事件通知也可产生陷阱。

以下是系统中发生部件故障时生成的 SNMP-Trap 的示例。

```
Aug 12 06:07:16 paplsv2 snmptrapd[11958]: 2012-08-12 06:07:16
A4U4S141 [10.26.147.50] (via UDP: [10.26.147.50]:38221) TRAP,
SNMP v1, community abccommunity XSCF-SP-MIB::scfMIBTraps
Enterprise Specific Trap (XSCF-SP-MIB::scfComponentStatusEvent)
Uptime: 6:27:33.28 XSCF-SP-MIB::scfComponentErrorStatus.bb.
0.cmuu.0.notApplicable.0 = INTEGER: deconfigured(4) XSCF-
SP-MIB::scfTrapStatusEventType.0 = INTEGER: alarm(1)
```

此示例包含以下信息:

- 发出陷阱的 XSCF 的 IP 地址 (如: 10.26.147.50)
- SNMPv1 的团体字符串 (如: adcommunity)
- 陷阱类型 (如: EnterpriseSpecific、model-specific trap)
- 陷阱 发出时间 (如: Uptime: 6:27:33:28)
- 其它陷阱信息
包含可能发生故障的部件、事件类型或错误级别。

对于固件版本 XCP 2050 或更高版本, 如果您启用 XSCF SNMP 代理功能, XSCF 检测信号通知 (存在信息) 陷阱将被发送到系统。

以下事件发生时发送检测信号通知。

- 当 XSCF SNMP 代理功能启动或恢复时。
- XSCF SNMP 代理功能启动后每隔 12 小时
- 当执行 `rastest -c hb` 命令时

以下是有关 XSCF 检测信号通知的 SNMP 陷阱示例。

当陷阱代码是 "FF010001" 和陷阱 MessageId 是 "M10-Heartbeat" 时, 您可确认 XSCF 检测信号通知。

```
(solaris.4.1.1.12.2.1.13.100.0.254.0.254.0 [1 1 0] 1)
(solaris.4.1.2.1.2.0 [1 1 0] 4)
(solaris.4.1.1.4.3.0 [2 10 0] PZ31426015)
(solaris.4.1.1.4.2.0 [2 11 0] SPARC M10-1)
(solaris.4.1.1.4.1.0 [2 10 0] x-integ-ts)
(solaris.4.1.2.1.14.0 [2 8 0] FF010001)
(solaris.4.1.2.1.15.0 [2 28 0] Oct 23 03:06:04.367 JST 2014)
(solaris.4.1.2.1.16.0 [2 0 0] )
(solaris.4.1.2.1.17.0 [2 0 0] )

(solaris.4.1.2.1.18.0 [2 0 0] )
(solaris.4.1.2.1.19.0 [2 0 0] )
(solaris.4.1.2.1.20.0 [2 0 0] )
(solaris.4.1.2.1.21.0 [2 0 0] )
(solaris.4.1.2.1.22.0 [2 0 0] )
(solaris.4.1.2.1.23.0 [2 0 0] )
(solaris.4.1.2.1.24.0 [2 13 0] Fujitsu M10-1)
(solaris.4.1.2.1.25.0 [1 1 0] 1)
(solaris.4.1.2.1.26.0 [2 13 0] M10-Heartbeat)
```

有关 XSCF 心跳通知的 OID 信息的详细信息，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists》中的 "Chapter 5 XSCF Trap Type List"。

XSCF 陷阱信息

XSCF 陷阱包括报告发生故障的陷阱和报告系统状态改变的陷阱。如需将相应的陷阱发送给所使用的系统，请使用 SNMP 管理器对所需的陷阱接收进行设置。

有关 XSCF SNMP MIB 陷阱的列表信息，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists》。

10.3.5 查看与 SNMP 代理相关的设置项目和命令

表 10-5 列出了与 XSCF SNMP 代理相关的设置项目以及对应的 XSCF shell 命令。

表 10-5 与 SNMP 代理相关的设置项目

设置项目	必须或可选设置	相关命令
系统管理信息 - 代理系统安装位置 - 管理员电子邮件地址 - 代理系统说明 - 代理端口号（侦听端口号）	可选	setsnmp(8), showsnmp(8)
启用/禁用代理	可选 默认：禁用	setsnmp(8), showsnmp(8)
SNMPv3 陷阱 - 用户名 - 验证密码 - 加密密码 - 来自接收主机确认的本地代理引擎 ID 或请求 - 验证算法 - 加密协议 - 陷阱目标端口号 - 陷阱目标主机名	可选	setsnmp(8), showsnmp(8)
禁用 SNMPv3 陷阱	可选	setsnmp(8), showsnmp(8)
启用/禁用 SNMPv1 和 SNMPv2c 通信	可选	setsnmp(8), showsnmp(8)
SNMPv1/SNMPv2c 陷阱 - 陷阱类型规格 - 团体字符串 - 陷阱目标端口号 - 陷阱目标主机名	可选	setsnmp(8), showsnmp(8)
禁用 SNMPv1/SNMPv2c 陷阱	可选	setsnmp(8), showsnmp(8)
初始化 SNMP 设置	可选	setsnmp(8), showsnmp(8)

表 10-5 与 SNMP 代理相关的设置项目 (续)

设置项目	必须或可选设置	相关命令
USM 管理信息 (SNMPv3 的设置) - 用户验证/加密密码注册 - 用户验证/加密密码更改 - 指定验证算法 - 指定加密协议 - 复制用户 - 删除用户	可选	setsnmpusm(8), showsnpusm(8)
VACM 管理信息 (SNMPv3 的设置) - 注册用户访问控制组 - 删除用户访问控制组 - 创建 MIB 访问控制视图 - 删除 MIB 访问控制视图 - 将 MIB 访问控制视图分配给组 - 从所有 MIB 访问控制视图删除组	可选	setsnmpvacm(8), showsnpvacm(8)

10.3.6 SNMP 代理设置流程

本节介绍 XSCF SNMP 代理设置流程。

有关每个步骤的详细信息，请参见“[10.3.7 在 SNMP 代理上设置系统管理信息，并启用/禁用 SNMP 代理](#)”和后续章节。

对于 SNMPv1 和 SNMPv2c，不能进行安全通信是因为没有提供通信数据加密。对于 SNMPv3，通过设置验证/在代理和管理器两端都进行加密，可以进行更安全的传输和接收。系统提供 SNMPv3 作为默认 SNMP 代理。

开始发送和接收

1. 登录 **XSCF**。
2. 设置以下 **SNMPv1**、**SNMPv2c** 和 **SNMPv3** 代理协议通用的管理信息（见 **setsnmp(8)**）。
 - 代理系统安装位置
 - 管理员电子邮件地址
 - 代理系统说明
 - 代理端口号（侦听端口号）
3. 为 **SNMPv3** 或 **SNMPv1** 和 **SNMPv2c** 设置以下管理信息。（见 **setsnmp(8)**）。
 - 设置 SNMPv3 管理信息
 - 用户名
 - 验证密码
 - 加密密码

- 验证算法
 - 加密协议
 - 陷阱目标端口号
 - 陷阱目标主机名
 - 设置 SNMPv1 和 SNMPv2c 管理信息
 - 陷阱类型规格（选择 v1、v2c 或 inform <v2c 和响应>）
 - 团队名
 - 陷阱目标端口号
 - 陷阱目标主机名
4. 启用 **XSCF SNMP** 代理功能。根据用户环境，以下面一种或两种方式启用该功能（请参见 **setsnmp(8)**）。
- 启用 SNMPv1 和 SNMPv2c
 - 启用 SNMPv3

注 - 如果 XSCF SNMP 代理已启用，除步骤 3 设置项目以外的 MIB 信息全部会初始化。

停止或禁用发送和接收

- 禁用 XSCF SNMP 代理功能
根据用户环境，禁用以下其中一个或全部两个功能：
 - SNMPv1 和 SNMPv2c 无效
 - SNMPv3 无效
- 禁用到 SNMPv3 预期陷阱目标主机的传输
指定以下项目以禁用传输：
 - 用户名
 - 陷阱目标主机
- 禁用到 SNMPv1 或 SNMPv2c 预期陷阱目标主机的传输
指定以下项目以禁用传输：
 - 协议类型 (v1/v2c) 规格
 - 陷阱目标主机

管理用户（USM 管理）和 MIB 定义文件访问控制视图（VACM 管理）

为 SNMPv3 管理 USM 和 VACM。

使用 SNMPv3 代理时，使用 `setsnmp` 命令设置验证协议和加密协议。然后，需使用 `setsnmpusm` 命令为 User-based Security Model (USM) 设置管理信息，使用 `setsnmpvacm` 命令为 View-based Access Control Model (VACM) 设置管理信息。当设置 SNMPv3 时，需指定验证协议和加密协议。此外，使用 `setsnmp` 和 `setsnmpusm` 命令时需输入密码。

1. 登录 XSCF。

2. 注册、更改或删除以下用户管理信息。(见 **setsnmpusm(8)** 和 **setsnmpvacm(8)**)。
 - 指定用户验证算法
 - 指定用户加密算法
 - 用户验证/加密密码注册
 - 用户验证/加密密码更改
 - 复制用户
 - 删除用户
3. 注册、分配或删除以下用户的访问控制组和访问控制视图 (**MIB 视图**)：
 - 注册用户访问控制组
 - 删除用户访问控制组
 - 创建 MIB 访问控制视图
 - 删除 MIB 访问控制视图
 - 将 MIB 访问控制视图分配给组
 - 从所有 MIB 访问控制视图删除组

10.3.7 在 SNMP 代理上设置系统管理信息，并启用/禁用 SNMP 代理

默认情况下 SNMP 代理禁用。代理的默认端口号为 161。指定最多 128 个字符的电子邮件地址。如果对接收端电子邮件地址有限制，请确认设置。

1. 执行 **showsnpmp** 命令以查看 **SNMP** 设置。
下面是查看没有设置管理信息状态的示例。

```
XSCF> showsnmp
Agent Status:      Disabled
Agent port:       161
System Location:  Unknown
System Contact:   Unknown
System Description: Unknown
:
```

2. 执行 **setsnmp** 命令以配置 **SNMP**。
下面示例指定系统位置、说明和管理员的电子邮件地址。

```
XSCF> setsnmp -l MainTower21F -c foo@example.com -d DataBaseServer
```

3. 执行 **setsnmp** 命令以启用 **SNMP** 代理。
下面示例启用代理。

```
XSCF> setsnmp enable
```

下面示例禁用代理。

```
XSCF> setsnmp disable
```

4. 执行 **showsnmp** 命令并确认 **SNMP** 设置。
在下例中，启用 SNMP 代理。

```
XSCF> showsnmp  
Agent Status:      Enabled  
Agent port:        161  
System Location:   MainTower21F  
System Contact:    foo@example.com  
System Description: DataBaseServer  
:
```

10.3.8 设置 SNMPv3 陷阱

设置与发送和接收端通用的 SNMPv3 用户名和验证/密码。引擎 ID 必须以 "0x" 开始，且为十六进制的偶数。

验证算法为安全哈希算法 256 (SHA256) 或 MD5。

加密协议是 Data Encryption Standard (DES) 和 Advanced Encryption Standard (AES)。

陷阱目标主机没有设置默认值。陷阱目标的默认端口号为 162。

1. 执行 **showsnmp** 命令以查看 **SNMP** 设置。
下面示例显示设置了 SNMPv1 和 SNMPv2c 的状态。

```
XSCF> showsnmp  
Agent Status:      Enabled  
Agent port:        161  
System Location:   MainTower21F  
System Contact:    foo@example.com  
System Description: DataBaseServer  
Trap Hosts:None  
-----  
Hostname Port Type Community String Username Auth Encrypt  
-----  
host1     62  v1  public          n/a  n/a  n/a  
host2    1162 v2  public          n/a  n/a  n/a  
SNMP V1/V2c:  
Status:      Enabled  
Community String: public
```

2. 执行 **setsnmp** 命令以设置 **SNMPv3** 陷阱。
下面示例中使用 **addv3traphost** 操作数指定用户名、引擎 ID、验证算法、验证密码、加密密码和陷阱目标主机名或 IP 地址。

```
XSCF> setsnmp addv3traphost -u yyyyy -n 0x### -r SHA host3  
Enter the trap authentication passphrase: xxxxxxxx  
Enter the trap encryption passphrase: xxxxxxxx
```

3. 执行 **showsnmp** 命令并确认 **SNMPv3** 陷阱设置。

```
XSCF> showsnmp  
Agent Status:          Enabled  
Agent port:            161  
System Location:       MainTower21F  
System Contact:        foo@example.com  
System Description:    DataBaseServer  
  
Trap Hosts:  
  
-----  
Hostname Port Type Community String Username Auth Encrypt  
-----  
host3    162  v3      n/a      yyyyy   SHA   DES  
host1    62   v1      public   n/a     n/a   n/a  
host2    1162 v2      public   n/a     n/a   n/a  
SNMP V1/V2c:  
Status:          Enabled  
Community String: public  
  
Enabled MIB Modules:  
SP MIB
```

10.3.9 禁用到 SNMPv3 预期目标主机的陷阱

1. 执行 **showsnmp** 命令以查看 **SNMP** 设置。

```
XSCF> showsnmp
```

2. 执行 **setsnmp** 命令以禁用 **SNMPv3** 预期陷阱目标主机。
在以下示例中，使用 **remv3traphost** 操作数指定了用户名和主机名。

```
XSCF> setsnmp remv3traphost -u yyyyy host3
```

3. 执行 **showsnmp** 命令并确认预期陷阱目标主机已禁用。

```
XSCF> showsnmp
```

10.3.10 启用/禁用 SNMPv1 和 SNMPv2c 通信

用于启用 SNMPv1 和 SNMPv2c 的团队字符串为只读。

1. 执行 **showsnmp** 命令以查看 **SNMP** 设置。

```
XSCF> showsnmp
```

2. 执行 **setsnmp** 命令以启用 **SNMPv1** 和 **SNMPv2c** 通信。
在下面的示例中通过指定 **enablev1v2c** 操作数启用 SNMPv1 和 SNMPv2c。

```
XSCF> setsnmp enablev1v2c public
```

在下面的示例中通过指定 **disablev1v2c** 操作数禁用 SNMPv1 和 SNMPv2c。

```
XSCF> setsnmp disablev1v2c
```

3. 执行 **setsnmp** 命令以启用 **SNMP** 代理。

```
XSCF> setsnmp enable
```

4. 执行 **showsnmp** 命令并确认是启用还是禁用代理。

```
XSCF> showsnmp
```

10.3.11 设置 SNMPv1 和 SNMPv2c 陷阱

从以下三个陷阱类型中选择一个：

- v1
- v2
- inform

如果指定了 **inform** 时，使用 SNMPv2c 代理发送 InformRequest。

陷阱目标的默认端口号为 162。

1. 执行 **showsnmp** 命令以查看 **SNMP** 设置。

```
XSCF> showsnmp
```

2. 执行 **setsnmp** 命令以设置 **SNMPv1** 或 **SNMPv2c** 陷阱。
在下面的示例中通过指定 **addtraphost** 操作数指定 SNMPv2c 类型。

```
XSCF> setsnmp addtraphost -t v2 -s public host2
```

下面示例指定 SNMPv1 类型。

```
XSCF> setsnmp addtraphost -t v1 -s public host1
```

3. 执行 **showsnmp** 命令并确认 **SNMPv1** 和 **SNMPv2c** 陷阱设置。

```
XSCF> showsnmp
```

10.3.12 禁用对 SNMPv1 和 SNMPv2c 预期主机的陷阱

1. 执行 **showsnmp** 命令以查看 **SNMP** 设置。

```
XSCF> showsnmp
```

2. 执行 **setsnmp** 命令以禁用 **SNMPv1** 或 **SNMPv2c** 的预期陷阱目标主机。
在下面的示例中通过指定 **remtraphost** 操作数禁用 SNMPv2c 类型的主机。

```
XSCF> setsnmp remtraphost -t v2 host2
```

3. 执行 **showsnmp** 命令并确认陷阱目标主机已禁用。

```
XSCF> showsnmp
```

10.3.13 恢复 SNMP 设置的默认值

通过禁用 SNMP 代理可以将设置的数据恢复到默认值。

1. 执行 **showsnmp** 命令以查看 **SNMP** 设置。

```
XSCF> showsnmp
```

2. 执行 **setsnmp** 命令以将 **SNMP** 恢复到默认设置。
恢复默认后 SNMP 代理禁用。

```
XSCF> setsnmp default
```

3. 执行 **setsnmp** 命令并确认 **SNMP** 已恢复到默认设置。

```
XSCF> showsnmp
```

4. 执行 **setsnmp** 命令并再次配置 **SNMP**。然后，启用 **SNMP** 代理。

```
XSCF> setsnmp enable
```

5. 执行 **showsnmp** 命令并确认 **SNMP** 设置。

```
XSCF> showsnmp
```

10.3.14 设置 USM 管理信息

USM 管理信息包括 SNMPv3 的设置。设置以下各项：

- 用户验证算法
- 用户加密协议
- 验证/加密密码
- 复制/删除用户

1. 执行 **showsnmpusm** 命令以查看 **USM** 管理信息。

```
XSCF> showsnmpusm

Username  Auth  Encrypt
-----  -
yyyyyy   SHA  DES
user2    SHA  DES
```

2. 执行 **setsnmpusm** 命令以设置 **USM** 管理信息。
下面是为新用户注册验证算法、验证密码和密码的示例。指定 8 个字符以上的密码。

```
XSCF> setsnmpusm create -a SHA yyyyyy
Enter the user authentication passphrase: xxxxxxxx
Enter the user encryption passphrase: xxxxxxxx
```

下面示例只更改验证密码。

（如果没有输入密码，会要求用户输入。）

```
XSCF> setsnmpusm passwd -c auth -o xxxxxxxx -n xxxxxxxx yyyyyy
```

以下是通过复制既有用户，将用户以克隆进行添加的示例。

```
XSCF> setsnmpusm clone -u yyyyy newuser
```

下面是删除用户的示例。

```
XSCF> setsnmpusm delete yyyyy
```

3. 执行 **showsnmpusm** 命令以查看 **USM** 管理信息。

```
XSCF> showsnmpusm  
  
Username  Auth  Encrypt  
-----  ----  -----  
yyyyy    SHA  DES  
user2    SHA  DES
```

10.3.15 设置 VACM 管理信息

VACM 管理信息包括 SNMPv3 的设置。设置以下各项：

- 注册/删除访问控制组的用户
- 创建/删除 MIB 访问控制视图
- 将 MIB 访问控制视图分配给组
- 从所有 MIB 访问控制视图删除组

将访问控制视图分配给组时，分配只读视图。

1. 执行 **showsnmpvacm** 命令以查看 **VACM** 管理信息。

```
XSCF> showsnmpvacm  
Groups:  
Groupname  Username  
-----  -----  
xxxxx     user1, user2  
Views  
View       Subtree      Mask      Type  
-----  -----  
all_view   .1           ff        include  
Access  
View Group  
-----  -----  
all_view   xxxxx
```

2. 执行 **setsnmpvacm** 命令以设置 **VACM** 管理信息。 下面示例为将访问控制组 xxxxx 添加到用户 yyyyy。

```
XSCF> setsnmpvacm creategroup -u yyyyy xxxxx
```

下面示例为从访问控制组 xxxxx 中删除用户 yyyyy。

```
XSCF> setsnmpvacm deletegroup -u yyyyy xxxxx
```

下面示例为无条件创建 MIB 访问控制视图。

```
XSCF> setsnmpvacm createview -s .1 all_view
```

下面示例为使用 OID 掩码创建 MIB 访问控制视图。

```
XSCF> setsnmpvacm createview -s .1.3.6.1.2.1 -m fe excl_view
```

下面示例为删除 MIB 访问控制视图。

```
XSCF> setsnmpvacm deleteview -s .1.3.6.1.2.1 excl_view
```

下面示例为将 MIB 访问控制视图分配给组 xxxxx。

```
XSCF> setsnmpvacm createaccess -r all_view xxxxx
```

下面示例为从所有 MIB 访问控制视图中删除组 1。

```
XSCF> setsnmpvacm deleteaccess group1
```

3. 执行 **showsnmpvacm** 命令并确认设置的 VACM 管理信息。

```
XSCF> showsnmpvacm
```

10.4 监控系统

本节介绍 Oracle Solaris 的监控以及此系统中的每个固件。

10.4.1 了解主机看门狗功能/实时检查的机制

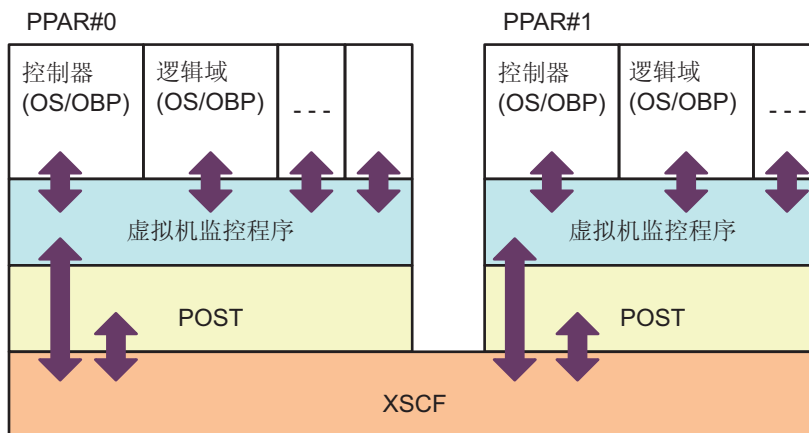
Oracle Solaris 的逻辑域、OpenBoot PROM、管理程序、POST 和 XSCF 相互通信并相互监控实时状态。如果检测到异常，会生成崩溃或他们各自停止，以防止故障影响的扩大。

在此系统中，虚拟机管理程序监控逻辑域/OpenBoot PROM，XSCF 监控 POST。

虚拟机管理程序和逻辑域之间以及虚拟机管理程序与 OpenBoot PROM 之间的监控机制被称为主机看门狗功能。XSCF 和 POST 之间的监控机制也称为实时检查功能。

图 10-4 显示了监控彼此各自的资源。

图 10-4 系统监控功能



注 - 图 10-4 中的 OBP 代表 OpenBoot PROM。

XSCF 监控 POST 并在特定的经过时间后没有响应时判断为故障，然后重置物理分区或关闭电源。

虚拟机管理程序定期监控逻辑域 (Oracle Solaris/OpenBoot PROM) 的操作状态以检测任何的 Oracle Solaris 挂起。检测到 Oracle Solaris 暂停时，管理程序在相关域中生成一个 Oracle Solaris 崩溃。

注 - 有关由 `setpparmode` 命令设置的 XSCF 和虚拟机监控程序之间的实时检查功能的支持信息，请参见服务器的最新《产品说明》。

10.4.2 控制监控和服务操作

当系统正在运行或在维护中，您可能想要限制各物理分区或逻辑域上的一些功能。例如，在系统维护时，您不希望系统自动启动（启用自动启动限制）和从控制台接收中断信号（启用中断信号限制）。

在此系统中，各物理分区的指定操作模式包括监控方法和诊断级别。使其能够控制逻辑域和物理分区的操作。

使用 `setpparmode` 命令，您可以为各指定的物理分区设置以下项目：硬件的初始诊断级别、信息级别、实时检查功能、主机看门狗程序超时时的反应、启用/禁用中断信号传输限制、启用/禁用来宾域的自动重启、启用/禁用节电功能和启用/禁用 IO 总线重新

配置功能。

此外，使用 `setpparparam` 命令，您可以设置各指定物理分区控制域自动重启的启用/禁用。

有关使用 `setpparmode` 命令服务器操作控制的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中的“第3章 域配置的操作”。

注 - 有关 `setpparmode` 命令和有关此命令的每个功能的支持信息的详情，请参见服务器的最新《产品说明》。

10.5 了解故障降级机制

硬件故障时将组件从系统中释放被称为降级。降级会断开对组件的访问，从而防止系统问题扩大。

降级情况如下。

- 保留的降级
如果重新启动或发生严重错误时不可能立即降级，则在系统中保留降级以在重新启动时生成降级。XSCF 可通过保留在内存中的降级位置达到相同的目的。
- Oracle Solaris 运行期间降级
在 Oracle Solaris 运行期间，当 CPU、内存等可被释放时，它们被降级。只有在 Oracle Solaris 运行时被允许释放的组件才降级。
- POST 运行期间降级
物理分区被降级，但不重置物理分区。
- OpenBoot PROM 运行期间保留的降级
降级在 OpenBoot PROM 运行期间被保留，并在重置后执行降级。PCI 适配器错误、内存错误等是降级的对象。
- 硬件内部路径动态降级
机箱（如 SPARC M12/M10 机箱、接线单元、接线盒中的接线单元）之间以及组件之间路径中的通道在未重置系统的情况下被动态降级。

使用 `showstatus` 命令查看组件降级信息。有关管理故障降级信息的详情，请参见“[11.1.4 查看故障/降级组件](#)”。

10.6 查看发生故障的硬件资源

SPARC M12/M10 系统自动检测和降级发生故障的内存和 CPU 资源。

您可以通过指定 `ldm list-domain` 和 `ldm list-devices` 命令的 `-S` 选项来查看是否发生了内存和 CPU 资源的故障。

有关 `ldm list-domain` 和 `ldm list-device` 命令的详情，请参见您所使用版本的《Oracle

VM Server for SPARC Reference Manual》。也请参见 "10.7 设置故障 CPU 内核的自动更换"。其中介绍了自动更换故障 CPU 内核的设置方法。

10.6.1 使用 list-domain 命令查看故障的内存或 CPU

1. 显示物理分区中逻辑域的详细信息，以及是否发生了内存或 CPU 故障的信息。

```
primary# ldm list-domain -l -S
```

10.6.2 使用 list-device 命令查看故障的内存或 CPU

1. 显示物理分区中可用内存或可用 CPU 的资源信息，以及是否发生了内存或 CPU 故障的信息。

```
primary# ldm list-devices -S mem cpu
```

10.7 设置故障 CPU 内核的自动更换

即使某些 CPU 内核发生故障，SPARC M12/M10 也可以通过使用 CPU 自动更换功能自动分配其他 CPU 内核，从而不缩减 CPU 资源的情况下持续运行系统。

根据 Oracle Solaris 的 `svccfg` 命令指定的 `ldmd` 服务的自动更换策略，启用/禁用 CPU 自动更换功能。默认启用。

如果启用自动更换策略，则自动更换的故障 CPU 内核将被控制，以便在之后不分配给逻辑域。如果故障 CPU 内核没有被自动更换，CPU 内核会仍然被分配给逻辑域。

如果禁用自动更换策略，故障 CPU 内核不被更换。

有关更改自动更换策略的步骤，请参见 "10.7.2 更改自动更换策略的方法"。

10.7.1 自动更换 CPU 内核的条件

执行 CPU 内核的自动更换，必须满足下面的条件。

- 在物理分区所搭载的所有 CPU 内核中，确保至少一个内核未分配给 PPAR。如果您使用 XSCF 固件的 `setcod(8)` 命令将 PPAR 上所搭载的所有 CPU 内核分配给 PPAR，则自动更换不可用。

对于 SPARC M10-4 (4-CPU×16 个内核配置)，例如，PPAR 上搭载 64 个 CPU 内核。如需在此配置中使用自动更换功能，必须通过使用 `setcod` 命令将分配在 PPAR 上的 CPU 内核的数量设置为 63 或少于 63。

当将 56 个 CPU 内核按如下所示分配给 PPAR-ID 0 时，则 PPAR 上安装了 64 个

CPU 内核，因此可以自动切换内核。

```
XSCF> setcod -p 0 -s cpu -c set 56
PROC Permits assigned for PPAR 0 : 0 -> 56

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

注 - XCP 2250 或更早版本的 XSCF 固件不支持 -c add、-c delete 和 -c set 选项。按如下所示指定 setcod 命令选项可交互式添加和删除分配。

```
XSCF> setcod -s cpu
```

可用于自动更换的 CPU 内核的数量与使用 CPU 激活密钥注册的 CPU 内核的数量没有任何关系。例如，如果在上述 SPARC M10-4 的示例中注册了 56 个 CPU 激活，则即使使用 setcod(8) 命令分配了 56 个 CPU 内核，也最多仅 8 个可用 CPU 内核可使用自动更换功能进行切换。在这种情况下，可用于切换的 8 个 CPU 内核不需要 CPU 激活密钥。

- CPU 内核可以动态删除。

在以下情况下，无法自动更换 CPU 内核。

- CPU 内核分配给逻辑域时，会指定物理内核 ID (cid 选项)。如果按如下所述使用指定 cid 选项将 CPU 内核分配给逻辑域，则 CPU 内核的自动更换将不可用。

```
# ldm set-core cid=20 ldom
# ldm add-core cid=20 ldom
```

如果已经使用 cid 指定分配 CPU 内核，则移除 cid 指定。有关移除 cid 指定的方法，请参见正在使用版本的《Oracle VM Server for SPARC Administration Guide》中的 "How to Remove the physical-bindings Constraint"。

注 - 如需使用 CPU 自动更换功能，则请勿使用 Oracle Solaris 内核区。当使用 Oracle Solaris 内核区时，分配给 Oracle Solaris 内核区的 CPU 内核不会自动以正确的方式更换。

Oracle VM Server for SPARC 3.3 和更高版本中废止了随后的六个限制条件。

- 仅将一个 CPU 内核分配给逻辑域时
使用 ldm set-core 或 ldm add-core 命令将两个或更多个 CPU 内核分配给域。可以使用 ldm list-domain -o core 命令确认逻辑域使用的 CPU 内核资源。
- 当资源池的处理器组不满足以下条件时
[SPARC M12]
pset.min 属性设置为等于或大于 9，并且 pset.max 属性设置为等于或大于 pset.min + 8。
[SPARC M10]

pset.min 属性设置为等于或大于 3，并且 pset.max 属性设置为等于或大于 pset.min + 2。

有关配置资源池处理器组的方法，请参见《System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones》。

- 为 Oracle Solaris 区域的 dedicated-cpu 资源指定任何特定数量的 CPU 时使用 Oracle Solaris 区域的 dedicated-cpu 资源时所指定的特定数量的 CPU 与自动 CPU 内核更换不兼容。
(例如，ncpu=5)
- 为 Oracle Solaris 区域的 dedicated-cpu 资源所指定的 CPU 范围不符合以下条件时 [SPARC M12]
对于最小值，九个或更多个 CPU (两个内核)，对于最大值，最小值 + 八个或更多个 CPU
(例如，ncpus=9-17)
[SPARC M10]
对于最小值，三个或更多个 CPU (两个内核)，对于最大值，最小值 + 两个或更多个 CPU
(例如，ncpus=3-5)
- 使用 pbind 命令将任何进程绑定到 CPU 内核时
您必须使用 pbind 命令检查/释放绑定到 CPU 内核的任何进程，以便采用自动 CPU 内核更换功能来使用 CPU 内核。
- 当使用 psrset 命令将进程仅绑定到一个 CPU 内核时
通过使用自动 CPU 内核更换功能释放您希望使用的 CPU 内核，将两个或更多个 CPU 内核分配给处理器组，或移除处理器组。

10.7.2 更改自动更换策略的方法

使用 Oracle VM Server for SPARC 的 svccfg 命令可以更改自动更换策略。使用 ldmd 服务的 autoreplacement_policy_cpu 属性，可启用/禁用自动更换策略。可为 autoreplacement_policy_cpu 属性使用以下值。

- autoreplacement_policy_cpu=1
故障 CPU 资源被自动更换。这是默认策略。
- autoreplacement_policy_cpu=0
如果 CPU 发生故障，则不会被自动更换。

设置步骤如下。

1. 登录控制域。
2. 成为管理员。
3. 查看 autoreplacement_policy_cpu 属性值。

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu
```

4. 停止 ldmd 服务。

```
# svcadm disable ldmd
```

5. 变更 autoreplacement_policy_cpu 属性值。

```
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=value
```

6. 刷新并重新启动 ldmd 服务。

```
# svcadm refresh ldmd  
# svcadm enable ldmd
```

以下是如何查看 autoreplacement_policy_cpu 属性的当前值以及如何改为新值的示例。本属性的初始值是 0。此时，禁用 CPU 指定更换功能。使用 svcadm 命令停止或重启 ldmd 服务。使用 svccfg 命令查看或设置属性值。

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu  
ldmd/autoreplacement_policy_cpu integer 0  
# svcadm disable ldmd  
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=1  
# svcadm refresh ldmd  
# svcadm enable ldmd
```

10.7.3 更改最大重试次数计数器和重试间隔的方法

除更改自动更换策略外，您还可以设置 CPU 自动更换过程的最大重试次数和两次重试之间的间隔时间。

- 通过设置 ldmd 服务的 autoreplacement_retry_counter 属性指定最大重试次数。如果指定为 0，没有重试次数的限制。默认值为 5。
- 通过设置 ldmd 服务的 autoreplacement_retry_interval 属性指定重试间隔。最小间隔为 1 秒。默认值为 300 秒。

修改这些属性的步骤与修改 autoreplacement_policy_cpu 属性值相同。请参见 ["10.7.2 更改自动更换策略的方法"](#)。

10.8 设置恢复模式

由于资源问题、资源不足等原因无法启动的域配置可通过设置由 Oracle VM Server for SPARC 3.1 和更高版本提供的恢复模式自动恢复。

在 Oracle VM Server for SPARC 3.3 或更高版本中默认启用此功能。

有关恢复模式的详情，请参见所使用版本的《Oracle VM Server for SPARC Administration Guide》中的 "Handling Hardware Errors"。此外，关于恢复模式所需的修复，请参见所使用版本的《Oracle VM Server for SPARC Release Notes》。

10.9 建立冗余组件配置

即使组件故障，如果组件有冗余配置，系统可以通过其余组件继续其操作。

有关冗余组件配置的详情，请参见服务器的《Service Manual》。

请使用 `showhardconf` 命令查看组件配置。有关如何检查组件的详情，请参见 "11.1.2 查看系统安装的组件"。

10.10 保存/恢复 XSCF 设置信息

如需保存/恢复 XSCF 设置信息，执行 XSCF 固件 `dumpconfig` 或 `restoreconfig` 命令。通过执行指定选项的命令可保存或恢复指定位置中的所有 XSCF 设置信息。

10.10.1 了解如何保存/恢复 XSCF 设置信息

本节介绍以下两种方法保存/恢复 XSCF 设置信息。

- 通过将 USB 设备连接到主 XSCF 的 XSCF 单元面板（后面板）上的 USB 端口，在本地保存/恢复设置信息。
- 通过网络将数据传输到网络主机。加密协议用于数据传输。

注 - 当更换 SPARC M12-2/M12-2S 的 XSCF 单元时，也可以通过交换 SD 卡来接管 XSCF 设置信息。当更换接线盒 (XBBOX) 或 SPARC M10-4/M10-4S 的 CPU 内存单元（下）(CMUL) 时，也可以通过交换 microSD 卡来接管 XSCF 设置信息。

有关详细信息，请参见服务器的《Service Manual》中的 "Replacing the SD card" 或 "Replacing microSD card"。更换接线盒的 XSCF 单元时，请参见《Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》中的 "8.5 Switching the microSD Card"。

保存的目的

用 `dumpconfig` 命令保存 XSCF 设置信息的目的如下。

- 备份设置信息可以在发生故障后使数据恢复。
- 复制主 XSCF 的设置信息可以使另一台服务器的 XSCF 使用相同的设置信息。

保存和恢复的注意事项

- USB 设备需要用 FAT32 文件系统进行格式化。请向服务工程师查询有关用于本地保存/恢复设置信息的 USB 的容量以及处理时的注意事项。
- 只能将设置信息恢复到保存有设置信息的相同型号的系统。例如，SPARC M10-1 系统中保存的设置信息只能恢复到 SPARC M10-1 系统。恢复数据时，要检查当前

系统和要恢复到系统的配置文件一致性。只有在确认配置文件版本、系统名称和其它信息的一致性后才能恢复配置文件。注意，配置文件版本不取决于 XCP 版本。即使 XCP 版本在保存/恢复时相同，每个配置文件的版本也可能相互不同。

- 具有两个或更多 XSCF 的系统在主 XSCF 端执行保存/恢复。
- 保存数据用指定选项的 `dumpconfig` 命令进行加密。通过输入在执行 `restoreconfig` 命令时指定保存的密钥，您可安全地恢复加密的数据。
- 所保存配置文件的标头包含以下标识信息。标识信息可以引用文本。
 - 用户注释
 - 数据版本
 - 加密是启用还是禁用
 - 保存时间
 - 系统名称
 - 序列号
 - XCP 版本
- XSCF 网络设置为恢复数据指定选项。
- 如需恢复设置信息，请关闭所有物理分区的电源。此外，在执行 `restoration` 命令后，加载 XSCF 设置信息并检查其内容的是否正确。确认完成后，XSCF 将重新启动，并恢复数据。

10.10.2 保存 XSCF 设置信息

本节介绍保存 XSCF 配置文件的步骤。

注 - 使用 `dumpconfig` 命令加密并保存 XSCF 设置信息。有关详细信息，请参见 `dumpconfig` (8) 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

在主 XSCF 的 USB 设备中保存设置信息

1. 将 **USB** 设备连接到主 **XSCF** 的 **XSCF** 单元面板（后面板）上的 **USB** 端口。
2. 在 **XSCF** 上的本地 **USB** 设备指定输出文件名并执行 `dumpconfig` 命令。

```
XSCF> dumpconfig file:///media/usb_msd/backup-file.txt
```

3. 数据传输完成后，从 **USB** 端口移除 **USB** 设备。
4. 确认所保存配置文件标头的标识信息。

通过网络指定目标目录并保存设置信息

1. 指定目标目录和输出文件名并执行 `dumpconfig` 命令。


```
XSCF> dumpconfig ftp://server/backup/backup-sca-ff2-16.txt
:
```

2. 数据传输完成后，确认所保存配置文件标头的标识信息。

配置文件格式

所保存配置文件的格式如下：

- 文件名：用户指定的名称
- 文件格式：base64 编码文本

10.10.3 恢复 XSCF 设置信息

本节介绍恢复 XSCF 配置文件的步骤。

注 - 使用 `restoreconfig` 命令可以解密使用 `dumpconfig` 命令加密的文件。有关详细信息，请参见 `restoreconfig(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

注 - 当执行 `dumpconfig` 命令后使用 `ldm add-spconfig` 命令在控制域上保存逻辑域配置信息时，使用 `restoreconfig` 命令可能无法恢复逻辑域配置信息。因此，使用 `restoreconfig` 命令恢复 XSCF 设置信息之前，请在所有控制域上使用 `ldm remove-spconfig` 命令移除所有除出厂默认之外的逻辑域配置信息。

如需检查使用 `ldm add-spconfig` 命令已经保存的配置信息文件的日期，需对所有物理分区执行 `showdomainconfig` 命令。

有关逻辑域配置信息的详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》中的 "Managing Domain Configurations" 的内容。

从主 XSCF 的 USB 设备中恢复设置信息

1. 关闭所有物理分区的电源。
2. 将包含配置文件的 **USB** 设备连接到主 **XSCF** 的 **XSCF** 单元面板（后面板）上的 **USB** 端口。
3. 将 **XSCF** 单元上的本地 **USB** 设备指定为输入文件并执行 `restoreconfig` 命令。

```
XSCF> restoreconfig file:///media/usb_msd/backup-file.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
:
*** You will need to power-cycle the entire system after this operation
is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

信息显示要恢复配置文件的标识信息。

4. 内容正确时，输入 **"y"** 进行恢复。
XSCF 重新启动。

5. 会话断开一次。重新连接。
6. 数据恢复完成后，从 **USB** 端口移除 **USB** 设备。

通过网络指定目标目录并恢复设置信息

1. 关闭所有域的电
2. 指定目标目录并执行 **restoreconfig** 命令。

```
XSCF> restoreconfig ftp://server/backup/backup-sca-ff2-16.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
:
*** You will need to power-cycle the entire system after this operation
is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

信息显示要恢复配置文件的标识信息。

3. 内容正确时，输入 **"y"** 进行恢复。
XSCF 重新启动。
4. 会话断开一次。重新连接。

10.11 保存/恢复 XSCF 中的逻辑域配置信息

本节介绍如何保存 XSCF 逻辑域配置信息和如何恢复保存的配置信息。

有关在 XML 文件中保存/恢复逻辑域配置信息的方法，请参见 ["10.12 在 XML 文件中保存/恢复逻辑域配置信息"](#)。

10.11.1 保存/显示逻辑域配置信息

您可为各物理分区保存逻辑域配置信息。要保存配置信息，请登录目标物理分区的控制域。保存的配置信息存储在物理分区内的服务处理器上。

最多可以为各物理分区保存八组逻辑域配置信息。其中一个包含出厂默认状态，被命名为 **factory-default**。由于 **factory-default** 已经保存，因此您最多可以保存其余七组配置信息。通过提前保存不同的配置方式，在重新启动物理分区时，您便可以指定适合业务的逻辑域配置。有关逻辑域配置信息的详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》中的 **"Managing Domain Configurations"** 的内容。

保存逻辑域配置信息

如需保存逻辑域配置信息，请执行 Oracle VM Server for SPARC 的 **ldm** 命令并指定子命令 **add-spconfig**。

```
primary# ldm add-spconfig config_name
```

对于 `config_name`，请指定用于在 XSCF 中保存逻辑域配置信息的文件名。

注 - `add-spconfig` 子命令不能重写已存在文件的配置信息。为 `config_name` 指定已存在文件的文件名之前，您需使用 `remove-spconfig` 子命令删除已存在文件。

显示逻辑域配置信息

您可查看在物理分区的控制域上或主 XSCF 上的逻辑域配置信息。

- 查看物理分区的控制域上的信息
如需查看保存在控制域上的逻辑域配置信息，请执行 Oracle VM Server for SPARC 的 `ldm` 命令并指定子命令 `list-spconfig`。

```
primary# ldm list-spconfig
```

- 在 XSCF shell 上查看信息
如需在 XSCF shell 上查看保存的逻辑域配置信息，请使用 XSCF 固件的 `showdomainconfig` 命令。

```
XSCF> showdomainconfig -p ppar_id
```

对于 `ppar_id`，指定希望查看的已保存逻辑域配置信息的物理分区 PPAR-ID。根据系统配置，您只能指定 0 到 15 的一个整数。

操作步骤

1. 将 **XSCF shell** 切换到目标物理分区的控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 [“8.3 从 XSCF Shell 切换到控制域控制台”](#)。
2. 执行 `ldm list-spconfig` 命令查看当前保存的逻辑域配置信息。

```
primary# ldm list-spconfig
```

3. 执行 `ldm add-spconfig` 命令以将逻辑域状态保存为配置信息。
以下是名为 `ldm-set1` 的文件是保存目标的示例。

```
primary# ldm add-spconfig ldm_set1
```

4. 执行 `ldm list-spconfig` 命令并确认配置信息已正确保存。

```
primary# ldm list-spconfig
```

10.11.2 恢复逻辑域配置信息

重新启动物理分区时，您可以指定所保存的物理分区配置列表中的逻辑域配置信息。当您想要使用当前的配置在不同的逻辑域配置中重新启动时，对您有所帮助。

注 - 如需恢复逻辑域配置信息，必须提前保存逻辑域配置信息。有关详情，请参见“10.11.1 保存/显示逻辑域配置信息”。

恢复保存的逻辑域配置信息

如需恢复保存在控制域上的逻辑域配置信息，请执行如下 XSCF 固件的 `setdomainconfig` 命令。

```
XSCF> setdomainconfig -p ppar_id [-i index]
```

`ppar_id` 用于指定物理分区的 PPAR-ID。根据系统配置，您只能指定 0 到 15 的一个整数。`index` 用于指定配置信息的索引号。如果省略，您可以在查看所保存配置信息时以交互方式指定索引号。

操作步骤

1. 执行 `setdomainconfig` 命令，并指定下次启动物理分区时要使用的逻辑域配置。在以下示例中，在查看所保存配置信息列表时，以交互方式指定 PPAR-ID 0 的逻辑域配置。

```
XSCF> setdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :ldm-set2
(Next)       :ldm-set2
-----
Index        :1
config_name  :factory-default
domains      :1
date_created:-
-----
Index        :2
config_name  :ldm-set1
domains      :8
date_created:'2012-08-08 11:34:56'
-----
Index        :3
config_name  :ldm-set2
domains      :20
date_created:'2012-08-09 12:43:56'
-----
Select Index of Using config_name:2
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "ldm-set1".
```

```
Continue? [y|n] :y
XSCF>
```

在以下示例中，通过为 PPAR-ID 0 指定索引号 1 指定配置信息。

```
XSCF> setdomainconfig -p 0 -i 1
Index          :1
config_name    :factory-default
domains        :1
date_created:-
-----
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "factory-default".
Continue? [y|n] : y
XSCF>
```

将逻辑域恢复为出厂状态

如需将逻辑域配置信息恢复到出厂状态，请执行如下 XSCF 固件的 setdomainconfig 命令。

```
XSCF> setdomainconfig -p ppar_id -c default
```

ppar_id 用于指定物理分区的 PPAR-ID。根据系统配置，您只能指定 0 到 15 的一个整数。指定 -c default，将逻辑域恢复为出厂状态。

操作步骤

1. 执行 **setdomainconfig** 命令并指定用于重启逻辑域时间的配置信息。
以下是将 PPAR-ID 0 逻辑域配置恢复为出厂状态的示例。

```
XSCF> setdomainconfig -p 0 -c default
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "factory-default".
Continue? [y|n] : y
XSCF>
```

10.12 在 XML 文件中保存/恢复逻辑域配置信息

本节介绍如何在 XML 文件中保存所有逻辑域配置信息 and 如何恢复保存在 XML 文件中的配置信息。

当保存到 XSCF 的信息丢失时，使用 XML 文件恢复系统。

10.12.1 保存/确认逻辑域配置信息

您可将每个物理分区的逻辑域配置信息保存到 XML 文件。如需将逻辑域配置信息保存到 XML 文件，请登录到目标物理分区的控制域。

有关详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》中的 "Managing Domain Configurations" 的内容。

保存逻辑域配置信息

执行 Oracle VM Server for SPARC 的 `ldm list-constraints -x` 命令保存逻辑域配置信息。

```
primary# ldm list-constraints -x > file_name.xml
```

在 `file_name.xml` 中指定保存配置信息的文件名。

操作步骤

1. 将 **XSCF shell** 切换到目标物理分区的控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 "8.3 从 XSCF Shell 切换到控制域控制台"。
2. 执行 `ldm list-sponfig` 命令确认当前逻辑域配置信息已保存到 **XSCF** 中。

注 `-ldm list-sponfig` 命令列出了已保存的域配置信息的名称。该命令的操作结果并不显示创建时间、域的数量或任何已保存的配置信息是否与当前域配置匹配。管理员需要跟踪保存的配置文件名、其所映射到的配置以及其是否与当前逻辑域配置匹配。您也可以使用 `showdomainconfig` 命令查看每个已保存配置中的创建日期/时间和逻辑域的数量。

以下示例中，将当前配置信息设置为 `test1`。

当前配置信息未被保存在 XSCF 上时，使用 `ldm add-sponfig` 命令保存信息。

```
primary# ldm list-sponfig
factory-default
test1 [current]
test2
test3
```

3. 执行 `ldm list-constraints -x` 命令并将逻辑域配置信息保存到 **XML** 文件。
以下是如何将信息保存到 `/ldm-set1.xml` 的示例。

```
primary# ldm list-constraints -x > /ldm-set1.xml
```

4. 执行 `more` 命令等命令，并确认信息已被保存到 **XML** 文件。

```
primary# more /ldm-set1.xml
<?xml version="1.0"?>
<LDM_interfaceversion="1.3" xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
```

为了防止已保存 XML 文件的丢失，请在其他介质备份。

注 - 如果使用 SR-IOV 功能将虚拟功能 (VF) 分配给逻辑域，则提前执行 ldm 命令可保存为每个 VF 设置的信息。

10.12.2 恢复逻辑域配置信息

执行 ldm init-system 命令反映保存的 XML 文件，并执行 shutdown 命令重启逻辑域。

恢复保存的逻辑域配置信息

如需恢复保存在 XML 文件的配置信息，执行如下控制域的 ldm init-system 命令。

```
primary# ldm init-system -i file_name.xml
```

操作步骤

1. 确认当前的逻辑域配置是出厂默认状态。

```
primary# ldm list-config | grep "factory-default"
factory-default [current]
```

如果 factory-default 的后面不是 [current]，当前的逻辑域配置不是出厂默认状态。此时，按照如下的步骤将当前的逻辑域配置更改到出厂默认状态。

指定 factory-default 并执行 ldm set-sponfig 命令。

```
primary# ldm set-sponfig factory-default
```

执行 XSCF 固件的 poweroff 命令关闭物理分区的电源。

```
XSCF> poweroff -p ppar_id
```

2. 执行 ldm init-system 命令反映已保存 XML 文件的设置。
以下是如何恢复保存在 /ldm-set1.xml 的信息的示例。

```
primary# ldm init-system -i /ldm-set1.xml
Initiating a delayed reconfiguration operation on the primary
domain.
All configuration changes for other domains are disabled until
```

```
the primary
domain reboots, at which time the new configuration for the
primary domain
will also take effect.
```

3. 执行 **shutdown** 命令重启控制域。

```
primary# shutdown -y -g0 -i6
```

4. 启动域时，将资源绑定到非控制域的逻辑域。
在以下示例中，启动域时资源被绑定到 ldom1。

```
primary# ldm bind ldom1
primary# ldm start ldom1
```

10.13 保存/恢复 OpenBoot PROM 环境变量

如需从 XML 文件恢复逻辑域配置信息，请在将逻辑域变更为出厂默认配置之前，将 OpenBoot PROM 环境变量记录并保存在控制域中。

变更为出厂默认配置后，使用已保存的信息恢复 OpenBoot PROM 环境变量。

保存/恢复 OpenBoot PROM 环境变量时，请通过执行 OpenBoot PROM 的 **printenv** 命令检查 OpenBoot PROM 环境变量并保存内容。然后，使用 **setenv** 命令恢复。

10.13.1 保存 OpenBoot PROM 环境变量

本节介绍保存 OpenBoot PROM 环境变量的步骤。

1. 执行 **printenv** 命令检查 OpenBoot PROM 环境变量。

```
{0} ok printenv
Variable Name           Value           Default Value
ttya-rts-dtr-off       false          false
ttya-ignore-cd         true           true
keyboard-layout
reboot-command
security-mode           none           No default
security-password      No default
security-#badlogins    1             No default
diag-switch?          false         false
local-mac-address?    false         true
fcode-debug?          false         false
scsi-initiator-id      7             7
oem-logo               No default
oem-logo?             false         false
```



```

oem-banner                                No default
oem-banner?                               false
ansi-terminal?                            true
screen-#columns                            80
screen-#rows                               34
ttya-mode                                  9600,8,n,1,-
output-device                              virtual-console
input-device                               virtual-console
auto-boot-on-error?                       false
load-base                                  16384
auto-boot?                                 true
os-root-device
network-boot-arguments host-ip=192.168.123.100, ...
boot-command                               boot
boot-file
boot-device                                mydisk1 mydisk2 mydisk3 ...
multipath-boot?                            false
boot-device-index                          0
use-nvramrc?                               true
nvramrc                                    devalias mydisk1 /pci@80 ...
error-reset-recovery                       boot
{0} ok

```

2. 将输出结果保存到文本文件。
3. 如果在步骤 1 中有一个变量，其值被替换为“...”，请执行指定相应变量的 **printenv** 命令。
以下示例检查 `boot-device` 变量。

```

{0} ok printenv boot-device
boot-device =                mydisk1 mydisk2 mydisk3 mynet

```

以下示例检查 `nvramrc` 设置。

```

{0} ok printenv nvramrc
nvramrc =                devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@
0/disk@p3,0:a
                        devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p0,0:a
                        devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p1,0:a
                        devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
h# 8 value video-mode

```

以下示例检查 `network-boot-arguments` 设置。

```

{0} ok printenv network-boot-arguments
network-boot-arguments = host-ip=192.168.123.100,subnet-mask=255.255.255.
0,iscsi-target-ip=192.168.100.10,iscsi-target-name=iqn.2016-12.com.fujitsu:02:
iscsiboot,iscsi-lun=0

```

4. 将步骤 3 中输出结果保存到文本文件。

10.13.2 恢复 OpenBoot PROM 环境变量

本节介绍恢复 OpenBoot PROM 环境变量的步骤。

- 当恢复 nvramrc 变量以外的变量时

1. 检查文本文件中保存的 **OpenBoot PROM** 环境变量。
2. 执行 **setenv** 命令恢复该值并执行 **printenv** 命令查看内容。
如果您计划使用保存的 XML 文件恢复逻辑域信息，则在发出下一次重启之前将 **auto-boot?** 设置为 "false"，并将 **security-mode** 设置为 "none"。
以下示例将 **local-mac-address?** 恢复为 "false"。

```
{0} ok setenv local-mac-address? false
local-mac-address? = false
{0} ok printenv local-mac-address?
local-mac-address? = false
```

以下示例将 **boot-device** 恢复为 "mydisk1 mydisk2 mydisk3 mynet"。

```
{0} ok setenv boot-device mydisk1 mydisk2 mydisk3 mynet
boot-device = mydisk1 mydisk2 mydisk3 mynet
{0} ok printenv boot-device
boot-device = mydisk1 mydisk2 mydisk3 mynet
```

以下示例将 **use-nvramrc?** 恢复为 "true"。

```
{0} ok setenv use-nvramrc? true
use-nvramrc? = true
{0} ok printenv use-nvramrc?
use-nvramrc? = true
```

- 当恢复 nvramrc 变量时

1. 检查文本文件中保存的 **OpenBoot PROM** 环境变量。
2. 执行 **nvedit** 命令将值设置为 **nvramrc**。
以下示例将步骤 1 中检查的内容写入 **nvramrc**。

```
{0} ok nvedit
0: devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3,0:a
1: devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0,0:a
2: devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1,0:a
3: devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
4: h# 8 value video-mode
5:
```

3. 按下 **[Ctrl]** 和 **[C]** 键，退出 **nvedit** 并返回 **ok** 提示符。
4. 执行 **nvstore** 命令保存编辑。

```
{0} ok nvstore
```

5. 执行 **printenv nvramrc** 命令检查 **nvramrc** 是否正确写入。

```
{0} ok printenv nvramrc
nvramrc =
0/disk@p3,0:a          devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@
0/disk@p0,0:a          devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p1,0:a          devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@
                        devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
                        h# 8 value video-mode
```

6. 如果 **OpenBoot PROM** 环境变量 **auto-boot?** 是 **“true”**，则执行 **setenv** 命令将其设置为 **“false”**。

```
{0} ok setenv auto-boot? false
```

7. 执行 **reset-all** 命令重新启动 **OpenBoot PROM**。

```
{0} ok reset-all
```

8. 然后，启动 **Oracle Solaris** 并使用 **XML** 文件恢复逻辑域信息。
这允许在物理分区（包括控制域）中恢复除 **security-password** 之外的所有逻辑域中的 **OpenBoot PROM** 环境变量。

有关使用 **XML** 文件恢复逻辑域配置信息的详情，请参见 [“10.12 在 XML 文件中保存/恢复逻辑域配置信息”](#)。

对于 **security-mode** 设置为 **command** 或 **full** 的逻辑域，请求系统管理员设置 **security-password**。

10.14 保存/恢复硬盘中的内容

为了防止由于硬盘故障等造成的重要数据丢失，定期备份硬盘内容非常重要。

SPARC M12/M10 系统支持使用硬件 **RAID** 功能的冗余磁盘配置。冗余磁盘配置让系统操作更加可靠。

为应对由于多个磁盘故障造成的数据丢失，需要定期备份硬盘内容。

应确认适用于您的运行系统的备份方法，然后执行备份。保存和恢复硬盘内容的方法根据所执行的备份方法而有所不同。按照所执行的备份方法采用合适的方法。

10.15 重启逻辑域

请使用 XSCF 固件 `reset` 命令重启指定的逻辑域。

请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。另外，对于目标逻辑域所属的物理分区，具有 `pparadm` 或 `pparmgr` 权限的用户帐户也能执行此操作。

注 `-reset` 命令强制重启指定的物理分区，因此可能造成磁盘故障等故障。只有在紧急情况先才使用此命令，例如 Oracle Solaris 死机后的恢复时。

```
XSCF> reset -p ppar_id -g domainname sir | panic
```

`ppar_id` 用于指定重启逻辑域所属物理分区的 PPAR-ID。根据系统配置，您只能指定 0 到 15 的一个整数。

`domainname` 用于指定将要重启逻辑域的名称。

如需重启逻辑域自身，指定 `sir`。如需在逻辑域执行崩溃，指定 `panic`。

操作步骤

1. 执行 `reset` 命令重置指定逻辑域。输入 "y"，确认信息。
下面是重置来宾域 PPAR-ID 00 的 `ldom1` 的示例。

```
XSCF> reset -p 0 -g ldom1 sir
PPAR-ID:00 GuestDomain to sir:ldom1
Continue? [y|n] : y
00 ldom1 :Resetting

*Note*
This command only issues the instruction to reset.
The result of the instruction can be checked by the
"showdomainstatus".
XSCF>
```

2. 执行 `showdomainstatus` 命令并确认指定逻辑域已重启。
下面是查看逻辑域 PPAR-ID 0 状态的示例。在状态栏显示 `OpenBoot` 正在初始化或 `OpenBoot` 正在运行，然后最终显示 `Solaris` 运行。

```
XSCF> showdomainstatus -p 0
```

10.16 在逻辑域中引起崩溃

本节介绍如何在指定逻辑域中引起崩溃。

逻辑域负荷异常激增或挂起导致指定逻辑域崩溃后，收集转储文件。

10.16.1 在来宾域中引起崩溃

从控制域执行 Oracle VM Server for SPARC 的 `ldm panic-domain` 命令，引起指定来宾域的崩溃。

有关 `ldm` 命令的详情，请参见您所使用版本的《Oracle VM Server for SPARC Reference Manual》。

注 - `ldm panic-domain` 命令在指定的来宾域强制引起崩溃，因此可能导致磁盘故障等故障。因此在处置突发事件以外请限制使用。

```
primary# ldm panic-domain ldom
```

`ldom` 用于发生崩溃时指定将要关闭来宾域的名称。

注 - 您还可使用 XSCF 固件 `reset` 命令引起崩溃。有关详细信息，请参见 `reset(8)` 命令 `man` 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

10.16.2 在控制域中引起崩溃

请使用 XSCF 固件 `reset` 命令重启指定的控制域。

请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。对于目标物理分区，具有 `pparadm` 或 `pparmgr` 权限的用户帐户也能执行此操作。

注 - `reset` 命令在指定的控制域强制引起崩溃，因此可能导致磁盘故障等故障。因此处置突发事件时请限制使用。

```
XSCF> reset -p ppar_id -g primary panic
```

`ppar_id` 用于指定与发生崩溃的控制域（属于物理分区）有关的物理分区 ID。根据系统配置，可指定 0 到 15 的整数。

当输入电源关闭和控制域关闭时，`reset` 命令无效。

操作步骤

1. 执行 **reset** 命令以在指定控制域中引起崩溃。
下面是在物理分区 ID 0 的控制域中引起崩溃的示例。

```
XSCF> reset -p 0 -g primary panic
PPAR-ID:00
GuestDomain to panic:primary
Continue? [y|n] : y
00 primary :Resetting

*Note*
  This command only issues the instruction to reset.
  The result of the instruction can be checked by the
  "showdomainstatus".
XSCF>
```

2. 执行 **showdomainstatus** 命令并确认在指定控制域中已发生的崩溃。

```
XSCF> showdomainstatus -p 0
```

10.17 重启物理分区

请使用 XSCF 固件 **reset** 命令重启指定的物理分区。

请使用拥有 **platadm** 或 **fieldeng** 权限的用户账户执行此命令。另外，对于目标物理分区，具有 **pparadm** 或 **pparmgr** 权限的用户帐户也能执行此操作。

注 - **reset** 命令强制重启指定的物理分区，因此可能造成磁盘故障等故障。只有在紧急情况先才使用此命令，例如 Oracle Solaris 死机后的恢复时。

```
XSCF> reset -p ppar_id por | xir
```

ppar_id 用于指定重置物理分区的 PPAR-ID。根据系统配置，您只能指定 0 到 15 的一个整数。

如需重启物理分区自身，指定 **por**。如需重置物理分区中的所有 CPU，指定 **xir**。

注 - 如果物理分区使用指定的 **xir** 重启并且管理程序启用，收集管理程序转储文件，然后逻辑域在重启时使用出厂默认配置启动。如需返回到物理分区重启前的逻辑域配置，请关闭一次物理分区电源后再打开。有关管理程序转储功能的详情，请参见“[8.13 收集管理程序转储文件](#)”。

如果逻辑域的自动重启功能被 **setpparparam** 命令设置为禁用，执行 **reset** 命令时，执行过程在 Oracle Solaris 启动前停止。

操作步骤

1. 执行 **reset** 命令重置指定物理分区。输入 "y", 确认信息。
以下是重启 PPAR-ID 00 的示例。

```
XSCF> reset -p 0 por
PPAR-ID to reset:00 Continue? [y/n] : y
00 :Resetting

*Note*
This command only issues the instruction to reset.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

2. 执行 **showpparprogress** 命令并确认指定物理分区已重启。

```
XSCF> showpparprogress -p 0
PPAR Power On Preprocessing PPAR#0 [ 1/12]
PPAR Power On                PPAR#0 [ 2/12]
XBBOX Reset                  PPAR#0 [ 3/12]
PSU On                        PPAR#0 [ 4/12]
CMU Reset Start              PPAR#0 [ 5/12]
XB Reset 1                   PPAR#0 [ 6/12]
XB Reset 2                   PPAR#0 [ 7/12]
XB Reset 3                   PPAR#0 [ 8/12]
CPU Reset 1                  PPAR#0 [ 9/12]
CPU Reset 2                  PPAR#0 [10/12]
Reset released               PPAR#0 [11/12]
CPU Start                    PPAR#0 [12/12]
The sequence of power control is completed.
XSCF>
```

10.18 将服务器恢复为出厂默认状态

本节介绍如何将 SPARC M12/M10 恢复为出厂时的状态。
如需恢复 SPARC M12/M10 机箱中的 XSCF 设置信息的备份数据, 或者将 XSCF 单元中的 XSCF 设置信息恢复为出厂时的状态, 请执行 XSCF 固件的 `initbb` 命令或 `restoredefaults` 命令。



注意 - 执行命令将删除用户定义的 XSCF 单元设置信息和错误信息或各机柜中的 XSCF 备份信息。

10.18.1 了解初始化命令

initbb 和 restoredefaults 命令各自具有以下作用。

- **restoredefaults 命令**
此命令初始化主 XSCF 机柜。此命令初始化 XSCF 单元设置信息及其备份信息，或者只初始化 XSCF 单元设置信息。
- **initbb 命令**
此命令从主 XSCF 初始化除主机柜以外的机柜的信息。此命令不能用于具有一个 XSCF 的系统。

注 - restoredefaults 命令恢复 XSCF 设置信息和备份信息到出厂状态。

注 - 如果没有保存 CPU 激活并且已经执行了 restoredefaults 命令，CPU 激活密钥需要再次登录。

10.18.2 初始化服务器

有一个 XSCF 的系统中

使用 restoredefaults 命令初始化服务器。

操作步骤

1. 与 **XSCF** 建立串行连接。
2. 登录 **XSCF**。
3. 执行 **poweroff-a** 命令以停止系统。
4. 执行 **restoredefaults** 命令以初始化机柜（**XSCF** 单元设置信息及其备份信息）或初始化 **XSCF** 单元设置信息。

注 - 有关如何指定 restoredefaults 命令的选项以及相关注意事项，请参见 restoredefaults(8) 命令 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

有多个 XSCF 的系统中

初始化的前提条件如下。

- 每个机柜连接到 XSCF 网络。
- 如果运行中的物理分区的 PPAR-ID 与被初始化机柜 BB-ID 的相同，请关闭该物理分区的电源。
- 被初始化机柜的 PSB 必须处于系统板池状态。
- 被初始化机柜的 PSB 不得属于任何 PPAR。

- 初始化主 XSCF 以外的接线盒时，请执行 `poweroff -a` 命令关闭系统。

操作步骤

1. 为了初始化主 XSCF，执行指定 `-a` 选项的 `poweroff` 命令停止系统。
2. 与主 XSCF 建立串行连接。
3. 登录主 XSCF。
4. 指定目标机柜的 **BB-ID** 并执行 `initbb` 命令，初始化目标机柜。
对主机柜以外的目标机柜执行此步骤。
下一步初始化主机柜，请执行以下步骤。
5. 执行 `restoredefaults` 命令以初始化机柜（XSCF 单元设置信息及其备份信息）或初始化 XSCF 单元设置信息。

注 - 有关如何指定 `initbb(8)` 和 `restoredefaults(8)` 命令的选项以及相关注意事项，请参见各命令 `man` 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

注 - 有关如何连接线缆的详情，请参见《Fujitsu SPARC M12-2S 安装指南》中的 "第4章 设置模块化架构配置中的 SPARC M12-2S" 或《Fujitsu M10-4S/SPARC M10-4S 安装指南》中的 "第4章 配置模块化架构连接"。

注 - 有关此命令的支持信息的详情，请参见服务器的最新《产品说明》。

10.19 使用延迟转储收集崩溃转储文件

在 XCP 2290 或更高版本以及 Oracle Solaris 11.2 SRU11.2.8.4.0 或更高版本中，崩溃转储文件可能会保存在内存中，直到系统崩溃后重新启动系统。

在系统重新启动期间，崩溃转储文件将从内存提取到由转储配置定义的文件系统。

在写入这些文件后，系统将自动重新启动到正常的多用户配置。

此过程称为延迟转储。当使用此延迟转储时，系统可以在内核崩溃后的短时间内返回到操作状态。

有关延迟转储功能的详细信息，请参见您的 Solaris 版本的《Managing Devices in Oracle Solaris》。

查看系统状态

本章介绍配置或操作系统时如何查看系统硬件配置/状态和物理分区配置/状态。

- 查看系统配置/状态
- 查看物理分区

11.1 查看系统配置/状态

11.1.1 查看与系统配置/状态相关的设置项目和命令

表 11-1 列出了检查系统配置/状态的项目和 XSCF shell 命令。

有关各项目的详情，请参见以下章节。

表 11-1 用于查看配置和状态的命令

检查项目	相关命令
查看搭载的组件 - 所有搭载在系统中的部件 - 模式开关状态	showhardconf(8)
查看故障/降级组件	showstatus(8)
查看系统环境信息 - 环境温度 - 电压 - 风扇速度级别 - 功耗 - 排气	showenvironment(8)
查看 PCI 扩展单元设置信息	ioxadm(8)

11.1.2 查看系统安装的组件

使用 `showhardconf` 命令可查看系统上搭载的所有组件及其状态。任何问题部件会显示一个星号 (*)。系统管理员可掌控组件配置、搭载的单元数、模式开关状态和现场可更换单元 (FRU)。

组件信息

表 11-2 列出了 SPARC M12 的各个组件的信息。您可以通过执行 `showhardconf` 命令来检查分层结构中组件的详细信息。

表 11-2 SPARC M12 的各个组件的信息

组件	说明
系统信息	序列号、模式切换状态、系统电源状态、系统电源相位、物理分区状态
SPARC M12-2/M12-2S 信息	单元编号、状态、角色、版本、序列号、FRU 编号、输入电源类型、内存容量 角色显示为主、备用或从。
CPU 内存单元 (下) (CMUL) 信息 (SPARC M12-2/M12-2S)	状态、版本、序列号、FRU 号、内存容量、类型
CPU 内存单元 (上) (CMUU) 信息 (SPARC M12-2/M12-2S)	状态、版本、序列号、FRU 号、内存容量、类型
主板单元 (MBU) 信息 (SPARC M12-1)	状态、版本、序列号、FRU 号、内存容量、类型
CPU 信息	单元编号、状态、版本、序列号、CPU 工作频率、CPU 类型、CPU 内核数、CPU 线程数
内存 (MEM) 信息	单元编号、状态、代码、类型 (唯一 ID)、容量
PCI 信息	单元号、状态、名称属性、厂商 ID、设备 ID、子系统厂商 ID、子系统 ID、VPD 号、连接、PCI 扩展单元信息
PCI 扩展单元 (PCIBOX) 信息	单元编号、状态、版本、序列号、FRU 编号 IO 板 (IOB) 信息: 状态、序列号、类型、FRU 编号 链路板信息: 状态、版本、序列号、FRU 号 PCI 信息: 单元编号、名称属性、供应商 ID、设备 ID、子系统供应商 ID、子系统 ID、VPD 编号 风扇背板 (FANBP) 信息: 单元编号、状态、序列号、FRU 编号 PSU 背板 (PSUBP) 信息: 单元编号、状态、序列号、FRU 编号 电源单元 (PSU) 信息: 单元编号、状态、序列号、FRU 编号 风扇单元 (FAN) 信息: 单元编号、状态
接线单元 (XBU) 信息 (SPARC M12-2/M12-2S)	单元号、状态、版本、序列号、FRU 号、类型
接线 (CBL) 信息	单元编号、状态、供应商 ID、版本、线缆类型、长度
XSCF 单元 (XSCFU) 信息	状态、版本、序列号、FRU 号、类型

表 11-2 SPARC M12 的各个组件的信息 (续)

组件	说明
操作面板 (OPNL) 信息	状态、版本、序列号、FRU 号、类型
PSU 背板 (PSUBP) 信息	状态、版本、序列号、FRU 号、类型
电源单元 (PSU) 信息	单元号、状态、序列号、FRU 号、电源状态、电源类型、电压、类型 电源类型为 AC (交流)。
风扇单元 (FANU) 信息	单元号、状态、类型
HDD 背板 (HDDBP) 信息	单元号、状态、类型
接线盒 (XBBOX) 信息 (SPARC M12-2S)	单元编号、状态、角色、版本、序列号、FRU 编号、输入电源类型 接线单元 (XBU) 信息：单元编号、状态、版本、序列号、FRU 编号、类型 接线 (CBL) 信息：单元编号、状态、FRU 编号、版本、线缆类型、长度 XSCF 单元 (XSCFU) 信息：状态、版本、序列号、FRU 编号 操作面板 (OPNL) 信息：状态、版本、序列号、FRU 编号 接线背板 (XBBPU) 信息：状态、版本、序列号、FRU 编号、类型 XSCF 接口单元 (XSCFIFU) 信息：状态、版本、序列号、FRU 编号、类型

表 11-3 列出了 SPARC M10 的各个组件的信息。您可以通过执行 `showhardconf` 命令来检查分层结构中组件的详细信息。

表 11-3 SPARC M10 的各个组件的信息

组件	说明
系统信息	序列号、模式切换状态、系统电源状态、系统电源相位、物理分区状态
SPARC M10-4/M10-4S 信息	单元编号、状态、角色、版本、序列号、FRU 编号、输入电源类型、内存容量 作用显示为 Master (主)、Standby (备用) 或 Slave (从)。
CPU 内存单元 (下) (CMUL) 信息 (SPARC M10-4/M10-4S)	状态、版本、序列号、FRU 号、内存容量、类型
CPU 内存单元 (上) (CMUJ) 信息 (SPARC M10-4/M10-4S)	状态、版本、序列号、FRU 号、内存容量、类型
主板单元 (MBU) 信息 (SPARC M10-1)	状态、版本、序列号、FRU 号、内存容量、类型
CPU 信息	单元号、状态、版本、序列号、 CPU 工作频率、CPU 类型、CPU 内核数、CPU 线程数
内存 (MEM) 信息	单元编号、状态、代码、类型 (唯一 ID)、容量
PCI 信息	单元号、状态、名称属性、厂商 ID、设备 ID、子系统厂商 ID、子系统 ID、VPD 号、连接、PCI 扩展单元信息

表 11-3 SPARC M10 的各个组件的信息 (续)

组件	说明
PCI 扩展单元 (PCIBOX) 信息	单元编号、状态、版本、序列号、FRU 编号 IO 板 (IOB) 信息: 状态、序列号、类型、FRU 编号 链路板信息: 版本、序列号、FRU 编号 PCI 信息: 单元编号、名称属性、供应商 ID、设备 ID、子系统供应商 ID、子系统 ID、VPD 编号 风扇背板 (FANBP) 信息: 单元编号、状态、序列号、FRU 编号 PSU 背板 (PSUBP) 信息: 单元编号、状态、序列号、FRU 编号 电源单元 (PSU) 信息: 单元编号、状态、序列号、FRU 编号 风扇单元 (FAN) 信息: 单元编号、状态
接线单元 (XBU) 信息 (SPARC M10-4/M10-4S)	单元号、状态、版本、序列号、FRU 号、类型
接线 (CBL) 信息	单元号、状态、FRU 号、版本、线缆类型、长度
操作面板 (OPNL) 信息	状态、版本、序列号、FRU 编号
XSCF 单元 (XSCFU) 信息	状态、版本、序列号、FRU 编号
PSU 背板 (PSUBP) 信息	状态、版本、序列号、FRU 号、类型
电源单元 (PSU) 信息	单元号、状态、序列号、FRU 号、电源状态、电源类型、电压、类型 显示的电源类型是 AC (交流电) 或 DC (直流电)。
风扇单元 (FANU) 信息	单元号、状态、类型
接线盒 (XBBOX) 信息 (SPARC M10-4S)	单元编号、状态、角色、版本、序列号、FRU 编号、输入电源类型 接线单元 (XBU) 信息: 单元编号、状态、版本、序列号、FRU 编号、类型 接线 (CBL) 信息: 单元编号、状态、FRU 编号、版本、线缆类型、长度 XSCF 单元 (XSCFU) 信息: 状态、版本、序列号、FRU 编号 操作面板 (OPNL) 信息: 状态、版本、序列号、FRU 编号 接线背板 (XBBPU) 信息: 状态、版本、序列号、FRU 编号、类型 XSCF 接口单元 (XSCFIFU) 信息: 状态、版本、序列号、FRU 编号、类型

操作步骤

1. 执行 **showhardconf** 查看组件配置和模式开关状态。

下面是 SPARC M10-1 系统的示例。

```
XSCF> showhardconf
SPARC M10-1;
+ Serial:2101151008A; Operator_Panel_Switch:Locked;
+ System_Power:On; System_Phase:Cabinet Power On;
  Partition#0 PPAR_Status:Powered Off;
MBU Status:Normal; Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
+ Power_Supply_System:Single;
+ Memory_Size:16 GB;
```

```
CPU#0 Status:Normal; Ver:0201h; Serial:PP0629L068
+ Freq:2.800 GHz; Type:32;
+ Core:16; Strand:2;
MEM#00A Status:Normal;
:
```

2. 执行 **showhardconf** 命令查看已搭载的 **FRU** 的数量。
在下面的示例中，使用 **-u** 选项查看 SPARC M10-1 系统中已搭载的 FRU 的数量。

```
XSCF> showhardconf -u
SPARC M10-1; Memory_Size:16 GB;
+-----+-----+
| FRU                                     | Quantity |
+-----+-----+
| MBU                                     | 1        |
|   CPU                                  | 1        |
|   Freq:2.800 GHz;                       | ( 1)     |
|   MEM                                   | 16       |
|   Type:01; Size:4 GB;                   | ( 16)    |
| PCIBOX                                  | 1        |
|   IOB                                   | 1        |
|   PSU                                   | 2        |
|   FAN                                   | 2        |
| OPNL                                    | 1        |
| PSUBP                                   | 1        |
|   PSU                                   | 2        |
|   FAN_A                                 | 2        |
+-----+-----+
```

11.1.3 查看系统环境

showenvironment 命令可显示所有系统传感器的值。通过了解系统入口温度、电压和风扇速度，系统管理员可以检查系统环境是否有任何异常。另外，如果了解系统的功耗和排气，设备管理员可以识别系统安装现场的哪一个部分可用于降低能耗。

操作步骤

1. 执行 **showenvironment** 命令查看系统环境信息和电压。
下面是查看入口温度的示例。

```
XSCF> showenvironment
BB#00
  Temperature:30.71C
BB#01
  Temperature:29.97C
```

在下面的示例中通过指定 **temp** 操作数查看组件的温度。

```

XSCF> showenvironment temp
BB#00
    Temperature:30.71C
    CMUU
        CPU#0
            CPU#0:45.21C
            CPU#0:45.42C
            CPU#0:43.24C
            CPU#0:47.11C
        CPU#1
            CPU#1:45.21C
            CPU#1:45.42C
            CPU#1:43.24C
            CPU#1:47.11C
    ...

```

在下面的示例中通过指定 `volt` 操作数查看组件的电压。

```

XSCF> showenvironment volt
MBU
    0.89V Power Supply Group:0.891V
    0.90V#0 Power Supply Group:0.898V
    0.90V#1 Power Supply Group:0.894V
    0.90V#2 Power Supply Group:1.023V
    0.90V#3 Power Supply Group:1.024V
    1.0V#0 Power Supply Group:1.038V
    1.0V#1 Power Supply Group:1.041V
    1.35V#0 Power Supply Group:1.346V
    1.35V#1 Power Supply Group:1.348V
    1.5V#0 Power Supply Group:1.539V
    1.5V#1 Power Supply Group:1.506V
    1.8V#0 Power Supply Group:1.804V
PSUBP
    3.3V Power Supply Group:3.300V
    5.0V Power Supply Group:5.000V
XSCF>

```

环境温度和风扇速度级别

作为对安装地点海拔高度设置的结果，风扇速度级别根据环境温度而变化。风扇速度级别数字越大，风扇速度越快。

表 11-4 列出了由 `showenvironment` 命令显示的风扇速度级别、相应设置的海拔高度和环境温度。

表 11-4 对应海拔高度和环境温度的风扇转速级别（SPARC M12/M10 通用）

风扇速度级别	海拔高度的环境温度			
	500 米或更低	501 至 1000 米	1001 至 1500 米	1501 至 3000 米
高速 (级别-3 ->级别-4)	31°C 或更高	29°C 或更高	27°C 或更高	25°C 或更高

表 11-4 对应海拔高度和环境温度的风扇转速级别（SPARC M12/M10 通用）(续)

风扇速度级别	海拔高度的环境温度			
	500 米 或更低	501 至 1000 米	1001 至 1500 米	1501 至 3000 米
中速 (级别-4 ->级别-3)	29°C 或更低	27°C 或更低	25°C 或更低	23°C 或更低
中速 (级别-2 ->级别-3)	26°C 或更高	24°C 或更高	22°C 或更高	20°C 或更高
低速 (级别-3 ->级别-2)	24°C 或更低	22°C 或更低	20°C 或更低	18°C 或更低
低速 (级别-1 ->级别-2)	22°C 或更高	20°C 或更高	18°C 或更高	16°C 或更高
低速 (级别-2 ->级别-1)	20°C 或更低	18°C 或更低	16°C 或更低	14°C 或更低

操作步骤

1. 执行 **showenvironment** 命令查看风扇速度级别。

下面是指定 Fan 操作数查看风扇单元的速度级别的示例。

```
XSCF> showenvironment Fan
BB#00
  FANU#0: Middle speed (Level-3)
    FAN#0: 14323rpm
    FAN#1: 14285rpm
  FANU#1: Middle speed (Level-3)
    FAN#0: 14173rpm
    FAN#1: 14285rpm
  FANU#2: Middle speed (Level-3)
    FAN#0: 14248rpm
    FAN#1: 14136rpm
  FANU#3: Middle speed (Level-3)
    FAN#0: 14099rpm
    FAN#1: 14062rpm
  FANU#4: Middle speed (Level-3)
    FAN#0: 14323rpm
    FAN#1: 14099rpm
```

功耗和排气

如需查看系统的功耗和排气，请使用电源监视器功能和气流指示器。电源监视器功能和气流指示器可以让您例行检查运行中系统的实际电消耗量和排气量。

请使用 **showenvironment power** 命令查看功耗。使用该命令可查看系统的功耗值、机柜的最大功耗值 (Permitted AC power consumption) 和实际功耗值 (Actual AC power consumption) 等。如果电源类型为直流，则改为显示 "...DC power..."。

注 - 在 SPARC M12 系统中，机箱中的额定功耗显示为 "Available AC power consumption"

(可用交流电源功耗值)。

请使用 `showenvironment air` 命令查看排气。也可以通过 SNMP 代理功能获得有关功耗和排气的信息。

如需通过 SNMP 代理功能获得有关功耗和排气的信息，请为 SNMP 管理器安装最新的 XSCF 扩展 MIB 定义文件。关于获取 XSCF 扩展 MIB 定义文件的位置，请参见您的服务器的最新《产品说明》或固件下载网站上 MIB 定义文件相关的信息。

注 - 在以下情况下，功耗和排气值可能无法通过 MIB 信息、`showenvironment power` 命令、`showenvironment air` 命令和 XSCF Web 查看。一分钟后再次查看。

- 在系统开启或关闭期间，或者在完成开启或关闭后的一瞬间
 - 在主动更换电源单元期间，或者在完成主动更换后的一瞬间
-

注 - 功耗和排气不包括 PCI 扩展单元和 I/O 外设的信息。

操作步骤

1. 执行 `showenvironment` 命令查看系统的排气量。
以下示例中，指定 `air` 操作数查看系统的排气量。

```
XSCF> showenvironment air
BB#00
    Air Flow:306CMH
```

注 - 排气量的单位 (CMH = m³/h) 表示每小时产生多少立方米的气流。

2. 执行 `showenvironment` 命令查看系统的功耗。
在下面的示例中通过指定 `power` 操作数查看功耗信息。下面示例从上面向下显示，整个系统供电单元 (PSU) 的最大值、系统最小功耗值和最大功耗值、后面是机柜的最大功耗值和实际功耗值。

```
XSCF> showenvironment power
Power Supply Maximum :5000W
Installed Hardware Minimum:1268W
Peak Permitted :2322W
BB#00
Permitted AC power consumption:5000W
Actual AC power consumption :1719W
```

注 - 电源监视器和气流指示器测得的值为参考值。这些值根据系统负载而变化。

11.1.4 查看故障/降级组件

showstatus 命令可用于查看组成系统的 FRU 中一些故障或降级的单元和组件。故障状态的单元或组件标有星号 (*)。

有五种类型的状态如表 11-5 所示。

表 11-5 组件状态

组件	含义
Faulted (故障)	由于可疑的部件有故障，单元没有运行。
Degraded (降级)	单元有部分故障，但是单元继续运行。
Deconfigured (解除配置)	正常运行，但是因为另一个单元的降级导致包括低级组件的单元降级。
Maintenance (维护)	单元正在维护状态。replacefru、addfru 或 initbb 命令正在运行。
Normal (正常)	单元正常。

操作步骤

1. 执行 **showstatus** 命令查看组件状态。

故障状态的单元标有星号 (*)。

下面示例显示 BB#00 CPU 内存单元 (下) 上的 CPU 和内存，以及 XBBOX#80 的 PSU 由于故障而降级。

```
XSCF> showstatus
BB#00;
    CMUL Status:Normal;
*      CPU#0 Status:Faulted;
*      MEM#00A Status:Faulted;
XBBOX#80;
*      PSU#0 Status:Faulted;
```

下面示例显示主板单元上的内存由于故障而降级。

```
XSCF> showstatus
MBU Status:Normal;
*      MEM#0A Status:Faulted;
```

下面示例显示 CPU 内存单元由于接线盒单元降级而降级。

```
XSCF> showstatus
BB#00
    CMUU Status:Normal;
*      CPU#1 Status:Deconfigured;
*      XBU#0 Status:Degraded;
```

下面示例显示没有单元降级。

```
XSCF> showstatus
No failures found in System Initialization.
```

注 - 更换可疑部件会清除有关故障/降级组件的故障和降级信息。如需部件更换工作，请联系现场工程师。

11.1.5 查看 PCI 扩展单元状态

本节介绍如何查看系统中连接的 PCI 扩展单元、PCI 扩展单元中的部件、系统内置 PCI 槽中搭载的链路卡，以及 PCI 扩展单元状态。

您可使用 `ioxadm` 命令查看 PCI 扩展单元状态和设置。

注 - 有关 PCI 扩展单元硬件配置的详情，请参见《PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》中的“第2章 Understanding the PCI Expansion Unit Components”。有关 `ioxadm` 命令的详细信息或使用示例，请参见 `ioxadm(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

查看的信息

表 11-6 概述了执行 `ioxadm` 命令显示的信息。

表 11-6 查看的 PCI 扩展单元信息

显示项目	说明
列表查看 (list)	<ul style="list-style-type: none">- PCI 扩展单元和机柜内置槽中所安装链路卡之间的路径 (host_path) 列表- PCI 扩展单元的详细信息- PCI 扩展单元中 FRU (I/O 板、供电单元等) 的详细信息 查看的信息包括 FRU 类型、固件版本、序列号、部件号和状态。
环境查看 (env)	<ul style="list-style-type: none">- 指定 PCI 扩展单元或链路卡上传感器测量值所显示的环境条件- PCI 扩展单元中 FRU 或 PCI 槽中所安装卡的环境信息 查看的信息包括： <ul style="list-style-type: none">- 电流 (A)- 电压 (V)- 风扇速度 (RPM)- 温度 (C)- LED 状态- 开关
定位器 LED 显示 (locator)	<ul style="list-style-type: none">- 指定 PCI 扩展单元定位器 LED 和 PCI 扩展单元中每个部件的状态 定位器 LED 状态如下： <ul style="list-style-type: none">- 闪烁- 亮- 灭

表 11-6 查看的 PCI 扩展单元信息 (续)

显示项目	说明
版本比较结果 (versionlist)	显示 PCI 扩展单元固件版本、连接目标链路卡固件版本以及这些固件比较结果。 比较结果如下： - 相等 - 不匹配

列表查看

以下介绍查看 PCI 扩展单元、I/O 板、链路卡和供电单元信息列表的步骤。

1. 执行 `ioxadm` 命令查看 PCI 扩展单元和链路卡。

以下是查看所有 PCI 扩展单元和链路卡信息列表的示例。

```
XSCF> ioxadm list
PCIBOX          Link
PCIBOX#0033 BB#00-PCI#1
PCIBOX#12B4 BB#01-PCI#0
```

下面是查看单个 PCI 扩展单元的示例。

```
XSCF> ioxadm list PCIBOX#12B4
PCIBOX          Link
PCIBOX#12B4 BB#01-PCI#0
```

下面是使用主机路径通过隐藏标头的详细输出模式查看卡的示例。

```
XSCF> ioxadm -A -v list BB#00-PCI#1
BB#00-PCI#1 F20 - 000004 5111500-01 On
```

环境查看

以下介绍用传感器测量值查看环境的步骤。

1. 执行 `ioxadm` 命令查看环境信息。

以下是查看温度、电压、电流、风扇速度等传感器测量值的示例。

```
XSCF> ioxadm env -te PCIBOX#A3B4
Location Sensor Value Res Units

PCIBOX#A3B4/PSU#0 FAN 3224.324 - RPM
PCIBOX#A3B4/PSU#1 FAN 3224.324 - RPM
PCIBOX#A3B4/FAN#0 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#1 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#2 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#0 FAN 3522.314 - RPM
PCIBOX#A3B4/IOBT T_INTAKE 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO1 32.000 - C
```

```

PCIBOX#A3B4/IOBT T_PART_NO2 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO3 32.000 - C
PCIBOX#A3B4/IOBT V_12_0V 12.400 - V
PCIBOX#A3B4/IOBT V_3_3_NO0 3.320 - V
PCIBOX#A3B4/IOBT V_3_3_NO1 3.310 - V
PCIBOX#A3B4/IOBT V_3_3_NO2 3.310 - V
PCIBOX#A3B4/IOBT V_3_3_NO3 3.320 - V
PCIBOX#A3B4/IOBT V_1_8V 1.820 - V
PCIBOX#A3B4/IOBT V_0_9V 0.910 - V

```

以下是查看一个链路所有传感器测量值的示例。

```

XSCF> ioxadm -A env BB#00-PCI#1
BB#00-PCI#1 LINK On - LED
BB#00-PCI#1 MGMT On - LED

```

位置查看

以下介绍查看 PCI 扩展单元和指定部件定位器 LED 状态的步骤。

1. 执行 **ioxadm** 命令查看 PCI 扩展单元状态。

以下是查看 PCI 扩展单元定位器 LED 状态的示例。

```

XSCF> ioxadm locator PCIBOX#12B4
Location          Sensor      Value Resolution Units
PCIBOX#12B4      LOCATE     Blink -      LED

```

版本比较结果

查看 PCI 扩展单元固件版本、连接目标链路卡固件版本以及比较结果的方法如下。

1. 执行 **ioxadm** 命令确认 PCI 扩展单元固件版本、连接目标链路卡固件版本以及比较结果。

以下是查看比较所有 PCI 扩展单元和链路卡的结果示例。

```

XSCF> ioxadm versionlist
PCIBOX          Ver. Link      Ver. Info
PCIBOX#0033 1010 BB#00-PCI#1 1010 equal
* PCIBOX#12B4 1010 BB#00-PCI#0 1011 mismatch

```

11.2 查看物理分区

11.2.1 查看有关物理分区和逻辑域配置/状态的项目和命令

表 11-7 列出了查看物理分区配置/状态、模块化架构 (PSB) 状态和逻辑域状态的项目和 XSCF shell 命令。有关各项目的详情，请参见以下章节。

表 11-7 用于查看配置和状态的命令

检查项目	相关命令
查看物理分区配置信息 - PPAR-ID - LSB 号 - PSB 号 - 配置策略 - 是否使用 I/O - 是否使用内存	showpcl(8)
查看物理分区操作状态	showpparstatus(8), showpcl(8)
查看 PSB 设置 - 位置 (PSB、CPU) - 内存镜像模式	showfru(8)
查看 PSB 状态	showboards(8)
查看逻辑域状态	showdomainstatus(8) Oracle VM Server for SPARC 命令

注 - 有关物理分区设置/配置/状态以及从物理分区配置逻辑域的详细信息，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

11.2.2 查看物理分区配置

showpcl 命令显示每个物理分区或构成物理分区的每个逻辑系统板的配置信息。系统管理员在将逻辑系统板并入物理分区时需参考 PCL（物理分区配置列表）。

showpcl 命令可用于查看指定物理分区的 PCL。

物理分区上的逻辑系统板 (LSB) 和物理系统板 (PSB) 之间的映射关系由 PCL 信息确定。

图 11-1 显示了 PCL 映射的示例。

PSB 是指配置物理分区的硬件资源。以 xx-y 格式指定（或显示）PSB。xx 是 BB-ID，y 固定为 0。

图 11-1 逻辑系统板和物理系统板之间的映射图

物理分区配置信息

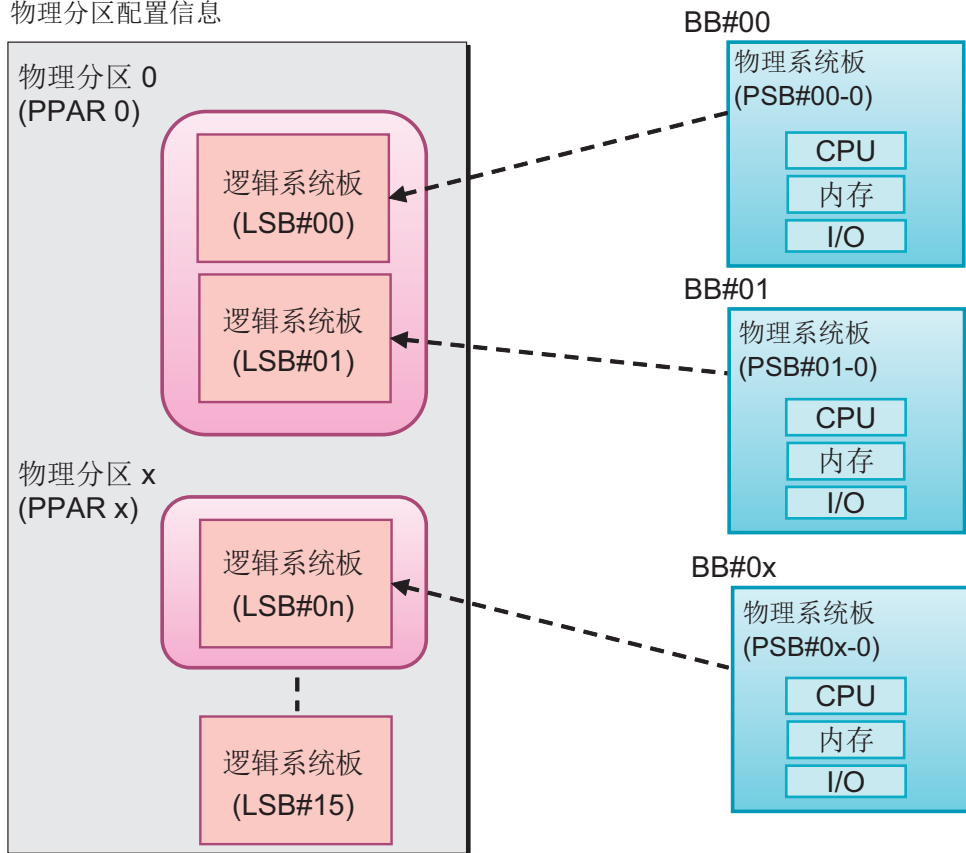


表 11-8 介绍了与物理分区相关的术语。

表 11-8 与物理分区相关的术语

术语	说明
物理系统板 (PSB)	PSB 表示物理系统板。PSB 由安装在一个 SPARC M12/M10 机箱中的物理组件 (CPU、内存和 I/O) 组成。在 SPARC M12-1/M10-1 中, 物理系统板是主板单元。在 SPARC M12-2/M12-2S/M10-4/M10-4S 中, 物理系统板是 CPU 内存单元 (包括下部 (CMUL) 及上部 (CMUU))。物理系统板可用作代表机箱的单元, 维护时用于添加/移除/更换 SPARC M12/M10 机箱。对于模块化架构配置中的系统, 物理系统板是指一个模块化架构 (BB)。
逻辑系统板 (LSB)	LSB 表示逻辑系统板。逻辑单元名称分配给 PSB。每个物理分区有一组分配给它的逻辑系统板。将一个 PSB 编号分配给物理分区中的逻辑系统板, 即可在系统中对其进行识别。LSB 号用于控制对于物理分区的资源 (如内存) 分配。

表 11-8 与物理分区相关的术语 (续)

术语	说明
物理分区配置	本术语是指将系统硬件资源分割成独立单元以便执行软件操作的内容。物理分区是 PSB 的群集，并且系统包括一个或多个物理分区。通过以下步骤使用 XSCF 配置物理分区。 1.将 LSB 号分配给 PSB。 2.将 PSB 分配给物理分区。 3.物理分区对 LSB 资源和 LSB 号执行操作。
物理分区配置信息	本术语是指硬件资源信息，配置给每个物理分区或组成物理分区的每个 LSB。使用 setpctl 和 showpctl 命令设置和查看 PCL。
配置策略	硬件初始诊断检测到错误时，指定每个物理分区将被降级的逻辑资源单元。配置策略指定 PSB 或不连续的资源作为降级范围。
I/O 禁用 (no-io)	本术语是指在物理分区中禁用 PSB 上的 I/O 单元的逻辑使用。
内存禁用 (no-mem)	本术语是指在物理分区中禁用 PSB 上的内存的逻辑使用。
PSB 状态	每个 PSB 的状态显示电源状态 (power)、诊断状态 (test)、分配状态 (assignment)、并入状态 (connection)、操作状态 (configuration) 和降级状态 (fault)。您可以了解到物理分区中 PSB 状态变化的进度。使用 showpctl 和 showboards 命令可以查看 PSB 状态信息。
系统板池 (SP)	本术语是指不属于任何物理分区的 BB (PSB) 的状态。对于具有高 CPU 或内存负荷的物理分区，可以将 BB (PSB) 添加到此物理分区。在不需要时，此系统板可以回到系统板池。

PCL 是为单个 LSB 设置信息的定义列表。每个物理分区您最多可以设置 16 个 LSB 的 LSB 信息。

表 11-9 列出了物理分区配置信息的详情。仅能在 SPARC M12-2/M10-1/M10-4 系统中设置配置策略。

表 11-9 PCL

术语	说明
PPAR-ID	PPAR 的 ID
LSB 号	LSB 号
PSB 号	分配给 LSB 的 PSB 号。 不能将相同的 PSB 号分配给同一物理分区中的另一个 LSB。
no-mem (内存无效选项)	True: 内存禁用 False: 内存启用 (默认)
no-io (I/O 无效选项)	True: I/O 未整合 False: I/O 已整合 (默认)
配置策略	FRU: 以现场可更换单元为单位执行降级 (FRU)。(默认) PSB: 以 PSB 为单位执行降级。 System: 以物理分区为单位，不降级关闭物理分区电源。
物理分区状态	指示物理分区操作状态，如：电源是否断开，或 POST 初始化是否已完成。有关详细的定义，请参见 showpctl(8) 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

操作步骤

1. 执行 **showpcl** 命令查看 PCL 信息。
以下是查看 PPAR-ID 00 的设置 PCL 信息的示例。

```
XSCF> showpcl -p 0
PPAR-ID   LSB     PSB     Status
00
          00     00-0
          04     01-0
          08     02-0
          12     03-0
```

以下是查看 PPAR-ID 00 的设置 PCL 信息详情的示例。

```
XSCF> showpcl -v -p 0
PPAR-ID   LSB     PSB     Status  No-Mem  No-IO  Cfg-policy
00
          00     -
          01     -
          02     -
          03     -
          04     01-0   False  False
          05     -
          06     -
          07     -
          08     02-0   True   False
          09     -
          10     -
          11     -
          12     03-0   False  True
          13     -
          14     -
          15     -
          System
```

注 - 有关物理分区配置的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

11.2.3 查看物理分区操作状态

showpparstatus 命令可用于查看物理分区操作状态，如电源断开状态或初始化状态。您可以使用 **showpcl** 命令的 “Status” 获取相同的信息。

注 - 有关物理分区操作状态的详细信息，请参见 **showpparstatus(8)** 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

注 - 您可使用 `showdomainstatus` 命令查看物理分区中逻辑域的状态。有关详情，请参见“11.2.6 查看逻辑域状态”。

注 - 有关物理分区状态的详情，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

操作步骤

下面是介绍查看物理分区操作状态的步骤。

1. 执行 `showpparstatus` 命令查看物理分区状态。
以下是查看所有物理分区操作状态的示例。

```
XSCF> showpparstatus -a
PPAR-ID PPAR Status
00          Powered Off
01          Initialization Phase
02          Initialization Phase
03          Running
```

11.2.4 查看内存镜像模式设置

使用 `showfru` 命令查看内存镜像模式设置。您可查看如下有关各自用于构成物理分区 PSB 的内容。

- Device
sb: 您可以查看 BB (PSB)。
示例: 00-0: BB-ID 0 的 PSB
cpu: 您可以查看安装在 BB 上的 CPU。
示例: 00-0-2: BB-ID 0 的 PSB 上的 CPU#2
- 内存镜像模式
您可以查看为每个 CPU 设置的内存镜像模式设置的状态。
yes: 内存镜像模式
no: 非内存镜像模式

注 - 有关内存镜像模式的设置/详细信息，请参见“第14章 配置高可靠性系统”。

操作步骤

1. 执行 `showfru` 命令查看设备信息。
以下是查看所有设备设置信息的示例。

```

XSCF> showfru -a
Device      Location      Memory Mirror Mode
sb          00-0
  cpu       00-0-0       yes
  cpu       00-0-1       yes
  cpu       00-0-2       yes
  cpu       00-0-3       yes
sb          01-0
  cpu       01-0-0       yes
  cpu       01-0-1       yes
  cpu       01-0-2       yes
  cpu       01-0-3       yes
sb          02-0
  cpu       02-0-0       no
  cpu       02-0-1       no
  cpu       02-0-2       no
  cpu       02-0-3       no
sb          03-0
  cpu       03-0-0       yes
  cpu       03-0-1       yes
  cpu       03-0-2       no
  cpu       03-0-3       no
:

```

以下示例中，指定 `sb` 操作数查看特定 PSB 的设置信息。

```

XSCF> showfru sb 01-0
Device      Location      Memory Mirror Mode
sb          01-0
  cpu       01-0-0       yes
  cpu       01-0-1       yes
  cpu       01-0-2       yes
  cpu       01-0-3       yes

```

以下示例中，指定 `cpu` 操作数查看特定 CPU 的设置信息。

```

XSCF> showfru cpu 01-0-3
Device      Location      Memory Mirror Mode
sb          01-0
  cpu       01-0-3       yes

```

11.2.5 查看 PSB 状态

系统板 (PSB) 是指 SPARC M12/SPARC M10 机箱。

您可以通过执行 `showboards` 命令来查看 PSB 电源状态 (`power`)、诊断状态 (`test`) 和降级状态 (`fault`)。在模块化架构配置中，执行 `addboard` 或 `deleteboard` 命令分别配置或断开物理分区中的 PSB 后，可以使用 `showboards` 命令了解该操作的进程，如操作是成功还是失败。进程是物理分区的 PSB 分配 (`assignment`) 等状态、配置/断开状态 (`connection`) 或操作状态 (`configuration`)。

通过使用 `showboards` 命令，您可以查看 PSB 电源状态 (power)、诊断状态 (test)、分配状态 (assignment)、配置状态 (connection)、操作状态 (configuration) 和降级状态 (fault)。

注 - 有关 PSB 状态的详细信息，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》、`showboards(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

操作步骤

查看 PSB 状态的步骤如下所述。

1. 执行 `showboards` 命令查看 PSB 状态。

下面的示例显示所有 PSB 的状态。

```
XSCF> showboards -a
```

PSB	PPAR-ID(LSB)	Assignment	Pwr	Conn	Conf	Test	Fault
00-0	00(00)	Assigned	y	y	y	Passed	Normal
01-0	SP	Unavailable	n	n	n	Testing	Normal
02-0	Other	Assigned	y	y	n	Passed	Degraded
03-0	SP	Unavailable	n	n	n	Failed	Faulted

下面是查看 PSB 00-0 详细信息的示例。

```
XSCF> showboards 00-0
```

PSB	PPAR-ID(LSB)	Assignment	Pwr	Conn	Conf	Test	Fault
00-0	00(00)	Assigned	y	y	y	Passed	Normal

下面是查看定义为 PPAR-ID 00 的系统板池 PSB 的示例。

```
XSCF> showboards -p 0 -c sp
```

PSB	PPAR-ID(LSB)	Assignment	Pwr	Conn	Conf	Test	Fault
01-0	SP	Available	n	n	n	Passed	Normal

11.2.6 查看逻辑域状态

`showdomainstatus` 命令可用于查看物理分区中控制域上 Oracle Solaris 的操作状态、控制域上 OpenBoot PROM 的状态等。

注 - 有关逻辑域操作状态的详细定义，请参见 `showdomainstatus(8)` 命令手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。您也可以使用 Oracle VM Server for SPARC 的 `ldm list-domain` 命令查看逻辑域状态。有关 `ldm` 命令的详情，请参见您所使用版本的《Oracle VM Server for SPARC Reference Manual》。

操作步骤

下面是介绍查看逻辑域操作状态的步骤。

1. 执行 **showdomainstatus** 命令查看属于指定物理分区的逻辑域的操作状态。
下面是查看 PPAR-ID 0 所有逻辑域的状态的示例。

```
XSCF> showdomainstatus -p 0
Logical Domain Name  Status
primary              Solaris running
guest00              Solaris running
guest01              Solaris booting
guest02              Solaris powering down
guest03              Solaris panicking
guest04              Shutdown Started
guest05              OpenBoot initializing
guest06              OpenBoot Primary Boot Loader
```

下面是查看名为 "guest01" 的 PPAR-ID 0 逻辑域状态的示例。

```
XSCF> showdomainstatus -p 0 -g guest01
Logical Domain Name  Status
guest01              Solaris powering down
```

检查日志和信息

本章介绍了系统上显示和存储的日志和消息的类型以及引用日志和消息的命令。

- 检查 XSCF 保存的日志
- 检查警告和通知信息

12.1 检查 XSCF 保存的日志

本节介绍如何检查 XSCF 日志信息。

XSCF 日志信息用于调查系统问题。系统管理员、域管理员和现场工程师可参考日志信息。异常发生时，他们可以查看服务器运行状态、使用状态以及发生的任何异常细节。

12.1.1 检查日志类型和参考命令

系统收集/管理的日志包括与故障信息相关的日志、记录事件的日志、与安全相关的日志，以及与服务器环境相关的日志。

本节介绍各种日志类型。

日志类型

以下类型的日志由系统收集并由系统管理员参考。

- 与故障信息相关的日志
 - 故障管理日志 (FM log) (*1)
 - 错误日志
 - 系统日志 (*1)
 - 监控消息日志

*1 此日志只能在 Oracle Solaris 上参考。有关详情，请参见 Oracle Solaris 相关手册。

- 记录事件的日志
 - 电源日志

- 时间日志
- 控制台日志
- 崩溃日志
- IPL 日志
- 与安全验证有关的日志
 - 审核日志
 - COD 日志
 - 活动目录日志
 - LDAP over SSL 日志
- 与服务器环境有关的日志
 - 温度历史日志

日志的概要和参考方法

表 12-1 列出了与故障信息相关的日志的类型、概述和引用方法。有关 XSCF 命令的详细信息，请参见各命令的 man 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。有关各日志类型的详情，请参见后续章节。

表 12-1 与故障信息相关的日志

日志类型	说明	大小（条目大小）/ <标准存储期限> 存档	输出显示目标/ 参考方法
故障管理日志（FM 日志）	系统中所发生错误、通知和故障的日志。		域/ fmdump
错误日志	系统中所发生错误、通知和故障的日志。日志显示格式特定于平台。	关于 1,024 生成 （长度可变） <约一个月的量> 已存档	XSCF/ showlogs(8) XSCF Web
系统日志 (SYSLOG)	记录输出 Oracle Solaris 信息的日志。如果发生故障，则输出故障概要。		域/ 使用 Oracle Solaris 命令参考。
监视信息日志 (Monitor message log)	记录 XSCF 中信息，报告故障的日志	512 KB，约 10,000 行	XSCF/ showlogs(8) XSCF Web

注 - Oracle Solaris 命令显示的日志不会被存档。

表 12-2 列出了记录事件的日志的类型、概述和引用方法。

表 12-2 记录事件的日志

日志类型	说明	大小 (条目大小) / <标准存储期限> 存档	参考方法
电源日志 (Power Log)	记录服务器电源事件的日志	1,920 生成 (x 16 B) <约一个月的量 已存档	showlogs(8) XSCF Web
事件日志 (XSCF Event Log)	用于记录系统操作、操作面板操作 和报告给 Oracle Solaris 的事件的日志。	4,096 生成 (x 48 B) <约一个月的量 已存档	showlogs(8) XSCF Web
控制台日志 (Console Log)	用于记录控制域控制台信息的日志。 关闭输入电源以清除日志。	512 KB/PPAR, 约 10,000 和 /PPAR <约一周的量> 已存档	showlogs(8) XSCF Web
崩溃日志 (Panic Log)	发生崩溃的控制台日志	一次生成, 64 KB/PPAR (约 1,200 行) <一次的量> 已存档	showlogs(8) XSCF Web
IPL 日志 (IPL Log)	从 Oracle Solaris 开启到完成启动 期间的日志	一次生成 32 KB/PPAR, 约 600 行/PPAR <一次的量> 已存档	showlogs(8) XSCF Web

表 12-3 列出了与安全相关的日志的类型、概述和引用方法。

表 12-3 与安全有关的日志

日志类型	说明	大小 (条目大小) / <标准存储期限> 存档	参考方法
审核日志 (Audit Log)	XSCF 的与审核有关的日志	4 MB <约一个月的量 已存档	viewaudit(8) XSCF Web
COD 日志 (CoD 激活日志)	CPU 激活添加和删除的日志	1,024 生成 (x 32 KB) 每个内核许可证 已存档	showcodactivat ionhistory(8) XSCF Web
活动目录日志	活动目录诊断验证和授权的信息日志。	250 KB (约 3000 行) 未存档	showad(8) XSCF Web
LDAP over SSL 日志 (LDAP over SSL Log)	LDAP over SSL 诊断验证和授权的信息日志。	250 KB (约 3000 行) 未存档	showldapssl(8) XSCF Web

表 12-4 列出了与服务器环境有关的日志的类型、概述和引用方法。

表 12-4 与服务器环境有关的日志

日志类型	说明	大小 (条目大小) / <标准存储期限> 存档	参考方法
温度历史记录日志 (Thermal and humidity History)	记录服务器温度历史的与环境有关的日志	16,384 生成 (x 16 B) (每 10 分钟) <约一年的量> 已存档	showlogs(8) XSCF Web

注 - 日志满时, 从最旧日志数据开始, 日志会被覆盖。

12.1.2 如何查看日志

本节介绍如何浏览各 XSCF 日志的信息。

在 XSCF shell 或 XSCF Web 上检查日志

以下是参考各日志的一般步骤。

1. 确认查看日志所需的用户权限。
各日志的用户权限如表 12-5 所示。

表 12-5 查看日志所需的用户权限

日志类型	所需的用户权限
错误日志	platadm, platop, fieldeng
监视信息日志	platadm, platop, fieldeng
电源日志	platadm, platop, pparadm, pparmgr, fieldeng
事件日志	platadm, platop, fieldeng
控制台日志	platadm, platop, pparadm, pparmgr, pparop, fieldeng
崩溃日志	platadm, platop, pparadm, pparmgr, pparop, fieldeng
IPL 日志	platadm, platop, pparadm, pparmgr, pparop, fieldeng
审核日志	auditadm, auditop
COD 日志	platadm, platop, fieldeng
温度历史记录日志	platadm, platop, fieldeng
活动目录日志	useradm
LDAP over SSL 日志	useradm

2. 指定主机名或 IP 地址以连接到 XSCF shell 终端或 XSCF Web。

3. 指定具有所需权限的用户账户，输入密码后登录 **XSCF**。
4. 执行查看相关日志的命令，或从菜单选择操作命令。
5. 查看日志。

注 - 有关 XSCF Web 菜单的详细信息，请参见 "附录 C XSCF Web 页面列表"。

12.1.3 检查错误日志

错误日志是与故障信息有关的日志。使用 `showlogs` 命令并指定 `error` 操作数查看系统中所发生的通知或故障相关的日志。

使用场景

XSCF 的错误日志使用场景如下。

- 在有信息输出到域控制台、XSCF shell 终端或 XSCF Web 时，日志用于检查是否有故障发生。
- 向已注册电子邮件地址的发送了通知，日志用于检查是否有故障发生。
- 由 SNMP 管理器生成陷阱时，日志用于检查是否有故障发生。

操作步骤

1. 在 **XSCF shell** 上执行指定有 `error` 操作数的 `showlogs` 命令。

```
XSCF> showlogs error
Date: Oct 20 17:45:31 JST 2012
Code: 00112233-444555666777-888999aaabbbcccddeeefff
Status: Warning Occurred: Oct 20 17:45:31.000 JST 2012
FRU: /PSU#1
Msg: ACFAIL occurred (ACS=3) (FEP type = A1)
Date: Oct 20 17:45:31 JST 2012
Code: 00112233-444555666777-888999aaabbbcccddeee000
Status: Alarm Occurred: Oct 20 17:45:31.000 JST 2012
FRU: /PSU#1
Msg: ACFAIL occurred (ACS=3) (FEP type = A1)
```

在以上的示例中显示一下的内容。

- 记录每个问题的时间 (Date)
此日期以本地时间显示。
- DIAGCODE，现场工程师和服务工程师用于故障排除的诊断代码 (Code)

注 - 要求用户将此代码报告给现场工程师或服务工程师。该代码有助于早期解决问题。

- 部件的故障级别 (Status)

显示以下其中一项:

Alarm: 相关部件故障或异常

Warning: 相关部件的部分降级或警报

Information: 通知

Notice: 系统状态通知

- 问题发生的时间 (Occurred)

此日期以本地时间显示。

- 可能故障的更换部件 (FRU)

如果有第一、第二和第三可疑部件, 则列出时会以逗号 (,) 将它们分隔。对于其它可疑部件, "*" (星号) 会显示在最后一个逗号 (,) 后。各部件以部件的安装路径格式分层次显示。是否显示第二个和之后的最可能的故障部分的决定取决于检测到的故障位置。

以下示例显示了所显示的 "FRU:" 内容的含义。

a. 显示 **"/PSU#0,/PSU#1"** 时。

分别检测到 PSU#0 和 PSU#1 是第一和第二个可疑部件。这意味着根据其状况每个部件都可能需要更换。

b. 显示 **"/BB#1/XBU#0/CBL#0R,/XBBOX#80/XBU#0,/BB#1/XBU#0,*"** 时。

分别检测到 BB#1 和 XBBOX#80 之间的 CBL#0R、XBBOX#80 中的 XBU#0 以及 BB#1 中的 XBU#0 是第一、第二和第三个可疑部件, 并且也检测到其它异常部件。这意味着根据其状况每个部件都可能需要更换。

c. 显示 **"/BB#0/PCI#3"** 时。

检测到 BB#0/PCI#3 为可疑组件, BB-ID 0 的 PCI 槽号 3 有问题。这意味着根据其状况连接到 PCI 插槽 3 的部件可能需要更换。

d. 显示 **"/MBU/MEM#02A"** 时。

检测到 /MBU/MEM#02A 为可疑组件, 母版单元的内存槽 02A 有问题。这意味着根据其状况内存槽 02A 可能需要更换。

e. 显示 **"/BB#0/CMUL/MEM#02A"** 时。

检测到 /BB#0/CMUL/MEM#02A 为可疑组件, BB-ID 0 的 CPU 内存单元 (下) 的 02A 号内存槽存在问题。这意味着根据其状况内存槽 02A 可能需要更换。

f. 显示 **"/BB#0/CMUL/MEM#02A-03A"** 时。

/BB#0/CMUL/MEM#02A-03A 为可疑组件, 并且 BB-ID 0 的 CPU 内存单元 (下) 的 02A 和 02B 号内存槽有问题。这意味着根据其状况内存槽 02A 和 02B 中的内存可能需要更换。

- 用一行信息显示发生问题的概要 (Msg)

注 - 有关 showlogs(8) 命令的详细信息, 请参见手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

12.1.4 检查监视信息日志

系统中发生的事件针对已登录 XSCF 的用户实时显示监控信息。XSCF 固件在监视信息日志中收集这些信息。使用指定 monitor 操作数的 showlogs 命令来查阅监视信息日志。

操作步骤

1. 在 XSCF shell 上执行指定有 monitor 操作数的 showlogs 命令。

```
XSCF> showlogs monitor
Oct 20 17:45:31 monitor message: xxxxxxxx
Oct 20 17:55:31 monitor message: xxxxxxxx
```

显示以下内容。

- 监视信息日志收集时间 (Date)
此日期以本地时间显示。
- 监视信息 (Message)

12.1.5 检查电源日志

当在系统上执行电源操作或重置时，会收集电源日志。使用指定 power 操作数的 showlogs 命令来查阅电源日志。

操作步骤

1. 在 XSCF shell 上执行指定有 power 操作数的 showlogs 命令。
以下是查看电源日志的示例。

```
XSCF> showlogs power
Date           Event           Cause           ID Switch
Oct 20 17:25:31 JST 2012 Cabinet Power On Operator        00 Service
Oct 20 17:35:31 JST 2012 PPAR Power On Operator        00 Locked
Oct 20 17:45:31 JST 2012 PPAR Power Off Software Request 00 Locked
Oct 20 17:50:31 JST 2012 Cabinet Power Off Self Reset     00 Service
```

在以下的示例中，指定开始时间和结束时间，以便按照从最新到最旧的顺序以列表显示电源日志。

```
XSCF> showlogs power -t Oct2017:302012 -T Oct2017:492012 -r
Date           Event           Cause           ID Switch
Oct 20 17:45:31 JST 2012 PPAR Power Off Software Request 00 Locked
Oct 20 17:35:31 JST 2012 PPAR Power On Operator        00 Locked
```

注 - 命令示例的布局可能会随时变化，对于功能改进恕不另行通知。

在以上的示例中显示一下的内容。

- 电源日志收集时间 (Date)
此日期以本地时间显示。
- 所发生电源事件的类型 (Event)
下表列出了电源事件 (Event) 及其含义。

事件	含义
SCF Reset:	执行了 XSCF 重新启动或重置。
PPAR Power On:	物理分区电源开启。
PPAR Power Off:	物理分区电源关闭。
PPAR Reset:	物理分区被重置。
Cabinet Power On:	服务器电源开启。
Cabinet Power Off:	服务器电源关闭。
XIR:	XIR 被重置。

- 引发电源事件指令的要因 (Cause)
下面列出了要因 (Cause) 及其含义。

要因	含义
Self Reset:	XSCF 被重新启动。
Power On:	输入电源开启导致 XSCF 重新启动。
System Reset:	监测到的故障导致 XSCF 重置。
Panel:	在操作面板上操作一个开关导致电源事件。
Scheduled:	TOD 计时器设置导致电源事件。
IPMI:	连接到 RCIL 的 I/O 设备导致电源事件。
Power Recover:	由于电源恢复电源被开启。
Operator:	操作员的指令导致电源事件。
Power Failure:	停电导致电源关闭。
Software Request:	Oracle Solaris 指令导致电源事件。
Alarm:	服务器环境或硬件故障导致电源事件。
Fatal:	"Fatal" 错误导致电源事件。

- 电源事件的 PPAR-ID 或 BB-ID (ID)
如果事件是系统开机或系统关机，则显示 BB-ID。
如果事件是 PPAR 电源开启、PPAR 电源关闭或 PPAR 重置，则显示 PPAR-ID。
如果事件是所有 SPARC M12/M10 系统或所有物理分区的原因，则显示 "--"。
- 操作面板上的模式开关状态 (Switch)
下面列出了开关状态及其含义。

开关状态	含义
Locked:	模式开关被设置为锁定。
Service:	模式开关被设置为维护。

12.1.6 检查事件日志

系统或物理分区中发生事件时，如：系统状态被更改，配置被更改，操作面板被操作或 Oracle Solaris 收到事件通知，则会收集事件日志。使用指定 event 操作数的 showlogs 命令来查阅事件日志。

操作步骤

1. 在 **XSCF shell** 上执行指定有 event 操作数的 **showlogs** 命令。

```
XSCF> showlogs event
Date                               Message
Oct 20 17:45:31 JST 2012           System power on
Oct 20 17:55:31 JST 2012           System power off
```

显示以下内容。

- 事件日志收集时间 (Date)
以本地时间显示。
- 事件信息 (Message)

12.1.7 检查控制台日志

XSCF 将控制域控制台消息写入控制台日志。控制台日志每行包含一条消息条目。在一些情况下，控制台日志可能被称为控制台信息日志。使用指定 console 操作数的 showlogs 命令来查阅控制台日志。

操作步骤

1. 在 **XSCF shell** 上执行指定有 console 操作数的 **showlogs** 命令。

```
XSCF> showlogs console -p 0
PPAR-ID: 00
Oct 20 17:45:31 JST 2012   console message: xxxxxxxx
Oct 20 17:55:31 JST 2012   console message: xxxxxxxx
```

显示以下内容。

- 物理分区 ID (PPAR ID)
- 控制台日志收集时间 (Date)
以本地时间显示。

- 控制台消息 (Message)

12.1.8 检查崩溃日志

发生崩溃时，控制台信息被输出到域控制台。这些被输出的控制台信息收集在崩溃日志中。在一些情况下，崩溃日志可能被称为崩溃信息日志。使用指定 `panic` 操作数的 `showlogs` 命令来查阅崩溃日志。

操作步骤

1. 在 **XSCF shell** 上执行指定有 `panic` 操作数的 `showlogs` 命令。

```
XSCF> showlogs panic -p 0
<<panic>>
Date: Oct 20 18:45:31 JST 2012      PPAR-ID: 00
Oct 20 17:45:31 JST 2012      panic message: xxxxxxxx
Oct 20 17:55:31 JST 2012      panic message: xxxxxxxx
```

显示以下内容。

- 物理分区 ID (PPAR-ID)
- 崩溃日志收集时间 (Date)
以本地时间显示。
- 崩溃消息 (Message)

12.1.9 检查 IPL 日志

开启物理分区电源后，控制台信息会输出到控制域控制台，直到设置了运行状态。这些控制台信息收集在 IPL 日志中。在一些情况下，IPL 日志可能被称为 IPL 信息日志。使用指定 `ipl` 操作数的 `showlogs` 命令来查阅 IPL 日志。

操作步骤

1. 在 **XSCF shell** 上执行指定有 `ipl` 操作数的 `showlogs` 命令。

```
XSCF> showlogs ipl -p 0
<<ipl>>
Date: Oct 20 18:45:31 JST 2012      PPAR-ID: 00
Oct 20 17:45:31 JST 2012      ipl message: xxxxxxxx
Oct 20 17:55:31 JST 2012      ipl message: xxxxxxxx
```

显示以下内容。

- 物理分区 ID (PPAR-ID)
- IPL 日志收集时间 (Date)
以本地时间显示。
- IPL 消息 (Message)

12.1.10 检查审核日志

当系统使用审核功能时，会收集审核日志。使用 `viewaudit` 命令查阅审核日志。

操作步骤

1. 在 **XSCF shell** 中执行 **viewaudit** 命令。
以下是查看 所有审核记录的示例。

```
XSCF> viewaudit
file,1,2012-04-26 21:37:25.626
+00:00,20120426213725.0000000000.SCF-4-0
header,20,1,audit - start,0.0.0.0,2012-04-26 21:37:25.660 +00:00
header,43,1,authenticate,0.0.0.0,2012-04-26 22:01:28.902 +00:00
authentication,failure,,unknown user,telnet 27652 0.0.197.33
header,37,1,login - telnet,0.0.0.0,2012-04-26 22:02:26.459 +00:
00
subject,1,opl,normal,telnet 50466 10.18.108.4
header,78,1,command - setprivileges,0.0.0.0,2012-04-26
22:02:43.246
+00:00
subject,1,opl,normal,telnet 50466 10.18.108.4
command,setprivileges,opl,useradm
platform access,granted
return,0
```

如上面示例中显示，默认情况下，记录以文本格式显示。每行显示一个标记，并将逗号作为字段分隔符。

标记类型及其字段在 [表 12-6](#) 中显示（按照显示顺序）。

表 12-6 标记类型及其字段（按照显示顺序）

标记类型	字段（显示顺序）
File 标记	标签、版本、时间、文件名
Header 标记	标签、记录字节计数、版本、事件类型、机器地址、时间（时间记录事件）
Subject 标记	标签、审核会话 ID、UID、操作模式、终端类型、远程 IP 地址、远程端口
Upriv 标记	标签、成功/失败
Udpriv 标记	标签、成功/失败、用户权限、域 ID 1、...、域 ID N
Command 标记	标签、命令名、操作数 1、...、操作数 N
Authentication 标记	标签、验证结果、用户名、信息、终端类型、远程 IP 地址、远程端口
Return 标记	标签、返回值
Text 标记	标签、文本字符串

注 - 根据环境，有些字段可能无法输出。

主要的审核事件和标记如下：

- 登录 telnet
 - header
 - subject
 - text
 - return
- 登录 SSH
 - 与登录 telnet 相同
- 登录 BUI
 - 与登录 telnet 相同
- 注销
 - Header
 - Subject
- 审核开始
 - Header
- 审核停止
 - Header
- Shell 命令
 - Header
 - Subject
 - Command
 - Text
 - Upriv | Updpriv
 - Return

注 - 根据环境，有些标记可能无法输出。另外，信息可能会随时变化，对于功能改进恕不另行通知。

注 - 有关 viewaudit(8) 命令的日志选项、审核类别和审核事件的详细信息，请参见手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

12.1.11 检查 COD 日志

当添加或删除 CPU 内核激活时会收集 COD 日志。COD 日志也称为 CPU 激活日志。使用 `showcodactivationhistory` 命令查看 COD 日志。

操作步骤

1. 在 **XSCF shell** 中执行 **showcodactivationhistory** 命令。
下面是查看 COD 日志的示例。

```
XSCF> showcodactivationhistory
11/30/2012 01:42:41PM PST: Report Generated M10-1 SN: 843a996d
10/02/2012 02:08:49PM PST: Activation history initialized: PROC 0 cores
10/15/2012 01:36:13PM PST: Capacity added: PROC 2 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 2 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 2 cores
11/27/2012 01:46:23PM PST: Configuration backup created: PROC 2 cores
11/27/2012 21:26:22PM PST: Configuration restored: PROC 2 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 2 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 2 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 2 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 2 cores
11/30/2011 01:42:41PM PST: Summary: PROC 10 cores
Signature: yU27yb00th41UL7hleA2vHL7S1aX4pmkBTIxesD1XEs
```

注 - 有关 showcodactivationhistory(8) 命令的详细信息, 请参见手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

12.1.12 检查活动目录日志

本节介绍使用 showad 命令查看活动目录日志的方法。关于 showad 命令日志选项的详情, 请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》或 showad(8) 命令的手册页面。有关每个日志的大小和生成编号, 请参见表 12-3。

使用 showad 命令查看活动目录日志

当使用活动目录功能执行用户验证和授权时, 收集诊断信息日志。这些日志用于处理故障, 在重新启动 XSCF 时被清除。可以通过在 XSCF shell 上执行带日志操作数的 showad 命令来引用活动目录日志。显示以下项目。

- 收集活动目录日志的时间
- 诊断信息

12.1.13 检查 LDAP over SSL 日志

本节介绍使用 showldapssl 命令查看 LDAP over SSL 日志的方法。关于 showldapssl 命令日志选项的详情, 请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》或 showldapssl(8) 命令的手册页面。有关每个日志的大小和生成编号, 请参见表 12-3。

使用 showldapssl 命令查看 LDAP over SSL 日志

当使用 LDAP over SSL 功能执行用户验证和授权时, 收集诊断信息日志。这些日志用于处理故障, 在重新启动 XSCF 时被清除。可以通过在 XSCF shell 上指定 log 操作数并执行 showldapssl 命令来查阅 LDAP over SSL 日志。显示以下项目。

- LDAP over SSL 日志收集时间
- 诊断信息

12.1.14 检查温度历史日志

温度历史日志是服务器入口温度的历史记录。入口温度每 10 分钟记录一次。使用指定 env 操作数的 showlogs 命令来查阅温度历史日志。

操作步骤

1. 在 XSCF shell 上执行指定有 env 操作数的 showlogs 命令。

```
XSCF> showlogs env
BB#00
Date                Temperature  Power
Oct 20 17:45:31 JST 2012  32.56 (C)   Cabinet Power On
Oct 20 17:55:31 JST 2012  32.56 (C)   Cabinet Power Off
:
```

显示以下内容。

- 温度历史日志收集时间 (Date)。此日期以本地时间显示。
- 温度 (Temperature)
- 机箱 电源状态 (On 或 Off) (Power)

12.1.15 使用快照将日志保存到文件

本节介绍如何将 XSCF 日志信息保存到文件中。

如需保存日志信息, 在 XSCF shell 中执行 snapshot 命令。或者在 XSCF Web 选择 snapshot 菜单执行此操作。所有 XSCF 日志信息被保存到指定位置。

现场工程师或服务工程师保存日志信息。系统管理员也被要求保存日志。

保存日志的方法

以下是保存日志的方法。有关保存方法的详情, 请参见后续章节。

- 通过将 USB 设备连接到主 XSCF 机柜后面板上 XSCF 单元的 USB 端口来在本地保存日志信息。
- 通过网络将日志信息保存在使用 XSCF Web 的终端上。
加密协议用于数据传输。
- 通过网络将日志信息保存在使用 snapshot 命令指定的服务器上。
加密协议用于数据传输。

注 - USB 设备需要用 FAT32 文件系统进行格式化。请向服务工程师请教有关用于本地保存日志的 USB 设备容量和处理方法。

注 - 可以通过在 XSCF 上指定快照选项来加密保存的数据。有关处理或发送加密日志文件的信息, 请咨询服务工程师。

注 - 当系统有多个 XSCF 单元时，另一个机柜（如备用 XSCF）的日志数据可以从主 XSCF 中收集。

日志文件输出格式

保存日志文件的输出格式如下。

- 文件名: 文件生成时自动使用由 SXSCF 主机名、IP 地址和日志保存时间构成的名称。日志文件生成时不能使用用户指定的文件名。
- 文件格式: zip

在具有多个 XSCF 的系统中，单个生成的 zip 文件由构成模块化架构的 SPARC M12-2S/SPARC M10-4S 的每个机柜和接线盒的信息组成。如果指定了单个机柜编号，除系统通用的日志外，针对指定机柜的日志信息也会保存。如果指定所有机柜，则除系统通用的日志外，所有机柜的日志信息也会保存。

12.1.16 将日志保存到本地 USB 设备

本节介绍如何使用 XSCF Web 或 XSCF shell 将日志信息保存到 USB 设备。

在 XSCF shell 上的操作步骤

1. 将 **USB** 设备连接到服务器后面板上 **XSCF** 单元上的 **USB** 端口。
2. 在 **XSCF shell** 中，对输出文件指定的 **USB** 设备执行 **snapshot** 命令。

```
XSCF> snapshot -d usb0 -a
```

执行数据传输。

3. 确保日志保存已完成。
日志保存完成后，如果需要，请联系服务工程师。

注 - snapshot 命令可用于加密数据，然后将其输出。有关 snapshot 命令加密选项的详细信息，请参见其手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

在 XSCF Web 上的操作步骤

1. 将 **USB** 设备连接到服务器后面板上 **XSCF** 单元上的 **USB** 端口。
2. 从 **snapshot** 菜单选择保存操作页。
3. 在 **Web** 浏览器窗口中，将 **USB** 设备选作保存日志信息的位置。
4. 如果输出日志文件需要加密，查看 **[Encrypt Output File]** 并指定加密密码。点击 **[Download]** 按钮，传输数据。
5. 确保日志保存已完成。
日志保存完成后，如果需要，请联系服务工程师。

12.1.17 通过网络将日志保存在使用 XSCF Web 的终端

通过网络将日志保存在使用 XSCF Web 的终端内的步骤如下。

1. 通过选择 **[Snapshot]** 菜单查看保存操作页。
2. 在 **Web** 浏览器窗口中将目标目录指定为保存位置。
3. 如果输出日志文件需要加密，查看 **[Encrypt Output File]** 并指定加密密码。点击 **[Download]** 按钮，传输数据。
4. 确保日志保存已完成。
日志保存完成后，如果需要，请联系服务工程师。

12.1.18 通过网络将日志保存在使用快照指定的服务器

通过网络将日志保存在使用 snapshot 命令指定的服务器上的步骤如下。

1. 指定完整目标目录，如 **XSCF shell** 上的 **SSH** 服务器和目录，然后执行 **snapshot** 命令。

```
XSCF> snapshot -t user@host:directory
```

执行数据传输。

2. 确保日志保存已完成。
日志保存完成后，如果需要，请联系服务工程师。

注 - snapshot 命令可用于加密数据，然后将其输出。有关 snapshot 命令加密选项的详细信息，请参见 snapshot(8) 命令的手册页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

12.2 检查警告和通知信息

本节介绍如何检查主要输出到控制域控制台并通过电子邮件和 SNMP 代理功能报告的故障和通知信息。

12.2.1 检查信息类型和参考方法

信息类型

以下类型的信息是用户在服务器错误或状态通知中最常看到的信息：

- 系统日志信息 (*1)

- FMA 信息 (*1)
 - IPL 信息
 - 崩溃信息
 - 控制台信息
 - 监视信息
 - 其它通知信息
- *1 本日志只能在 Oracle Solaris 上参考。有关详情，请参见 Oracle Solaris 相关手册。

信息的概要和参考方法

表 12-7 列出了单个消息的类型、概述和参考方法。

表 12-7 各信息概览

信息类型	说明	输出显示目标/ 参考方法
系统日志信息	此信息由 Oracle Solaris 通知。	域/ 可以在控制域 控制台上查看。
FMA 信息	是硬件或软件故障的自动诊断结果。Oracle Solaris 故障管理架构 (FMA) 执行诊断。通过此信息输出，用户可以了解系统中的哪个部分与故障通知相对应。FMA 信息存储为日志信息（在故障日志或错误日志中）。Oracle Solaris 的 <code>fmdump</code> 命令和 XSCF shell 的 <code>showlogs</code> 命令可用于查看信息内容以供更详细调查。用户也可以使用指定的 URL 基于控制域控制台上显示的 MSG-ID 确认内容。	域/ 可以在控制域 控制台上查看。
IPL 信息	此信息在控制域上启动 Oracle Solaris 时输出。IPL 信息输出到控制域控制台并在 XSCF 中存储为日志信息（IPL 日志中）。IPL 日志仅保留每个控制域的最新系统启动信息。XSCF shell 的 <code>showlogs</code> 命令可用于显示 IPL 日志。	域/ 可以在控制域 控制台上查看。
崩溃信息	发生崩溃时输出此信息。崩溃信息输出到域控制台并在 XSCF 中存储为日志信息（崩溃日志中）。崩溃日志保留各控制域的最近一次崩溃事件的信息。XSCF shell 的 <code>showlogs</code> 命令可用于显示崩溃日志。	域/ 可以在控制域 控制台上查看。
控制台信息	控制台信息是一个通用术语，用来描述系统日志信息、FMA 信息、崩溃信息、IPL 信息以及 POST、OpenBoot PROM 和 Oracle Solaris 的其它信息输出。输出到各控制域的域控制台的控制台信息在 XSCF 中存储为日志信息（控制台日志中）。XSCF shell 的 <code>showlogs</code> 命令可用于显示控制台日志。注意，来宾域上的控制台信息由逻辑域管理器管理。有关详情，请参见 "8.10 域控制台日志功能"。	域/ 可以在控制域 控制台上查看。

从最旧的信息开始，覆盖控制台信息。即使控制台信息已被覆盖，系统启动信息仍保留在 IPL 日志中，在发生崩溃时，日志保留在崩溃日志中。

在有多个 XSCF 单元的系统，主 XSCF 中存储的控制台信息不会复制到备用 XSCF。因此，切换 XSCF 单元后，将不能参考以前主设备端上的控制台信息。

表 12-7 各信息概览 (续)

信息类型	说明	输出显示目标/ 参考方法
监视信息	<p>XSCF 输出此信息来报告系统故障或通知。监视信息使用 <code>showmonitorlog</code> 命令输出。在 XSCF 中存储为日志信息（监视信息日志或错误日志中）。XSCF shell 的 <code>showlogs</code> 命令可用于显示监视信息日志和错误日志以供更详细调查。</p> <p>另外，服务工程师使用信息中输出的 <code>DIAGCODE</code>（诊断代码）来获取详细的信息。</p> <p>从最旧的信息开始，覆盖监视信息。</p> <p>在有多 XSCF 单元的系统，主 XSCF 输出的监视信息也在备用 XSCF 上管理。即使切换 XSCF 单元后，也能参考以前主设备端上的监视信息。</p>	<p>域, XSCF/ 可以在控制域 控制台上查看。 可以使用 <code>showmonito</code> <code>r-log</code> 命令查看。</p>
其它通知信息	<p>除以上信息外，在正常关机、重置操作和一些其他事件时，域控制台上会显示通知信息。</p>	<p>域/ 可以在控制域 控制台上查看。</p>

12.2.2 处理通知信息

本节介绍在识别 Oracle Solaris 中信息或者各 XSCF 功能报告的信息后，针对这些信息采取的措施。

控制域控制台上通知或故障信息的识别/处理

1. 用户识别控制台信息中的通知或故障，如：系统日志信息或输出到控制域控制台的 **FMA** 信息。

下面是控制域控制台上 FMA 信息的示例。

```
SUNW-MSG-ID: SUNOS-8000-J0, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Thu Apr 19 10:48:39 JST 2012
PLATFORM: ORCL,SPARC64-X, CSN: PP115300MX, HOSTNAME: 4S-LGA12-D0
SOURCE: eft, REV: 1.16
EVENT-ID: fcbb42a5-47c3-c9c5-f0b0-f782d69afb01
DESC: The diagnosis engine encountered telemetry from the listed devices for
which it was unable to perform a diagnosis - ereport.io.pciex.rc.epkt@
chassis0/cpubeard0/chip0/hostbridge0/pciexrc0 class and path are incompatible.
AUTO-RESPONSE: Error reports have been logged for examination.
IMPACT: Automated diagnosis and response for these events will not occur.
REC-ACTION: Use 'fmadm faulty' to provide a more detailed view of this event.
Use 'fmdump -eV' to view the unexpected telemetry. Please refer to the
associated reference document at http://support.oracle.com/msg/SUNOS-8000-J0
for the latest service procedures and policies regarding this diagnosis.
```

注 - 信息示例可能会随时变化，恕不另行通知。

2. **FMA** 信息中的故障信息保存在日志中，因此，参考控制域控制台上的日志文件。

此时，请在控制域控制台上执行一个 **Oracle Solaris** 命令，如：**syslog reference** 命令或 **fmdump** 命令。

如需了解如何使用这些命令识别故障信息，请参见 Oracle Solaris 相关手册。

3. 通过按照控制域控制台显示的信息 **ID (SUNW-MSG-ID)** 访问指定的 **URL**，确认通知或故障的内容。
如果没有找到信息 **ID (MSG-ID)**，请从系统日志信息中获得详细信息。
4. 要获得更详细信息，请登录 **XSCF** 并执行 **showlogs** 命令识别故障信息。
5. 根据指定 **URL** 所提供信息建议的处理方法解决故障。

注 - 有关最新的 **URL** 信息，请参见您的服务器最新的《产品说明》中介绍的有关消息的网站。

除系统日志信息和 **FMA** 信息外，用户可以通过参考 **XSCF** 日志中存储的控制台信息、崩溃信息、**IPL** 信息或监视信息识别故障。您可通过执行 **XSCF shell** 指定了各日志选项的 **showlogs** 命令参考日志信息。

有关 **showlogs** 命令的详细信息，请参见 "12.1 检查 **XSCF** 保存的日志"。

识别/处理通过电子邮件报告的故障

1. 用户根据 **XSCF** 所报告电子邮件的主题或信息文本，识别通知或故障。
有关发生故障时电子邮件的示例，请参见 "10.2 故障发生时通过电子邮件接收通知"。
2. 如需获得更详细信息，请登录 **XSCF** 并执行 **showlogs** 命令识别故障信息。
3. 检查日志信息。如有必要，将电子邮件信息或日志中的诊断代码输出告知服务工程师。
服务工程师可使用诊断代码获取详细的信息。

识别/处理 **SNMP** 陷阱信息中的通知或故障

1. 用户通过 **SNMP** 管理器识别从 **XSCF** 中发出的陷阱信息中的通知或故障。
有关陷阱的示例，请参见 "10.3 通过 **SNMP** 代理监控/管理系统状态"。
2. 如需获得更详细信息，请登录 **XSCF** 并执行 **showlogs** 命令识别故障信息。
3. 检查日志信息。如有必要，将输出在日志的诊断代码通知服务工程师。

识别/处理 **XSCF shell** 中监视信息中的通知或故障

1. 用户通过执行 **showmonitorlog** 命令识别 **XSCF** 监视信息输出中的通知或故障。
下面是监视信息的示例。

```
XSCF> showmonitorlog
PAPL2-5-0:Alarm:/BB#0/CPU#0:XSCF:Uncorrectable
error ( 80006000-20010000-0108000112345678):
```

注 - 命令示例可能会随时变化，对于功能改进恕不另行通知。

2. 如需获得更详细信息，请登录 **XSCF** 并执行 **showlogs** 命令识别故障信息。
3. 检查日志信息。如有必要，将输出在日志的诊断代码通知服务工程师。

切换到锁定/维护模式

本章介绍用于维护工作的维护模式与锁定模式之间的差异，以及如何进行切换。

- 了解锁定模式和维护模式的差异
- 切换操作模式

13.1 了解锁定模式和维护模式的差异

SPARC M12/M10 系统有两种工作模式：锁定模式和服务模式。

- 锁定模式

锁定模式专门用于常规操作。本模式中，开关被设置为“锁定”。

在 XSCF 中配置的用户帐户会在工作中使用。可进行的工作范围根据用户帐户类型而有所不同。

在锁定模式中，因为设置了防止用户误操作关闭电源的机制，所以电源不会被轻易关闭。操作面板上的电源开关可用于开启电源，但不能关闭电源。

- 维护模式

维护模式专门用于维护工作。本模式中，开关被设置为“维护”。必须在整个系统停止的维护模式下执行维护工作。

锁定模式和维护模式下开启和关闭电源的控制不仅影响电源开关的操作，而且也影响远端的电源控制、自动电源控制等。表 13-1 显示了两种模式之间电源控制的差异。

表 13-1 锁定模式和维护模式之间电源控制的差异

项目	操作模式	
	锁定模式	维护模式
用电源开关开机	允许开机	不允许开机
用电源开关关机	不允许关机	允许关机 长按（4 秒或以上）开始关机处理。
中断信号	根据设置 (默认启动。)	信号发送到控制域
断电恢复后开机	电源开启	电源不开启

表 13-1 锁定模式和维护模式之间电源控制的差异 (续)

项目	操作模式	
	锁定模式	维护模式
实时检查	根据设置 (默认启动。)	禁用
主机监视程序超时的反应	根据设置 (默认为 PPAR 重置)	根据设置 (默认为 PPAR 重置)
Oracle Solaris 的自动启动	根据设置 (默认为自动启动)	根据设置 (默认为自动启动) (*1)
按计划自动开机	允许开机	不允许开机
按计划自动关机	允许关机	不允许关机
远程电源管理	可以	不可用

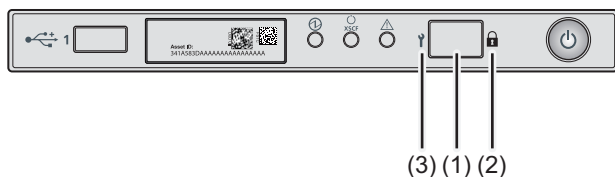
*1 有关 Oracle Solaris 自动启动-停止的详细信息，请参见“6.4 禁止在开机时启动 Oracle Solaris”。

使用 XSCF 固件的 `setpparmode` 命令可以配置锁定模式和维护模式控制项目中显示“根据设置”的项目。

13.2 切换操作模式

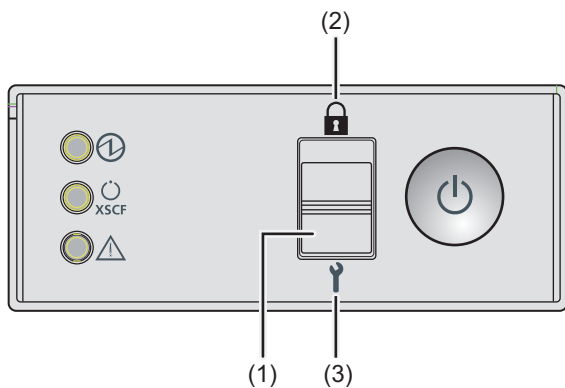
如需在 SPARC M12/M10 系统中切换操作模式，需使用操作面板上的模式开关。

图 13-1 操作面板模式开关 (SPARC M12-1/M10-1)



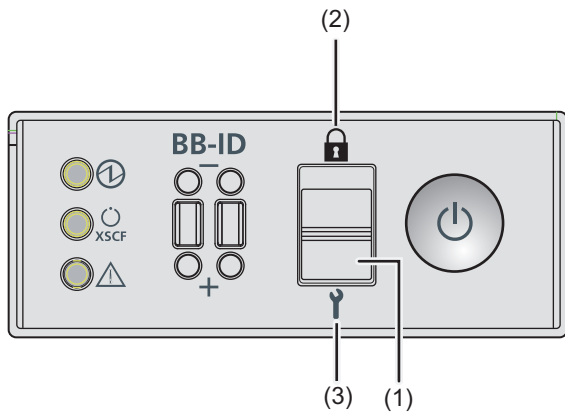
编号	组件
1	模式开关
2	锁定模式
3	维护模式

图 13-2 操作面板模式开关 (SPARC M12-2/M10-4)



编号	组件
1	模式开关
2	锁定模式
3	维护模式

图 13-3 操作面板模式开关 (SPARC M12-2S/M10-4S)



编号	组件
1	模式开关
2	锁定模式
3	维护模式

对于模块化架构配置中的各 SPARC M12-2S 或 SPARC M10-4S，需通过滑动具有主 XSCF 或备用 XSCF 的 SPARC M12-2S 或 SPARC M10-4S 操作面板上的模式开关来切

换模式。在不使用接线盒时，主 XSCF 是 BB#00 或 BB#01。在使用接线盒时，主 XSCF 是 XBB#80 或 XBB#81。

注 - 对于模块化架构配置中的 SPARC M12-2S 或 SPARC M10-4S，将主 XSCF 和备用 XSCF 的模式开关设置为同一模式。如果在设置不同时，使用 `switchscf` 命令切换主 XSCF 和处于备用状态的 XSCF，则会更改识别每个 SPARC M12-2S 或 SPARC M10-4S 机箱的服务开关的状态。为了报告此状态，`showhardconf` 和 `showstatus` 命令输出中会显示一个星号 (*)，指示出现故障的组件。

下面介绍如何从锁定模式切换到维护模式和如何从维护模式切换到锁定模式。

切换到维护模式

如需对 SPARC M12/M10 系统执行冷系统维护作业或进行初始 XSCF 设置，请设置服务模式。

下面介绍如何将锁定模式切换到维护模式。

1. 在操作面板上，将模式开关调到 **Service (Y)**。

切换到锁定模式

对 SPARC M12/M10 系统从服务模式切换到锁定模式的步骤如下所述。

1. 在操作面板上，将模式开关调到 **Locked (L)**。

配置高可靠性系统

本章介绍配置高可靠性和安全的 SPARC M12/M10 系统的方法。

- 配置内存镜像
- 配置硬件 RAID
- 使用 LDAP 服务
- 使用 SAN 启动
- 使用 iSCSI
- SPARC M12/M10 和 I/O 设备的远程电源管理
- 使用不间断电源
- 使用验证启动

14.1 配置内存镜像

本节介绍如何配置受 SPARC M12/M10 支持的内存镜像。

14.1.1 内存镜像概述

SPARC M12/M10 支持内存镜像配置，以通过内存复制来保护数据。数据的可靠性增加，但可用内存的容量减半。

内存访问控制器控制数据到内存的写入和数据从内存中的读取。SPARC M12/M10 通过将内存分成由两个内存访问控制器控制的组来配置镜像。

注 - 集中在一个镜像配置中的分组内存都必须具有相同的容量和等级。

有关内存物理配置的规则，请参见服务器的《Service Manual》中的“Checking the Memory Configuration Rules”。

14.1.2 配置内存镜像

使用 XSCF 固件的 `setupfru` 命令配置 SPARC M12/M10 中安装的内存的镜像。请使用拥有 `platadm` 或 `fieldeng` 权限的用户账户执行此命令。

注 - 如需配置内存镜像，必须关闭 PSB 所属的物理分区。

内存镜像配置

■ SPARC M12

若需在 SPARC M12 中配置内存镜像，请指定 `-c mirror=yes`。

```
XSCF> setupfru [[-q] -{y|n}] -c function=mode device location
```

■ SPARC M10

若需在 SPARC M10 中配置内存镜像，请指定 `-m y`。不能使用 `-c mirror` 选项。

```
XSCF> setupfru [-m {y|n}] device location
```

操作步骤

1. 执行 `setupfru` 命令以配置内存镜像。

以下示例显示了 SPARC M12 中所有安装在物理系统板 (PSB) 00-0 上的 CPU 被设置为内存镜像模式。

```
XSCF> setupfru -c mirror=yes sb 00-0
Notice:
- Logical domain config_name will be set to "factory-default".
Memory mirror mode setting will be changed, Continue? [y|n] :y
```

注 - 对于 SPARC M10，请指定以下内容。

```
XSCF> setupfru -m y sb 00-0
```

以下示例显示，PSB 02-0 中 CPU 芯片 #1 的 CPU 被设置为内存镜像模式。

```
XSCF> setupfru -m y cpu 02-0-1
```


14.2 配置硬件 RAID

本节介绍 SPARC M12/M10 支持的硬件 RAID 配置，以及如何配置和管理硬件 RAID。

您可以从以下两个实用程序中选择用于在 SPARC M12/M10 上创建和管理硬件 RAID 卷的环境。

- **FCode 实用程序**
此实用程序由一组特别的命令组成，用于显示目标和管理服务器上的逻辑卷。在 OpenBoot PROM 环境中使用这些命令。
- **集成 RAID 配置 SAS-2 实用程序 (SAS2IRCU)**
您可以通过使用 Broadcom Limited 公司的 14.00.00.00 版本或更高版本的 SAS-2 Integrated RAID Configuration Utility (SAS2IRCU)（以下简称 SAS2IRCU 实用程序）配置和管理系统上的 RAID 卷。

SAS-2 集成 RAID 配置实用程序 (SAS2IRCU) 的版权归 Broadcom Limited 及其附属公司所有。

从 Broadcom Limited 获取 SAS2IRCU 实用程序和详细的文档，网址如下：

<https://www.broadcom.com/site-search?q=sas2ricu>

本章将使用来自上述网站的 FCode 实用程序的示例进行说明。

有关 SAS2IRCU 实用程序输出的示例，请参见“附录 F SAS2IRCU 实用程序命令示例”。

如需在硬件 RAID 配置中创建系统（启动）卷，需使用 FCode 实用程序。FCode 实用程序和 SAS2IRCU 实用程序可支持以下任务。

表 14-1 硬件 RAID 实用程序所支持的任务

任务说明	FCode 实用程序	SAS2IRCU 实用程序
创建系统（启动）卷	支持	不支持
创建数据卷	支持	支持
创建热备盘	不支持	支持

14.2.1 硬件 RAID 基础知识

硬件 RAID 技术可通过集中管理至少两个内部磁盘驱动器加快数据访问速度并增加数据保护的可靠性。

SPARC M12/M10 通过内置板载 SAS 控制器的集成 RAID 功能提供硬件 RAID。在硬件 RAID 类型中，支持 RAID0、RAID1、RAID10 和 RAID1E。每个 SAS 控制器最多可以配置两个 RAID 卷。

表 14-2 支持的 RAID 类型

型号	每个机箱的 SAS 控制器的数量	支持的 RAID 类型
SPARC M12-1	1	RAID0/RAID1/RAID10/RAID1E
SPARC M12-2/M12-2S	2	RAID0/RAID1/RAID10/RAID1E
SPARC M10-1/M10-4/M10-4S	1	RAID0/RAID1/RAID1E

在 SPARC M12/M10 中，您可以通过组合上述 RAID 类型，为 SPARC M10 最多配置两个 RAID 卷，或为 SPARC M12 配置最多四个 RAID 卷。

注 - 您不能跨 SPARC M12-2/M12-2S 或跨组成多个设备的 M12-2S/M10-4S 中的 SAS 控制器配置 RAID 卷。

支持的磁盘驱动器

如需在 SPARC M12/M10 中配置硬件 RAID，请在配置中为每个 RAID 卷使用相同容量和速度的磁盘驱动器。

不支持固态硬盘 (SSD)。也不支持连接到 SAS 端口的的外部磁盘驱动器。

接下来，介绍 RAID0、RAID1、RAID10 和 RAID1E 的机制。

- RAID0（分段）

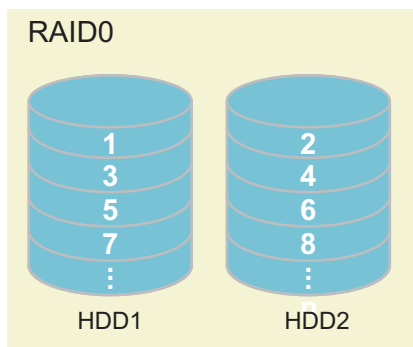
在此技术中，数据写入和读取被分散到多个内部磁盘驱动器以并行对其进行处理。RAID0 增加了数据的访问速度，因此用于需要磁盘加速的工作。

在 SPARC M12/M10 中，您可以使用两到八个磁盘驱动器配置 RAID0 卷。

表 14-3 可配置 RAID0 卷的磁盘驱动器的数量

型号	要配置的磁盘驱动器的数量
SPARC M12-1/M10-1/M10-4/M10-4S	2 至 8
SPARC M12-2/M12-2S	2 至 4

图 14-1 RAID0 机制



注 - 由于 RAID0 未冗余，构成 RAID0 的一个磁盘驱动器出现故障即可引起该 RAID 卷失败，导致所有数据丢失。

如果 RAID 卷出现故障，必须重新配置 RAID 卷，然后从备份数据中恢复。

■ RAID1（镜像）

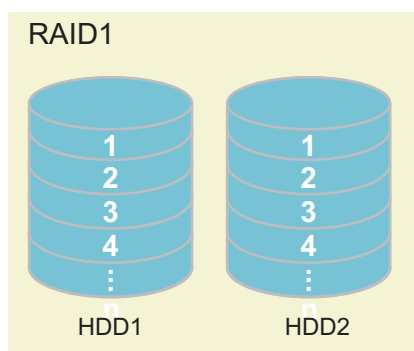
这种技术复制内部磁盘驱动器并将相同的数据写入到复制的驱动器，以增加数据的容错能力。即使内部磁盘驱动器中的一个出现故障，可以使用另一个驱动器继续操作。另外，也可以在操作进行时更换出现故障的内部磁盘驱动器。然而，保存数据的磁盘容量减半。

在 SPARC M12/M10 中，您可以使用两个磁盘驱动器配置 RAID1 卷。

表 14-4 可配置 RAID1 卷的磁盘驱动器的数量

型号	要配置的磁盘驱动器的数量
SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S	2

图 14-2 RAID1 机制



注 - 采用 RAID1 时，即使一个磁盘驱动器出现故障，系统也以降级状态连续运行。然而，两个磁盘驱动器出现故障将引起 RAID 卷故障，导致所有数据丢失。

如果 RAID 卷进入降级状态，请尽快更换出现故障的磁盘驱动器并恢复冗余。

■ RAID10（镜像 + 分段）

此技术复制内部磁盘驱动器，并将需要写入的数据分割成多个重复的组。RAID10 可以使用四个或更多的内部磁盘驱动器。

在 SPARC M12 中，您可以使用四个、六个或八个磁盘驱动器配置 RAID10 卷。

SPARC M10 不支持 RAID10。

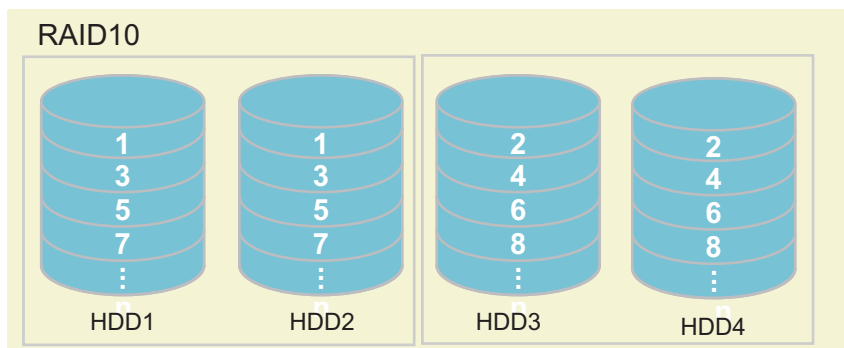
注 - 使用 RAID10 时，即使其中一个镜像的磁盘驱动器发生故障，系统在降级的状态下继续运行。但是，镜像的磁盘驱动器的故障会引起 RAID 卷故障，从而导致所有数据丢失。

如果 RAID 卷进入降级状态，请尽快更换出现故障的磁盘驱动器并恢复冗余。

表 14-5 可配置 RAID10 卷的磁盘驱动器的数量

型号	要配置的磁盘驱动器的数量
SPARC M12-1	4、6 或 8
SPARC M12-2/M12-2S	4

图 14-3 RAID10 的机制



■ RAID1E（扩展镜像）

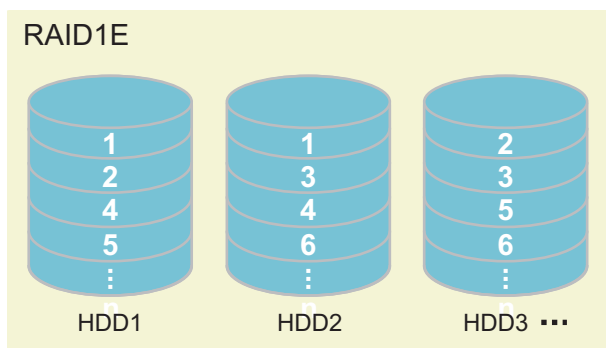
此技术分割并复制数据，然后将数据写入多个内部存储单元。RAID1E 是扩展型的 RAID1，可使用 3 个或更多内部磁盘驱动器。

在 SPARC M12/M10 中，您可以使用三个、五个或七个磁盘驱动器配置 RAID1E 卷。

表 14-6 可配置 RAID1E 卷的磁盘驱动器的数量

型号	要配置的磁盘驱动器的数量
SPARC M12-2/M12-2S	3
SPARC M12-1/M10-1/M10-4/M10-4S	3、5 或 7

图 14-4 RAID1E 机制



注 - 采用 RAID1E 时，即使一个磁盘驱动器出现故障，系统也以降级状态连续运行。然而，两个或两个以上磁盘驱动器出现故障将引起 RAID 卷故障，导致所有数据丢失。
如果 RAID 卷进入降级状态，请尽快更换出现故障的磁盘驱动器并恢复冗余。

14.2.2 FCode 实用程序命令

FCode 实用程序用于配置硬件 RAID。此实用程序提供了以下命令。

表 14-7 FCode 实用程序命令列表

FCode 命令	说明
show-children	列出所有已连接的逻辑驱动器和逻辑卷。
show-volumes	列出所有已连接的逻辑卷的详细信息。
create-raid0-volume	创建 RAID0 卷。指定至少 2 个目标。
create-raid1-volume	创建 RAID1 卷。指定 2 个目标。
create-raid1e-volume	创建 RAID1E 卷。指定至少 3 个目标。 注 - 如果此命令与指定的偶数目标（至少 4 个目标）一起使用， 则此命令将硬件 RAID 配置为 RAID10。
create-raid10-volume	创建 RAID10 卷。至少指定 4 个目标。 注 - 如果此命令与指定的奇数目标（至少 5 个目标）一起使用， 则此命令将硬件 RAID 配置为 RAID1E。
delete-volume	删除 RAID 卷。
activate-volume	更换 SPARC M12-2/M12-2S/M10-4/M10-4S 的 CPU 内存单元 （下）和 SPARC M12-1/M10-1 系统的主板单元后，再次启用 RAID 卷。

14.2.3 硬件 RAID 的注意事项

本节介绍使用硬件 RAID 的注意事项。

使用硬件 RAID 时的注意事项

- 定期执行重要数据和程序的备份。对于一些错误，您可以通过重新配置硬件 RAID 来从备份介质恢复数据或程序。
- 我们建议使用不间断电源 (UPS)，以确保系统中的数据在停电的情况下是安全的。
- 如果需要硬件 RAID 功能的高可用性，如控制器或数据路径的复制，则安装专用的 RAID 系统。
- 使用硬件 RAID 的磁盘冗余只能在一个 SAS 控制器下进行。

SAS2IRCU 实用程序

- 当您管理 SPARC M12/M10 的硬件 RAID 环境时，建议您使用 Broadcom Limited

提供的 SAS2IRCU 实用程序 (sas2ircu: SAS-2 集成 RAID 配置实用程序), 原因如下。

- SAS2IRCU: 您可以在逻辑域运行时配置和管理硬件 RAID。
- OpenBoot PROM 环境: 仅当逻辑域停止时您才能配置硬件 RAID, 但无法进行管理。

注 - 如果您在 SPARC M12-2S/M10-4S 中使用或计划使用 DR 功能, 请务必安装 SAS2IRCU 实用程序。DR 集成后, 需要使用 SAS2IRCU 实用程序来启用 RAID 卷。

- 有关如何获得 SAS2IRCU 实用程序的详细信息, 请参见 "14.2 配置硬件 RAID" 中所述的 Broadcom Limited 网站。有关如何使用此信息, 请参见同一网站上的《SAS-2 Integrated RAID Configuration Utility User Guide》。
- 如果 RAID 卷出现故障, 可以使用 SAS2IRCU 实用程序指定故障磁盘。
- SAS2IRCU 实用程序在 Oracle Solaris 环境中使用并需要 root 帐户权限。因此, SAS2IRCU 实用程序应该由系统管理员进行操作。
- SAS2IRCU 实用程序在分配 SAS 控制器的逻辑域中使用。因此, 在分配主板上的 SAS 控制器的 I/O 根域中安装 SAS2IRCU 实用程序。

注 - SPARC M12/M10 中的 SAS 控制器不支持 PCIe 端点设备的分配功能。

配置/移除硬件 RAID 时的注意事项

- 配置或移除硬件 RAID 时, 磁盘上数据的可靠性无法得到保证。在最初为系统配置硬件 RAID 或移除已安装的硬件 RAID 之前, 请务必进行数据的备份。配置硬件 RAID 后, 您可能需要安装新数据或从备份介质恢复数据。
- 硬件 RAID 重新配置的执行可更改 RAID 卷特定的信息 (WWID 值)。因此, 如果您执行类似激活设备规格或 Oracle Solaris 安装处理的操作, 需要变更设置。
- 下表显示, 由于硬件 RAID 的配置或维护, 在卸载状态下同步 600 GB 的磁盘驱动器和 900 GB 的磁盘驱动器的标准时间。根据磁盘驱动器的生成和使用状况或系统的负荷状态的不同, 同步时间将发生很大变化。

表 14-8 硬件 RAID 的标准同步时间

RAID	磁盘驱动器的数量	同步时间	
		600 GB 磁盘驱动器	900 GB 磁盘驱动器
1	2	6 个小时	8 个小时
10 (*1)	4	10 小时	15 小时
	6	16 个小时	21 个小时
	8	21 个小时	31 小时
1E	3	20 个小时	29 个小时
	5	35 个小时	45 个小时
	7	54 个小时	65 个小时

*1 仅 SPARC M12 支持 RAID10。

- 在磁盘驱动器正在配置或正在同步硬件 RAID 时，请勿执行要求您访问磁盘驱动器的任务，如安装 Oracle Solaris 或恢复数据。从 RAID 卷安全的角度来看，我们建议在完成 RAID 卷的配置之前，请勿重写磁盘驱动器的内容。请务必在完成 RAID 卷的配置后，才能执行这些任务。
- 每个 SAS 控制器一次仅能配置一个 RAID 卷。当为正在进行 RAID 卷配置 of SAS 控制器发出另一组配置 RAID 卷的命令时，第一个配置任务完成后会继续进行下一个 RAID 卷配置。
- 当您配置硬件 RAID 时，RAID 卷的容量将小于原来的磁盘。
- 如果在正在配置或同步硬件 RAID 时系统重新启动或发生停电然后恢复供电，则会再次启动 SPARC M10 的配置/同步过程。对于 SPARC M12，配置/同步过程会从发生运行中断时的点重新启动。

操作硬件 RAID 的注意事项

由于硬件 RAID 控制器无法完全判断磁盘是否发生故障，系统可能变慢。如果您的系统出现此问题，请按照以下步骤操作。由于将要移除硬件 RAID，在执行此步骤之前，请务必首先进行数据的备份。

1. 阻止应用程序使用内部存储。
2. 移除硬件 RAID。
3. 查明问题是否与磁盘有关。
4. 如果问题未解决，则更换硬件 RAID 所使用的所有磁盘。
5. 重新配置硬件 RAID。
6. 从备份介质恢复数据。

接下来，对硬件 RAID 卷的操作步骤进行说明。根据将要执行的操作，查看相应的显示项目。

表 14-9 硬件 RAID 操作和参考

RAID 卷操作	参考
配置 RAID 卷	"14.2.4 硬件 RAID 操作前的准备工作" "14.2.5 创建硬件 RAID 卷" "14.2.7 管理硬件 RAID 卷的热备盘"
删除 RAID 卷	"14.2.4 硬件 RAID 操作前的准备工作" "14.2.6 删除硬件 RAID 卷"
更换组成 RAID 卷的磁盘驱动器	"14.2.9 检查出现故障的磁盘驱动器" "14.2.10 更换出现故障的磁盘驱动器"
更换 SPARC M12-2/M12-2S/M10-4/M10-4S 的 CPU 内存单元（下）和 SPARC M12-1/M10-1 系统的主板单元后，重新启用硬件 RAID	"14.2.11 重新启用硬件 RAID 卷" "14.2.12 指定硬件 RAID 卷为启动设备"

14.2.4 硬件 RAID 操作前的准备工作

使用 FCode 实用程序，以便准备硬件 RAID 操作。从 xterm 或支持滚动的等效终端执行此项工作。

操作步骤

1. 开启系统。
如果电源已经开启，重新启动系统并禁用 OpenBoot PROM 中的自动启动。
2. 确认显示 **ok** 提示符。
3. 执行 **show-devs** 命令，显示服务器设备路径列表。
下面是 SPARC M10 的示例。

```
{0} ok show-devs
      .
      .
      /pci@8000/pci@4/pci@0/pci@0/scsi@0
      /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
      /pci@8000/pci@4/pci@0/pci@0/scsi@0/tape
      .
      .
{0} ok
```

4. 执行 **select** 命令选择创建硬件 RAID 卷的控制器。

注 - 执行 **select** 命令后，需要执行 **unselect-dev** 命令。步骤完成后，根据 14.2.5 或 14.2.6 中的方向执行 **unselect-dev** 命令。

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

5. 执行 **.properties** 命令检查内部 SAS 控制器的 SAS 地址。

```
{0} ok .properties
assigned-addresses 81030010 00000000 00000000 00000000 00000100
83030014 00000001 00000000 00000000 00010000
8303001c 00000001 00040000 00000000 00040000
82030030 00000000 00200000 00000000 00100000
firmware-version 17.00.00.00
mpt-version 2.00
local-wwid 50 00 00 e0 e0 45 00 00 <- SAS 地址
:
略
:
{0} ok
```

注 - **.properties** 命令的输出结果是维护 RAID 卷所需的信息。请务必记下此信息。

6. 执行 **show-children** 命令显示所连驱动器的 SAS 地址。


```

{0} ok show-children

FCode    Version    1.00.56,    MPT    Version    2.00,    Firmware    Version    13.
00.66.00

Target   a
  Unit    0          Disk    TOSHIBA    MBF2600RC    3706
  1172123568    Blocks,    600    GB
  SASDeviceName    50000393c813ae74    SASAddress    50000393c813ae76
PhyNum    0
Target   b
  Unit    0          Disk    TOSHIBA    MBF2600RC    3706
  1172123568    Blocks,    600    GB
  SASDeviceName    50000393b81b24ec    SASAddress    50000393b81b24ee
PhyNum    1
:
略
:
Target   12
  Unit    0          Encl    Serv    device    FUJITSU    NBBEXP
  0d32
  SASAddress    500000e0e04d003d    PhyNum    14

```

注 - show-children 命令的输出结果是维护 RAID 卷的必须信息。请务必记下此信息。

执行 show-children 命令显示所连驱动器的 SAS 地址。

14.2.5 创建硬件 RAID 卷

根据所创建的硬件 RAID 配置，使用下列命令之一来创建硬件 RAID 卷。

- 创建 RAID0 卷

```
{0} ok target1 target2 create-raid0-volume
```

- 创建 RAID1 卷

```
{0} ok target1 target2 create-raid1-volume
```

- 创建 RAID10 卷

```
{0} ok target1 target2 target3 target4 create-raid10-volume
```

注 - SPARC M10-4/M10-4S/M10-1 不支持 RAID10。

- 创建 RAID1E 卷

```
{0} ok target1 target2 target3 create-raidle-volume
```

下面的设置对所有这些命令都通用。

指定可以使用 `show-children` 命令检查的目标编号为 `target 1`、`target 2`、`target 3` 和 `target 4`。`target` 不能属于多个卷。

这些命令是交互式命令，可以以 MB 指定卷容量，并且卷名最多可指定 15 个字符。当未指定卷的容量时，则将以最大容量进行创建。

操作步骤

1. 为创建硬件 RAID 卷做准备。
有关详情，请参见 "14.2.4 硬件 RAID 操作前的准备工作"。
2. 从 `show-children` 命令的执行结果，确定创建硬件 RAID 卷的目标。
3. 执行 `create-raid0-volume`、`create-raid1-volume`、`create-raid10-volume` 或 `create-raid1e-volume` 命令创建使用物理磁盘的硬件 RAID 卷。
在下面的示例中，`a` 和 `b` 被指定为目标，使用最大容量卷创建 RAID0 卷，未指定卷名。

```
{0} ok a b create-raid0-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 1142500 MB
What size do you want? [1142500] [Enter]
Volume size will be 2339840000 Blocks, 1197 GB
Enter a volume name: [0 to 15 characters] [Enter]
Volume has been created
```

在下面的示例中，`a` 和 `b` 被指定为目标，使用最大容量卷创建 RAID1 卷，未指定卷名。

```
{0} ok a b create-raid1-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 571250 MB
What size do you want? [571250] [Enter]
Volume size will be 1169920000 Blocks, 598 GB
Enter a volume name: [0 to 15 characters] [Enter]
Volume has been created
```

在以下示例中，将 `a`、`b`、`c` 和 `d` 指定为目标，并创建了具有最大卷容量但未指定卷名的 RAID10 卷。

```
{0} ok a b c d create-raid10-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
Target c size is 1169920000 Blocks, 598 GB
Target d size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 1142500 MB
What size do you want? [1142500] [Enter]
```

```
Volume size will be 2339840000 Blocks, 1197 GB
Enter a volume name: [0 to 15 characters]      [Enter]
Volume has been created
```

在下面的示例中，a、b 和 c 被指定为目标，使用最大容量卷创建 RAID1E 卷，未指定卷名。

```
{0} ok a b c create-raidle-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
Target c size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 856875 MB
What size do you want? [856875]              [Enter]
Volume size will be 1754880000 Blocks, 898 GB
Enter a volume name: [0 to 15 characters]     [Enter]
Volume has been created
```

4. 执行 **show-volumes** 命令以检查创建的 RAID 卷。

下面的示例检查 RAID 1 卷的内容。

```
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
WWID 0d061173730f12d5
Optimal Enabled Data Scrub In Progress
2 Members                               1169920000 Blocks, 598 GB
Disk 0
  Primary Optimal
  Target a TOSHIBA MBF2600RC 3706 PhyNum 0
Disk 1
  Secondary Optimal
  Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok
```

注 - 当在同一个 SAS 控制器下创建两个 RAID 卷时，首先创建的 RAID 卷被编号为 "1"，第二个创建的 RAID 卷被编号为 "0"。

5. 执行 **unselect-dev** 命令取消选择准备工作期间所选择的控制器。

```
{0} ok unselect-dev
{0} ok
```

注 - 在 Oracle Solaris 上，所创建的每个 RAID 卷，都被识别为一个磁盘驱动器（Vendor 是 "LSI"，Product 是 "Logical Volume"）。此外，整合的 RAID 卷变更设备路径如下。

未并入硬件 RAID 的磁盘驱动器的设备路径：

/device path of the sas controller/iproto@f/disk@w[SAS address of the disk drive] (or, /scsi_vhci/disk@g[SAS device name of the disk drive])

变更为：

RAID 卷的设备路径：

/device path of the sas controller/iport@v0/disk@w[device name of the RAID volume]

以下是 `format` 命令在 [磁盘驱动器未整合在硬盘 RAID 中] 和 [硬件 RAID 卷] 同时存在的环境中执行时的输出示例。

- 输出信息 1 示例
Oracle Solaris 安装时和 Oracle Solaris 安装后

```
root# format
Searching for disks... done

AVAILABLE DISK SELECTIONS:
[未整合到硬件 RAID 的磁盘驱动器]
  0. c2t50000394882899F6d0 <TOSHIBA-AL13SEB600-3702 cyl 64986 alt 2 hd 27
sec 668>
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394882899f6,0
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d257f/013P_HDD00/disk
[RAID 卷]
  1. c3t3DF694DFC21FFDA9d0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
sec 557>
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3df694dfc21ffda9,0
```

- 输出信息 2 示例
使内置磁盘驱动器 MPxIO 的设置被执行时的环境（或应用 Enhanced Support Facility 5.0 或更高版本）

```
root# format
Searching for disks... done

AVAILABLE DISK SELECTIONS:
[未整合到硬件 RAID 的磁盘驱动器]
  0. c0t50000394882899F4d0 <TOSHIBA-AL13SEB600-3702 cyl 64986 alt 2 hd 27
sec 668>
    /scsi_vhci/disk@g50000394882899f4
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d257f/013P_HDD00/disk
[RAID 卷]
  1. c3t3DF694DFC21FFDA9d0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
sec 557>
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3df694dfc21ffda9,0
```

注 - 当 Oracle Solaris 启动时，可能显示以下信息。这表明在 RAID 卷上没有标签信息。处于这种状态的 RAID 卷无法用于 Oracle Solaris。执行 `format` 命令，选择合适的 RAID 卷，然后对其进行标记后，则可在 Oracle Solaris 上使用。

- 输出信息示例

```
Jan 16 02:46:48 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:48 solaris          Corrupt label; wrong magic number
```

■ 执行 format 命令的示例

```
root@solaris:/root# format
Searching for disks...
Jan 16 02:46:35 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:35 solaris          Corrupt label; wrong magic number
Jan 16 02:46:35 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:35 solaris          Corrupt label; wrong magic number
done
c2t3AA6D102F1BF517Ad0: configured with capacity of 556.97GB
AVAILABLE DISK SELECTIONS:
    0. c2t3AA6D102F1BF517Ad0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
    sec 557>
        /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3aa6d102f1bf517a,0
Specify disk (enter its number): 0
selecting c2t3AA6D102F1BF517Ad0
[disk formatted]
Jan 16 02:46:48 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:48 solaris          Corrupt label; wrong magic number
Jan 16 02:46:54 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:54 solaris          Corrupt label; wrong magic number
Disk not labeled. Label it now? yes
```

14.2.6 删除硬件 RAID 卷

使用 FCode 实用程序的 `delete-volume` 命令来删除创建的硬件 RAID 卷。

```
{0} ok volume_number delete-volume
```

`volume_number` 指定由 `show-volumes` 命令输出的卷编号。

执行命令后，显示询问是否删除 RAID 卷的确认信息。相应选择 "yes" 或 "no"。

操作步骤

1. 为删除硬件 RAID 卷做准备。
有关详情，请参见“14.2.4 硬件 RAID 操作前的准备工作”。
2. 执行 `show-volumes` 命令以检查要删除的 RAID 卷。
下面的示例显示已创建卷编号 0 的 RAID1 卷。

```
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
Name raid1-volume WWID 0c233a838262c6c5
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
```

```
Disk 0
  Primary Optimal
  Target a      TOSHIBA  MBF2600RC      3706  PhyNum 0
Disk 1
  Secondary Optimal
  Target b      TOSHIBA  MBF2600RC      3706  PhyNum 1
{0} ok
```

3. 执行 **delete-volume** 命令以删除 RAID 卷。
下面的示例删除卷编号 0 的 RAID 卷。

```
{0} ok 0 delete-volume
The volume and its data will be deleted
Are you sure (yes/no)? [no] yes
Volume 0 has been deleted
{0} ok
```

4. 执行 **show-volumes** 命令，确认 RAID 卷已被删除。

```
{0} ok show-volumes
No volumes to show
{0} ok
```

5. 执行 **unselect-dev** 命令取消选择准备工作期间所选择的控制器。

```
{0} ok unselect-dev
{0} ok
```

14.2.7 管理硬件 RAID 卷的热备盘

使用已创建的热备驱动器时，如果镜像的 RAID 卷（RAID1、RAID10 或 RAID1E）的其中一个磁盘驱动器出现故障，则板载 RAID 控制器将使用该热备驱动器替换出现故障的磁盘驱动器并重新同步数据。

使用 SAS2IRCU 实用程序来创建或删除 RAID 卷的热备盘。有关 SAS2IRCU 实用程序的详细信息，请参见“14.2 配置硬件 RAID”的开始部分。或者，有关输出示例，请参见“附录 F SAS2IRCU 实用程序命令示例”。

注 - 如果配置两个 RAID 卷具有不同的磁盘驱动器容量，由于以下原因不建议创建热备。

- 当热备的磁盘驱动器容量小于配置 RAID 卷的磁盘驱动器容量时不执行重新同步，因为热备驱动器无法替换故障的磁盘驱动器。
- 当热备的磁盘驱动器容量大于配置 RAID 卷的磁盘驱动器容量时热备驱动器替换故障的磁盘驱动器并执行重新同步。但是，RAID 磁盘卷配置不同磁盘驱动器容量。（不支持此配置。）

14.2.8 检查硬件 RAID 卷的状态和磁盘驱动器

本节介绍如何检查硬件 RAID 卷的状态以及硬件 RAID 卷的内部磁盘驱动器。

若需检查硬件 RAID 卷的状态以及硬件 RAID 卷内的磁盘驱动器，请使用 Fcode 实用程序或 SAS2IRCU 实用程序，并使用以下命令。

表 14-10 硬件 RAID 的状态显示命令

实用程序的名称	命令的名称
FCode 实用程序	show-volumes 命令
SAS2IRCU 实用程序	STATUS 命令 DISPLAY 命令

下面介绍执行每个实用程序命令时的主要状态及说明。

表 14-11 硬件 RAID 的实用程序命令所显示的状态

项目	输出值		说明
	FCode 实用程序 show-volumes 命令	SAS2IRCU 实用程序 STATUS 命令 DISPLAY 命令	
RAID 级别	RAID0 (Striping)	RAID0	RAID0 (分段) 卷
	RAID1 (Mirroring)	RAID1	RAID1 (镜像) 卷
	RAID10 (Striped Mirroring)	RAID10	RAID10 (镜像 + 分段) 卷
	RAID1E (Mirroring Extended)	RAID1E	RAID1E (扩展镜像) 卷
硬件 RAID 卷的状态 (典型示例)	Optimal	Optimal	硬件 RAID 卷运行正常
	Degraded	Degraded	硬件 RAID 卷降级
	Missing	Missing	未发现硬件 RAID 卷
	Failed	Failed	硬件 RAID 卷出现故障
	Enabled	Enabled	硬件 RAID 卷激活
	Inactive	Inactive	硬件 RAID 卷非活动状态
	Data Scrub In Progress	无	硬件 RAID 卷的数据擦除状态 由于硬件 RAID 固件自动执行，此显示没有问题。
	Background Init In Progress	Background Init	硬件 RAID 卷正在配置处理中 硬件 RAID 卷未完全配置。
	Resync In Progress	Synchronize	RAID 卷正在重新同步处理中 硬件 RAID 卷未完全配置。
Consistency Check In Progress	Consistency Check	正在检查硬件 RAID 卷的一致性	

表 14-11 硬件 RAID 的实用程序命令所显示的状态 (续)

项目	输出值		说明
	FCode 实用程序 show-volumes 命令	SAS2IRCU 实用程序 STATUS 命令 DISPLAY 命令	
磁盘驱动器的状态 (典型示例)	Optimal	Optimal (OPT)	目标磁盘驱动器整合到硬盘 RAID 卷
	Offline	Failed (FLD)	目标磁盘驱动器未整合到硬盘 RAID 卷
	Degraded	Degraded (DGD)	目标磁盘驱动器降级
	Rebuilding	Rebuilding (RBLD)	目标磁盘驱动器正在整合到硬盘 RAID 卷
	Out Of Sync	Out of Sync (OSY)	目标磁盘驱动器未与硬盘 RAID 卷同步

使用 FCode 实用程序显示状态

若需检查硬件 RAID 卷的状态以及硬件 RAID 卷内的内部磁盘驱动器，请停止系统并使用 Fcode 实用程序执行 show-volumes 命令。

1. 确认显示 **ok** 提示符。
2. 执行带控制器名称的 **select** 命令以显示其硬件 RAID 卷。

注 - 执行 select 命令后，需要执行 unselect-dev 命令。完成此步骤后，按照步骤 4 中的说明，执行 unselect-dev 命令。

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

3. 执行 **show-volumes** 命令以检查 RAID 卷。

下面示例显示如下内容：

- (1) 硬件 RAID 卷的 RAID 类型是 "RAID1 (镜像)"。
- (2) 硬件 RAID 卷是 "降级" 和 "启用"。
- (3) 构成硬盘 RAID 卷的磁盘驱动器中, Disk 0 是 "整合为主 (最优)"。
- (4) 构成硬盘 RAID 卷的磁盘驱动器中, Disk 1 是 "未整合为次级 (Offline)", 同时是 "不同步 (Out Of Sync)"。

```
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring) <-- (1)
Name raid1-volume WWID 0c233a838262c6c5
Degraded Enabled <-- (2)
2 Members 1169920000 Blocks, 598 GB
Disk 0
Primary Optimal <-- (3)
Target a TOSHIBA MBF2600RC 3706 PhyNum 0
Disk 1
Secondary Offline Out Of Sync <-- (4)
```



```
Target b      TOSHIBA MBF2600RC      3706  PhyNum 1
{0} ok
```

注 - 磁盘驱动器从硬件 RAID 被释放后，可显示该磁盘驱动器本身的错误状态。

4. 使用 **unselect-dev** 命令取消选择准备工作期间所选择的控制器。

```
{0} ok unselect-dev
{0} ok
```

使用 SAS2IRCU 实用程序显示状态

您也可使用 SAS2IRCU 实用程序来检查硬件 RAID 卷的状态以及硬件 RAID 卷内的内部磁盘驱动器。

有关 SAS2IRCU 实用程序的详细信息，请参见“14.2 配置硬件 RAID”的开始部分。

14.2.9 检查出现故障的磁盘驱动器

本节介绍如何检查构成 RAID 卷的内部磁盘驱动器中的故障。

您可以使用任何下面列出的方法或这些方法的组合来确认出现故障的磁盘驱动器。

检查磁盘驱动器的 LED

如果系统中的任何一个磁盘驱动器出现故障，则该驱动器前面的 CHECK LED（琥珀色）会点亮。通过此 CHECK LED，您可以识别系统中出现故障的磁盘驱动器。有关这些 LED 的位置和详细说明，请参见服务器的《Service Manual》中的“Understanding the System Components”。

检查错误信息

如果磁盘驱动器出现故障，控制台画面会显示错误信息。您也可以通过打开 `/var/adm/messages` 文件检查此类信息。

在以下示例中，在“14.2.4 硬件 RAID 操作前的准备工作”中显示的 `show-children` 命令的输出结果中，控制台上显示的错误消息告知您，Target ID 10 和 11 创建的 RAID1 卷的 Target 11 磁盘 (DevHandle 0x11) 出现故障，并且 RAID 卷已降级。由于作为 `show-children` 命令输出的 Target 11 的 PhyNum 值显示 HDD 插槽，此值可以用来确定包含出现故障的硬盘的插槽。在本示例中，可以从 `show-children` 命令的输出结果中确定，如“14.2.4 硬件 RAID 操作前的准备工作”所示，Target 11 的 PhyNum 值为 7。因此，出现故障的磁盘驱动器是插槽 7。

注 - 磁盘驱动器安装状态的变化也改变 DevHandle 值。

```
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now offline
```

```

Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now , active, out of sync, write cache enabled
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now , active, out of sync
Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now , enabled, active, data scrub in
progress
Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now , enabled, active, data scrub in
progress

```

在以下示例中，在“[14.2.4 硬件 RAID 操作前的准备工作](#)”中显示的 `show-children` 命令的输出结果中，控制台上显示的错误消息告知您，Target ID c 创建的热备盘 (DevHandle 0xc) 出现故障。

```

Jun 4 18:05:53 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 4 18:05:53 1S-341-D0 PhysDiskNum 5 with DevHandle 0xc in slot 0 for
enclosure with handle 0x0 is now offline

```

使用 FCode 实用程序显示状态

如需检查磁盘驱动器是否有故障，请停止系统，然后使用 FCode 实用程序命令的 `show-volumes` 命令。

有关详情，请参见“[14.2.8 检查硬件 RAID 卷的状态和磁盘驱动器](#)”。

使用 SAS2IRCU 实用程序显示状态

也可使用 SAS2IRCU 实用程序来检查磁盘驱动器故障。

有关 SAS2IRCU 实用程序的详细信息，请参见“[14.2 配置硬件 RAID](#)”的开始部分。另外，关于 SAS2IRCU 实用程序的显示状态，请参见“[14.2.8 检查硬件 RAID 卷的状态和磁盘驱动器](#)”，有关显示示例，请参见“[附录 F SAS2IRCU 实用程序命令示例](#)”。

14.2.10 更换出现故障的磁盘驱动器

本节介绍如何更换构成 RAID 卷的磁盘驱动器中出现故障的磁盘驱动器。

RAID0

如果 RAID0 卷中的磁盘驱动器出现故障，此卷中的所有数据将丢失。使用相同容量的新磁盘驱动器更换出现故障的磁盘驱动器，重新创建 RAID0 卷，并从备份中恢复数据。

RAID1/RAID10/RAID1E

使用相同容量的新磁盘驱动器更换出现故障的磁盘驱动器。当将新磁盘驱动器整合到 RAID 卷时，同步开始。

注 - 如果两个磁盘驱动器同时出现故障，RAID 卷进入故障状态（失败）。

更换出现故障的磁盘驱动器，重新创建 RAID 卷，然后从备份中恢复数据。在热备配置中，热备磁盘驱动器将自动重新同步，以恢复数据。无需启动或重新启动 Oracle Solaris 或启动 OpenBoot PROM 即可立即更换出现故障的磁盘驱动器。否则，如果在启动或重新启动 Oracle Solaris 或启动 OpenBoot PROM 后，您更换出现故障的磁盘驱动器，则在磁盘驱动器再次出现故障时，将无法切换到热备磁盘驱动器。此种情况下，更换出现故障的磁盘驱动器后，删除磁盘驱动器的热备设置，然后再次创建热备以便可恢复。

使用 SAS2IRCU 实用程序删除/创建热备。请参见附录 "F.6 删除硬件 RAID 卷的热备盘" 和 "F.5 创建硬件 RAID 卷的热备盘"。

14.2.11 重新启用硬件 RAID 卷

本节介绍如何在更换 SPARC M12-2/M12-2S/M10-4/M10-4S 的 CPU 内存单元（下）或 SPARC M12-1/M10-1 主板单元后重新启用硬件 RAID 卷。

更换上述单元后，由于 SAS 控制器（硬件 RAID 控制器）上没有硬件 RAID 的信息，硬件 RAID 卷处于非活动状态。因此，需要使用以下步骤，重新启用硬件 RAID 卷。

1. 选择设备，显示其卷信息并确认未被启用。

注 - 执行 select 命令后，需要执行 unselect-dev 命令。完成此步骤后，按照步骤 4 中的说明，执行 unselect-dev 命令。

在下面的示例中，显示 Inactive，这意味着 RAID 卷处于非活动状态。

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
  Name raid1-volume WWID 0c233a838262c6c5
  Optimal Enabled Inactive Consistent
  2 Members 1169920000 Blocks, 598 GB
  Disk 0
    Primary Optimal
    Target a TOSHIBA MBF2600RC 3706 PhyNum 0
  Disk 1
    Secondary Optimal
    Target b TOSHIBA MBF2600RC 3706 PhyNum 1
```

```
{0} ok
```

2. 执行 **activate-volume** 命令以启用 RAID 卷。
下面的示例表明重新启用卷编号 0 的 RAID 卷。

```
{0} ok 0 activate-volume  
Volume 0 is now activated  
{0} ok
```

3. 执行 **show-volumes** 命令，确认 RAID 卷已启用。
在下面的示例中，显示 Data Scrub in Progress，这意味着 RAID 卷激活。

```
{0} ok show-volumes  
Volume 0 Target 11e Type RAID1 (Mirroring)  
Name raid1-volume WWID 0c233a838262c6c5  
Optimal Enabled Data Scrub In Progress  
2 Members 1169920000 Blocks, 598 GB  
Disk 0  
Primary Optimal  
Target a TOSHIBA MBF2600RC 3706 PhyNum 0  
Disk 1  
Secondary Optimal  
Target b TOSHIBA MBF2600RC 3706 PhyNum 1  
{0} ok
```

4. 执行 **unselect-dev** 命令取消选择准备工作期间所选择的控制器。

```
{0} ok unselect-dev  
{0} ok
```

注 - 更换 SPARC M12-2/M12-2S/M10-4/M10-4S 的 CPU 内存单元（下）或 SPARC M12-1/M10-1 主板单元之前，请正确执行关机处理。然后，确认系统停止，并更换该部件。如果由于停电等原因，系统未进行关闭处理而停止，在 RAID 卷启用后，可能执行非计划中的介质检查。

在介质检查期间，您无法从 Fcode 实用程序或 SAS2IRCUC 实用程序获取介质检查状态。在此期间，RAID 卷状态变为 Optimal。确认磁盘驱动器的 LED 是否闪烁，以确认介质检查的执行状态。当磁盘驱动器的 LED 从闪烁变更为常亮时，这意味着介质检查已结束。

在介质检查期间，您可以正常访问硬件 RAID 卷，但与未执行介质检查时的硬件 RAID 卷相比较，I/O 性能可能不足。

所需的介质检查时间与硬件 RAID 配置或维护的同步时间相同。有关标准的所需时间，请参见“表 14-8 硬件 RAID 的标准同步时间”。

14.2.12 指定硬件 RAID 卷为启动设备

本节介绍如何指定硬件 RAID 卷为启动设备。

有关指定启动设备的详细信息，请参见“附录 I 如何指定启动设备”。

1. 选择设备并显示其卷信息。

检查 RAID 卷的 WWID。

下面是 SPARC M10 的示例。检查 RAID 卷的 WWID。

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
Name raid1-volume WWID 0c233a838262c6c5
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
Disk 1
Primary Optimal
Target a TOSHIBA MBF2600RC 3706 PhyNum 0
Disk 0
Secondary Optimal
Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok unselect-dev
{0} ok
```

2. 指定在步骤 1 中确认的 RAID 卷为启动设备。

指定 RAID 卷时，请遵循下面的规则。

- a. 将 RAID 卷的 WWID 开头的数字“0”更换为“3”。
由于步骤 1 中确认的 RAID 卷的 WWID 为“0c233a838262c6c5”，因此 WWID 成为了“3c233a838262c6c5”。
- b. 对于步骤 2a 中的 RAID 卷的 WWID（您更换数字的那个），在其开头添加“disk@w”，并将“,0:a”追加到其末尾。
- c. 指定 RAID 启动设备的完整路径名作为下面 `setenv boot-device` 命令的参数。
完整路径名是步骤 1 中选择的设备路径“/pci@8000/pci@4/pci@0/pci@0/scsi@0/”，随后是步骤 2b 中的 RAID 启动设备名称“disk@w3c233a838262c6c5,0:a”。

```
{0} ok setenv boot-device /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@
w3c233a838262c6c5,0:a
```

14.3 使用 LDAP 服务

Lightweight Directory Access Protocol (LDAP) 是用于在网络上访问目录服务的协议。通常，SPARC M12/M10 上的 XSCF 用户帐户的用户验证和用户权限由本地 XSCF 管理。但是，使用 LDAP 也可通过网络目录服务管理进行管理。另外，如果安装了多

个 SPARC M12/M10 系统，则所有系统通用的 XSCF 用户帐户都可以用于 LDAP。如需管理 XSCF 用户帐户设置，如用户验证和用户权限，请使用 LDAP 将 XSCF 配置成 LDAP 客户端。

有关如何通过网络上的目录服务使用 LDAP 来管理 XSCF 用户帐户设置的详细信息，请参见 ["3.5.12 使用 LDAP 管理 XSCF 用户帐户"](#)。

14.4 使用 SAN 启动

SPARC M12/M10 支持 SAN 启动。

SAN 启动是被配置为启动盘，具有外部存储的系统，而不是服务器中内置的内部磁盘驱动器。

SPARC M12/M10 使用光纤通道卡进行外部存储设备之间的连接，并且可以对系统进行配置以便通过 OpenBoot PROM 的 Fcode 功能使用 SAN 启动。

有关采用 SAN 启动构筑系统的详情，请参见以下 Oracle 文档：

- Oracle Solaris 管理: SAN 配置和多路径

14.5 使用 iSCSI

iSCSI 是一个通过 IP 网络交换 SCSI 命令的协议。此命令用于服务器和外部存储之间的通信。

在 SPARC M12/M10 中，您可以对系统进行配置以便使用 iSCSI。一旦系统被配置为使用 iSCSI，则多个服务器可以共享通过 TCP/IP 网络连接的大容量存储区。

14.6 SPARC M12/M10 和 I/O 设备的远程电源管理

本节对远程电源管理功能以及 SPARC M12/M10 的设置进行简要说明。

14.6.1 SPARC M12/M10 的远程电源管理功能

SPARC M12/M10 系统的远程电源管理功能（通过 LAN 的远程机柜接口：RCIL）是控制 SPARC M12/M10 系统或 I/O 设备之间电源的远程电源管理功能的接口。RCIL 功能采用基于 IPMI over LAN 的专用接口。如果支持常规 IPMI 的以下功能，则可以将

RCIL 设置为远程电源管理的对象，而不考虑控制的硬件或操作系统上的差异。RCIL 使用 SPARC M12/M10 上的 XSCF-LAN。

- 开启电源和关闭电源：Chassis Control
- 获取电源状态：Get Chassis Status

表 14-12 显示了 SPARC M12/M10 的远程电源管理功能中使用的术语和定义。

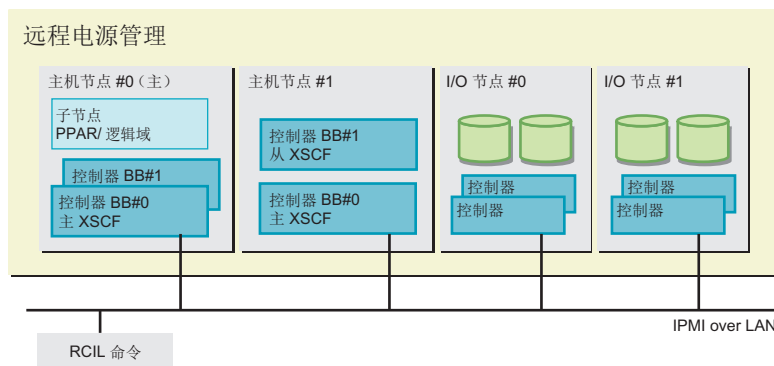
表 14-12 用于远程电源管理的术语及定义

术语	定义
主机节点	支持远程电源管理功能的 SPARC M12/M10 机箱。 SPARC M12-2、M12-2S、M10-1、M10-4 和 M10-4S 支持系统的远程电源管理功能。 设置远程电源管理组时设置为主的主机节点称为主要主机节点。主要主机节点是监控其它主机节点和 I/O 节点的主机节点。
子节点	SPARC M12/M10 中的物理分区
I/O 节点	支持 SPARC M12/M10 的远程电源管理功能的 I/O 设备或电源控制盒
远程电源管理组	从分组远程电源管理目标中获得的组，如主节点、子节点和 I/O 节点。特定的组 ID 被分配给远程电源管理组。
控制器	一种控制远程电源管理功能的机制。需要在每个节点中安装一个控制器。在 SPARC M12/M10 中，XSCF 是一个控制器。

如果远程电源管理功能被使用，则电源连锁节点组合创建一个远程电源管理组。您可以按照所创建的远程电源管理组控制远程电源管理。

注 - 各个主机节点、子节点或 I/O 节点可以仅设置在一个远程电源管理组中。

图 14-5 SPARC M12/M10 远程电源管理组的示例



14.6.2 了解远程电源管理的连接形式

通过 LAN 连接支持 SPARC M12/M10 远程电源管理功能的主机节点、子节点和 I/O 节点。

连接规格如下：

表 14-13 电源控制连接规格

项目	说明
连接形式	LAN 连接 采用以下任一形式进行连接： - 使用 XSCF-LAN #0 - 使用 XSCF-LAN #0 和 XSCF-LAN #1
传输速率	100 Mbps 或更高
Internet 协议	IPv4
DHCP	不支持 如果使用 SPARC M12/M10 的远程电源管理功能，则必须为连接目标设置固定的 IP 地址。
连接协议	IPMI(*1) over LAN (智能平台管理接口)

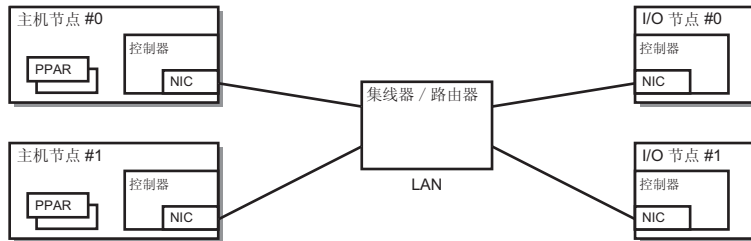
*1 受支持的 IPMI 的版本为 IPMI 2.0。

在 SPARC M12/M10 中，IPMI 服务仅在内部由远程电源管理功能使用。IPMI 不能由 ipmitool 或 SPARC M12/M10 的远程电源管理功能以外的任何功能使用。

远程电源管理的标准连接

通过同一个 LAN 连接配备有支持 SPARC M12/M10 远程电源管理功能的控制器的主机节点、子节点和 I/O 节点。

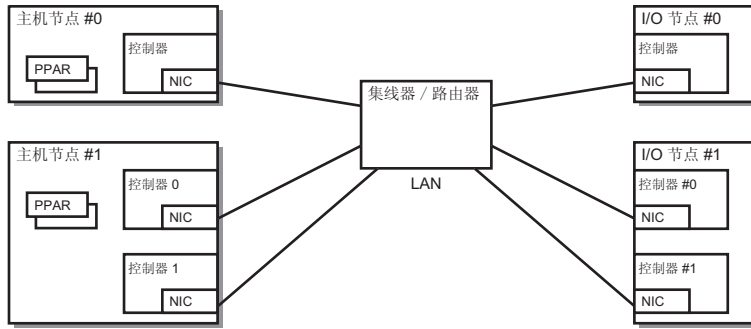
图 14-6 远程电源管理的连接形式



复制控制器时的连接

当主机节点的控制器被复制时，每个控制器都可以连接到同一 LAN。从主 XSCF 执行远程电源管理的操作。

图 14-7 复制控制器时的远程电源管理连接形式



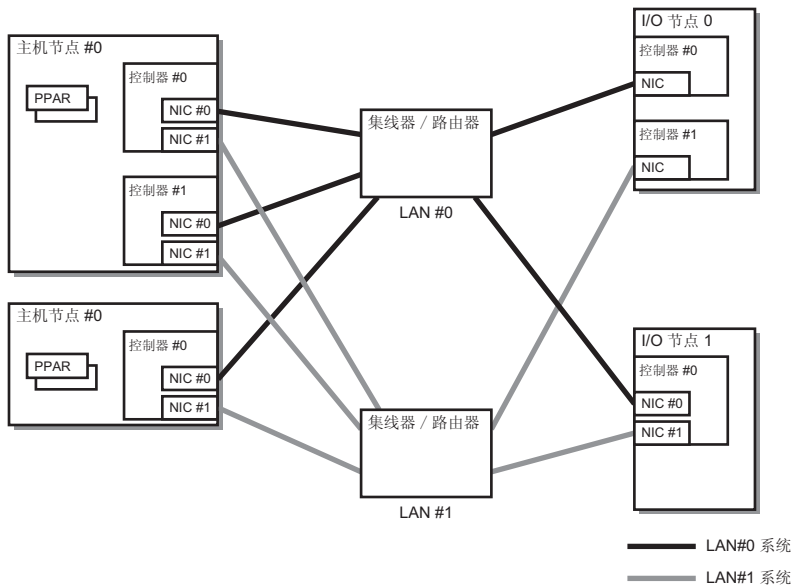
注 - 当控制器被复制时，如果 LAN 卡的 IP 地址在控制器之间被共享为虚拟 IP，则配置其中任意一个控制器。

复制路径时的连接

如果满足以下条件，可以复制远程电源管理的连接路径。

- 当两个 LAN 卡可被安装到所有节点的各个控制器上时
- 当两个 LAN 卡可被安装到主机节点的控制器上，I/O 节点具有以下两个配置中的一个时
 - I/O 节点的控制器被复制
 - 两个 LAN 卡可被安装到 I/O 节点的控制器上

图 14-8 复制路径时的远程电源管理的连接形式



— LAN#0 系统
— LAN#1 系统

14.6.3 远程电源管理的结构

由远程电源管理组控制 SPARC M12/M10 的远程电源管理。

对于组中的主机节点，启用远程电源管理功能的主机节点将会成为远程电源管理的对象。远程电源管理组的电源状态由组中的主机节点状态确定。

- 开状态
当远程电源管理组中任何一个主机节点的电源状态是开启时
- 关状态
当远程电源管理组中所有主机节点的电源状态都是关闭时

本节将基于以下设置介绍远程电源开启和电源关闭的管理结构。

表 14-14 远程电源管理的结构（示例）

设置项目	主机节点 #0	主机节点 #1	主机节点 #2	I/O 节点 #0	I/O 节点 #1
远程管理设置	Disable	Enable	Enable	设置被禁用	设置被禁用
主节点	Yes	No	Yes	设置被禁用	设置被禁用

电源开启时的联锁机制

如果远程电源管理组中的任何主机节点的电源开启，则所有的主机节点、子节点以及组中的 I/O 节点的电源都开启。开启主机节点的电源，然后开启 I/O 节点。

注 - 您可以设置主机节点的等待时间，直至可以访问 I/O 节点设备。使用 XSCF 固件的 `setpowerupdelay` 命令进行设置。有关详情，请参见“4.2.2 设置/确认启动等待时间”。如果不设置等待时间，则当主机节点尝试访问不可访问的 I/O 节点设备时，系统可能无法启动。此外，如果 I/O 节点被切换或设置发生变化，则访问设备的时间也发生变化。因此，当主机节点试图访问这些设备时，该设备可能无法被访问。如果您已经切换 I/O 节点或变更了设置，则需使用 `setpowerupdelay` 命令来设置一个新的等待时间。

远程电源关闭管理的结构

关闭远程电源管理组中的所有主机节点的电源，然后关闭该组中的所有 I/O 节点的电源。

通过 LAN 唤醒远程电源管理

通常，SPARC M12/M10 远程电源管理功能的目标节点是安装有控制器的主机和 I/O 设备。即使主机和 I/O 设备的电源处于关闭状态，控制器也可以进行 IPMI 通讯。当满足以下所有条件时，不安装这种控制器的设备也可以使用 SPARC M12/M10 的远程电源管理功能远程管理电源。

- 设备条件
 - 支持 LAN 唤醒。
使用 LAN 唤醒执行上电。
 - 可执行 IPMI 通讯。
使用 LAN 唤醒上电后，通过 LAN 的 IPMI 通讯被用于执行断电并获取电源的状

态。

注 - 已为其设置 Wake on LAN 的主机节点不能成为主节点。

注 - 无法对 SPARC M12/M10 机箱设置 LAN 唤醒。因此，无法使用 LAN 唤醒功能对 SPARC M12/M10 机箱上电。

注 - 根据节点的不同，LAN 唤醒的设置将变化各异。请参见各节点的手册。

故障恢复时的联锁

如果从故障或其他问题恢复时远程电源管理组中的节点无法通讯，则按下述方法进行操
作。

- 在 I/O 节点故障的情况下
如果远程电源管理组的电源状态是开状态，主要主机节点发出开启电源指令。
- 在主机节点故障的情况下
即使远程电源管理组的电源状态是开状态，主要主机节点也不发出开启电源指令。

14.6.4 设置远程电源管理之前

如果您设置远程电源管理，则需提前连接 LAN 线并在执行远程电源管理的 XSCF-
LAN 和 I/O 设备上配置网络设置。

14.6.5 设置远程电源管理的流程

本节分以下几种情况介绍设置远程电源管理的流程:

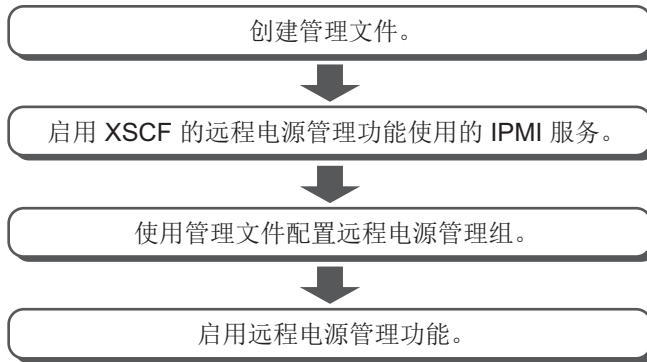
- 首次设置远程电源管理功能
- 在现有远程电源管理组中添加、删除或更换节点

首次设置远程电源管理

下图介绍首次设置远程电源管理的流程。

注 - 如果启用现有的远程电源管理设置，则初始化该远程电源管理的设置。

图 14-9 首次设置远程电源管理的流程

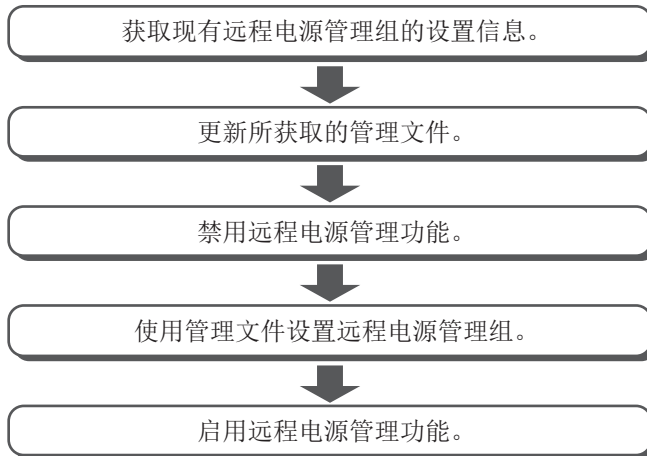


注 - XCP 2290 和更高版本支持 IPMI 服务的启用/禁用设置。

在现有远程电源管理组中添加、删除或更换节点

下图介绍在现有远程电源管理组中添加、删除或更换节点的流程。

图 14-10 在现有远程电源管理组中添加、删除或更换节点的流程



14.6.6 检查远程电源管理设置

使用 XSCF 固件的 `showremotepwrmgmt` 命令检查远程电源管理的设置。

```
XSCF> showremotepwrmgmt [-a|-G groupid [-N gnodeid]]
```

若需检查所有远程电源管理的设置，请指定 `-a`。若需指定远程电源管理组，请指定 `-G`

groupid。若需指定远程电源管理组中的节点，请指定 -N gnodeid。

14.6.7 初始化远程电源管理设置

使用 XSCF 固件的 clearremotepwrmgmt 命令初始化远程电源管理的设置。

```
XSCF> clearremotepwrmgmt [-a|-G groupid]
```

如需初始化所有远程电源管理组的设置，请指定 -a。若需指定远程电源管理组，请使用 -G 选项指定组 ID。如果省略 -a 和 -G，系统将假设指定了 -a。

14.6.8 启用/禁用远程电源管理功能

使用 XSCF 固件的 setremotepwrmgmt 命令启用/禁用远程电源管理功能。

```
XSCF> setremotepwrmgmt -c enable|disable
```

若需启用远程电源管理功能，请指定 -c enable。如需将其禁用，请指定 -c disable。

14.6.9 创建管理文件

可采用 csv 格式创建用于设置远程电源管理组的管理文件。可以在通过 http、https、ftp 或文件访问的 URL 位置，创建并存储管理文件。
管理文件的描述格式如下。

```
1,1,0x01,8a041209b35947899e7bfa5d578dbd3f,0x03,0x00,default,,10.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,"4,5,6,7,8,9,10,11,12"  
1,2,0x00,8a041209b35947899e7bfa5d578dbd40,0x03,0x00,default,,10.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,  
1,3,0x10,8a041209b35947899e7bfa5d578dbd41,0x03,0x00,default,,10.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,(略)  
1,128,0x20,8a041209b35947899e7bfa5d578dbd42,0x03,0x00,default,,10.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,
```

按照以下顺序在每行中指定以下内容： GroupID, NodeID, NodeType, NodeIdentName, Linkage, Operation, User, Password, IP0-0, Slave0-0, MAC0-0, IP0-1, Slave0-1, MAC0-1, IP1-0, Slave1-0, MAC1-0, IP1-1, Slave1-1, MAC1-1 和 SubNode。

设置项目的详情如下。

表 14-15 远程电源管理的管理文件的设置项目

项目	说明
GroupID	远程电源管理组的组 ID 您可以指定 1 到 32 间的一个整数（十进制）。一个管理文件中的所有组 ID 必须相同。
NodeID	远程电源管理设备的节点 ID 您可以指定 1 到 128 间的一个整数（十进制）。一个管理文件中的节点 ID 必须唯一。
NodeType	远程电源管理设备的节点类型 指定以下任何值。 0x00: 主机节点, 0x01: 主要主机节点, 0x10: I/O 节点, 0x20: 远程电源管理盒
NodeIdentName	远程电源管理设备的专有名称 您可以指定 System GUID 或任何唯一的字符串。 如示例中所示, System GUID 被指定为 32 个连续的数字。该值被处理为十六进制, 忽略大小写。 在任何字符串的情况下, 可以使用最多 32 位十六进制指定该值。
Linkage	表示远程电源开启管理的值（十六进制） 指定以下任何值。 0x00: 禁用, 0x01: 启用 (On), 0x02: 启用 (Off), 0x03: 启用 (On+Off)
Operation	表示电源开启方法的值 使用如下方法之一指定。 0x00: IPML, 0x01: WakeOnLAN
User	IPMI 用户名 不指定任何内容请将其留白。如果不留白, 则无法保证操作。
Password	IPMI 密码 不指定任何内容请将其留白。
IPAddress	控制器的 IPMI 的 IP 地址 可以用字符串指定一个 IPv4 地址。
SlaveAddress	表示控制器的 IPMI 从地址的值（十六进制） 指定为 "0x20"。
SubNodeID	表示控制对象的子节点 ID 的字符串 0 至 31, 或留白。 可以通过用逗号 (,) 分隔, 并用双引号 (") 将整个值括起来指定对象的子节点 ID（十进制）。 留白表示整个节点是控制对象。

14.6.10 启用/禁用 XSCF 的远程电源管理功能使用的 IPMI 服务

如需使用远程电源管理功能, 您必须启用 IPMI 服务。
IPMI 服务仅由远程电源管理功能使用。
在 XSCF 上使用 `setpacketfilters` 命令可启用/禁用 IPMI 服务。

```
XSCF> setpacketfilters -c ipmi_port [enable|disable]
```

如需启用 IPMI 服务，需指定 `-c ipmi_port enable`。如需将其禁用，请指定 `-c ipmi_port disable`。
默认值为禁用。

注 - XCP 2290 和更高版本支持 IPMI 服务的启用/禁用设置。

在 XCP 2280 以及更早版本中，IPMI 服务已启用，并且您无法禁用。

如果将固件从 XCP 2280 或更早版本更新到 XCP 2290 或更高版本，则需将 IPMI 服务设置如下：

- 当使用远程电源管理功能时：enable。
- 当不使用远程电源管理功能时：disable。

14.6.11 获取远程电源管理组的设置信息

使用 XSCF 固件的 `getremotepwrmgmt` 命令获取远程电源管理组的设置信息。

```
XSCF> getremotepwrmgmt -G groupid configuration_file
```

对于 `groupid`，您可以指定获取设置信息的远程电源管理组的 ID。对于配置文件，您可以指定存储所获取的设置信息的管理文件的名称。

14.6.12 设置远程电源管理组

使用管理文件配置远程电源管理组时，请使用 `setremotepwrmgmt` 命令。

```
XSCF> setremotepwrmgmt -c config configuration_file
```

如果配置远程电源管理组，您可以指定 `-c config`。对于 `configuration_file`，您可以指定用于配置的管理文件的名称。

14.7 使用不间断电源

作为选配，SPARC M12/M10 支持连接不间断电源 (UPS)。

使用不间断电源 (UPS) 可在电源出现故障、停电等情况下，保持系统供电稳定。支持 APC 制造的不间断电源 (UPS)，将 LAN 用作域和 UPS 之间的接口。

有关如何连接不间断电源的详情，请参见所使用服务器的《安装指南》中的“不间断电源 (UPS) 连接（选配）”。

14.8 使用验证启动

本节介绍当 Oracle Solaris 启动时，可提供安全保护的验证启动功能。

14.8.1 验证启动基础知识

验证启动是一种功能，可以保护 SPARC M12/M10 免受可能存在于驱动程序、模块或 Oracle Solaris 启动时加载的其他程序的威胁。

对系统的启动过程进行验证，并确保免于以下威胁：

- 损坏内核模块
- 插入伪装成合法内核模块的恶意程序（木马病毒、间谍软件、后门程序等），或以此类程序替换一个程序
- 加载未经批准的第三方内核模块

Oracle Solaris 11.2 提供了两种配置验证启动功能的方法：使用 XSCF 和使用 Oracle Solaris。在 Oracle Solaris 11.3 或更高版本中，仅使用 XSCF 的配置方法可用。本节介绍使用 XSCF 配置该功能的方法。有关使用 Oracle Solaris 配置该功能的方法，请参见 Oracle Solaris 的《Securing Systems and Attached Devices in Oracle Solaris 11.2》中的 "How to Enable Verified Boot on Legacy SPARC Systems and x86 Systems"。

14.8.2 验证启动启动验证的机制

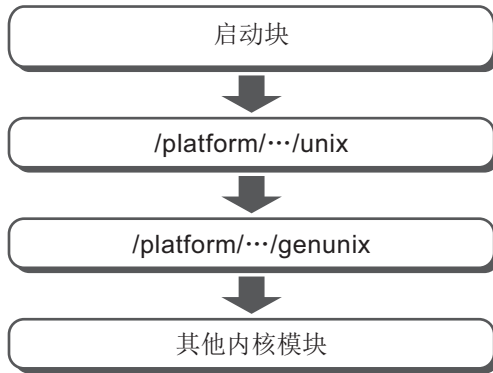
验证启动启动验证需要使用 XSCF 注册的 X.509 公共密钥证书。系统的启动过程通过使用包含在 X.509 公共密钥证书中的公共密钥执行启动验证。

执行启动验证的机制如下：

- 用户使用支持验证启动功能的 XSCF 配置验证启动。在此配置作业中，用户注册或选择 X.509 公共密钥证书，并设置用于控制启动验证操作的策略。配置信息保存在主 XSCF 中。
- 假设 XSCF 中的验证启动配置信息发生变化。变更后的配置信息将在下一次 OpenBoot PROM 启动时，对所有模块的启动验证有效。
- 当物理分区启动时，将配置信息通过 XSCF 报告给 OpenBoot PROM 固件和 Oracle Solaris，然后它们执行启动验证。在物理分区、OpenBoot PROM 固件或 Oracle Solaris 重新启动时也执行启动验证。

OpenBoot PROM 固件和 Oracle Solaris 的启动验证按照 [图 14-11](#) 中显示的顺序执行。

图 14-11 启动验证的顺序



14.8.3 验证启动用 X.509 公共密钥证书

表 14-16 显示了用于验证启动的两种类型的 X.509 公共密钥证书。

表 14-16 用于验证启动的 X.509 公共密钥证书

证书类型	说明
系统默认证书 (系统默认)	XSCF 设有系统默认证书 XSCF 设有与 Oracle Solaris 中包含的公共密钥证书 (/etc/certs/*SE) 相同的证书。 XSCF 设有 1 个或 2 个系统默认证书，固件更新时采用最新公共密钥证书进行更换。 因此，系统默认证书没有保存/恢复问题。另外，用户不可对系统默认证书进行篡改。
用户证书	用户注册的证书 使用 XSCF 由第三方颁发的证书被注册为用户证书。 使用 XSCF 对各物理分区最多可注册 5 个用户证书。当启用时，所注册的证书可用于启动验证。 用户证书没有保存/和在系统上恢复的问题。但是，所保存的证书无法在其他 SPARC M12/M10 中恢复。

通过使用系统默认证书来执行启动验证，并启用用户证书。

14.8.4 验证启动策略

表 14-17 列出了控制验证启动的两个策略。

表 14-17 验证启动策略

OS 版本	策略	说明
Oracle Solaris 11.2	启动策略 (boot_policy)	设置启动块、unix 和 genunix 的启动验证。启动过程中将首次加载这些模块。
	模块策略 (module_policy)	设置需要在 genunix 后加载的内核模块的启动验证。
Oracle Solaris 11.3	启动策略 (boot_policy)	设置启动块和 unix 的启动验证。启动过程中将首次加载这些模块。
	模块策略 (module_policy)	设置 genunix 和内核模块的启动验证。

使用 XSCF 固件的 setvbootconfig 命令设置每个策略。

用户可以通过设置策略来设置启动验证失败时启动过程的操作。

表 14-18 列出了可以设置为每个启动策略和模块策略的值。设置值决定了验证操作。

表 14-18 策略设置值

策略设置值	操作
none	不执行启动验证。(默认)
warning	<p>执行启动验证。</p> <p>验证目标加载之前，执行验证。即使验证失败，也加载验证目标，并且启动处理继续。如果启动块和 unix 的验证失败，系统控制台上将记录该验证失败。验证失败不记录在系统日志中，也不记录在 XSCF 错误日志中。</p> <p>如果 genunix 和其他内核模块的验证失败，系统控制台和系统日志中都将记录该验证失败。验证失败不记录在 XSCF 错误日志中。</p>
enforce	<p>执行启动验证。</p> <p>验证目标加载之前，执行验证。</p> <p>如果启动块和 unix 的验证失败，启动处理将停止。此时，验证失败记录在系统控制台和 XSCF 错误日志中。该验证失败不记录在系统日志中。</p> <p>如果 genunix 的验证失败，启动处理将停止。此时，验证失败记录在系统控制台上。该验证失败不记录在 XSCF 错误日志中，也不记录在系统日志中。</p> <p>如果其他内核模块的验证失败，启动将继续，但不加载该模块。此时，验证失败记录在系统控制台和系统日志中。验证失败不记录在 XSCF 错误日志中。</p>

注 - 在 Oracle Solaris 11.2 SRU11.2.8.4.0 或更高版本中，如果策略设置值是 enforce，genunix 验证失败后的操作会不同。如果 OpenBoot PROM 环境变量 auto-boot? 为真，会反复发生崩溃。如果这种现象持续存在，可对控制域执行 sendbreak 命令，对来宾域执行 ldm stop 命令，或对内核区执行 zoneadm halt 命令来阻止此现象。

表 14-19 显示了启动验证失败时输出的消息示例。

表 14-19 启动验证失败时消息输出的示例

策略设置值	消息
none	不执行启动验证。
warning	出现以下警告消息，但 Oracle Solaris 的启动继续。 - genunix 情况下的系统控制台消息 WARNING: module /platform/sun4v/kernel/sparcv9/genunix failed elfsign verification. - 其他内核模块情况下的系统控制台或系统日志 WARNING: module /kernel/drv/sparcv9/module failed elfsign verification.
enforce	- 在启动块的情况下 出现以下错误消息，启动停止在 ok 提示符。 - 系统控制台消息 FATAL: Bootblk signature verification failed, verified boot policy = enforce, halting boot - XSCF 错误日志 boot process failed - 其他内核模块情况下的系统控制台或系统日志 出现以下错误消息，但 Oracle Solaris 的启动继续。 Module /kernel/drv/sparcv9/module failed elfsign verification; "module-policy enforce" requested.

14.8.5 支持验证启动的 Oracle Solaris 和 XCP 的版本

表 14-20 列出了支持验证启动的 Oracle Solaris 和 XCP 的版本。当满足表 14-20 中的这两个条件时，可以使用验证启动。

表 14-20 可使用验证启动的 Oracle Solaris 和 XCP 的版本

Oracle Solaris 和 XCP	版本
Oracle Solaris	11.2 或更高版本
XCP	2250 或更高版本

Oracle Solaris 设置中的验证启动仅适用于 XCP 2240 或更早版本和 Oracle Solaris 11.2 的组合。

在 XCP 2250 或更高版本中，操作基于 XSCF 中的配置信息。从 XCP 2240 或早期版本到 XCP 2250 或更高版本的固件更新将对 XSCF 的验证启动策略设置默认的"none"。即使在 Oracle Solaris 上配置设置时，此设置也优先。如需使用验证启动，请使用 XSCF 进行策略设置。

14.8.6 验证启动支持的范围

在来宾域和内核区上的验证启动

仅 Oracle Solaris 11.2 中的全局区域支持验证启动。除此之外，Oracle Solaris 11.3 或更高版本的内核区域支持验证启动。有关在内核区域配置验证启动的详细信息，请参见

《Creating and Using Oracle Solaris Kernel Zones》。有关在来宾域配置验证启动的详细信息，请参见《Oracle VM Server for SPARC 3.4 Administration Guide》中的 "Using Verified Boot"。

启动设备和验证启动策略的设置

验证启动支持从硬盘驱动器 (HDD) 启动和从网络启动。其它的启动方式，需将验证启动策略设置为 "none"。

此外，执行验证启动时，确保从签署的设备执行启动。否则，验证启动的启动验证将失败。

表 14-21 显示了验证启动支持的范围。

表 14-21 验证启动支持的范围

	控制域		来宾域	
	全局区域	内核区	全局区域	内核区
从 HDD 启动	Oracle Solaris 11.2 或更高版本 (*1) XCP 2250 或更高版本	Oracle Solaris 11.3 或更高版本 XCP 2250 或更高版本	控制域: Oracle Solaris 11.3 SRU11.3.8.7.0 或更高版本 来宾域: Oracle Solaris 11.2 或更高版本 XCP 2280 或更高版本	Oracle Solaris 11.3 或更高版本 XCP 2250 或更高版本
从网络启动	Oracle Solaris 11.2 或更高版本 (*1) XCP 2320 或更高版本	-	控制域: Oracle Solaris 11.3 SRU11.3.8.7.0 或更高版本 来宾域: Oracle Solaris 11.2 或更高版本 XCP 2320 或更高版本	-

*1 使用 XSCF 中的设置，忽略 Oracle Solaris 中的设置。

14.8.7 注意事项和限制

使用验证启动时，请注意以下方面。

OpenBoot PROM 环境变量 use-nvramrc? 的设置值

如需使用验证启动，请将 OpenBoot PROM 环境变量 use-nvramrc? 的值设置为 "false"。如果将该变量设置为 "true" 时使用验证启动，启动验证将失败。根据启动策略设置值，启动验证失败时可以执行表 14-22 中列出的操作。

表 14-22 use-nvramrc? 为 "true" 时的启动验证操作

启动策略设置值	操作
none	不执行启动验证。

表 14-22 use-nvramrc? 为 "true" 时的启动验证操作 (续)

启动策略设置值	操作
warning	出现以下消息，Oracle Solaris 启动。 use-nvramrc? variable is set, continuing with signature verification
enforce	出现以下消息，启动停止在 ok 提示符。此外，XSCF 登记 "boot process failed" 错误日志。 use-nvramrc? variable is set, verified boot policy = enforce, halting boot

在 OpenBoot PROM ok 提示符下设置验证启动配置

假设您从 OpenBoot PROM ok 提示符变更 XSCF 中的验证启动配置信息，然后启动 Oracle Solaris。变更后的配置信息仅对 genunix 和其他内核模块有效。变更后的配置信息将在下一次 OpenBoot PROM 启动时，对所有模块有效。

14.8.8 查看验证启动相关的设置项目和命令

表 14-23 列出了与验证启动相关的设置项目以及对应的 XSCF shell 命令。配置各物理分区的验证启动。

表 14-23 配置验证启动相关的命令

设置项目	相关命令
注册/删除/查看证书	addvbootcerts(8), deletevbootcerts(8), showvbootcerts(8)
设置/查看配置信息 - 选择证书 - 设置启动和模块策略	setvbootconfig(8), showvbootconfig(8)

注 - 在对物理分区的 power-on 或 power-off 处理正在进行中时，请勿执行 setvbootconfig 命令。否则，该命令将错误结束。

14.8.9 验证启动的设置流程

图 14-12 显示了设置使用验证启动的流程。

图 14-12 使用启动验证时的设置流程

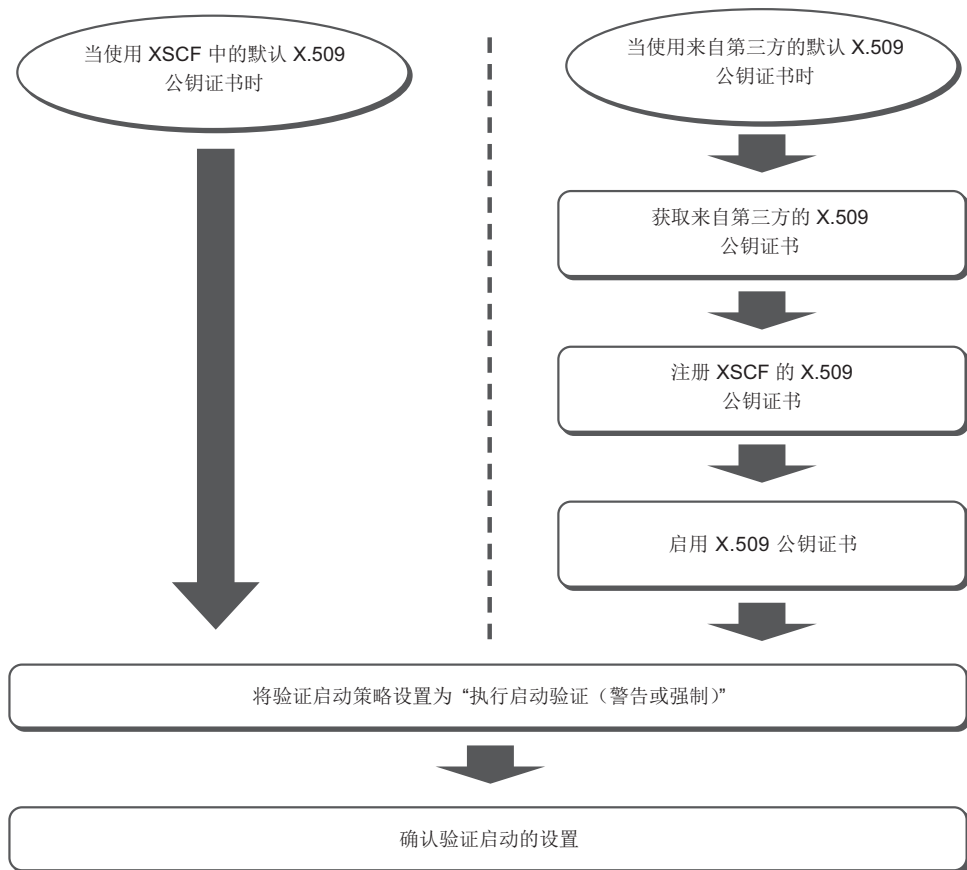
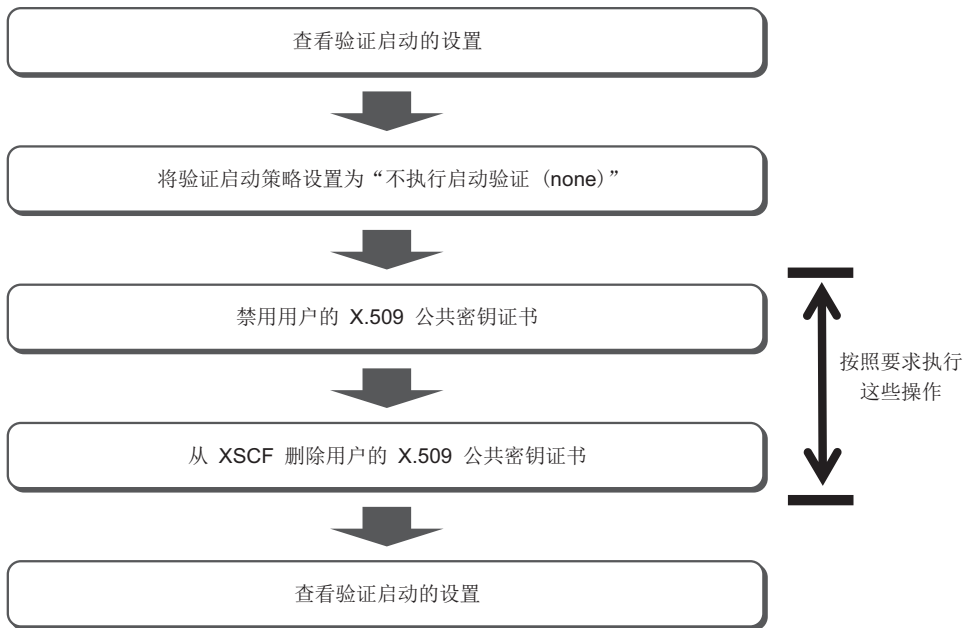


图 14-13 显示了不使用通过验证启动的启动验证时的设置流程。

图 14-13 不执行启动验证时的设置流程



14.8.10 注册 X.509 公共密钥证书

使用 `addvbootcerts` 命令在 XSCF 注册 X.509 公共密钥证书。请使用拥有 `platadm` 或 `pparadm` 权限的用户帐户执行 `addvbootcerts` 命令。

```
XSCF> addvbootcerts -p ppar_id certname {-F URL | signature}
```

`ppar_id` 用于指定目标物理分区。`certname` 用于指定需要注册的 X.509 公共密钥证书的名称。如需指定公共密钥证书，请复制和粘贴公共密钥证书的内容，或者从 USB 介质或指定 `-F` 选项的 `http/https` 服务器进行读取。

公共密钥证书使用 XSCF 注册为用户证书。最多可注册五个公共密钥证书。

在下面的示例中，指定公共密钥证书存储在 USB 介质。

```
XSCF> addvbootcerts -p ppar_id certname -F file:///media/usb_msd/file
```

注 - 使用 XSCF Web 也可注册 X.509 公共密钥证书。

注 - 逐个指定它们来注册 X.509 公共密钥证书。您无法在同一时间指定多个公共密钥证书。

注 - 在如果需要注册的公共密钥证书的数据格式是除 X.509 之外的格式以及如果数据损坏等情况下，公共密钥证书无法使用 XSCF 注册。addvbootcerts 命令导致错误。

注 - 系统默认证书是 XSCF 默认设有的一个公共密钥证书。X.509 公共密钥证书无法注册为系统默认证书。

操作步骤

1. 登录 **XSCF**。
有关详情，请参见 "2.2 登录 XSCF Shell"。
2. 执行 **addvbootcerts** 命令在 **XSCF** 注册用户证书。
在下面的示例中，将存储在 USB 介质上的 X.509 公共密钥证书添加到名为 "CUSTOM_CERT_2" 的 PPAR-ID 4。以“y（是）”响应确认消息。

```
XSCF> addvbootcerts -p 4 CUSTOM_CERT_2 -F file:///media/usb_msd/vboot/3rd_party_
cert_xyz
The above elfsign X.509 key certificate will be added to PPAR-ID 4,
Continue?[y|n]:y
.... done.
successfully added this certificate to PPAR-ID 4 as index 2.
```

3. 执行 **showvbootcerts** 命令确认 **X.509** 公钥证书已被正确注册到 **XSCF**。
在下面的示例中，显示 PPAR-ID 4 中注册为索引编号 2 的 X.509 公共密钥证书的详细信息。

```
XSCF> showvbootcerts -v -p 4 -u -i 2
-----
PPAR-ID 4 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution,
CN=www.example.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:de:f0:2c:45:61:7f:10:c7:16:56:a9:14:b4:a4:
      39:44:b9:2f:65:4f:7e:a7:c0:15:89:b0:e2:1d:c0:
      25:4c:a6:31:75:14:a3:c4:cd:11:d2:87:b7:1a:7c:
      b2:0d:41:99:4f:a6:e9:d4:8e:77:55:19:ce:f1:a4:
      3c:cf:00:8d:e6:d1:c6:bc:06:f7:71:85:28:a4:c5:
      e0:8d:b3:e1:62:25:d5:df:93:d2:d9:1c:5b:48:35:
      70:e1:8a:9b:bf:9d:8b:41:b3:be:b6:c0:50:66:3b:
```



```
d8:9d:2f:82:49:11:f7:6d:43:95:6e:ea:bc:57:dc:
1c:90:6b:7e:8b:e3:0f:89:bd:32:3a:88:50:f0:48:
d3:98:8c:bc:eb:7f:44:31:2b:86:01:d0:80:4c:a2:
36:6e:24:47:48:d5:86:8e:86:06:c3:8e:df:5f:fb:
6b:fe:6a:aa:0c:a8:ca:b6:ed:60:47:ea:8e:5d:63:
b1:4f:ff:94:00:34:52:82:cf:a6:6a:84:69:4c:26:
ac:a3:dc:d7:45:eb:7c:4e:fc:fc:92:4a:73:12:9f:
31:7a:75:b9:de:33:54:34:af:0b:cf:46:c0:ac:2f:
ec:28:af:0d:f7:c6:50:c0:e7:4c:88:16:13:95:54:
0e:01:6e:1a:b6:33:bf:20:52:34:f4:69:a6:9e:bf:
02:95
```

Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

```
44:65:95:e1:33:a4:ce:d1:c1:02:1a:ce:b3:2c:fa:c0:b2:34:
4e:12:d0:86:c7:09:23:9d:5b:46:f4:b2:bf:88:8b:5b:5d:d7:
57:c3:f9:9a:ba:95:bc:ed:4b:29:4b:19:97:ca:6c:bc:e1:44:
e0:e1:89:a3:ed:bd:29:ad:a7:91:c8:76:ea:62:d2:2c:e3:ff:
50:01:0a:3b:5a:28:53:38:53:82:ea:de:bc:24:84:bc:31:63:
ab:b2:10:81:81:73:f4:02:46:5f:2d:6d:22:b0:af:d7:70:c0:
db:de:ea:b9:23:87:3c:19:ef:c0:24:de:05:77:eb:89:d2:36:
d0:85:8a:ed:d1:7f:12:b0:58:5f:f5:53:f1:db:0b:44:53:a0:
72:8c:1a:e6:4a:fd:e8:8e:f8:ee:9e:7e:4e:85:59:42:44:fa:
1f:d3:70:4f:81:95:8e:a9:0f:83:49:a2:b0:fd:5b:f4:2d:5e:
86:ef:f3:56:b3:31:f3:58:3a:37:42:bb:39:c4:c1:b5:8c:e9:
b4:01:d2:2e:e8:7d:86:1a:66:88:34:1e:e5:36:ee:6d:6c:90:
78:45:a0:5b:a9:50:84:62:a8:88:ee:a6:70:fa:7c:ad:81:b7:
89:f1:d6:64:94:c4:17:69:c8:35:81:b2:f3:79:ad:a2:5a:a0:
02:28:a9:7f
```

4. 执行 **exit** 命令从 **XSCF shell** 注销。

如您在 **XSCF shell** 没有更多的任务，请从 **XSCF** 注销。如需继续配置其他设置，请执行相关步骤的操作。

注 - 如果 X.509 公钥证书信息被意外的操作破坏，**XSCF** 可能要求认证公钥。为了能够恢复，确保安全保管公钥证书。

14.8.11 启用/禁用已注册的 X.509 公共密钥证书

如需使用已经注册的用户 X.509 公共密钥证书，请从 **XSCF shell** 执行 **setvbootconfig** 命令来启用公共密钥证书。请使用拥有 **platadm** 或 **pparadm** 权限的用户帐户执行 **setvbootconfig** 命令。

在下例中，启用禁用的公钥证书。

```
XSCF> setvbootconfig -p ppar_id -i index -c enable
```

ppar_id 用于指定目标物理分区。**index** 用于指定启用的用户证书的索引号。

您可以使用用户证书列表查看索引编号以及公共密钥证书是否启用/禁用。如需查看用户证书列表，请执行指定 **-a** 选项的 **showvbootcerts** 命令。

```
XSCF> showvbootcerts -p ppar_id -a
```

在下面的示例中，将已启用的公共密钥证书禁用。

```
XSCF> setvbootconfig -p ppar_id -i index -c disable
```

ppar_id 用于指定目标物理分区。**index** 用于指定启用的用户证书的索引号。

注 - 您也可以使用 XSCF Web 启用/禁用 X.509 公共密钥证书。

注 - 在物理分区关闭或 Oracle Solaris 在逻辑域上运行时，您可以启用/禁用 X.509 公共密钥证书。如果物理分区或逻辑域处于启动或停止过程中，将发生错误。完成启动或停止后，再次执行该操作。

注 - 系统默认证书是 XSCF 默认设有的一个公共密钥证书。系统默认的证书无法启用/禁用。

操作步骤

1. 登录 **XSCF**。
有关详情，请参见 ["2.2 登录 XSCF Shell"](#)。
2. 执行 **showvbootcerts** 命令查看需要使用的用户证书的索引编号以及证书是否启用。
如果注册的公共密钥证书已经启用，将不需要后续步骤。
在下面的示例中，显示了所有在 PPAR-ID 2 中注册的 X.509 公共密钥证书。

```
XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
```

```

Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Disable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----

```

3. 执行 **setvbootconfig** 命令以启用公钥证书。

在下面的示例中，启用了 PPAR-ID 2 中注册为索引编号 5 的 X.509 公共密钥证书。以“y（是）”响应确认消息。

```

XSCF> setvbootconfig -p 2 -i 5 -c enable
Index 5, CUSTOM_CERT_5 on PPAR-ID 2 will be enabled,
Continue?[y|n]: y

```

4. 执行 **showvbootcerts** 命令，并确认公钥证书已启用。

在下面的示例中，可以确认启用了 PPAR-ID 2 中注册为索引编号 5 的 X.509 公共密钥证书。

```

XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70

```

```
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
```

```
-----
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Enable]
-----
```

Data:

```
Version: 3 (0x2)
Serial Number:
  07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
```

5. 执行 **exit** 命令从 **XSCF shell** 注销。

如您在 XSCF shell 没有更多的任务，请从 XSCF 注销。如需继续配置其他设置，请执行相关步骤的操作。

14.8.12 删除已注册的 X.509 公共密钥证书

如需将系统的公钥证书删除，请使用 XSCF shell 的 `deletevbootcerts` 命令。如需从系统中将 X.509 公共密钥证书删除，请使用 XSCF shell 的 `deletevbootcerts` 命令。请使用拥有 `platadm` 或 `pparadm` 权限的用户帐户执行 `deletevbootcerts` 命令。在公共密钥证书禁用时，您可以删除公共密钥证书。

```
XSCF> deletevbootcerts -p ppar_id -i index
```

`ppar_id` 用于指定目标物理分区。`index` 用于启用的用户证书的索引号。可以从执行指定 `-a` 选项的 `showvbootcerts` 命令所输出的用户证书列表中查看索引编号。

```
XSCF> showvbootcerts -p ppar_id -a
```

注 - 在公共密钥证书启用时，您无法删除公共密钥证书。使用 `setvbootconfig` 命令禁用后将其删除。请参见“[14.8.11 启用/禁用已注册的 X.509 公共密钥证书](#)”。

注 - 您也可以使用 XSCF Web 启用/禁用 X.509 公共密钥证书。

注 - 系统默认证书是 XSCF 默认设有的一个公共密钥证书。系统默认的证书无法删除。

操作步骤

1. 登录 **XSCF**。

有关详情，请参见 "2.2 登录 XSCF Shell"。

2. 执行 **showvbootcerts** 命令查看需要删除的用户证书的索引编号以及证书是否禁用。

在公共密钥证书启用时，您无法删除公共密钥证书。执行 **setvbootconfig** 命令以禁用。

在下面的示例中，显示了所有在 PPAR-ID 2 中注册的 X.509 公共密钥证书。

```
XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
```

3. 执行 **deletevbootcerts** 命令以删除公钥证书。

在下面的示例中，删除了 PPAR-ID 2 中注册为索引编号 5 的 X.509 公共密钥证书。以“y（是）”响应确认消息。

```
XSCF> deletevbootcerts -p 2 -i 5
Index 5, CUSTOM_CERT_5 will be deleted from PPAR-ID 2,
Continue?[y|n]: y
```

4. 执行 **showvbootcerts** 命令以确认公钥证书已被删除。
在下面的示例中，显示了所有在 PPAR-ID 2 中注册的 X.509 公共密钥证书。您可以看到索引编号 5 的公共密钥证书已经删除。

```
XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
Version: 3 (0x2)
Serial Number:
0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris Signed
Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
Version: 3 (0x2)
Serial Number:
07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
```

5. 执行 **exit** 命令从 **XSCF shell** 注销。
如您在 XSCF shell 没有更多的任务，请从 XSCF 注销。如需继续配置其他设置，请执行相关步骤的操作。

14.8.13 查看已注册的 X.509 公共密钥证书

使用 **showvbootcerts** 命令查看使用 XSCF 注册 X.509 公共密钥证书的信息。

如果您需要查看所有已注册的 X.509 公共密钥证书列表，请指定目标物理分区和 **-a** 选项。这将显示系统默认证书和用户证书列表。您也可以通过指定 **-v** 选项查看详细信息。

```
XSCF> showvbootcerts -p ppar_id -a
```

如需查看系统默认证书的信息，请指定目标物理分区、`-s` 选项以及系统默认证书的索引编号。您也可以通过指定 `-v` 选项查看详细信息。

```
XSCF> showbootcerts -p ppar_id -s -i index
```

如需查看使用 `addvbootcerts` 命令注册的用户证书的信息，请指定目标物理分区、`-u` 选项以及用户证书的索引编号。您也可以通过指定 `-v` 选项查看详细信息。

```
XSCF> showbootcerts -p ppar_id -u -i index
```

注 - 您也可以使用 XSCF Web 查看 X.509 公共密钥证书。

14.8.14 设置验证启动策略

在 XSCF shell 中使用 `setvbootconfig` 命令设置验证启动策略。请使用拥有 `platadm` 或 `pparadm` 权限的用户帐户执行此命令。

```
XSCF> setvbootconfig -p ppar_id -s policy=value
```

`ppar_id` 用于指定目标物理分区。`policy` 用于指定启动策略 "boot_policy" 或模块策略 "module_policy"。`value` 用于指定 "none"、"warning" 或 "enforce"。有关详情，请参见 "14.8.4 验证启动策略"。

操作步骤

1. 登录 XSCF。
有关详情，请参见 "2.2 登录 XSCF Shell"。
2. 执行 `showvbootconfig` 命令查看验证启动策略的设置值。
如果该策略设置被设置为所需的值，则不必设置一个策略。

```
XSCF> showvbootconfig -p ppar_id
```

3. 执行 `showvbootconfig` 命令设置验证启动策略。输入 "y"，确认信息。
下面的示例中，在 PPAR-ID 2 中将启动策略 (`boot_policy`) 设置为 "warning"，将模块策略 (`module_policy`) 设置为 "enforce"。

```
XSCF> setvbootconfig -p 2 -s boot_policy=warning  
XSCF> setvbootconfig -p 2 -s module_policy=enforce
```

4. 执行 `showvbootcerts` 命令确认验证启动策略的设置值已经变更。

```
XSCF> showvbootconfig -p ppar_id
```

5. 执行 **exit** 命令从 **XSCF shell** 注销。
如您在 XSCF shell 没有更多的任务，请从 XSCF 注销。如需继续配置其他设置，请执行相关步骤的操作。

14.8.15 查看验证启动策略

使用 `showbootconfig` 命令查看为物理分区设置的验证启动策略。

```
XSCF> showbootconfig -p ppar_id
```

对于 `ppar_id`，需指定需要查看策略的目标物理分区。

注 - 您也可以使用 XSCF Web 查看验证启动策略。

扩展系统配置

本章介绍如何更改系统 I/O 设备和硬件资源的配置，例如虚拟 CPU 和内存。

- 更改虚拟 CPU 配置
- 更改内存配置
- PCIe 端点设备的动态重新配置功能
- 使用 PCI 扩展单元
- 扩展 SPARC M12-2S/M10-4S

15.1 更改虚拟 CPU 配置

本节介绍如何通过使用 Oracle VM Server for SPARC 的动态重新配置功能 (DR) 更改虚拟 CPU 的配置。

注 - 如需动态更改逻辑域资源，逻辑域动态重新配置 (drd) 守护程序需要在目标域中运行。

在 SPARC M12/M10 系统上，各种业务处理在各个逻辑域上运行。根据系统操作状态，可以灵活地更改虚拟 CPU 配置。在有些使用中的进程中，负荷集中到特定的逻辑域，因此可以认为只是已配置的虚拟 CPU 的性能低下。在此情况下，同一物理分区中的逻辑域使保持系统能够继续运行。通过动态分配负荷相对较低的域的虚拟 CPU 实现。

虚拟 CPU 的配置可以针对每个线程进行更改。

如需更改虚拟 CPU 配置，首先使用 Oracle VM Server for SPARC 的 `ldm remove-vcpu` 命令从负荷相对较低的逻辑域删除虚拟 CPU。然后，使用 Oracle VM Server for SPARC 的 `ldm add-vcpu` 命令添加虚拟 CPU 到可能因负荷增加造成性能下降的逻辑域。执行这些命令需要 root 权限。

删除虚拟 CPU

```
primary# ldm remove-vcpu number ldom
```

对于 **number**，指定将删除的虚拟 CPU 数量。您可以以线程为单位进行指定。对于 **ldom**，指定从其中删除虚拟 CPU 的逻辑域。

添加虚拟 CPU

```
primary# ldm add-vcpu number ldom
```

对于 **number**，指定将添加的虚拟 CPU 数量。您可以以线程为单位进行指定。对于 **ldom**，指定添加到其中的虚拟 CPU 的逻辑域。

操作步骤

1. 从 **XSCF** 控制台切换到目标逻辑域所属的控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 "8.3 从 XSCF Shell 切换到控制域控制台"。
2. 使用 **ldm list-domain** 命令检查各域中虚拟 CPU 数量。
下面是查看 **primary**、**ldom1**、**ldom2** 和 **ldom3** 逻辑域状态的示例。

```
primary# ldm list-domain  
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME  
primary active -n-cv- SP 8 4G 3.1% 1d 36m  
ldom1 active -n---- 5001 16 2G 34% 1m  
ldom2 active -n---- 5002 16 1G 34% 17h 48m  
ldom3 active -n---- 5003 24 4G 17% 17h 48m
```

3. 使用 **ldm remove-vcpu** 命令从域中删除虚拟 CPU。
以下是从 **ldom3** 删除 8 个虚拟 CPU 的示例。

```
primary# ldm remove-vcpu 8 ldom3
```

4. 使用 **ldm add-vcpu** 命令将虚拟 CPU 添加到域。
以下是将 8 个虚拟 CPU 添加到 **ldom1** 的示例。

```
primary# ldm add-vcpu 8 ldom1
```

5. 使用 **ldm list-domain** 命令检查各域中虚拟 CPU 数量的配置更改。
以下是查看 **primary**、**ldom1**、**ldom2** 和 **ldom3** 逻辑域配置更改的示例。

```
primary# ldm list-domain  
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME  
primary active -n-cv- SP 8 4G 3.1% 1d 36m  
ldom1 active -n---- 5001 24 2G 34% 1m  
ldom2 active -n---- 5002 16 1G 34% 17h 48m  
ldom3 active -n---- 5003 16 4G 17% 17h 48m
```

您可观察到虚拟 CPU 已经从 **ldom3** 删除并添加到 **ldom1**。

6. 从控制域控制台注销并返回 **XSCF** 控制台。
有关如何从控制域控制台返回 XSCF 控制台的详细信息，请参见 ["8.4 从控制域控制台返回 XSCF Shell"](#)。

15.2 更改内存配置

本节介绍如何使用 Oracle VM Server for SPARC 的动态重新配置功能 (DR) 更改内存配置。

注 - 如需动态更改逻辑域资源，逻辑域动态重新配置 (ldr) 守护程序需要在目标域中运行。

在 SPARC M12/M10 系统上，各种业务处理在各个逻辑域上运行。可以根据系统操作状态，灵活地更改虚拟内存配置。在有些使用中的进程中，负荷集中到特定的逻辑域，因此可以认为只是已配置的内存的性能低下。在此情况下，可以重新分配同一物理分区中的逻辑域。通过动态分配负荷相对较低的域的内存实现。

内存配置可以在 256 MB 单元中更改。

如需更改内存配置，首先使用 Oracle VM Server for SPARC 的 `ldm remove-memory` 命令从负荷相对较低的逻辑域删除内存。然后，使用 Oracle VM Server for SPARC 的 `ldm add-memory` 命令添加内存到可能因负荷增加造成性能下降的逻辑域。

删除内存

```
primary# ldm remove-memory size[unit] ldom
```

对于 `size`，指定将要删除内存的容量。对于 `unit`，指定内存单位。对于 `ldom`，指定从其中删除内存的逻辑域。

添加内存

```
primary# ldm add-memory size[unit] ldom
```

对于 `size`，指定将要添加内存的容量。对于 `unit`，指定内存的单位。对于 `ldom`，指定为其中添加内存的逻辑域。

操作步骤

1. 从 **XSCF** 控制台切换到目标逻辑域所属的控制域控制台。
有关如何切换到控制域控制台的详细信息，请参见 ["8.3 从 XSCF Shell 切换到控制域控制台"](#)。
2. 用 `ldm list-domain` 命令检查各域的内存容量。

下面是查看 `primary`、`ldom1`、`ldom2` 和 `ldom3` 逻辑域状态的示例。

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n----- 5001 16 2G 34% 1m
ldom2 active -n----- 5002 16 1G 34% 17h 48m
ldom3 active -n----- 5003 24 4G 17% 17h 48m
```

3. 使用 `ldm remove-memory` 命令从域删除内存。

下面是从 `ldom3` 删除 1 GB 内存的示例。

```
primary# ldm remove-memory 1G ldom3
```

4. 使用 `ldm add-memory` 命令将内存添加到域。

下面是为 `ldom1` 添加 1 GB 内存的示例。

```
primary# ldm add-memory 1G ldom1
```

5. 使用 `ldm list-domain` 命令检查各域的内存容量的配置更改。

以下是查看 `primary`、`ldom1`、`ldom2` 和 `ldom3` 逻辑域配置更改的示例。

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n----- 5001 16 3G 34% 1m
ldom2 active -n----- 5002 16 1G 34% 17h 48m
ldom3 active -n----- 5003 16 3G 17% 17h 48m
```

您可观察到内存已经从域 `ldom3` 删除并添加到 `ldom1`。

6. 从控制域控制台注销并返回 **XSCF** 控制台。

有关如何从控制域控制台返回 XSCF 控制台的详细信息，请参见 ["8.4 从控制域控制台返回 XSCF Shell"](#)。

15.3 PCIe 端点设备的动态重新配置功能

从 Oracle VM Server for SPARC 3.1.1.1 开始支持 PCIe 端点设备的动态重新配置功能。这使您可以分配或删除 PCIe 端点设备，而无需重新配置根域或停止 I/O 域。

如需使用此功能，请查看服务器的《PCI Card Installation Guide》中的“Cards That Support the Dynamic Reassignment Function for the PCIe End Point Device (PCIe Card)”中的相应卡。

下表显示了所需的 XCP/Oracle Solaris 版本，以及执行 PCIe 端点设备动态重配置必需的 SRU/补丁。

表 15-1 执行 PCIe 端点设备 (SPARC M10) 的动态重新配置所必需的 XCP 和 Oracle Solaris 版本

服务器	XCP	Oracle Solaris	必需的软件包 必需品	必需的 SRU 必需的补丁
SPARC M10-1 SPARC M10-4 SPARC M10-4S	2230 或更 高版本	Oracle Solaris 11.3	system/ldoms (*1) system/ldoms/ldomsmanager (*2)	无
		Oracle Solaris 11.2	system/ldoms (*1) system/ldoms/ldomsmanager (*2)	SRU 11.2.2.5.0 或更高版本
		Oracle Solaris 11.1 (*4)	system/ldoms (*1)	SRU 11.1.17.5.0 或更高版本 (*3)
		Oracle Solaris 10 1/13	Oracle VM for SPARC 3.1 (*5)(*6)	150817-03 或更 高版本 (*5)

*1 对于控制域或其他域是必需的。包含在 group/system/solaris-large-server 和 group/system/solaris-small-server 中。

*2 仅对于控制域是必需的。包含在 group/system/solaris-large-server 和 group/system/solaris-small-server 中。

*3 对于控制域或其他域是必需的。

*4 仅控制域之外的域可使用。

*5 仅对于控制域是必需的。

*6 需要 Oracle VM Server for SPARC 补丁之外的补丁。有关详情，请参见《Oracle VM Server for SPARC 3.1.1.1, 3.1.1, and 3.1 Release Notes》中的 "Required Oracle Solaris OS Versions for Oracle VM Server for SPARC 3.1.1.1"。

表 15-2 执行 PCIe 端点设备 (SPARC M12) 的动态重新配置所必需的 Oracle Solaris 版本

OS 版本	域类型		
	控制域 非虚拟化环境	根域 (使用 I/O 租用)	I/O 域
Oracle Solaris 11	Oracle Solaris 11.3 (*1) SRU 11.3.17.5.0 或更高版本	Oracle Solaris 11.3 或更高版本 (*2)	Oracle Solaris 11.3 或更高版本 (*2)
	Oracle Solaris 11.2 (*1) SRU11.2.15.5.1	Oracle Solaris 11.2 或更高版本 (*2)	Oracle Solaris 11.2 或更高版本 (*2)
			Oracle Solaris 11.1 SRU 11.1.17.5.0 或更高版本
Oracle Solaris 10	Oracle Solaris 10 1/13 (*3) Oracle VM Server for SPARC 3.2 (*4) 151934-03 或更新版本	—	—

*1 system/ldoms 和 system/ldoms/ldomsmanager packages 软件包是必需的。这些软件包包含在 group/system/solaris-large-server 和 group/system/solaris-small-server 之中。

*2 system/ldoms 软件包是必需的。此软件包包含在 group/system/solaris-large-server 和 group/system/solaris-small-server 之中。

*3 当 Oracle Solaris 10 1/13 在控制域中运行时，逻辑系统板上安装的 LSB 编号为 0 到 7 的 CPU 可以分配给控制域。

*4 不包括在 Oracle Solaris 10 1/13 中。需单独安装。

如需使用此功能，目标逻辑域的热插拔服务必须提前启用。

```
# svcadm enable svc:/system/hotplug:default
```

15.3.1 将物理 I/O 设备添加到 I/O 域

本节介绍通过使用 PCIe 端点设备的动态重配置功能将物理 I/O 设备添加到 I/O 域的步骤。

1. 从根域移除物理 I/O 设备。

```
# ldm remove-io device root_domain
```

2. 将步骤 1 中移除的物理 I/O 设备分配给 I/O 域。

```
# ldm add-io device io_domain
```

3. 在 I/O 域上设置物理 I/O 设备。

进行此项设置的步骤根据目标 I/O 域的 Oracle Solaris 版本以及物理 I/O 设备的不同而有所不同。有关详情，请参阅下述 Oracle Solaris 相关手册。

- 对于以太网卡
 - 对于 Oracle Solaris 11.2
 - 《Configuring and Administering Network Components in Oracle Solaris 11.2》
 - 《Managing Network Datalinks in Oracle Solaris 11.2》
 - 《Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2》
 - 对于 Oracle Solaris 11.1
 - 《Connecting Systems Using Fixed Network Configuration in Oracle Solaris 11.1》
 - 《Managing Oracle Solaris 11.1 Network Performance》
 - 对于 Oracle Solaris 10
 - 《Oracle Solaris Administration: IP Services》
- 对于 SAS 卡或光纤通道卡
 - 对于 Oracle Solaris 11.2
 - 《Managing SAN Devices and Multipathing in Oracle Solaris 11.2》
 - 对于 Oracle Solaris 11.1
 - 《Oracle Solaris SAN Configuration and Multipathing Guide》
 - 对于 Oracle Solaris 10
 - 《Oracle Solaris SAN Configuration and Multipathing Guide》

15.3.2 从 I/O 域移除物理 I/O 设备

本节介绍通过使用 PCIe 端点设备的动态重配置功能从 I/O 域移除物理 I/O 设备的步骤。

1. 在 I/O 域上取消物理 I/O 设备的设置。
移除物理 I/O 设备之前，必须取消 I/O 域上的物理 I/O 设备的设置。

进行此项设置的步骤根据目标 I/O 域的 Oracle Solaris 版本以及物理 I/O 设备的不同而有所不同。有关详情，请参阅下述 Oracle Solaris 相关手册。

- 对于以太网卡
 - 对于 Oracle Solaris 11.2
 - 《Configuring and Administering Network Components in Oracle Solaris 11.2》
 - 《Managing Network Datalinks in Oracle Solaris 11.2》
 - 《Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2》
 - 对于 Oracle Solaris 11.1
 - 《Connecting Systems Using Fixed Network Configuration in Oracle Solaris 11.1》
 - 《Managing Oracle Solaris 11.1 Network Performance》
 - 对于 Oracle Solaris 10
 - 《Oracle Solaris Administration: IP Services》
- 对于 SAS 卡或光纤通道卡
 - 对于 Oracle Solaris 11.2
 - 《Managing SAN Devices and Multipathing in Oracle Solaris 11.2》
 - 对于 Oracle Solaris 11.1
 - 《Oracle Solaris SAN Configuration and Multipathing Guide》
 - 对于 Oracle Solaris 10
 - 《Oracle Solaris SAN Configuration and Multipathing Guide》

2. 从 I/O 域中移除物理 I/O 设备。

```
# ldm remove-io device io_domain
```

3. 如需使用 PCI 热插拔 (PHP) 等执行 PCIe 卡的主动维护，则需将步骤 2 中移除的物理 I/O 设备重新分配给根域。

```
# ldm add-io device root_domain
```

15.4 使用 PCI 扩展单元

本节简要介绍了 PCI 扩展单元，它是 SPARC M12/M10 的一个选配件。

PCI 扩展单元是一个机架安装设备，最多可以扩展 11 个 PCI-Express 槽。本单元可以安装在与 SPARC M12/M10 相同的机架中。假设 SPARC M12/M10 的内置 PCI-Express 插槽不足。此时，安装 PCI 扩展单元可灵活地扩展系统。

您可使用 XSCF 固件 `ioxadm` 命令检查 PCI 扩展单元状态和执行开机/关机。有关 `ioxadm` 命令的详细信息，请参见该命令的 `man` 页或《Fujitsu SPARC M12 and

Fujitsu M10/SPARC M10 XSCF Reference Manual》。

如果您考虑安装 PCI 扩展单元，请联络销售代表。

有关安装 PCI 扩展单元的详情，请参见所使用服务器《安装指南》中的“将 PCI 扩展单元安装到机架”。

15.4.1 检查 PCI 扩展单元

您可以检查系统管理的 PCI 扩展单元清单、温度、电压、电流、风扇转速传感器测量值、定位器 LED 状态和单元的固件状态。

有关如何检查的详情，请参见 [“11.1.5 查看 PCI 扩展单元状态”](#)。

15.4.2 控制 PCI 扩展单元的电源

本节介绍如何开启/关闭电源以移除 PCI 扩展单元、I/O 板和电源单元等。

执行开启或关闭电源必须具有 `platadm` 或 `fieldeng` 用户权限。

操作步骤

1. 使用 `ioxadm` 命令关闭 PCI 扩展单元中的电源单元。

在以下的示例中，关闭了电源单元等指定部件的电源，可进行单元移除。

```
XSCF> ioxadm -f poweroff PCIBOX#12B4/PSU#1
```

注 - 要强制关闭电源，请指定 `-f` 选项。注意使用 `-f` 选项可能会对域造成损坏。

2. 使用 `ioxadm` 命令恢复对 PCI 扩展单元中电源单元的供电。

以下是对已切断电源的部件再次开启电源的示例。

```
XSCF> ioxadm poweron PCIBOX#12B4/PSU#1
```

注 - 如需移除电源单元或 I/O 板，请关闭指定部件的电源。当电源开关设置为开启时，如需再次开启电源，请执行 `ioxadm` 命令。

15.4.3 连接 PCI 扩展单元系统配置的注意事项

SPARC M12-2/M12-2S/M10-4/M10-4S

假设在 SPARC M12-2/M12-2S 中使用 `setpciboxdio` 命令，或使用其他系统上的以下固件：SPARC M10-4 上的 XCP 2044 或更高版本，或 SPARC M10-4S 上的 XCP 2050 或更高版本，执行以下其中一种操作。则下次控制域启动时，物理分区的逻辑域配置将恢复到 `factory-default` 状态。此外，控制域的 OpenBoot PROM 环境变量可被初始化。

- 变更 PCI 扩展单元的直接 I/O 功能的启用/禁用设置
- 当 PCI 扩展单元被添加到/从其中移除/更换到具有启用直接 I/O 功能的 PCI 扩展单元的 SPARC M12/M10 的 PCI 插槽上时

无论是否有 PCI 扩展单元，您都可以执行 `setpciboxdio` 命令。进行上述操作之前，将逻辑域配置信息从 Oracle Solaris 保存到 XML 文件。另外，请记住控制域的 OpenBoot PROM 环境变量设置信息，以便再次设置。

表 15-3 显示了在通过执行 `setpciboxdio` 命令变更 PCI 扩展单元直接 I/O 功能的启用/禁用设置时，可能需要保存/恢复哪些信息。

表 15-3 切换启用/禁用直接 I/O 功能设置时所需的操作

PCI 扩展单元的配置	目前的域配置	重建 Oracle VM Server for SPARC 配置	再次设置 OpenBoot PROM 环境变量
否	<code>factory-default</code> (仅控制域)	不必须	不必须
否	控制域以外的逻辑域	必须 (XML 文件)	必须 (*1)
是	<code>factory-default</code> (仅控制域)	不必须	不必须
是	控制域以外的逻辑域	必须 (XML 文件)	必须 (*1)

*1 这在 XCP 2230 或更高版本或 SPARC M12-2/M12-2S 中不是必需的。

表 15-4 显示了添加/移除/更换启用 PCI 扩展单元直接 I/O 功能的 SPARC M12/M10 系统机柜 PCI 插槽中的 PCI 扩展单元时可能需要保存/恢复哪些信息。这里，`setpciboxdio` 命令已经执行以启用该功能。

注 - 使用 PCI 热插拔 (PHP) 功能维护 PCI 扩展单元时，直接 I/O 功能被禁用，因此并不需要保存/恢复上述信息。

表 15-4 添加/移除/更换启用直接 I/O 功能的 SPARC M12/M10 系统机柜 PCI 插槽中的 PCI 扩展单元时所需的操作

维护环境	目前的域配置	重建 Oracle VM Server for SPARC 配置	再次设置 OpenBoot PROM 环境变量
PPAR 停止时添加/移除	factory-default (仅控制域)	不必须	不必须
	控制域以外的逻辑域	必须 (XML 文件)	必须 (*2)
PPAR 停止时更换故障 PCI 扩展单元(*1)	factory-default (仅控制域)	不必须	不必须
	控制域以外的逻辑域	必须 (XML 文件)	必须 (*2)
PPAR 停止时更换正常 PCI 扩展单元(*1)	factory-default (仅控制域)	不必须	不必须
	控制域以外的逻辑域	不必须	不必须

*1 这甚至包括链路卡、连接线、控制线或链路板的更换。

*2 这在 XCP 2230 或更高版本或 SPARC M12-2/M12-2S 中不是必需的。

注 - 执行 `ldm list-constraints -x` 命令可保存到 XML 文件，执行 `ldm init-system -i` 命令可从 XML 文件恢复。如需显示 OpenBoot PROM 环境变量，请从 `ok` 提示符执行 `printenv` 命令。有关步骤的详情，请参见《PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》中的 "1.7.3 How to Save/Restore the Logical Domain Configuration Information and the OpenBoot PROM Environment Variable"。

SPARC M12-1/M10-1

如果将 PCI 扩展单元添加到 SPARC M12-1 或从 SPARC M12-1 中移除，或者如果在 SPARC M10-1 上执行以下其中一种操作，则在下一次控制域启动时物理分区的逻辑域配置将恢复为出厂默认状态。此外，控制域的 OpenBoot PROM 环境变量可被初始化。

- 将连接到 PCI 扩展单元的系统中的固件从 XCP 2043 或更早版本更新到 XCP 2044 或更高版本
- 添加/移除 XCP 2044 或更高版本固件所应用的系统中的 PCI 扩展单元

操作之前，需将逻辑域配置信息从 Oracle Solaris 保存到 XML 文件。另外，请事先记下控制域的 OpenBoot PROM 环境变量设置信息，以便再次设置。

表 15-5 显示了在连接到 PCI 扩展单元的系统，将固件从 XCP 2043 或更早版本更新到 XCP 2044 或更高版本时可能需要保存/恢复哪些信息。

表 15-5 将固件从 XCP 2043 或更早版本更新到 XCP 2044 或更高版本时所需的操作

PCI 扩展单元连接	目前的域配置	重建 Oracle VM Server for SPARC 配置	再次设置 OpenBoot PROM 环境变量
否	factory-default (仅控制域)	不必须	不必须
否	控制域以外的逻辑域	不必须	不必须
是	factory-default (仅控制域)	不必须	不必须

表 15-5 将固件从 XCP 2043 或更早版本更新到 XCP 2044 或更高版本时所需的操作 (续)

PCI 扩展单元连接	目前的域配置	重建 Oracle VM Server for SPARC 配置	再次设置 OpenBoot PROM 环境变量
是	控制域以外的逻辑域	必须 (XML 文件)	必须

表 15-6 显示了在应用 XCP 2044 或更高版本的固件的系统中添加/移除 PCI 扩展单元时可能需要保存/恢复哪些信息。

表 15-6 在应用固件 XCP 2044 或更高版本的系统中添加/移除 PCI 扩展单元时所需的操作

PCI 扩展单元连接	目前的域配置	重建 Oracle VM Server for SPARC 配置	再次设置 OpenBoot PROM 环境变量
否 (添加)	factory-default (仅控制域)	不必须	不必须
否 (添加)	控制域以外的逻辑域	必须 (XML 文件)	必须 (*1)
是 (添加/移除)	factory-default (仅控制域)	不必须	不必须
是 (添加/移除)	控制域以外的逻辑域	必须 (XML 文件)	必须 (*1)

*1 这在 XCP 2230 或更高版本或 SPARC M12-1 中不是必需的。

注 - 执行 `ldm list-constraints -x` 命令可保存到 XML 文件, 执行 `ldm init-system -i` 命令可从 XML 文件恢复。如需显示 OpenBoot PROM 环境变量, 请从 `ok` 提示符执行 `printenv` 命令。有关步骤的详情, 请参见《PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》中的 "1.7.3 How to Save/Restore the Logical Domain Configuration Information and the OpenBoot PROM Environment Variable"。

15.5 扩展 SPARC M12-2S/M10-4S

有关添加 SPARC M12-2S/M10-4S 来扩展系统的工作流程以及详细的准备和添加步骤, 请参见《Fujitsu SPARC M12-2S 安装指南》中的 "第8章 扩展模块化架构配置的系统" 或《Fujitsu M10-4S/SPARC M10-4S 安装指南》中的 "第8章 安装/卸载模块化架构配置的系统之前"。

有关如何将已添加的 SPARC M12-2S/M10-4S 机箱添加到物理分区以及如何将其分配给逻辑域的详细信息, 请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

更新 XCP 固件

本章介绍了如何通过下载管理 SPARC M12/M10 系统固件的程序 (XCP) 将当前固件更新到最新固件。

- 固件更新的基础知识
- 更新固件之前
- 更新流程
- 准备 XCP 映像文件
- 更新固件
- 从 XSCF Web 更新固件
- 部件更换时固件版本匹配
- 固件更新期间出现故障
- 与固件更新相关的常见问题

系统管理员和现场工程师更新固件。

16.1 固件更新的基础知识

16.1.1 要更新固件的类型

此类系统具有用于控制硬件/软件的多个固件。由多个固件组合而成的程序模块被称为 XCP (XSCF Control Package)。

从本公司的网站下载 XCP 固件并执行更新，用户可以使用新固件的功能。

XCP 固件有以下几种类型。

- POST 固件、OpenBoot PROM 固件和虚拟机监控程序固件（以下称为 CMU 固件）这三类固件被组合成为一个固件，以便在 CPU 内存单元上更新，并管理其版本。本手册中，这三类固件统称为 CMU 固件。

- XSCF 固件
此固件在 XSCF 单元中更新。

用户可以选择更新整个固件（以下简称 XCP 固件）或只更新 XSCF 固件。

16.1.2 固件更新的特点

XCP 固件更新有以下特点。

- 对新固件进行更新时不必关闭物理分区的电源。在更新 CMU 固件时，必须关闭然后打开物理分区电源。
- 如果使用模块化架构配置中的维护菜单更换了部件，则更换部件上的固件将自动与正在运行的固件版本相匹配。

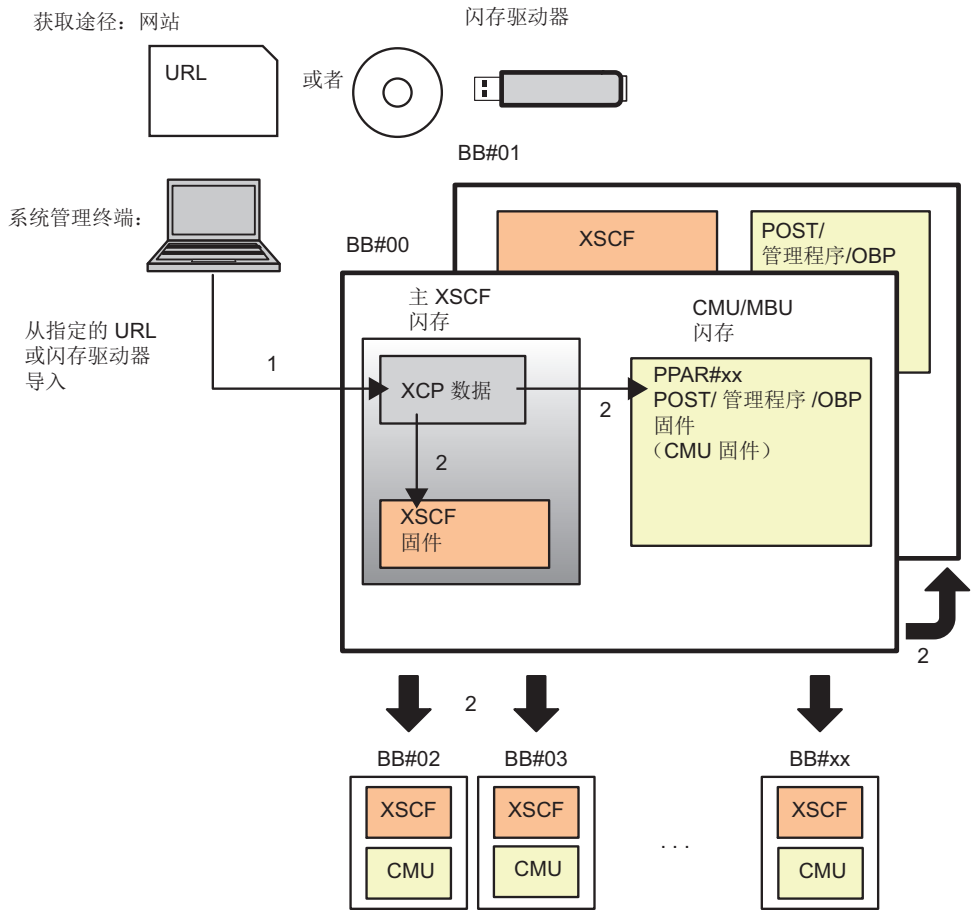
注 - 关闭输入电源、不使用维护菜单更换或添加部件时的有关自动版本匹配的支持信息，请参见您的服务器最新《产品说明》。

- 即使系统包含多个物理分区，也可将固件更新到最新固件而不影响其它物理分区。

16.1.3 固件更新的机制

图 16-1 是显示固件更新机制的概念图。

图 16-1 固件更新的概念



1 XCP 导入

2 更新

以下两个操作（XCP 导入和更新）提供此类系统的固件更新。

1. **XCP 导入（下载）**

将从网站获得的解压缩的 XCP 映像文件保存到任何此类系统称为 "XCP 导入"。导入 XCP 后，运行中的固件尚未更新。

2. **更新**

将导入的 XCP 映像文件写入到任何此类系统的闪存称为 "更新"。在此更新中，电源关闭时 XSCF 固件和 CMU 固件的更新被完成。

注 - 如需完成在电源开启时目标物理分区上的 CMU 固件更新，请关闭物理分区的电源，然后再将该电源开启。

在 SPARC M10-1/M10-4/M10-4S 中，具有已写入的固件的闪存有两个区域：当前储存

区和保留储存区。使用这两个储存区控制固件更新。CMU 固件更新时，仅使用当前储存区来控制固件更新。

注 - SPARC M10 系统上的 CMU 固件更新时，也显示保留储存区。CMU 固件更新时，控制仅由当前储存区处理，保留储存区的过时版本没有问题。

16.1.4 版本匹配

在以下任何情况下，此类系统自动匹配固件版本。

- 假设物理分区中的多个模块化架构（系统板）有不同的 CMU 固件版本。在此情况下，当开启物理分区的电源时，将自动匹配固件版本。
- 如果维护部件（XSCF 单元或 CPU 内存单元（下））使用维护菜单已经更换或添加，则其固件版本会自动与正在运行的固件的版本相匹配。
- 如果已执行 `flashupdate -c sync` 命令，所有的 XSCF 固件版本将匹配到主 XSCF。

16.1.5 使用多个 XSCF 时更新

在多个 XSCF 的系统中，主 XSCF 执行固件更新。固件更新按照先备用 XSCF 后主 XSCF 的顺序自动执行。在这种情况下，XSCF 自动重新启动或切换主和备用 XSCF 网络。此时，网络会一度断开。因此需要用户再次登录。

有关更新的详细信息，请参见“16.5 更新固件”。

16.2 更新固件之前

16.2.1 更新注意事项

- 随着 XCP 的发布，该版本的产品说明也会公布。产品说明介绍以下内容：新增的功能、软件补丁信息、新硬件和固件之间的对应、缺陷信息、文档更正等内容。此外，最新产品说明包含旧产品说明的更正。请务必阅读要应用的固件版本和最新版本的产品说明。
- 请勿在当前运行的系统上应用比 XCP 固件更旧的版本。如果应用更旧的版本，则无法保证系统的操作。
- 硬件出现故障时无法进行固件更新。更新之前，请确保硬件无故障。如果硬件出现故障，请消除故障，然后再更新固件。使用 `showhardconf` 命令检查硬件状态。确认没有标有星号 (*) 的硬件。
- 由于 XSCF 被重新启动，XSCF 通讯在整个 XCP 固件和 XSCF 固件更新期间会断开一次连接。在此情况下，再次连接到 XSCF 并登录。

- 为了安全更新固件，直到您已经确认 XCP 固件的更新完成消息 "XCP update has been completed" 时才可对物理分区执行电源操作。
- 可以更新一个或多个物理分区。当目标物理分区的电源开启时，若需完成 CMU 固件更新，请执行关闭物理分区电源，然后开启物理分区电源。
- 更新 XCP 固件时，请参见您的服务器最新《产品说明》中的“最新信息”和“现有 XCP 固件版本和支持信息”，以检查 CMU 固件是否已更新。有关检查 CMU 固件版本的方法，请参见“16.2.3 检查固件版本的方法”。

16.2.2 更新文件交付方法和格式

在以下位置和通过以下格式提供 XCP 固件的映像文件。

- 交付方法：网站
有关网站的详细信息，请参见您的服务器最新《产品说明》中的有关固件下载的说明。现场工程师可以使用 CD-ROM、DVD-ROM 或闪存盘执行此项作业。
- 格式：压缩 tar 文件 (tar.gz) 或 Windows 可执行文件 (exe)
示例：XCP2020.tar.gz

16.2.3 检查固件版本的方法

此类系统的固件版本称为 "XCP 版本"。版本号越高，固件越新。更新固件前，务必检查当前系统的 XCP 版本。

在下面的示例中，使用指定 `-c xcp` 选项的 `version` 命令显示 XCP 版本。

```
XSCF> version -c xcp
BB#00-XSCF#0 (Master)
XCP0 (Current): 2044
XCP1 (Reserve): 2044
BB#01-XSCF#0 (Standby)
XCP0 (Current): 2044
XCP1 (Reserve): 2044
BB#02-XSCF#0
XCP0 (Current): 2044
XCP1 (Reserve): 2044
```

使用 `version` 命令，您也可以检查 XCP 中各固件的版本。

XCP 版本由四位数表示，如 "xyz"。各数字含义如下：

- x: 主版本号
- yy: 次版本号
- z: 微版本号

微版本修订数可以超过文档修订数。因此，微版本号在文档中可能以变量显示。

示例: XCP201x

您可以使用 `-c xcp -v` 选项的 `version` 命令确认 XCP 中 XSCF 固件和 CMU 固件的各个版本。

以下示例显示 SPARC M10-1 的 XCP 固件版本。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU           : 02.04.0001
POST          : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor    : 0.26.9
XSCF          : 02.04.0001
XCP1 (Reserve): 2041
CMU           : 02.04.0001
POST          : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor    : 0.26.9
XSCF          : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..
```

以下示例显示 SPARC M12-2 的 XCP 固件版本。在 SPARC M12-1/M12-2/M12-2S 中，没有 CMU 保留区。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF          : 03.01.0000
XCP1 (Current): 3010
XSCF          : 03.01.0000
CMU           : 03.01.0000
      POST          : X.X.X
      OpenBoot PROM : X.XX.X+X.XX.X
      Hypervisor    : X.X.X
CMU BACKUP
#0: 03.01.0000
#1: ..
```

CMU 固件可能与 XCP 版本不同。

示例: 当 XCP 版本为 2042 时, XSCF 固件版本为 02.04.0002, CMU 固件版本为 02.04.0001。

关于与 XCP 版本对应的 CMU 固件版本, 请参见您的服务器最新《产品说明》中的“现有 XCP 固件版本和支持信息”。

16.2.4 更新方法和工作时间

表 16-1 列出了更新方法和大致工作时间。

表 16-1 更新方法和工作时间

更新方法	系统状态	时间
在有一个 XSCF 的系统中，更新 XCP。	物理分区电源已断开或开启。	约 45 分钟
在具有多个 XSCF 的模块化架构配置系统中，更新 XCP。 将更新以下固件：所有物理分区上的 CMU 固件和所有 XSCF 单元上的 XSCF 固件。 仅也可更新主 XSCF 固件。但是，如需完成在电源开启时目标物理分区上的 CMU 固件更新，请关闭物理分区的电源，然后再将该电源开启。	物理分区电源已断开或开启。	约 120 分钟
在部件更换时，自动更新固件，以便匹配固件版本。各更换的部件的固件版本自动匹配更换前的固件版本。对更换的部件执行以下作业。 - 添加/更换 SPARC M12-2S 的 XSCF 单元或 SPARC M10-4 的 CPU 内存单元（下），并匹配版本。 - 更换/添加接线盒的 XSCF 单元，并匹配版本。	物理分区电源已断开或开启。	约 5 分钟

注 - 更换 SPARC M12-1/M10-1 系统的主板单元、SPARC M10-4 系统和所有 SPARC M10-4S 系统的 CPU 内存单元（下）、所有 SPARC M12-2S 系统的 XSCF 单元，以及所有接线盒的 XSCF 单元后，版本与预更换固件版本将无法自动匹配。请求作业者更新固件。

注 - 有关不使用维护菜单且输入电源关闭的情况下更换内存单元（下）(CMUL)、更换 XSCF 单元、添加 SPARC M10-4S 或添加接线盒时自动版本匹配的支持信息，请参见最新 XCP 版本的《Fujitsu M10/SPARC M10 系统 产品说明》。

16.3 更新流程

使用 XSCF shell 或 XSCF Web，固件更新的顺序是：1) XCP 导入，2) XCP 更新。

基本的固件更新步骤如下。

1. 从网站获取 **XCP** 固件程序文件 (**tar.gz format**)，并将其放入 **USB** 设备或网络目录中。
2. 解压缩 **XCP** 固件程序文件。
3. 用具有 **platadm** 或 **fieldeng** 用户权限的用户帐户登录 **XSCF**。如果系统有多个 **XSCF**，登录主 **XSCF**。
4. 从 **USB** 设备或网络目录将 **XCP** 固件映像文件 (**BBXCPxxxx.tar.gz**) 导入系统（见 **getflashimage(8)**）。
XCP 可以在 Oracle Solaris 使用中或停止时导入到系统。
5. 更新 **XCP** 或 **XSCF** 固件（见 **flashupdate(8)**）。

6. 对于电源开启的目标物理分区上的 **CMU** 固件，关闭物理分区的电源然后开启物理分区的电源（见 **poweroff(8)** 和 **poweron(8)**）。

注 - 对于逻辑域配置，请在控制域中执行 Oracle VM Server for SPARC 的 `ldm add-spconfig` 命令，使得在关闭物理分区之前将最新配置信息保存在 XSCF 中。

有关详情，请参见 "6.2.2 系统停止之前保存逻辑域配置信息" 和 "10.11.1 保存/显示逻辑域配置信息"。

7. 确认固件版本（见 **version(8)**）。

有关这五个命令的详细信息，请参见各命令的 `man` 页或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。关于相关 XSCF Web 菜单的详情，请参见 "附录 C XSCF Web 页面列表"。

16.4 准备 XCP 映像文件

本节介绍如何准备 XCP 映像文件。

1. 从网站上将 **XCP** 固件程序文件 (**XCPxxxx.tar.gz** 或 **XCPxxxx.exe**) 下载到与本系统相连接的 **PC** 上的任意一个文件夹。
2. 检查 **XCP** 版本。
对于 XCP 版本，在固件程序的文件名中有 4 位数字（`tar.gz` 格式）。
示例：XCP2044.tar.gz 的 XCP 版本是 2044。
3. 解压缩下载的 **XCP** 固件程序。
导入到系统中的 XCP 映像文件被展开。
示例：如果解压缩 XCP2044.tar.gz，则 BBXCP2044.tar.gz 被展开。

16.5 更新固件

本节介绍如何使用 XSCF shell 更新固件。更新步骤与使用 XSCF Web 相同。有关 XSCF Web 步骤的详情，请参见 "16.6 从 XSCF Web 更新固件"。

16.5.1 在拥有一个 XSCF 的系统上更新 XCP

1. 登录 **XSCF**。
2. 执行 **showhardconf** 命令，并确认 **XSCF status (MBU Status)** 是 **Normal**。
下面是 SPARC M10-1 的示例。

```

XSCF> showhardconf
SPARC M10-1;
+ Serial:2101151019A; Operator_Panel_Switch:Service;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
MBU Status:Normal; Ver:2046h; Serial:USDA-P00008 ;
+ FRU-Part-Number:CA20366-B10X 002AB/LGA-MBU -01 ;
+ Power_Supply_System: ;
+ Memory_Size:32 GB;

```

3. 执行 **version** 命令检查正在运行的固件的版本。

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU      : 02.04.0001
  POST   : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor : 0.26.9
XSCF     : 02.04.0001
XCP1 (Reserve): 2041
CMU      : 02.04.0001
  POST   : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor : 0.26.9
XSCF     : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..

```

对于 SPARC M12-1/M12-2，没有 CMU 固件的保留储存区。下面显示了一个显示示例。

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF     : 03.01.0000
XCP1 (Current): 3010
XSCF     : 03.01.0000
CMU      : 03.01.0000
  POST   : X.X.X
  OpenBoot PROM : X.XX.X+X.XX.X
  Hypervisor : X.X.X
CMU BACKUP
#0: 03.01.0000
#1: ..

```

4. 执行 **getflashimage** 命令导入 XCP 映像文件。

下面的示例从连接到 XSCF 单元面板（后面板）上的 USB 端口（印刷 "MAINTENANCE ONLY"）的 USB 设备导入 XSCF 映像文件。

```

XSCF> getflashimage file:///media/usb_msd/xxxx/BXCP2044.tar.gz
Existing versions:
      Version                Size  Date
      BXCP2041.tar.gz       90004045  Tue Apr 09 04:40:12 JST 2013
Mounted USB device
0MB received
1MB received
...
44MB received
45MB received
Download successful: 46827 Kbytes in 109 secs (430.094 Kbytes/sec)
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a4
XSCF>

```

当正常结束消息 "Download successful: ..." 和 "MD5: ..." 出现时, XCP 映像文件导入完成。

注 - 如果 XCP 导入后出现 "Error:File is invalid or corrupt" 消息, 这意味着导入的 XCP 映像文件不是正确的文件。可能的原因是获得了未经授权的 XCP 映像文件, 或者客户下载的 XCP 映像文件随后被未经授权的访问更改。在此情况下, 请获取正确的 XCP 映像文件后重新导入 XCP。

5. 使用 **getflashimage -l** 命令来检查导入的 XCP 映像文件的版本。

```

XSCF> getflashimage -l
Existing versions:
      Version                Size  Date
      BXCP2044.tar.gz       90005045  Wed May 29 13:56:50 JST 2013

```

6. 执行 **flashupdate -c check** 命令来检查导入的 XCP 映像文件是否可用于更新。执行 **flashupdate** 命令后, 立即执行 **showresult** 命令。如果返回的结束值是 0, 则可使用更新文件。

```

XSCF> flashupdate -c check -m xcp -s 2044
XSCF> showresult
0
XSCF>

```

7. 执行 **flashupdate** 命令更新固件。

注 -

- 更新大约需要 30 分钟。
- 为了安全地更新固件, 在作业期间 (步骤 7 至 11) 请勿执行物理分区的电源操作。

```

XSCF> flashupdate -c update -m xcp -s 2044
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [3600sec]

```

```
0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....
:
```

此时，XSCF 被重新启动，XSCF 会话被断开。

此时，XCP 固件更新尚未完成。

8. 再次连接到 XSCF。
9. 执行 **showlogs monitor** 命令检查 XCP 固件更新的完成情况。

```
XSCF> showlogs monitor
May 29 14:30:09 M10-1-0 Event: SCF:XCP update is started (XCP version=2044:
last version=2041)
May 29 14:31:59 M10-1-0 Event: SCF:XSCF update is started (BBID=0, bank=1)
May 29 14:32:18 M10-1-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 14:39:27 M10-1-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=1)
May 29 14:39:28 M10-1-0 Event: SCF:XSCF bank apply has been completed (BBID=0,
bank=1, XCP version=2044:last version=2041)
May 29 14:47:12 M10-1-0 Event: SCF:XSCF ready
May 29 14:48:32 M10-1-0 Event: SCF:XSCF update is started (BBID=0, bank=0)
May 29 14:48:52 M10-1-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 14:55:51 M10-1-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=0)
May 29 14:57:04 M10-1-0 Event: SCF:CMU update is started (BBID=0)
May 29 14:57:07 M10-1-0 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 14:59:07 M10-1-0 Event: SCF:CMU update has been completed (BBID=0)
May 29 15:00:19 M10-1-0 Event: SCF:CMU update is started (BBID=0)
May 29 15:00:20 M10-1-0 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 15:02:18 M10-1-0 Event: SCF:CMU update has been completed (BBID=0)
May 29 15:02:20 M10-1-0 Event: SCF:XCP update has been completed (XCP
version=2044:last version=2041)
```

下面是 SPARC M12-2 上显示消息的示例。

```
XSCF> showlogs monitor
Mar 15 15:29:34 M12-2-0 Event: SCF:XCP update is started (XCP version=3010:
last version=3009)
Mar 15 15:39:20 M12-2-0 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Mar 15 15:42:59 M12-2-0 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Mar 15 15:43:13 M12-2-0 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=0)
Mar 15 15:43:20 M12-2-0 Event: SCF:Updating XCP:XSCF bank has changed (BBID=0,
bank=0, XCP version=3010:last version=3009)
Mar 15 16:02:49 M12-2-0 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=1)
Mar 15 16:04:18 M12-2-0 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
```

```
version=03010000)
Mar 15 16:04:22 M12-2-0 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=1)
Mar 15 16:04:47 M12-2-0 Event: SCF:XSCF ready
Mar 15 16:07:47 M12-2-0 Event: SCF:Updating XCP:Preparing to update CMU (BBID=0)
Mar 15 16:08:17 M12-2-0 Event: SCF:Updating XCP:Updating CMU (BBID=0, CMU
version=03010000)
Mar 15 16:08:28 M12-2-0 Event: SCF:Updating XCP:CMU updated (BBID=0)
Mar 15 16:08:31 M12-2-0 Event: SCF:XCP update has been completed (XCP
version=3010:last version=3009)
```

如果出现 "XCP update has been completed" 信息，则 XCP 固件更新已经完成。

注 - SPARC M10 上将显示类似于 "XSCF update has been completed" 或 "CMU update has been completed" 的消息。然而，在消息出现时，所有 XCP 固件的更新并没有完成。为了安全地更新固件，请勿对物理分区执行电源操作，直到您已确认 XCP 固件的更新完成信息 "XCP update has been completed"。

如果没有出现 "XCP update has been completed" 信息，则更新尚未完成。再次执行 `showlogs monitor` 命令检查更新的完成情况。通常，在出现 "XSCF ready" 消息之后约 20 分钟更新完成。

如果物理分区的电源关闭，并且您已经确认了 "XCP update has been completed" 消息，则 XCP 固件更新完成。转到步骤 11。

如果物理分区的电源开启，此时目标 CMU 固件尚未更新。因此，对于 CMU 固件，此消息不会出现。确认了消息 "XCP update has been completed" 后，请转到步骤 10。

10. 当物理分区的电源开启时，若需完成 **CMU** 固件更新，请执行关闭物理分区电源，然后开启物理分区电源。

注 - 对于逻辑域配置，请在控制域中执行 Oracle VM Server for SPARC 的 `ldm add-spconfig` 命令，使得在关闭物理分区之前将最新配置信息保存在 XSCF 中。有关详情，请参见 "6.2.2 系统停止之前保存逻辑域配置信息" 和 "10.11.1 保存/显示逻辑域配置信息"。

执行 `poweroff` 命令来关闭物理分区的电源。

```
XSCF> poweroff -p 0
```

执行 `showpparstatus power` 命令，并确认物理分区电源已关闭。

```
XSCF> showpparstatus -p 0
PPAR-ID          PPAR Status
00               Powered Off
```

执行 `poweron` 命令来开启物理分区的电源。


```
XSCF> poweron -p 0
```

执行 `showpparstatus` 命令，并确认 PPAR Status 是 "Running"。

```
XSCF> showpparstatus -p 0
PPAR-ID          PPAR Status
00               Running
```

11. 执行 `version` 命令，并确认固件版本是最新版本。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
CMU BACKUP
#0: 02.04.0004
#1: ..
```

注 - 在 SPARC M10-1/M10-4/M10-4S 上，如果通过开启物理分区的电源来更新固件，则会更新 CMU 固件的当前储存区。
如果通过停止物理分区的电源来更新固件，则不但会更新 CMU 固件的保留储存区，而且会更新当前储存区。
关于与 XCP 版本对应的 CMU 固件版本，请参见您的服务器最新《产品说明》中的“现有 XCP 固件版本和支持信息”。

16.5.2 更新具有多个 XSCF 的模块化架构配置系统上的 XCP

1. 登录主 XSCF。
2. 执行 `showhardconf` 命令，并确认主 XSCF 和备用 XSCF 的 Status 是 Normal。
下面是 SPARC M10-4S 的示例。

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
```

```

+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;

```

3. 执行 **version** 命令检查正在运行的固件的版本。

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF         : 02.04.0001
XCP1 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF         : 02.04.0001
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF         : 02.04.0001
XCP1 (Current): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF         : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..

```

对于 SPARC M12-2S, 没有 CMU 固件的保留储存区。下面显示了一个显示示例。

```

XSCF# version -c xcp -v
BB#00-XSCF#0 (Standby)
XCP0 (Reserve): 3010
XSCF         : 03.01.0000
XCP1 (Current): 3010
XSCF         : 03.01.0000
CMU          : 03.01.0000
  POST       :
  OpenBoot PROM :

```

```

Hypervisor      :
BB#01-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF            : 03.01.0000
XCP1 (Current): 3010
XSCF            : 03.01.0000
CMU             : 03.01.0000

POST           :
OpenBoot PROM  :
Hypervisor     :
CMU BACKUP
#0: 03.01.0000
#1: ..
XSCF#

```

4. 执行 **getflashimage** 命令导入 XCP 映像文件。

下面的示例从连接到主 XSCF 的 XSCF 单元面板（后面板）上的 USB 端口（印刷“MAINTENANCE ONLY”）的 USB 设备导入 XSCF 映像文件。

```

XSCF> getflashimage file:///media/usb_msd/xxxx/BXCP2044.tar.gz
Existing versions:
      Version                Size  Date
      BXCP2041.tar.gz        90004045  Tue Apr 09 04:40:12 JST 2013
Mounted USB device
0MB received
1MB received
...
44MB received
45MB received
Download successful: 46827 Kbytes in 109 secs (430.094 Kbytes/sec)
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a4
XSCF>

```

当正常结束消息 "Download successful: ..." 和 "MD5: ..." 出现时，XCP 映像文件导入完成。

注 - 如果 XCP 导入后出现 "Error:File is invalid or corrupt" 消息，这意味着导入的 XCP 映像文件不是正确的文件。可能的原因是获得了未经授权的 XCP 映像文件，或者客户下载的 XCP 映像文件随后被未经授权的访问更改。在此情况下，请获取正确的 XCP 映像文件后重新导入 XCP。

5. 使用 **getflashimage -l** 命令来检查导入的 XCP 映像文件的版本。

```

XSCF> getflashimage -l
Existing versions:
      Version                Size  Date
      BXCP2044.tar.gz        90005045  Wed May 29 09:11:40 JST 2013

```

6 执行 **flashupdate -c check** 命令来检查导入的 XCP 映像文件是否可用于更新。执行 **flashupdate** 命令后，立即执行 **showresult** 命令。如果返回的结束值是 0，

则可使用更新文件。

```
XSCF> flashupdate -c check -m xcp -s 2044
XSCF> showresult
0
XSCF>
```

7. 执行 **flashupdate** 命令更新固件。

注 -

- 更新大约需要 60 分钟。
- 为了安全地更新固件，在作业期间（步骤 7 至 11）请勿执行物理分区的电源操作。

```
XSCF> flashupdate -c update -m xcp -s 2044
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [3600sec]
 0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....|
540.....570.....600.....630.....660.....690.....720.....750.....780.....-
810.....840.....870.....900.....930
:
```

此时，XSCF 被重新启动，XSCF 会话被断开。

此时，XCP 固件更新尚未完成。

8. 再次连接到主 XSCF。

在 XSCF 重新启动之后，主和备用 XSCF 的状态将从其原始状态反转。例如，当在 BB-ID 号 0 的主 XSCF 上执行固件更新时，重新连接到 XSCF 会将 BB-ID 号 1 的状态更改为主，将 BB-ID 号 0 的状态更改为备用。在此示例中，连接了主 XSCF (BB-ID 1)。

注 - 对于已经设置接管 IP 地址的客户，当使用接管 IP 地址连接时，将自动将机器连接到主 XSCF。

9. 执行 **showbbstatus** 命令，并确认已经登录主 XSCF。如果登录到备用 XSCF，则重新连接到主 XSCF。

注 - 如果固件更新为 XCP 2050 或更高版本，当 XCP 固件更新完成时，已切换的主/备用 XSCF 将返回到原始状态。在这种情况下，请再次连接到主 XSCF，因为 XSCF 被重新启动并且 XSCF 会话已断开连接。

```
XSCF> showbbstatus
BB#01 (Master)
```

10. 执行 **showlogs monitor** 命令检查 XCP 固件更新的完成情况。

XSCF> **showlogs monitor**

```
May 29 09:38:05 M10-4S-0 Event: SCF:XCP update is started (XCP version=2044:
last version=2041)
May 29 09:40:31 M10-4S-0 Event: SCF:XSCF update is started (BBID=0, bank=0)
May 29 09:40:46 M10-4S-0 Event: SCF:XSCF update is started (BBID=1, bank=0)
May 29 09:41:03 M10-4S-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 09:41:12 M10-4S-0 Event: SCF:XSCF writing is performed (BBID=1, XSCF
version=02040004)
May 29 09:48:18 M10-4S-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=0)
May 29 09:50:39 M10-4S-0 Event: SCF:XSCF update has been completed (BBID=1,
bank=0)
May 29 09:50:41 M10-4S-0 Event: SCF:XSCF bank apply has been completed
(BBID=1, bank=0, XCP version=2044:last version=2041)
May 29 10:01:50 M10-4S-0 Event: SCF:XSCF bank apply has been completed
(BBID=0, bank=0, XCP version=2044:last version=2041)
May 29 10:01:51 M10-4S-0 Event: SCF:Change Master Start(BB#01)
May 29 10:03:26 M10-4S-1 Event: SCF:Change Master Complete(BB#01)
May 29 10:05:00 M10-4S-1 Event: SCF:Standby XSCF Ready (BBID#00)
May 29 10:12:56 M10-4S-1 Event: SCF:XSCF update is started (BBID=1, bank=1)
May 29 10:13:23 M10-4S-1 Event: SCF:XSCF update is started (BBID=0, bank=1)
May 29 10:13:24 M10-4S-1 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 10:13:42 M10-4S-1 Event: SCF:XSCF writing is performed (BBID=1, XSCF
version=02040004)
May 29 10:20:22 M10-4S-1 Event: SCF:XSCF update has been completed (BBID=0,
bank=1)
May 29 10:23:34 M10-4S-1 Event: SCF:XSCF update has been completed (BBID=1,
bank=1)
May 29 10:24:42 M10-4S-1 Event: SCF:CMU update is started (BBID=0)
May 29 10:24:58 M10-4S-1 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 10:25:44 M10-4S-1 Event: SCF:CMU update is started (BBID=1)
May 29 10:25:46 M10-4S-1 Event: SCF:CMU writing is performed (BBID=1, CMU
version=02040004)
May 29 10:26:44 M10-4S-1 Event: SCF:CMU update has been completed (BBID=0)
May 29 10:27:51 M10-4S-1 Event: SCF:CMU update has been completed (BBID=1)
May 29 10:29:30 M10-4S-1 Event: SCF:CMU update is started (BBID=0)
May 29 10:29:36 M10-4S-1 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 10:29:45 M10-4S-1 Event: SCF:CMU update is started (BBID=1)
May 29 10:30:04 M10-4S-1 Event: SCF:CMU writing is performed (BBID=1, CMU
version=02040004)
May 29 10:31:18 M10-4S-1 Event: SCF:CMU update has been completed (BBID=0)
May 29 10:31:51 M10-4S-1 Event: SCF:CMU update has been completed (BBID=1)
May 29 10:32:38 M10-4S-1 Event: SCF:XCP update has been completed (XCP
version=2044:last version=2041)
May 29 10:32:39 M10-4S-1 Event: SCF:This XSCF will be switched back to standby
mode after completion of firmware update
May 29 10:32:39 M10-4S-1 Event: SCF:Change Master Start(BB#00)
May 29 10:33:29 M10-4S-1 Event: SCF:Change Master Complete(BB#00)
May 29 10:42:29 M10-4S-1 Event: SCF:Standby XSCF Ready (BBID#01)
```

下面是 SPARC M12-2S 上显示消息的示例。

```
XSCF> showlogs monitor
Apr  5 06:51:06 M12-2S-1 Event: SCF:XCP update is started (XCP version=3010:
last version=3009)
Apr  5 07:01:41 M12-2S-1 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=1, bank=1)
Apr  5 07:03:46 M12-2S-1 Event: SCF:Updating XCP:Updating XSCF (BBID=1, XSCF
version=03010000)
Apr  5 07:03:54 M12-2S-1 Event: SCF:Updating XCP:XSCF updated (BBID=1, bank=1)
Apr  5 07:06:58 M12-2S-1 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Apr  5 07:09:22 M12-2S-1 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Apr  5 07:10:39 M12-2S-1 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=0)
Apr  5 07:12:50 M12-2S-1 Event: SCF:Updating XCP:XSCF bank has changed
(BBID=1, bank=1, XCP version=3010:last version=3009)
Apr  5 07:20:06 M12-2S-1 Event: SCF:Updating XCP:XSCF bank has changed
(BBID=0, bank=0, XCP version=3010:last version=3009)
Apr  5 07:21:27 M12-2S-1 Event: SCF:Change Master Start(BB#01)
Apr  5 07:22:28 M12-2S-2 Event: SCF:Standby XSCF Ready(BB#01)
Apr  5 07:24:05 M12-2S-2 Event: SCF:Change Master Complete(BB#01)
Apr  5 07:30:08 M12-2S-2 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=1, bank=0)
Apr  5 07:30:35 M12-2S-2 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Apr  5 07:34:41 M12-2S-2 Event: SCF:Standby XSCF Ready(BB#00)
Apr  5 07:35:21 M12-2S-2 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Apr  5 07:40:32 M12-2S-2 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=1)
Apr  5 07:40:39 M12-2S-2 Event: SCF:Updating XCP:Updating XSCF (BBID=1, XSCF
version=03010000)
Apr  5 07:45:49 M12-2S-2 Event: SCF:Updating XCP:XSCF updated (BBID=1, bank=0)
Apr  5 07:46:18 M12-2S-2 Event: SCF:Updating XCP:Preparing to update CMU
(BBID=0)
Apr  5 07:46:41 M12-2S-2 Event: SCF:Updating XCP:Updating CMU (BBID=0, CMU
version=03010000)
Apr  5 07:48:21 M12-2S-2 Event: SCF:Updating XCP:CMU updated (BBID=0)
Apr  5 07:49:00 M12-2S-2 Event: SCF:Updating XCP:Preparing to update CMU
(BBID=1)
Apr  5 07:49:30 M12-2S-2 Event: SCF:Updating XCP:Updating CMU (BBID=1, CMU
version=03010000)
Apr  5 07:51:24 M12-2S-2 Event: SCF:Updating XCP:CMU updated (BBID=1)
Apr  5 07:51:25 M12-2S-2 Event: SCF:XCP update has been completed (XCP
version=3010:last version=3009)
Apr  5 07:51:26 M12-2S-2 Event: SCF:This XSCF will be switched back to standby
mode after completion of firmware update
Apr  5 07:51:57 M12-2S-1 Event: SCF:Change Master Complete(BB#00)
```

如果出现 "XCP update has been completed" 信息，则 XCP 固件更新已经完成。

注 - SPARC M10 上将显示类似于 "XSCF update has been completed" 或 "CMU update has been completed" 的消息。然而，在消息出现时，所有 XCP 固件的更新并没有完成。为了安全地更新固件，请勿对物理分区执行电源操作，直到您已确认 XCP 固件的更新完成信

息 "XCP update has been completed"。

如果没有出现 "XCP update has been completed" 信息，则更新尚未完成。再次执行 `showlogs monitor` 命令检查更新的完成情况。
通常，在 XSCF 重新启动后约 40 分钟更新完成。

- 如果物理分区的电源开启

在执行 `flashupdate` 命令和检查更新完成时，目标 CMU 固件的更新还没有开始。因此，对于 CMU 固件，此消息不会出现。当在步骤 12 中物理分区电源关闭然后开启时，目标 CMU 固件的更新开始。

- 如果将固件更新到版本 XCP 2050 或更高版本

固件更新完成后，将自动切换主 XSCF 和备用 XSCF。自动切换大约需要 10 分钟。

如果出现 "This XSCF will be switched back to standby mode after completion of firmware update", "Change Master Complete" 和 "Stand by XSCF Ready" 信息，已经完成切换。

如需检查切换的完成情况，请执行 `showhardconf` 命令，并确认主 XSCF 和备用 XSCF 的 Status 是 Normal。

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

确认切换已经完成后，转到步骤 12。

注 - 如果执行 `showhardconf` 命令后显示 "Cannot communicate with the other XSCF.Check the other XSCF's state."，则主和备用 XSCF 的切换尚未完成。再次执行 `showhardconf` 命令检查切换的完成情况。

注 - 固件更新处理将两次切换主和备用 XSCF。因此，您所执行 `flashupdate` 命令的 XSCF 返回到作为主 XSCF。切换主和备用 XSCF 可能会断开 XSCF 会话。如果 XSCF 会话断开，则重新进行连接。

- 如果将固件更新到版本 XCP 2044 或早期版本

固件更新处理将切换主 XSCF 和备用 XSCF。其结果是，与您执行 `flashupdate` 命令的 XSCF 配对的另一个 XSCF 成为主 XSCF。

11. 执行 **switchscf** 命令，将主和备用 **XSCF** 返回到其更新前的状态。

注 - 当将固件更新到版本 XCP 2050 或更高版本时，由于 XSCF 已经被切换，您不必进行此项作业。

```
XSCF> switchscf -t Standby
The XSCF unit switch between the Active and Standby states.
Continue? [y|n] :y
```

由于 XSCF 重新启动会断开 XSCF 会话，因此主 XSCF 将再次连接。

如需检查切换的完成情况，请执行 **showhardconf** 命令，并确认主 XSCF 和备用 XSCF 的 Status 是 Normal。

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

注 - 如果执行 **showhardconf** 命令后显示 "Cannot communicate with the other XSCF.Check the other XSCF's state."，则主和备用 XSCF 的切换尚未完成。再次执行 **showhardconf** 命令检查切换的完成情况。

12. 当物理分区的电源开启时，若需完成 **CMU** 固件更新，请执行关闭物理分区电源，然后开启物理分区电源。

注 - 对于逻辑域配置，请在控制域中执行 Oracle VM Server for SPARC 的 **ldm add-sponfig** 命令，使得在关闭物理分区之前将最新配置信息保存在 XSCF 中。有关详情，请参见 "6.2.2 系统停止之前保存逻辑域配置信息" 和 "10.11.1 保存/显示逻辑域配置信息"。

注 - 如果物理分区的电源关闭，由于 CMU 固件更新已经完成，您不必进行此项作业。转到步骤 13。

如果物理分区的电源开启，执行 **poweroff** 命令关闭物理分区的电源。

```
XSCF> poweroff -p xx
```


执行 `showpparstatus power` 命令，并确认物理分区电源已关闭。

```
XSCF> showpparstatus -p xx
PPAR-ID          PPAR Status
xx               Powered Off
```

执行 `poweron` 命令来开启物理分区的电源。

```
XSCF> poweron -p xx
```

执行 `showpparstatus` 命令，并确认 PPAR Status 是 "Running"。

```
XSCF> showpparstatus -p xx
PPAR-ID          PPAR Status
xx               Running
```

13. 执行 `version` 命令，并确认固件版本是最新版本。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCPO (Reserve): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCPL (Current): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
BB#01-XSCF#0 (Standby)
XCPO (Current): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCPL (Reserve): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
CMU BACKUP
#0: 02.04.0004
#1: ..
```

注 - 在 SPARC M10-1/M10-4/M10-4S 上, 如果通过开启物理分区的电源来更新固件, 则会更新 CMU 固件的当前储存区。

如果通过停止物理分区的电源来更新固件, 则不但会更新 CMU 固件的保留储存区, 而且会更新当前储存区。

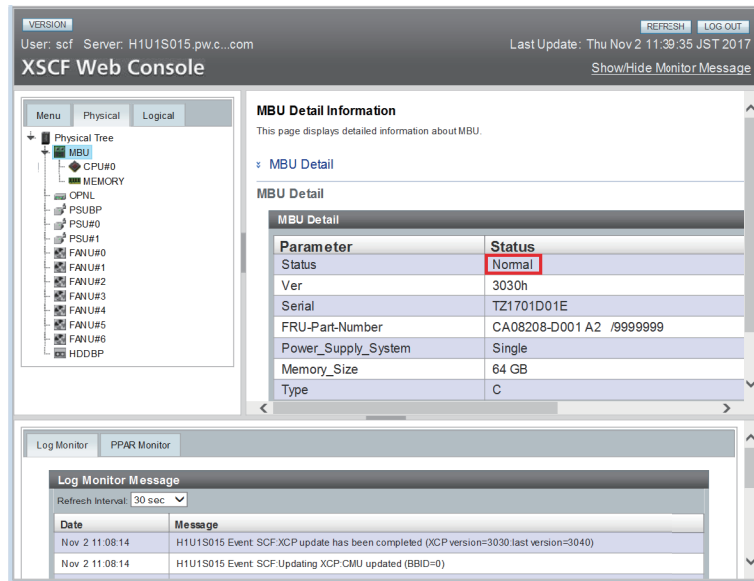
关于与 XCP 版本对应的 CMU 固件版本, 请参见您的服务器最新《Fujitsu M10/SPARC M10 系统产品说明》中的“现有 XCP 固件版本和支持信息”。

16.6 从 XSCF Web 更新固件

本节以 SPARC M12-1 的示例介绍如何从 XSCF Web 更新固件。

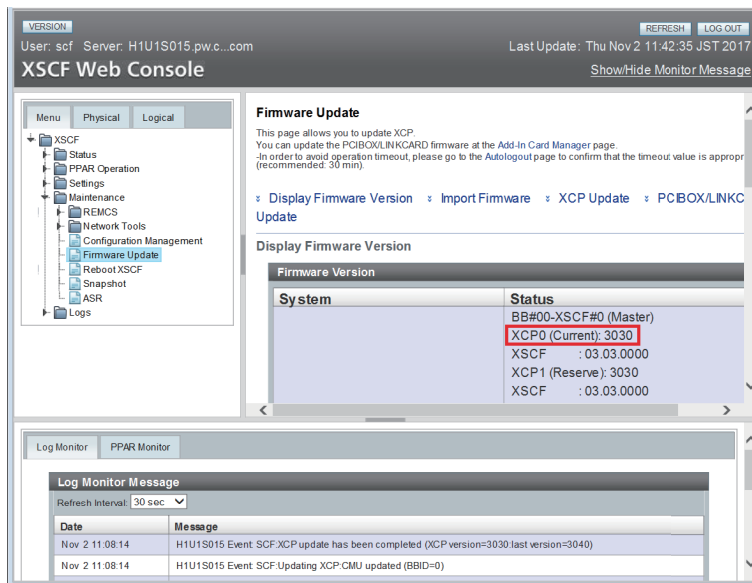
1. 登录到 **XSCF Web**。
2. 选择 **[Physical]** (物理) - **[MBU]**。
3. 在 **[MBU Detail]** (MBU 详细信息) 画面上确认 **MBU** 的状态为 **Normal**, 如 [图 16-2](#) 所示。

图 16-2 [MBU Detail] (MBU 详细信息) 画面



4. 选择 **[Menu]** (菜单) - **[Maintenance]** (维护) - **[Firmware Update]** (固件更新)。
5. 在 [图 16-3](#) 中所示的 **[Display Firmware Version]** (显示固件版本) 画面中确认运行中的 **XCP** 固件的版本。

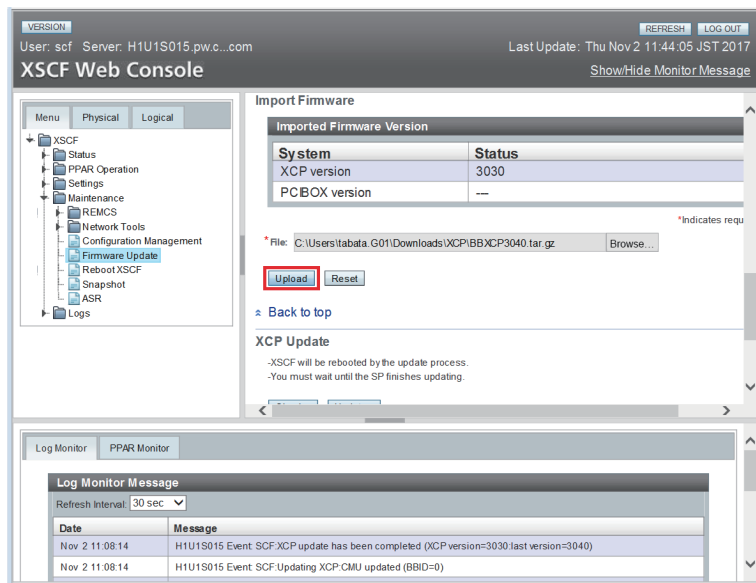
图 16-3 [Display Firmware Version] (显示固件版本) 画面



- 从图 16-4 中所示的 [Import Firmware] (导入固件) 画面导入 XCP 图像文件。指定 XCP 图像文件的路径，然后单击 [Upload] (上传) 按钮。导入大约需要五分钟。

注 - 如果出现覆盖警告消息 "An existing file will be overwritten, continue to process?", 单击 [OK] (确定) 按钮。

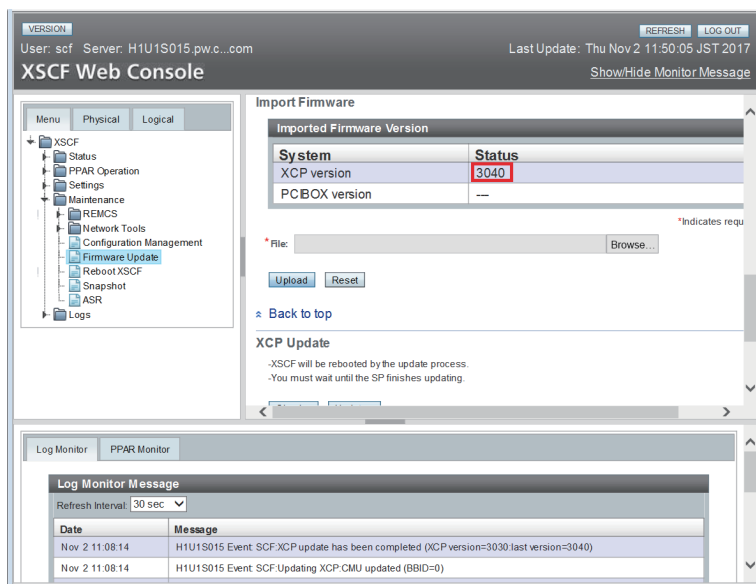
图 16-4 [Import Firmware] (导入固件) 画面



出现 "The file has been uploaded successfully." 时，导入完成。

图 16-5 中显示的 [Import Firmware] (导入固件) 画面上的 XCP 版本行已更新。确认该行显示所导入的 XCP 映像文件的固件版本。

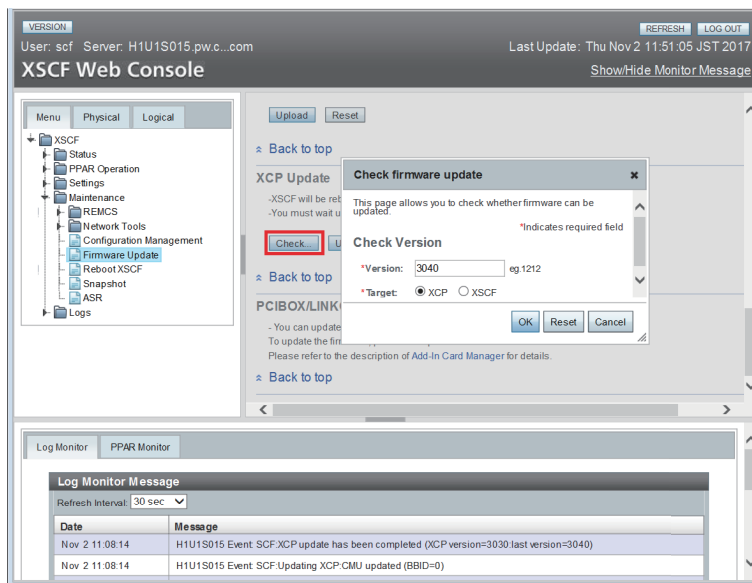
图 16-5 导入结束后的 [Import Firmware] (导入固件) 画面



7. 检查 图 16-6 中显示的 [XCP Update] (XCP 更新) 画面，以便查看所导入的 XCP 映像文件是否可用于更新固件。
单击 [Check] (检查) 按钮并在弹出窗口中指定固件版本，以便启动文件检查。如

果出现 "The XCP file has been checked successfully.", 该文件可用于固件更新。

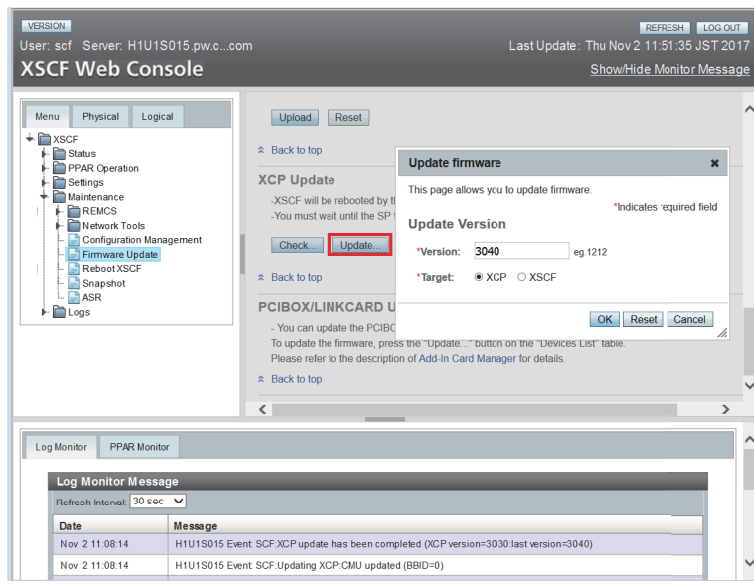
图 16-6 从 [XCP Update] (XCP 更新) 画面检查 XCP 图像文件



8. 从 图 16-7 中显示的 [XCP Update] (XCP 更新) 画面更新固件。
单击 [Update] (更新) 按钮, 并在弹出窗口中指定固件版本来启动固件更新。更新大约需要 30 分钟。

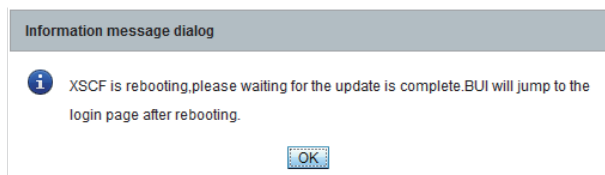
注 - 在模块化架构配置中, 更新过程大约需要 60 分钟。

图 16-7 从 [XCP Update] (XCP 更新) 画面更新固件



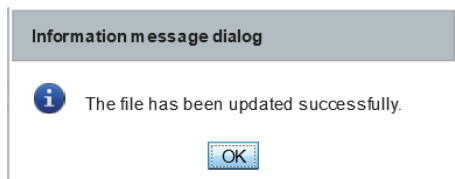
更新的中途，重新启动 XSCF，并断开 XSCF 会话。
输出 图 16-8 中显示的消息。

图 16-8 XSCF 重新启动消息



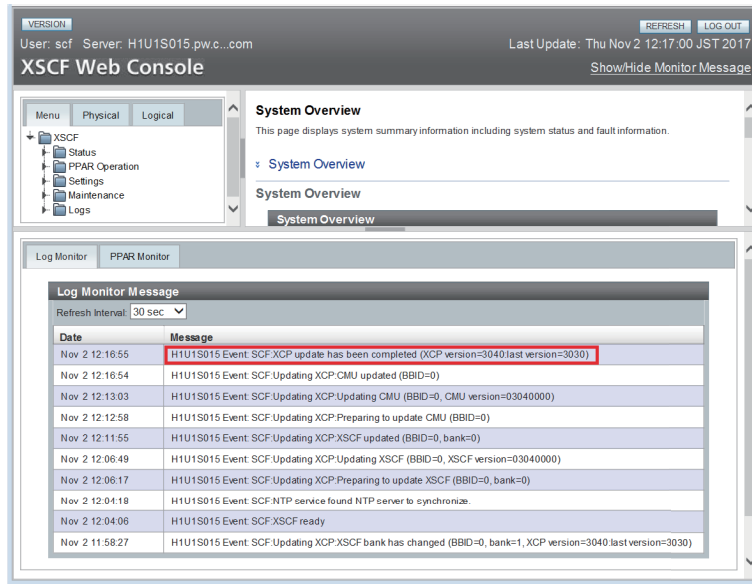
更新的中途，图 16-9 中显示的消息 "The file has been updated successfully" 也会出现。
此时，固件更新尚未完成。

图 16-9 更新期间的消息



9. 重新登录到 XSCF Web。
10. 查看 图 16-10 显示的窗口底部边框中 [Log Monitor Message] (日志监视器消息) 画面上的固件更新消息。

图 16-10 [Log Monitor Message] (日志监视器消息) 画面

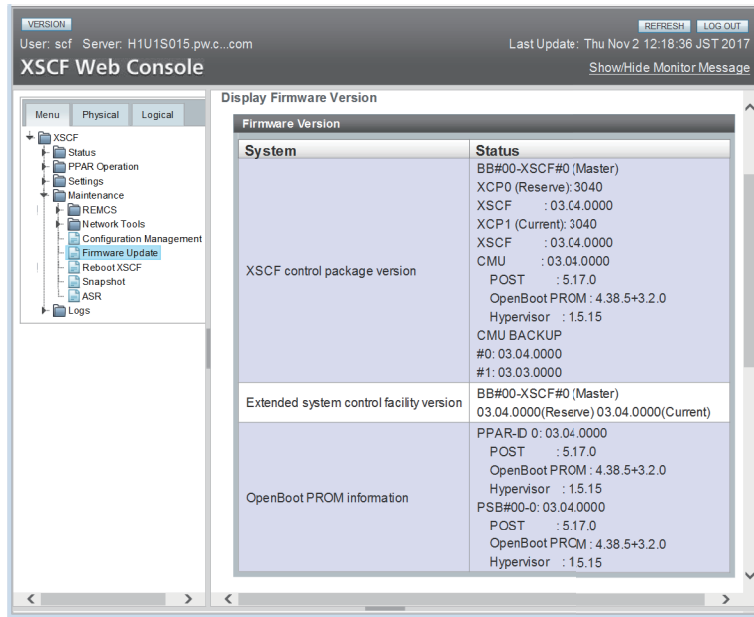


如果出现 "XCP update has been completed" 信息，则 XCP 固件更新已经完成。

注 - SPARC M10 上将显示类似于 "XSCF update has been completed" 或 "CMU update has been completed" 的消息。然而，在消息出现时，所有 XCP 固件的更新并没有完成。为了安全地更新固件，请勿对物理分区执行电源操作，直到您已确认 XCP 固件的更新完成信息 "XCP update has been completed"。

- 物理分区的电源开启：此时目标 CMU 固件尚未更新。因此，对于 CMU 固件，此消息不会出现。若需在 XCP 固件更新完成后完成 CMU 固件更新，请执行关闭物理分区电源，然后开启物理分区电源。
 - 在模块化架构配置中：模块化架构配置中的主 XSCF 和备用 XSCF 的状态在 XCP 固件更新完成后立即从其更新前状态反转。主 XSCF 和备用 XSCF 被切换可将其返回到其初始状态。自动切换大约需要 10 分钟。
11. 如 图 16-11 中所示，确认 [Display Firmware Version] (显示固件版本) 画面上的固件版本是最新版。

图 16-11 [Display Firmware Version] (显示固件版本) 画面



16.7 部件更换时固件版本匹配

按下述情况，更换部件和匹配固件版本。

- 当使用维护菜单已经添加/更换 SPARC M12-2S 的 XSCF 单元或 SPARC M10-4S 的 CPU 内存单元（下）时，固件版本会进行匹配。
- 当使用维护菜单已经添加/更换接线盒的 XSCF 单元时，XSCF 固件版本会进行匹配。

注 - 更换 SPARC M12-1/M10-1 系统的主板单元、SPARC M10-4 系统和所有 SPARC M10-4S 系统的 CPU 内存单元（下）、SPARC M12-2 和所有 SPARC M12-2S 系统的 XSCF 单元、以及所有接线盒的 XSCF 单元后，版本与预更换固件版本将无法自动匹配。请求作业者更新固件。

注 - 有关不使用维护菜单且输入电源关闭的情况下更换内存单元（下）(CMUL)、更换 XSCF 单元、添加 SPARC M10-4S 或添加接线盒时自动版本匹配的支持信息，请参见最新 XCP 版本的《Fujitsu M10/SPARC M10 系统 产品说明》。

16.7.1 输入电源开启情况下添加/更换时固件版本的匹配

本节介绍如何在输入电源开启情况下更换 CPU 内存单元（下）(CMUL)、更换 XSCF 单元、添加 SPARC M12-2S/M10-4S 或添加接线盒时匹配版本。

1. 执行 **addfru** 命令或 **replacefru** 命令后，如果使用维护菜单进行了添加/更换作业，则 **XSCF** 固件版本将自动匹配。
如果使用 **addfru** 命令、**replacefru** 命令或 **testsb** 命令执行诊断测试，则自动匹配 CMU 固件版本。
2. 完成 **addfru**、**replacefru** 或 **testsb** 命令后，执行 **version** 命令检查 **XCP** 固件版本。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF        : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF        : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..
```

16.7.2 输入电源关闭情况下添加/更换时固件版本的匹配

本节介绍如何在输入电源关闭情况下更换 CPU 内存单元（下）(CMUL)、更换 XSCF 单元、添加 SPARC M12-2S/M10-4S 或添加接线盒时匹配版本。

1. 更换 **CPU** 内存单元（下）(CMUL)、更换 **XSCF** 单元、添加 **SPARC M10-4S** 或添加接线盒后，登录 **XSCF** 并执行 **version** 命令检查 **XCP** 固件版本。

注 - 登录后，如果显示 "XSCF firmware update now in progress.BB#xx, please wait for XSCF firmware update complete." 信息，则正在自动执行 XCP 固件版本匹配。
开始下一步任务之前，执行 **showlogs monitor** 命令，并确认已显示消息 "XCP firmware version synchronization completed"。

以下示例显示，在不使用维护菜单的情况下完成添加/更换后，BB#01 的固件版本不匹配。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor   : 0.26.9
XSCF         : 02.04.0001
XCP1 (Current): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor   : 0.26.9
XSCF         : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..
```

注 - 使用维护菜单进行添加/更换后，固件版本与所有 SPARC M12-2S/M10-4S 系统和所有接线盒的 XSCF 单元相匹配。

2. 如果固件版本不匹配，执行 **flashupdate -c sync** 命令将其匹配到主 XSCF 固件版本。

```
XSCF> flashupdate -c sync
XCP update is started. [3600sec]
 0.....30.....60.....90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....|
540.....570.....600.....630.....660.....690.....720.....750.....780.....-
810.....840.....870.....900.....930.....960.....990.....1020.....1050.....\
1080.....1110.....1140.....1170.....1200.....1230.....1260.....1290.....
1320...../
1350.....1380.....1410.....1440.....1470.....1500.....1530.....1560.....15
90.....\
1620.....1650.....1680.....1710.....1740.....1770.....1800.....1830.....
```

```
1860...../  
1890.....1920.....1950.....1980.....2010.....2040.....2070.....2100.....  
2130.....\  
2160.....2190..XSCF>  
XSCF>
```

3. 执行 **version** 命令，并确认 **XCP** 固件版本匹配 **XSCF** 固件版本。

```
XSCF> version -c xcp -v  
BB#00-XSCF#0 (Master)  
XCP0 (Reserve): 2044  
CMU          : 02.04.0004  
  POST       : 1.43.0  
  OpenBoot PROM : 4.34.0+1.19.0  
  Hypervisor   : 0.27.3  
XSCF         : 02.04.0004  
XCP1 (Current): 2044  
CMU          : 02.04.0004  
  POST       : 1.43.0  
  OpenBoot PROM : 4.34.0+1.19.0  
  Hypervisor   : 0.27.3  
XSCF         : 02.04.0004  
BB#01-XSCF#0 (Standby)  
XCP0 (Reserve): 2044  
CMU          : 02.04.0001  
  POST       : 1.42.0  
  OpenBoot PROM : 4.34.0+1.16.0  
  Hypervisor   : 0.26.9  
XSCF         : 02.04.0004  
XCP1 (Current): 2044  
CMU          : 02.04.0001  
  POST       : 1.42.0  
  OpenBoot PROM : 4.34.0+1.16.0  
  Hypervisor   : 0.26.9  
XSCF         : 02.04.0004  
CMU BACKUP  
#0: 02.04.0001  
#1: ..
```

此时目标 CMU 固件未更新。

4. 上电目标物理分区，进行 **CMU** 固件版本匹配。 执行 **poweron** 命令来开启物理分区的电源。

```
XSCF> poweron -p xx
```

执行 **showpparstatus** 命令，并确认 PPAR Status 是 "Running"。

```
XSCF> showpparstatus -p xx  
PPAR-ID          PPAR Status  
XX               Running
```

5. 执行 `version` 命令检查目标物理分区的 **CMU** 固件版本。

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..
```

16.8 固件更新期间出现故障

如果在固件更新时发生异常停止或输出类似下列的错误信息，则异常的 XSCF 单元无法使用并被作为故障部件处理：

- 有一个 XSCF 的系统中
写入或重新启动故障相关的错误
- 有多个 XSCF 的系统中
备用 XSCF 或主 XSCF 上的写入或重新启动故障相关的错误

但是，如果在固件更新时出现故障，请尝试重新执行固件更新。在第二次尝试时，固件更新可能正常结束。

16.9 与固件更新相关的常见问题

问题: 更新 **CMU** 固件时是否可以重新启动两次?

回答: 没问题。

问题: 在有多个 **XSCF** 的系统中, 为什么主 **XSCF** 和备用 **XSCF** 在更新中途切换?

回答: 主 **XSCF** 执行控制以便对备用 **XSCF** 进行固件更新。当备用侧固件更新完成后, 备用侧具有新固件。备用侧切换到主侧, 再次对备用侧 (旧主侧) 的 **XSCF** 进行固件更新。

问题: 是否可以一次将全部物理分区都执行 **CMU** 固件更新?

回答: 是。如果所有物理分区的电源都关闭, 可一次更新固件。如果物理分区的电源开启, 通过执行 `poweroff -a` 命令可将其更新到新固件, 然后指定所有物理分区执行 `poweron -a` 命令。

更新 Oracle Solaris 和 Oracle VM Server for SPARC

本章介绍如何更新安装在逻辑域上的 Oracle Solaris。

为物理分区配置的各逻辑域已经安装了 Oracle Solaris。您可以在各逻辑域上单独更新 Oracle Solaris。

更新之前

更新控制域上的 Oracle Solaris 之前，请事先保存下列数据。更新后需恢复数据。

- 自动保存配置目录
/var/opt/SUNWldm/autosave-*
- 逻辑域约束数据库文件
/var/opt/SUNWldm/ldom-db.xml 提供了对逻辑域约束数据库文件的引用。

有关详情，请参见您所使用版本的《Oracle VM Server for SPARC Administration Guide》中的 "Installing and Enabling Software"。

更新

更新 Oracle Solaris 时，请使用最新的 SRU（支持存储库更新）。

有关受支持的 Oracle Solaris 版本和最新 SRU 相关信息，请参见服务器的最新《产品说明》。

有关如何更新 Oracle Solaris 和 Oracle VM Server for SPARC 的详细信息，请参见 Oracle Solaris 的相关手册和所使用版本的《Oracle VM Server for SPARC Administration Guide》中的 "Installing and Enabling Software"。

故障排除

本章介绍使用 XSCF 期间或系统运行时可能发生的问题，以及如何解决问题。

- 关于 XSCF 的故障排除
- 使用 RESET 开关的注意事项
- 常见问题/FAQ
- 使用 XSCF 进行系统故障排除

18.1 关于 XSCF 的故障排除

本节介绍使用 XSCF 期间可能发生的问题，以及如何解决问题。

无法登录到 XSCF

- 检查所输入的登录用户名是否正确。
- 检查所使用的密码是否正确。
- 检查当前连接到 XSCF 的用户的数量。有关用户数量的详情，请参见“2.6 可连接的用户数”。

忘记了 XSCF 的登录密码

- 请系统管理员重置密码。具有 platadm 或 useradm 用户权限的系统管理员可以使用 password 命令重置密码。
- 如果系统管理员忘记了登录密码，请使用“默认”帐户登录，并使用 password 命令再次设置密码。有关使用“默认”帐户登录验证的详细信息，请参见您的服务器的《安装指南》中的“执行初始系统诊断”。

通过串行端口无法连接 XSCF

- 检查终端软件是否连接到串行端口。
- 检查终端软件的设置（波特率 9600bps，0 以外的延迟等）。有关设置的详细信息，请参见“2.2.1 如何使用串行连接登录 XSCF shell”。

注 - 如果即使已经执行上述措施后, XSCF 连接仍然失败, 则按下后面板上的 RESET 开关可能会解决问题。有关详情, 请参见 "18.2 使用 RESET 开关的注意事项"。

使用 Telnet 通过 XSCF-LAN 无法连接 XSCF

- 检查 XSCF shell 终端和服务器之间的 LAN 线是否正确连接。
- 检查终端软件是否连接到 Telnet 端口。
- 使用 `shownetwork` 命令检查 XSCF-LAN 是否启用。
- 使用 `showtelnet` 命令检查 Telnet 服务是否启用。
- 确认所输入的 IP 地址和端口编号与设置没有不同。
- 确认通过 Telnet/SSH 连接的数量没有超过上限。有关上限的详情, 请参见 "2.6 可连接的用户数"。
- 如有必要, 请使用通过串行端口直接连接到 XSCF 的 PC 上的控制台登录到 XSCF shell, 并使用 `shownetwork` 命令检查 XSCF-LAN 设置。

注 - 如果即使已经执行上述措施后, XSCF 连接仍然失败, 则按下后面板上的 RESET 开关可能会解决问题。有关详情, 请参见 "18.2 使用 RESET 开关的注意事项"。

使用 SSH 通过 XSCF-LAN 无法连接 XSCF

- 确认 XSCF shell 终端和服务器之间的 LAN 线是否正确连接。
- 执行 `shownetwork` 命令确认 XSCF-LAN 设置是否已启用。
- 执行 `showssh` 命令确认 SSH 服务是否已启用。
- 确认所输入的 IP 地址和端口编号与设置没有不同。
- 确认通过 Telnet/SSH 连接的数量没有超过上限。有关上限的详情, 请参见 "2.6 可连接的用户数"。
- 如有必要, 请使用通过串行端口直接连接到 XSCF 的 PC 上的控制台登录到 XSCF shell, 并执行 `shownetwork` 命令检查 XSCF-LAN 设置。
- 确认主机密钥设置是否正确。请注意, 更换 XSCF 单元会将主机密钥返回到 XSCF 上预设的密钥。
- 确认客户端软件是否具有正确的设置。

注 - 如果即使已经执行上述措施后, XSCF 连接仍然失败, 则按下后面板上的 RESET 开关可能会解决问题。有关详情, 请参见 "18.2 使用 RESET 开关的注意事项"。

XSCF 的 IP 地址未知

- 使用 `shownetwork` 命令检查当前的网络配置。如果地址尚未设置, 请通知网络管理员检查设置。
- 如有必要, 请使用通过串行端口直接连接到 XSCF 的 PC 上的控制台登录到 XSCF shell, 并使用 `shownetwork` 命令检查 XSCF-LAN 设置。

XSCF shell 终端或域控制台突然断开连接

- 由其他用户执行与 XSCF 网络相关的 `setnetwork`、`setroute`、`sethostname`、`setnameserver` 和 `setsscp` 命令后，`applynetwork` 和 `rebootxscf` 命令可能已被执行。或者，`flashupdate` 命令可能已被执行。如需使用 XSCF，请建立其他连接，并再次登录。
- 其他用户可能已执行有关 XSCF 的 `setdate` 或 `switchscf` 命令。如需使用 XSCF，请建立其他连接，并再次登录。
- 登录后，如果 XSCF shell 在特定时间内未使用，则 XSCF 会自动终止 shell。只有在启用了时间监控功能并且在 XSCF 设置中为此功能设置了时间段时，才会在该时间段过后发生此强制终止。
- 输入由客户端设定的转义字符（例如“#”和“.”）（句号）密钥断开了 Oracle Solaris Secure Shell 或 OpenSSH 的 SSH 客户端。如果 Oracle Solaris Secure Shell 或 OpenSSH 的 SSH 客户端的转义字符与控制台命令设置的转义字符具有相同的设置，则终端会断开连接。因此，需变更其中一个的设置值。有关详细信息，请参见 SSH 客户端手册。

无法进行服务器开机/关机操作

- 对于使用 `platadm` 或 `fieldeng` 权限之外的用户权限的操作，整个系统的开机/关机操作不可用。有关用户权限的详情，请参见“3.5.3 用户权限类型”。

无法添加 XSCF 用户

- 检查 XSCF 用户的注册数量。有关注册数量的详情，请参见“2.6 可连接的用户数”。或者通知系统管理员。

没有来自 XSCF 的电子邮件通知

- XSCF 不一定报告所有事件。它发送有关部件故障、验证失败事件等的电子邮件。如需检查错误日志中的预期通知或事件日志中报告的事件，请参见“12.1 检查 XSCF 保存的日志”。
- 使用 `showemailreport` 命令检查是否启用该设置。如果没有电子邮件到达，请检查是否向错误电子邮件通知收件人发送错误电子邮件，或检查错误日志中记录的错误。
- 如果使用手机接收此类电子邮件，请检查手机设置中是否有其电子邮件地址的任何接收限制。

无法访问 XSCF Web 的首页

- 使用 `showhttps` 命令检查 XSCF Web 是否启用。
- 检查所输入的 URL 是否正确。（例如包括 `https` 是否缺失“s”。）
- 请与系统管理员确认 IP 地址的权限设置。
- 检查 Web 浏览器的 TLS 1.0 连接设置是否已启用。

不显示 XSCF Web 窗口

- 如果从 XSCF Web 的首页登录后，XSCF Web 的个别窗口不出现，则可能禁用了

Web 浏览器设置中的 JavaScript。启用 Web 浏览器设置中的 JavaScript，然后再次登录。

- 如果 Web 浏览器的设置阻止弹出窗口，则 XSCF Web 窗口无法显示。检查 Web 浏览器的设置。

忘记了 XSCF Web 的密码

- XSCF Web 验证与 XSCF shell 验证相同。请参见上述“[忘记了 XSCF 的登录密码](#)”。

使用 XSCF Web 登录后初始访问失败

- 检查 Web 浏览器设置中是否接受 cookie。

Web 浏览器窗口中未正确显示 XSCF Web

- 某些版本的 Web 浏览器可能在其窗口中无法正确显示 XSCF。请参见“[2.4 登录 XSCF Web](#)”中支持的浏览器，并将 Web 浏览器更新到最新版本。

XSCF Web 上显示警告

- 检查安全警告的内容，并停止使用 XSCF Web。根据所检查警告的内容采取适当的措施。如果已过期，请再次配置 XSCF 的 HTTPS 服务。有关 HTTPS 服务的详情，请参见“[3.8 配置用于登录 XSCF 的 HTTPS 服务](#)”。

其他故障

- 通知系统管理员。如果需要收集/保存 XSCF 日志，请使用 XSCF shell 命令保存 XSCF 日志。有关如何保存日志的详细信息，请参见“[12.1.15 使用快照将日志保存到文件](#)”。

18.2 使用 RESET 开关的注意事项

RESET 开关是紧急开关，它位于 SPARC M12/M10 和接线盒的后面板上，可以重新启动 XSCF。

当应用本节中介绍的措施后 XSCF 还不启动也不能对 XSCF 进行访问时，请使用 RESET 开关作为紧急措施。

使用 RESET 开关时，请注意以下事项。

- 使用 RESET 开关作为启动 XSCF 的最后手段。
- 如果即使按下 RESET 开关后 XSCF 也不启动，请咨询维修工程师。
- XSCF 运行时，请勿多次按 RESET 开关。如果反复按 RESET 开关，CHECK LED 指示灯会点亮，XSCF READY LED 指示灯会熄灭。然后，XSCF 停止。如果发生这种情况，您需要关闭/开启连接到 XSCF 的输入电源。

对于 RESET 开关的位置，请参见您的服务器的《Service Manual》或《Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》中的“附录 C External Interface Specifications”。

18.3 常见问题/FAQ

本节包含有关使用 XSCF 的常见问题。

问题：XSCF-LAN 是否使用默认情况下分配给 LAN 端口的 IP 地址？

回答：XSCF-LAN 的 IP 地址不是默认分配的 IP 地址。有关 XSCF-LAN IP 地址的详情，请参见 ["3.9.2 了解 XSCF 网络接口"](#)。

问题：是否为 SSCP 分配了默认 IP 地址？

回答：默认分配 IP 地址。有关默认 SSCP IP 地址，请参见 ["3.9.5 了解使用 SSCP 设置的 IP 地址"](#)。如果默认 IP 地址可能会影响用户 LAN 环境，请将其进行变更。

问题：如果在服务器上电后 Oracle Solaris 启动期间 Oracle Solaris 挂起，则是否可以从 XSCF 对服务器关机？

回答：如果来宾域挂起，请使用 `ldm panic-domain` 命令收集 Oracle Solaris 转储。有关 `ldm` 命令的详情，请参见您所使用版本的《Oracle VM Server for SPARC Reference Manual》。

如果控制域挂起，请执行以下操作。

1. 执行带有在 **XSCF shell** 中指定的 **panic** 选项的 **reset** 命令，为 **Oracle Solaris** 转储提供指示。
2. 如果即使执行了步骤 1.，**Oracle Solaris** 转储也失败，则在 **XSCF shell** 中执行 **poweroff** 命令关闭电源。

问题：在向服务器提供输入电源直到 Oracle Solaris 启动之后，XSCF 执行什么样的处理？

回答：直到系统启动的处理流程如下。有关详情，请参见 ["第6章 启动/停止系统"](#)。

1. 作业人员开启输入电源。
2. XSCF 启动。
3. 作业人员对服务器上电。
4. XSCF 初始化硬件。
5. POST 启动并执行初始硬件诊断。
6. OpenBoot PROM 启动。
7. OpenBoot PROM 开始启动过程。
8. Oracle Solaris 启动。

问题：XSCF 正常登录或注销期间，终端上出现什么样的消息？

回答：XSCF 登录成功/失败如下所述。
以下是登录成功的示例。

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

以下是登录失败的示例。

```
login: jsmith
Password: xxxxxxxx
Login incorrect
```

回答：XSCF 注销成功/失败如下所述。
以下是注销成功的示例。

```
XSCF> exit
Logout
```

以下是注销失败的示例。

```
XSCF> exit
Not supported in this system.
```

注 - 上述示例根据终端上的客户端软件的不同而有所差异。

问题：XSCF 错误日志和 MIB 定义文件中的错误信息之间有什么关系？

回答：反映在 MIB 定义文件中的错误信息是最新的 XSCF 错误日志。

18.4 使用 XSCF 进行系统故障排除

本节介绍如何在服务器未响应（这意味着系统中出现问题或崩溃）时有效地使用 XSCF。

通知维修工程师之前

联系维修工程师之前，按照以下步骤进行操作。该步骤不仅有助于解决问题，而且消除了查询的需要。

1. 如果服务器没有响应，请将操作面板上的 **Mode** 开关设置为 **Service** 模式。
2. 使用以下其中一种方法检查系统状态。
 - XSCF shell 通过 SSH/Telnet 无法使用时的方法
 - a. 将终端连接到 XSCF 的串行端口。
 - b. 输入您的用户帐户和密码登录到 XSCF shell。
 - c. 使用 XSCF shell 检查错误日志和其他信息。
 - XSCF shell 通过 SSH/Telnet 和串行端口可以使用时的方法
 - a. 使用 XSCF 用户帐户登录到 XSCF。
 - b. 连接到 XSCF-LAN 端口，并使用 XSCF shell 检查错误日志和其他信息。
有关错误日志的详情，请参见 "12.1 检查 XSCF 保存的日志"。检查并采取相应措施。

- c. 或者，通过串行端口使用 XSCF shell 来检查 XSCF 事件日志和服务器状态。
执行以下命令来检查出现问题时发生的事件：

```
showlogs error
```

```
showlogs event
```

```
showlogs power
```

```
showlogs monitor
```

```
showlogs console
```

如果出现故障，请参见 "12.1 检查 XSCF 保存的日志"。检查并采取相应措施。

- d. 检查 XSCF 控制台日志或崩溃日志以获取最新消息。
Oracle Solaris 可能已经检测到问题并显示了一条消息。另外，对于涉及崩溃的情况，请使用带 panic 选项的 showlogs 命令来检查发生崩溃时发生的事件。
3. 当上述检查没有发现任何问题时，重新启动系统。
 4. 如果发生故障，请参见 "12.1 检查 XSCF 保存的日志"。采取相应的措施，如按照 XSCF shell 命令的维护指导来更换部件。

SPARC M12/M10 系统设备路径列表

本附录介绍 SPARC M12/M10 系统的设备路径。

- SPARC M12-1 设备路径
- SPARC M12-2 设备路径
- SPARC M12-2S 设备路径
- SPARC M10-1 设备路径
- SPARC M10-4 设备路径
- SPARC M10-4S 设备路径

A.1 SPARC M12-1 设备路径

由 SPARC M12-1 识别的设备路径以及与设备路径对应的硬件模块图如下。

表 A-1 SPARC M12-1 机箱和 PCI 扩展单元侧的 I/O 设备路径

实例优先级	设备	设备路径	图中编号
1	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@1/network@0	1
2	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@1/network@0,1	2
3	内部 SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0	3
-	内部 HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	4
-	内部 HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	5
-	内部 HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	6
-	内部 HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	7
-	内部 HDD#4	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p4	8
-	内部 HDD#5	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5	9
-	内部 HDD#6	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p6	10
-	内部 HDD#7	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p7	11

表 A-1 SPARC M12-1 机箱和 PCI 扩展单元侧的 I/O 设备路径 (续)

实例优先级	设备	设备路径	图中编号
-	外部 SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	12
4	内部 USB 端口 (后面: USB 3.0)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/****@1	13
	内部 USB 端口 (后面: USB 2.0/1.1)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/****@1	14
5	内部 USB 端口 (前面: USB 2.0/1.1)	/pci@8100/pci@4/pci@0/pci@8/usb@0/****@6	15
6	远程存储	/pci@8100/pci@4/pci@0/pci@8/usb@0/storage@7	16
7	PCI#0	/pci@8100/pci@4/pci@0/pci@9/****@0	17
	PCI#0 下的 PCI 扩展单元		
8	PCI#1	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
9	PCI#2	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
10	PCI#3	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
11	PCI#4	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
12	PCI#5	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
13	PCI#6	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
14	PCI#7	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
15	PCI#8	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
16	PCI#9	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
17	PCI#10	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
18	PCI#11	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
19	内部 LAN#2	/pci@8200/pci@4/pci@0/pci@0/network@0	18
20	内部 LAN#3	/pci@8200/pci@4/pci@0/pci@0/network@0,1	19
21	PCI#1	/pci@8200/pci@4/pci@0/pci@8/****@0	20
	PCI#1 下的 PCI 扩展单元		
22	PCI#1	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
23	PCI#2	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	

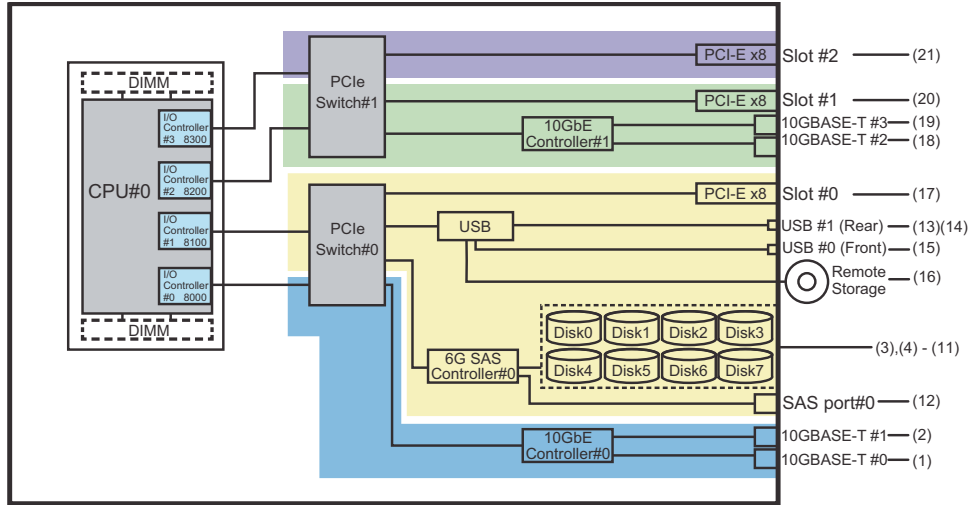
表 A-1 SPARC M12-1 机箱和 PCI 扩展单元侧的 I/O 设备路径 (续)

实例优先级	设备	设备路径	图中编号
24	PCI#3	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@8/****@0	
25	PCI#4	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
26	PCI#5	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
27	PCI#6	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
28	PCI#7	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
29	PCI#8	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
30	PCI#9	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
31	PCI#10	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
32	PCI#11	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
33	PCI#2	/pci@8300/pci@4/pci@0/pci@1/****@0	21
	PCI#2 下的 PCI 扩展单元		
34	PCI#1	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@0/****@0	
35	PCI#2	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@1/****@0	
36	PCI#3	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@8/****@0	
37	PCI#4	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
38	PCI#5	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
39	PCI#6	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
40	PCI#7	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
41	PCI#8	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
42	PCI#9	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
43	PCI#10	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@10/****@0	

表 A-1 SPARC M12-1 机箱和 PCI 扩展单元侧的 I/O 设备路径 (续)

实例优先级	设备	设备路径	图中编号
44	PCI#11	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@11/****@0	

图 A-1 SPARC M12-1 模块图



A.2 SPARC M12-2 设备路径

由 SPARC M12-2 识别的设备路径以及与设备路径对应的硬件模块图如下。

A.2.1 对应初始安装 1-CPU 配置の場合

以下是初始安装 1-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令禁用 I/O 总线重新配置 (`ioreconfigure`)，则以下设备路径也适用于将单 CPU 配置扩展为 2 个 CPU 配置的添加情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 1 个 CPU 配置扩展为 2 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 2 个 CPU 配置 (表 A-4)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后扩展配置。

SPARC M12-2 机箱中 I/O 设备路径

表 A-2 SPARC M12-2 机箱中 I/O 设备路径（初始安装时: 单CPU）

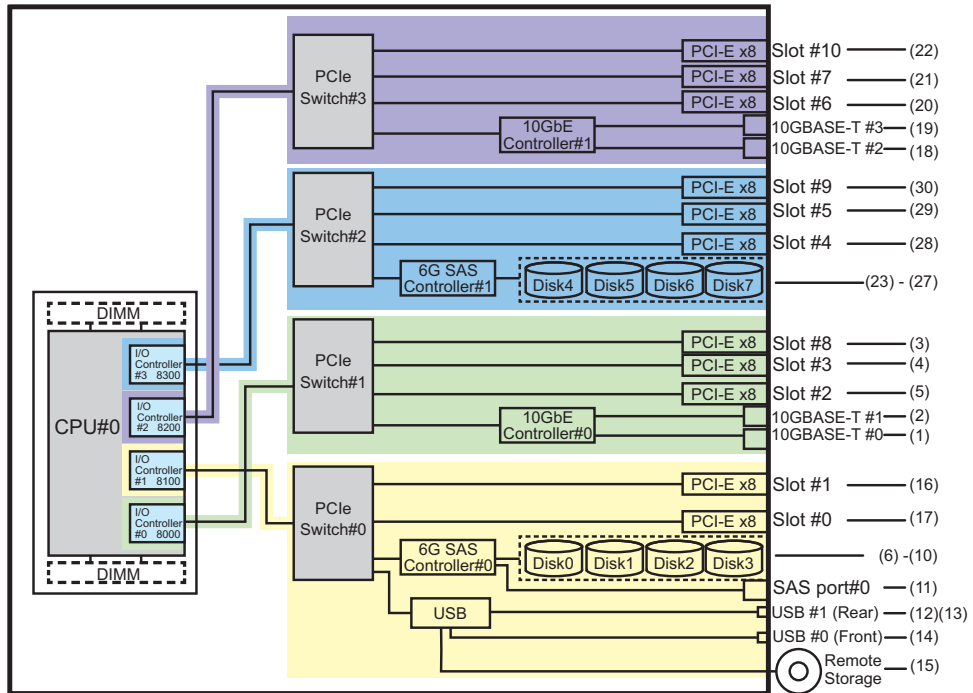
实例 优先级	设备	设备路径	图中编号
1	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#8	/pci@8000/pci@4/pci@0/pci@1/****@0	3
4	PCI#3	/pci@8000/pci@4/pci@0/pci@10/****@0	4
5	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	5
6	内部 SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	6
-	内部 HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	7
-	内部 HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	8
-	内部 HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	9
-	内部 HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	10
-	外部 SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	11
7	内部 USB 端口 (后面:USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	12
8	内部 USB 端口 (后面:USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	13
9	内部 USB 端口 (前面:USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	14
10	远程存储	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	15
11	PCI#1	/pci@8100/pci@4/pci@0/pci@10/****@0	16
12	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	17
13	内部 LAN#2	/pci@8200/pci@4/pci@0/pci@0/network@0	18
14	内部 LAN#3	/pci@8200/pci@4/pci@0/pci@0/network@0,1	19
15	PCI#6	/pci@8200/pci@4/pci@0/pci@1/****@0	20
16	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	21
17	PCI#10	/pci@8200/pci@4/pci@0/pci@9/****@0	22
18	内部 SAS#1	/pci@8300/pci@4/pci@0/pci@0/scsi@0	23
-	内部 HDD#4	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p4	24
-	内部 HDD#5	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p5	25
-	内部 HDD#6	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p6	26
-	内部 HDD#7	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p7	27
19	PCI#4	/pci@8300/pci@4/pci@0/pci@1/****@0	28

表 A-2 SPARC M12-2 机箱中 I/O 设备路径（初始安装时: 单CPU）(续)

实例优先级	设备	设备路径	图中编号
20	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	29
21	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	30

*1 如果使用了 USB3.0 设备，则其按 USB2.0 工作。

图 A-2 SPARC M12-2 模块图（单CPU）



PCI 扩展单元侧 I/O 设备路径

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在表 A-2 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-3 PCI 扩展单元侧 I/O 设备路径（单CPU）

实例优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0

表 A-3 PCI 扩展单元侧 I/O 设备路径（单CPU）(续)

实例优先级	设备	设备路径
4	PCI#4	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.2.2 对应初始安装 2-CPU 配置的场所

以下是初始安装 2-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令禁用 I/O 总线重新配置 (`ioreconfigure`)，则以下设备路径也适用于将 2 个 CPU 配置缩减为 1 个 CPU 配置的移除情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 2 个 CPU 配置缩减为 1 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 1 个 CPU 配置 (表 A-2)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后缩减配置。

SPARC M12-2 机箱中 I/O 设备路径

表 A-4 SPARC M12-2 机箱中 I/O 设备路径（初始安装时: 2 个 CPU）

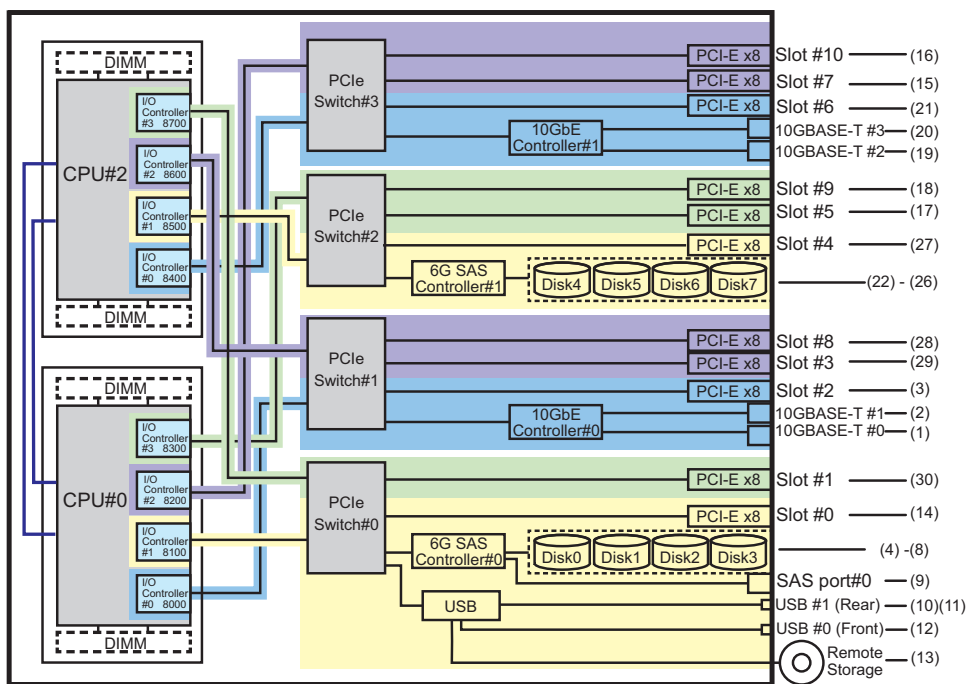
实例优先级	设备	设备路径	图中编号
1	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	3

表 A-4 SPARC M12-2 机箱中 I/O 设备路径（初始安装时: 2 个 CPU）(续)

实例 优先级	设备	设备路径	图中编号
4	内部 SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	4
-	内部 HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	5
-	内部 HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	6
-	内部 HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	7
-	内部 HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	8
-	外部 SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	9
5	内部 USB 端口 （后面:USB3.0）	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	10
6	内部 USB 端口 （后面:USB2.0/1.1）	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	11
7	内部 USB 端口 （前面:3.0/2.0/1.1） (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	12
8	远程存储	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	13
9	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	14
10	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	15
11	PCI#10	/pci@8200/pci@4/pci@0/pci@9/****@0	16
12	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	17
13	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	18
14	内部 LAN#2	/pci@8400/pci@4/pci@0/pci@0/network@0	19
15	内部 LAN#3	/pci@8400/pci@4/pci@0/pci@0/network@0,1	20
16	PCI#6	/pci@8400/pci@4/pci@0/pci@1/****@0	21
17	内部 SAS#1	/pci@8500/pci@4/pci@0/pci@0/scsi@0	22
-	内部 HDD#4	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p4	23
-	内部 HDD#5	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p5	24
-	内部 HDD#6	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p6	25
-	内部 HDD#7	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p7	26
18	PCI#4	/pci@8500/pci@4/pci@0/pci@1/****@0	27
19	PCI#8	/pci@8600/pci@4/pci@0/pci@1/****@0	28
20	PCI#3	/pci@8600/pci@4/pci@0/pci@10/****@0	29
21	PCI#1	/pci@8700/pci@4/pci@0/pci@10/****@0	30

*1 如果使用了 USB3.0 设备，则其按 USB2.0 工作。

图 A-3 SPARC M12-2 模块图 (2 个 CPU)



PCI 扩展单元侧 I/O 设备路径

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在表 A-4 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-5 PCI 扩展单元侧 I/O 设备路径 (2 个 CPU)

实例优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0

表 A-5 PCI 扩展单元侧 I/O 设备路径 (2 个 CPU) (续)

实例优先级	设备	设备路径
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.3 SPARC M12-2S 设备路径

由 SPARC M12-2S 识别的设备路径以及与设备路径对应的硬件模块图如下。

A.3.1 对应初始安装 1-CPU 配置的情况

以下是初始安装 1-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令禁用 I/O 总线重新配置 (`ioreconfigure`)，则以下设备路径也适用于将单 CPU 配置扩展为 2 个 CPU 配置的添加情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 1 个 CPU 配置扩展为 2 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 2 个 CPU 配置 (表 A-9)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后扩展配置。

SPARC M12-2S 机箱中 I/O 设备路径

表 A-6 SPARC M12-2S 机箱中 I/O 设备路径 (初始安装时: 单 CPU)

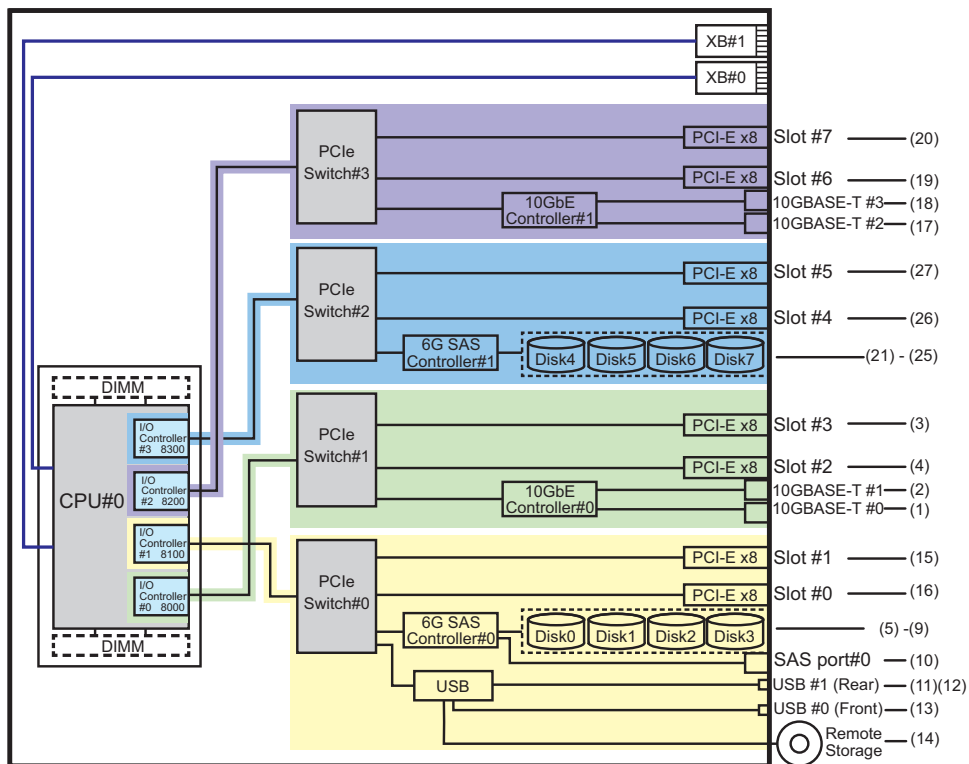
实例优先级	设备	设备路径	图中编号
1	LSB#0	内部 LAN#0 /pci@8000/pci@4/pci@0/pci@0/network@0	1
2		内部 LAN#1 /pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#3	/pci@8000/pci@4/pci@0/pci@10/****@0	3
4	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	4
5	内部 SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	5
-	内部 HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	6

表 A-6 SPARC M12-2S 机箱中 I/O 设备路径（初始安装时:单CPU）(续)

实例优先级	设备	设备路径	图中编号
-	内部 HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	7
-	内部 HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	8
-	内部 HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	9
-	外部 SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
6	内部 USB 端口 （后面:USB3.0）	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	11
7	内部 USB 端口 （后面:USB2.0/1.1）	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	12
8	内部 USB 端口 （前面:USB3.0/2.0/1.1）(*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	13
9	远程存储	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	14
10	PCI#1	/pci@8100/pci@4/pci@0/pci@10/****@0	15
11	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	16
12	内部 LAN#2	/pci@8200/pci@4/pci@0/pci@0/network@0	17
13	内部 LAN#3	/pci@8200/pci@4/pci@0/pci@0/network@0,1	18
14	PCI#6	/pci@8200/pci@4/pci@0/pci@1/****@0	19
15	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	20
16	内部 SAS#1	/pci@8300/pci@4/pci@0/pci@0/scsi@0	21
-	内部 HDD#4	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p4	22
-	内部 HDD#5	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p5	23
-	内部 HDD#6	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p6	24
-	内部 HDD#7	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p7	25
17	PCI#4	/pci@8300/pci@4/pci@0/pci@1/****@0	26
18	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	27

*1 如果使用了 USB3.0 设备，则其按 USB2.0 工作。

图 A-4 SPARC M12-2S 模块图



PCI 扩展单元侧 I/O 设备路径

如果具有连接到 PCI 扩展单元链路卡的服务器侧 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在表 A-6 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-7 PCI 扩展单元侧 I/O 设备路径

实例优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0

表 A-7 PCI 扩展单元侧 I/O 设备路径 (续)

实例优先级	设备	设备路径
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

逻辑系统板的 I/O 设备路径

对于 LSB#1 至 LSB#15 的 I/O 设备路径，表 A-7 中 I/O 设备路径开头的设备节点 (/pci@vwww) 将变为表 A-8 中所示。其他设备节点与表 A-7 中相同。

例如，对于 LSB#1，如下所示解释表 A-7 中的节点值。LSB#2 到 LSB#15 的节点值按照同样的方法说明。

/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00

表 A-8 LSB#1 至 LSB#15 的 I/O 设备路径 (初始安装时: 单 CPU)

LSB 编号	设备路径
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ...
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ...
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ...
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ...
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ...

表 A-8 LSB#1 至 LSB#15 的 I/O 设备路径（初始安装时: 单CPU）(续)

LSB 编号	设备路径
LSB#6	/pci@b000/ ...
	/pci@b100/ ...
	/pci@b200/ ...
	/pci@b300/ ...
LSB#7	/pci@b800/ ...
	/pci@b900/ ...
	/pci@ba00/ ...
	/pci@bb00/ ...
LSB#8	/pci@c000/ ...
	/pci@c100/ ...
	/pci@c200/ ...
	/pci@c300/ ...
LSB#9	/pci@c800/ ...
	/pci@c900/ ...
	/pci@ca00/ ...
	/pci@cb00/ ...
LSB#10	/pci@d000/ ...
	/pci@d100/ ...
	/pci@d200/ ...
	/pci@d300/ ...
LSB#11	/pci@d800/ ...
	/pci@d900/ ...
	/pci@da00/ ...
	/pci@db00/ ...
LSB#12	/pci@e000/ ...
	/pci@e100/ ...
	/pci@e200/ ...
	/pci@e300/ ...
LSB#13	/pci@e800/ ...
	/pci@e900/ ...
	/pci@ea00/...
	/pci@eb00/...
LSB#14	/pci@f000/...
	/pci@f100/...
	/pci@f200/...
	/pci@f300/...
LSB#15	/pci@f800/...
	/pci@f900/...
	/pci@fa00/...
	/pci@fb00/...

A.3.2 对应初始安装 2-CPU 配置の場合

以下是初始安装 2-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令禁用 I/O 总线重新配置 (`ioreconfigure`)，则以下设备路径也适用于将 2 个 CPU 配置缩减为 1 个 CPU 配置的移除情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 2 个 CPU 配置缩减为 1 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 1 个 CPU 配置 (表 A-6)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后缩减配置。

SPARC M12-2S 机箱中 I/O 设备路径

表 A-9 SPARC M12-2S 机箱中 I/O 设备路径 (初始安装时: 2 个 CPU)

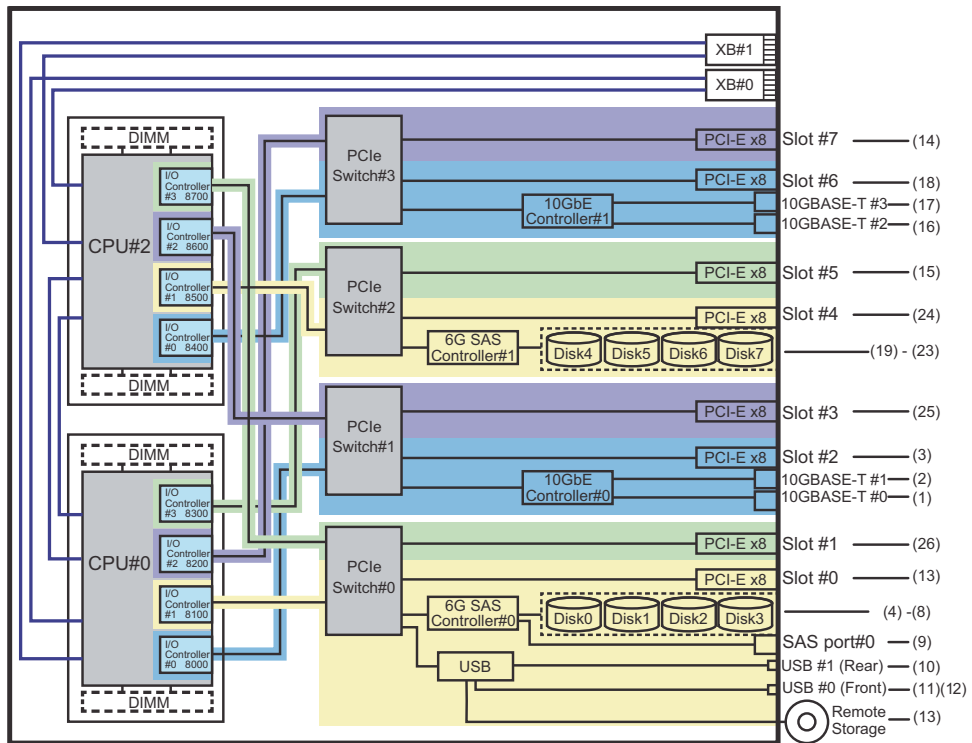
实例优先级	设备	设备路径	图中编号
1	LSB#0 内部 LAN#0	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	3
4	内部 SAS#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0	4
-	内部 HDD#0	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	5
-	内部 HDD#1	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	6
-	内部 HDD#2	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	7
-	内部 HDD#3	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	8
-	外部 SAS	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	9
5	内部 USB 端口 (后面:USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	10
6	内部 USB 端口 (后面:USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	11
7	内部 USB 端口 (前面:USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	12
8	远程存储	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	13
9	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	14
10	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	15
11	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	16
12	内部 LAN#2	/pci@8400/pci@4/pci@0/pci@0/network@0	17
13	内部 LAN#3	/pci@8400/pci@4/pci@0/pci@0/network@0,1	18
14	PCI#6	/pci@8400/pci@4/pci@0/pci@1/****@0	19
15	内部 SAS#1	/pci@8500/pci@4/pci@0/pci@0/scsi@0	20
-	内部 HDD#4	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p4	21

表 A-9 SPARC M12-2S 机箱中 I/O 设备路径 (初始安装时: 2 个 CPU) (续)

实例优先级	设备	设备路径	图中编号
-	内部 HDD#5	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p5	22
-	内部 HDD#6	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p6	23
-	内部 HDD#7	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p7	24
16	PCI#4	/pci@8500/pci@4/pci@0/pci@1/****@0	25
17	PCI#3	/pci@8600/pci@4/pci@0/pci@10/****@0	26
18	PCI#1	/pci@8700/pci@4/pci@0/pci@10/****@0	27

*1 如果使用了 USB3.0 设备, 则其按 USB2.0 工作。

图 A-5 SPARC M12-2S 模块图



PCI 扩展单元侧 I/O 设备路径

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X, 则将创建以下相应 vvvv 和 u 显示在表 A-9 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-10 PCI 扩展单元侧 I/O 设备路径

实例优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

逻辑系统板的 I/O 设备路径

LSB#1 至 LSB#15 的设备路径具有类似 LSB#0 的按 LSB# 升序的实例优先级。开头的设备节点（表 A-10 中的 /pci@vwww）将变为表 A-11 中所示。其他设备节点与表 A-10 中相同。

例如，对于 LSB#1，如下所示解释表 A-11 中的节点值。LSB#2 到 LSB#15 的节点值按照同样的方法说明。

```
/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00
/pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00, /pci@8700->/pci@8f00
```

表 A-11 LSB#1 至 LSB#15 的 I/O 设备路径 (初始安装时: 2 个 CPU)

LSB 编号	设备路径
LSB#1	/pci@8800/ ...
	/pci@8900/ ...
	/pci@8a00/ ...
	/pci@8b00/ ...
	/pci@8c00/...
	/pci@8d00/...
	/pci@8e00/...
LSB#2	/pci@8f00/...
	/pci@9000/ ...
	/pci@9100/ ...
	/pci@9200/ ...
	/pci@9300/ ...
	/pci@9400/...
	/pci@9500/...
LSB#3	/pci@9600/...
	/pci@9700/...
	/pci@9800/ ...
	/pci@9900/ ...
	/pci@9a00/ ...
	/pci@9b00/ ...
	/pci@9c00/...
LSB#4	/pci@9d00/...
	/pci@9e00/...
	/pci@9f00/...
	/pci@a000/ ...
	/pci@a100/ ...
	/pci@a200/ ...
	/pci@a300/ ...
LSB#5	/pci@a400/...
	/pci@a500/...
	/pci@a600/...
	/pci@a700/...
	/pci@a800/ ...
	/pci@a900/ ...
	/pci@aa00/ ...
LSB#6	/pci@ab00/ ...
	/pci@ac00/...
	/pci@ad00/...
	/pci@ae00/...
	/pci@af00/...
	/pci@b000/ ...
	/pci@b100/ ...
LSB#7	/pci@b200/ ...
	/pci@b300/ ...
	/pci@b400/...
	/pci@b500/...
	/pci@b600/...
	/pci@b700/...

表 A-11 LSB#1 至 LSB#15 的 I/O 设备路径 (初始安装时: 2 个 CPU) (续)

LSB 编号	设备路径
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ... /pci@bc00/... /pci@bd00/... /pci@be00/... /pci@bf00/...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ... /pci@c400/... /pci@c500/... /pci@c600/... /pci@c700/...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ... /pci@cc00/... /pci@cd00/... /pci@ce00/... /pci@cf00/...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ... /pci@d400/... /pci@d500/... /pci@d600/... /pci@d700/...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ... /pci@dc00/... /pci@dd00/... /pci@de00/... /pci@df00/...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ... /pci@e400/... /pci@e500/... /pci@e600/... /pci@e700/...

表 A-11 LSB#1 至 LSB#15 的 I/O 设备路径（初始安装时: 2 个 CPU）(续)

LSB 编号	设备路径
LSB#13	/pci@e800/ ...
	/pci@e900/ ...
	/pci@ea00/ ...
	/pci@eb00/ ...
	/pci@ec00/ ...
	/pci@ed00/ ...
	/pci@ee00/ ...
LSB#14	/pci@ef00/ ...
	/pci@f000/ ...
	/pci@f100/ ...
	/pci@f200/ ...
	/pci@f300/ ...
	/pci@f400/ ...
	/pci@f500/ ...
LSB#15	/pci@f600/ ...
	/pci@f700/ ...
	/pci@f800/ ...
	/pci@f900/ ...
	/pci@fa00/ ...
	/pci@fb00/ ...
	/pci@fc00/ ...
	/pci@fd00/ ...
	/pci@fe00/ ...
	/pci@ff00/ ...

A.4 SPARC M10-1 设备路径

由 SPARC M10-1 识别的设备路径以及与设备路径对应的硬件模块图如下。

表 A-12 SPARC M10-1 机箱和 PCI 扩展单元侧的 I/O 设备路径

实例 优先级	设备	设备路径	图中编 号
1	内部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-	内部 HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-	内部 HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	内部 HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	内部 HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	内部 HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	内部 HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	内部 HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8

表 A-12 SPARC M10-1 机箱和 PCI 扩展单元侧的 I/O 设备路径 (续)

实例 优先级	设备	设备路径	图中编 号
-	内部 HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	外部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@1/network@0	11
3	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@1/network@0,1	12
4	内部 USB 端口 (后面: USB 1.1)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4/****@1	13
5	内部 USB 端口 (前面: USB 1.1)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4/****@2	14
6	内部 USB 端口 (后面: USB 2.0)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/****@1	13
7	内部 USB 端口 (前面: USB 2.0)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/****@2	14
8	远程存储	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3	15
9	PCI#0	/pci@8000/pci@4/pci@0/pci@8/****@0	16
	PCI#0 下的 PCI 扩展单元		
10	PCI#1	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
11	PCI#2	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
12	PCI#3	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
13	PCI#4	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@0/****@0	
14	PCI#5	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@1/****@0	
15	PCI#6	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@10/****@0	
16	PCI#7	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@11/****@0	
17	PCI#8	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@0/****@0	
18	PCI#9	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@1/****@0	
19	PCI#10	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@10/****@0	
20	PCI#11	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@11/****@0	
21	内部 LAN#2	/pci@8100/pci@4/pci@0/pci@0/network@0	17
22	内部 LAN#3	/pci@8100/pci@4/pci@0/pci@0/network@0,1	18
23	PCI#1	/pci@8100/pci@4/pci@0/pci@1/****@0	19
	PCI#1 下的 PCI 扩展单元		

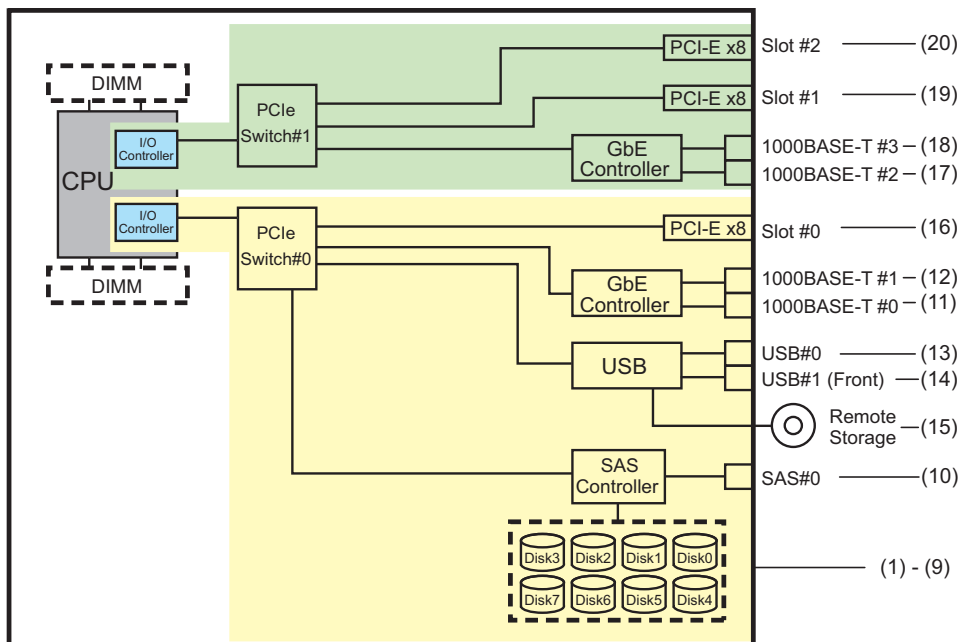
表 A-12 SPARC M10-1 机箱和 PCI 扩展单元侧的 I/O 设备路径 (续)

实例 优先级	设备	设备路径	图中编 号
24	PCI#1	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
25	PCI#2	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
26	PCI#3	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
27	PCI#4	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@0/****@0	
28	PCI#5	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@1/****@0	
29	PCI#6	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@10/****@0	
30	PCI#7	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@11/****@0	
31	PCI#8	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@0/****@0	
32	PCI#9	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@1/****@0	
33	PCI#10	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@10/****@0	
34	PCI#11	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@11/****@0	
35	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
	PCI#2 下的 PCI 扩展单元		
36	PCI#1	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
37	PCI#2	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
38	PCI#3	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
39	PCI#4	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@0/****@0	
40	PCI#5	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@1/****@0	
41	PCI#6	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@10/****@0	
42	PCI#7	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@11/****@0	
43	PCI#8	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@0/****@0	
44	PCI#9	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@1/****@0	
45	PCI#10	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@10/****@0	

表 A-12 SPARC M10-1 机箱和 PCI 扩展单元侧的 I/O 设备路径 (续)

实例 优先级	设备	设备路径	图中编 号
46	PCI#11	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@11/****@0	

图 A-6 SPARC M10-1 模块图



A.5 SPARC M10-4 设备路径

由 SPARC M10-4 识别的设备路径以及与设备路径对应的硬件模块图如下。

A.5.1 对应初始安装 2-CPU 配置の場合

以下是初始安装 2-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令禁用 I/O 总线重新配置 (`ioreconfigure`)，则以下设备路径也适用于将 2 个 CPU 配置扩展为 4 个 CPU 配置的添加情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 2 个 CPU 配置扩展为 4 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 4 个 CPU 配置 (表 A-16)。此时，系统将更改为出厂默认

配置。在这种情况下，逻辑域需要重新配置。
 另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。
 如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后扩展配置。

SPARC M10-4 机箱的 I/O 设备路径

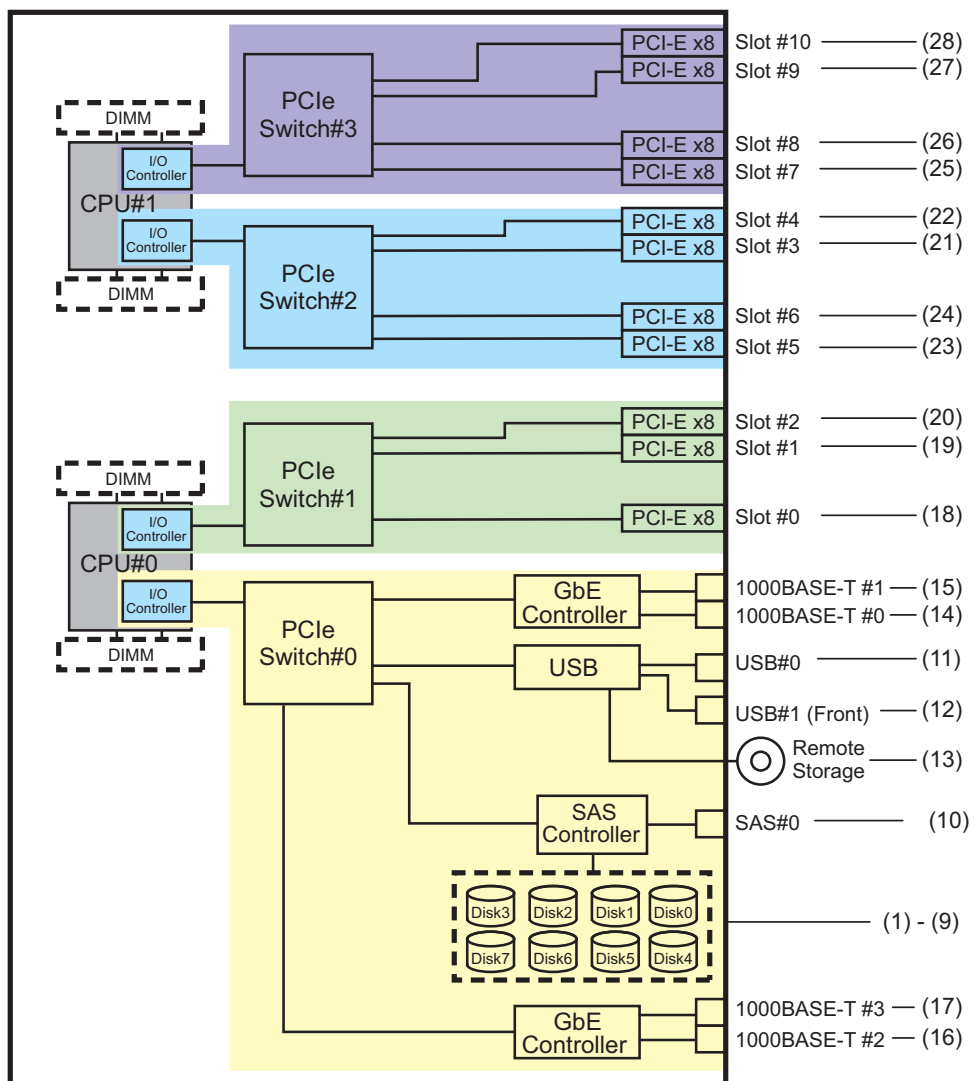
表 A-13 SPARC M10-4 机箱的 I/O 设备路径（初始安装时：2 个 CPU）

实例 优先级	设备	设备路径	图中编号
1	LSB#0 内部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-	内部 HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-	内部 HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	内部 HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	内部 HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	内部 HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	内部 HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	内部 HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	内部 HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	外部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	内部 USB 端口 （后面：USB 1.1）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	内部 USB 端口 （后面：USB 2.0）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	内部 USB 端口 （前面：USB 1.1/2.0）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	远程存储	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	内部 LAN#2	/pci@8000/pci@4/pci@0/pci@a/network@0	16
9	内部 LAN#3	/pci@8000/pci@4/pci@0/pci@a/network@0,1	17
10	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	18
11	PCI#1	/pci@8100/pci@4/pci@0/pci@8/****@0	19
12	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
13	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	21
14	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	22
15	PCI#5	/pci@8200/pci@4/pci@0/pci@9/****@0	23

表 A-13 SPARC M10-4 机箱的 I/O 设备路径（初始安装时：2 个 CPU）（续）

实例 优先级	设备	设备路径	图中编号
16	PCI#6	/pci@8200/pci@4/pci@0/pci@11/****@0	24
17	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	25
18	PCI#8	/pci@8300/pci@4/pci@0/pci@8/****@0	26
19	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	27
20	PCI#10	/pci@8300/pci@4/pci@0/pci@11/****@0	28

图 A-7 SPARC M10-4 模块图（2 个 CPU）



PCI 扩展单元侧 I/O 设备路径

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在 表 A-13 中 PCI#X 设备路径 /pci/vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-14 PCI 扩展单元侧 I/O 设备路径（初始安装时: 2 个 CPU）

实例 优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci/vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.5.2 对应初始安装 4-CPU 配置の場合

以下是初始安装 4-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 setpparmode 命令禁用 I/O 总线重新配置 (ioreconfigure)，下面的设备路径也适用于将 4-CPU 配置减少为 2-CPU 配置的移除情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (ioreconfigure) 并将 4 个 CPU 配置缩减为 2 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 2 个 CPU 配置 (表 A-13)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后缩减配置。

SPARC M10-4 机箱的 I/O 设备

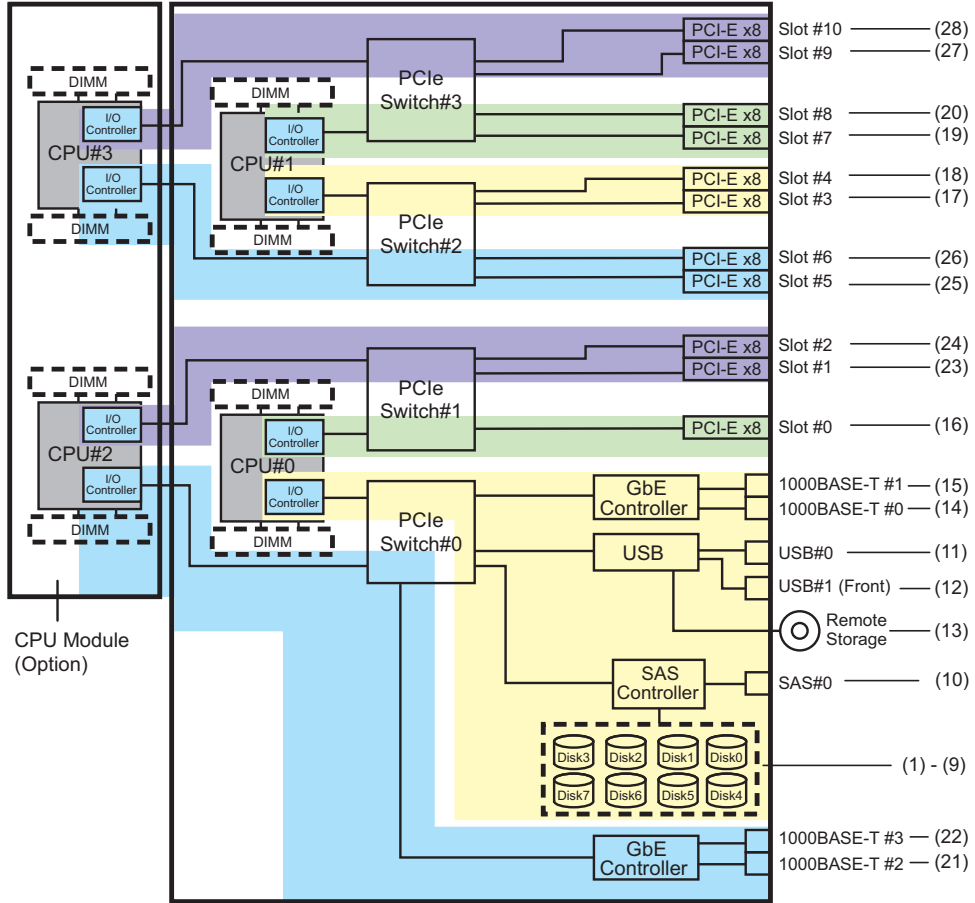
表 A-15 SPARC M10-4 机箱的 I/O 设备（初始安装时：4 个 CPU）

实例 优先级	设备	设备路径	图中编号
1	LSB#0 内部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-	内部 HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-	内部 HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	内部 HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	内部 HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	内部 HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	内部 HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	内部 HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	内部 HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	外部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	内部 USB 端口 （后面：USB 1.1）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	内部 USB 端口 （后面：USB 2.0）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	内部 USB 端口 （前面：USB 1.1/2.0）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	远程存储	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	16
9	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	17
10	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	18
11	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	19
12	PCI#8	/pci@8300/pci@4/pci@0/pci@8/****@0	20
13	内部 LAN#2	/pci@8400/pci@4/pci@0/pci@a/network@0	21
14	内部 LAN#3	/pci@8400/pci@4/pci@0/pci@a/network@0,1	22
15	PCI#1	/pci@8500/pci@4/pci@0/pci@8/****@0	23
16	PCI#2	/pci@8500/pci@4/pci@0/pci@9/****@0	24
17	PCI#5	/pci@8600/pci@4/pci@0/pci@9/****@0	25
18	PCI#6	/pci@8600/pci@4/pci@0/pci@11/****@0	26

表 A-15 SPARC M10-4 机箱的 I/O 设备（初始安装时：4 个 CPU）(续)

实例 优先级	设备	设备路径	图中编号
19	PCI#9	/pci@8700/pci@4/pci@0/pci@9/****@0	27
20	PCI#10	/pci@8700/pci@4/pci@0/pci@11/****@0	28

图 A-8 SPARC M10-4 模块图（4 个 CPU）



PCI 扩展单元侧的 I/O 设备

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在表 A-15 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-16 PCI 扩展单元侧 I/O 设备路径（初始安装时: 4 个 CPU）

实例 优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.6 SPARC M10-4S 设备路径

由 SPARC M10-4S 识别的设备路径以及与设备路径对应的硬件模块图如下。

A.6.1 对应初始安装 2-CPU 配置的场所

以下是初始安装 2-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令将 I/O 总线重新配置 (`ioreconfigure`) 设置为 `disabled` 状态（默认），则以下设备路径也适用于将 2 个 CPU 配置扩展为 4 个 CPU 配置的安装情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 2 个 CPU 配置扩展为 4 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 4 个 CPU 配置 (表 A-20)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

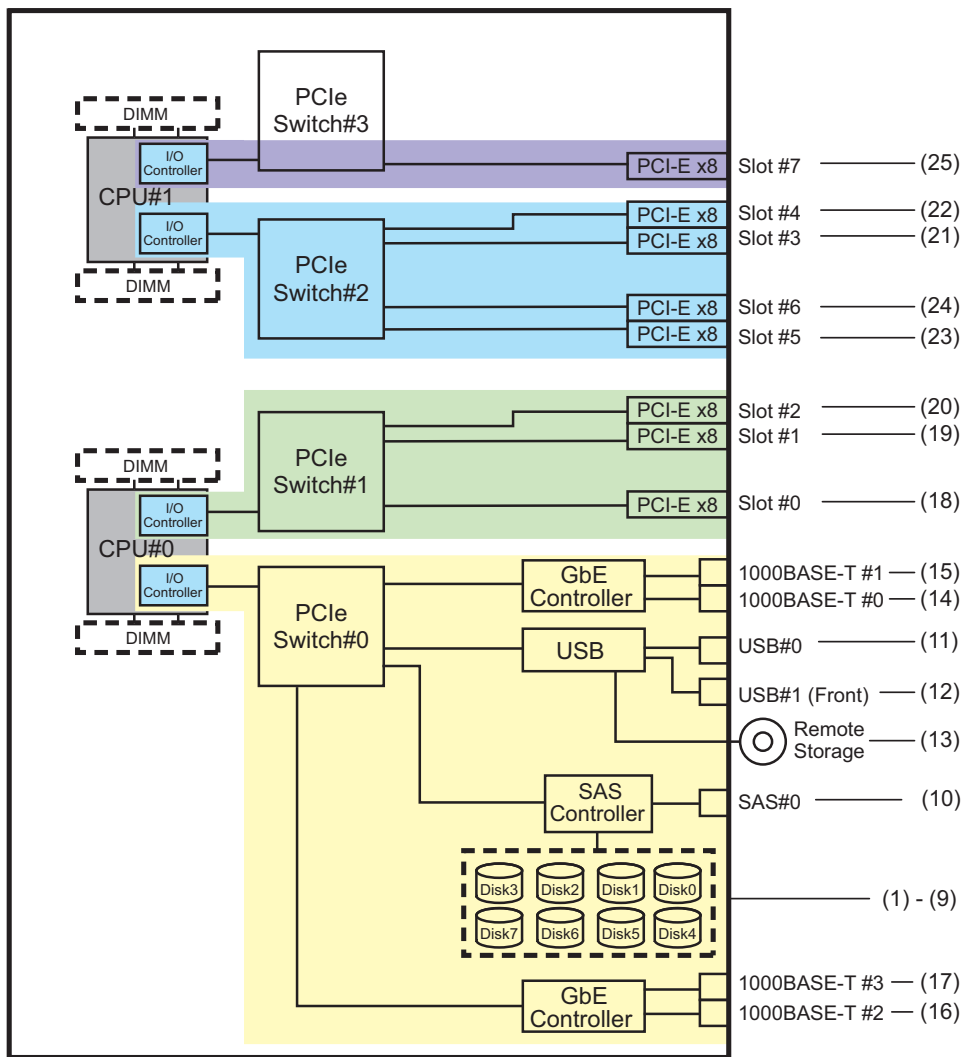
如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后扩展配置。

SPARC M10-4S 机箱的 I/O 设备路径

表 A-17 SPARC M10-4S 机箱的 I/O 设备路径（初始安装时：2 个 CPU）

实例 优先级	设备	设备路径	图中编号
1	LSB#0 内部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-	内部 HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-	内部 HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	内部 HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	内部 HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	内部 HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	内部 HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	内部 HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	内部 HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	外部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	内部 USB 端口 （后面: USB 1.1）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	内部 USB 端口 （后面: USB 2.0）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	内部 USB 端口 （前面: USB 1.1/2.0）	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	远程存储	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	内部 LAN#2	/pci@8000/pci@4/pci@0/pci@a/network@0	16
9	内部 LAN#3	/pci@8000/pci@4/pci@0/pci@a/network@0,1	17
10	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	18
11	PCI#1	/pci@8100/pci@4/pci@0/pci@8/****@0	19
12	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
13	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	21
14	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	22
15	PCI#5	/pci@8200/pci@4/pci@0/pci@9/****@0	23
16	PCI#6	/pci@8200/pci@4/pci@0/pci@11/****@0	24
17	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	25

图 A-9 SPARC M10-4S 模块图 (2 个 CPU)



PCI 扩展单元侧 I/O 设备路径

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在表 A-17 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-18 PCI 扩展单元侧 I/O 设备路径 (初始安装时: 2 个 CPU)

实例 优先级	设备	设备路径
	PCI#X 下的 PCI 扩展单元	
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0

表 A-18 PCI 扩展单元侧 I/O 设备路径（初始安装时: 2 个 CPU）(续)

实例 优先级	设备	设备路径
2	PCI#2	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

逻辑系统板的 I/O 设备路径

LSB#1 至 LSB#15 的设备路径具有类似 LSB#0 的按 LSB# 升序的实例优先级。开头的设备节点 (表 A-18/pci@vwww) 将变为 表 A-19 中所示。其他设备节点与 表 A-18 中相同。例如, 对于 LSB#1, 如下所示解释 表 A-19 中的节点值。LSB#2 到 LSB#15 的节点值按照同样的方法说明。

/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00, /pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00, /pci@8700->/pci@8f00

表 A-19 LSB#1 至 LSB#15 的 I/O 设备路径（初始安装时: 2 个 CPU）

LSB 编号	设备路径
LSB#1	/pci@8800/ ...
	/pci@8900/ ...
	/pci@8a00/ ...
	/pci@8b00/ ...
LSB#2	/pci@9000/ ...
	/pci@9100/ ...
	/pci@9200/ ...
	/pci@9300/ ...
LSB#3	/pci@9800/ ...
	/pci@9900/ ...
	/pci@9a00/ ...
	/pci@9b00/ ...
LSB#4	/pci@a000/ ...
	/pci@a100/ ...
	/pci@a200/ ...
	/pci@a300/ ...

表 A-19 LSB#1 至 LSB#15 的 I/O 设备路径 (初始安装时: 2 个 CPU) (续)

LSB 编号	设备路径
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ...
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/ ... /pci@eb00/ ...
LSB#14	/pci@f000/ ... /pci@f100/ ... /pci@f200/ ... /pci@f300/ ...
LSB#15	/pci@f800/ ... /pci@f900/ ... /pci@fa00/ ... /pci@fb00/ ...

A.6.2 对应初始安装 4-CPU 配置の場合

以下是初始安装 4-CPU 配置的设备路径以及与之对应的硬件模块图列表。

注 - 如果使用 `setpparmode` 命令禁用 I/O 总线重新配置 (`ioreconfigure`)，下面的设备路径也适用于将 4-CPU 配置减少为 2-CPU 配置的移除情况。在这种情况下，您不需要重新配置逻辑域、重新安装 Oracle Solaris 以及对其重新设置。

如果您启用 I/O 总线重新配置 (`ioreconfigure`) 并将 4 个 CPU 配置缩减为 2 个 CPU 配置，则在 PPAR 重置时，设备路径将更改为 2 个 CPU 配置 (表 A-17)。此时，系统将更改为出厂默认配置。在这种情况下，逻辑域需要重新配置。

另外，您可能需要重新安装 Oracle Solaris 或对其重新设置。

如果您需要保留逻辑域配置，请禁用 I/O 总线重新配置，然后缩减配置。

SPARC M10-4S 机箱的 I/O 设备

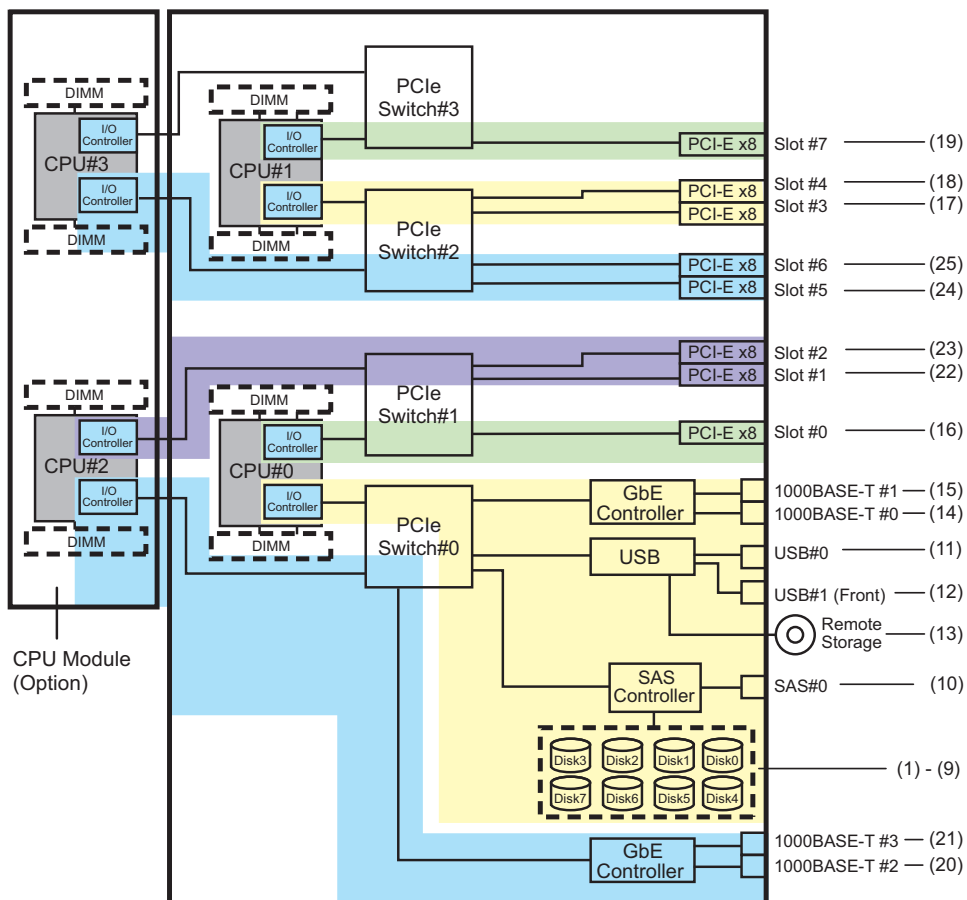
表 A-20 SPARC M10-4S 机箱的 I/O 设备 (初始安装时: 4 个 CPU)

实例 优先级	设备	设备路径	图中编号	
1	LSB#0	内部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		内部 HDD#0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		内部 HDD#1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		内部 HDD#2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-		内部 HDD#3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-		内部 HDD#4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-		内部 HDD#5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-		内部 HDD#6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-		内部 HDD#7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-		外部 SAS	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	内部 USB 端口 (后面: USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11	
3	内部 USB 端口 (后面: USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11	
4	内部 USB 端口 (前面: USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12	
5	远程存储	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13	
6	内部 LAN#0	/pci@8000/pci@4/pci@0/pci@9/network@0	14	
7	内部 LAN#1	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15	
8	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	16	

表 A-20 SPARC M10-4S 机箱的 I/O 设备（初始安装时：4 个 CPU）（续）

实例 优先级	设备	设备路径	图中编号
9	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	17
10	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	18
11	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	19
12	内部 LAN#2	/pci@8400/pci@4/pci@0/pci@a/network@0	20
13	内部 LAN#3	/pci@8400/pci@4/pci@0/pci@a/network@0,1	21
14	PCI#1	/pci@8500/pci@4/pci@0/pci@8/****@0	22
15	PCI#2	/pci@8500/pci@4/pci@0/pci@9/****@0	23
16	PCI#5	/pci@8600/pci@4/pci@0/pci@9/****@0	24
17	PCI#6	/pci@8600/pci@4/pci@0/pci@11/****@0	25

图 A-10 SPARC M10-4S 模块图（4 个 CPU）



PCI 扩展单元侧的 I/O 设备

如果具有连接到 PCI 扩展单元链路卡的服务器 PCI 插槽是 PCI#X，则将创建以下相应 vvvv 和 u 显示在 表 A-20 中 PCI#X 设备路径 /pci@vvvv/pci@4/pci@0/pci@u/****@0 中的设备路径。

表 A-21 PCI 扩展单元侧 I/O 设备路径（初始安装时: 4 个 CPU）

实例 优先级	设备	设备路径
PCI#X 下的 PCI 扩展单元		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

逻辑系统板的 I/O 设备

对于 LSB#1 至 LSB#15 的 I/O 设备路径，表 A-20 中 I/O 设备路径开头的设备节点 (/pci@vvvv) 将变为 表 A-22 中所示。其他设备节点与 表 A-20 中相同。

例如，对于 LSB#1，如下所示解释 表 A-20 中的节点值。LSB#2 到 LSB#15 的节点值按照同样的方法说明。

/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00

/pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00

表 A-22 LSB#1 至 LSB#15 的 I/O 设备路径（初始安装时: 4 个 CPU）

LSB 编号	设备路径
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ... /pci@8c00/ ... /pci@8d00/ ... /pci@8e00/ ...

表 A-22 LSB#1 至 LSB#15 的 I/O 设备路径 (初始安装时: 4 个 CPU) (续)

LSB 编号	设备路径
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ... /pci@9400/ ... /pci@9500/ ... /pci@9600/ ...
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ... /pci@9c00/ ... /pci@9d00/ ... /pci@9e00/ ...
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ... /pci@a400/ ... /pci@a500/ ... /pci@a600/ ...
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ... /pci@ac00/ ... /pci@ad00/ ... /pci@ae00/ ...
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ... /pci@b400/ ... /pci@b500/ ... /pci@b600/ ...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ... /pci@bc00/ ... /pci@bd00/ ... /pci@be00/ ...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ... /pci@c400/ ... /pci@c500/ ... /pci@c600/ ...

表 A-22 LSB#1 至 LSB#15 的 I/O 设备路径 (初始安装时: 4 个 CPU) (续)

LSB 编号	设备路径
LSB#9	/pci@c800/ ...
	/pci@c900/ ...
	/pci@ca00/ ...
	/pci@cb00/ ...
	/pci@cc00/...
	/pci@cd00/...
LSB#10	/pci@ce00/...
	/pci@d000/ ...
	/pci@d100/ ...
	/pci@d200/ ...
	/pci@d300/ ...
	/pci@d400/...
LSB#11	/pci@d500/...
	/pci@d600/...
	/pci@d800/ ...
	/pci@d900/ ...
	/pci@da00/ ...
	/pci@db00/ ...
LSB#12	/pci@dc00/...
	/pci@dd00/...
	/pci@de00/...
	/pci@e000/ ...
	/pci@e100/ ...
	/pci@e200/ ...
LSB#13	/pci@e300/ ...
	/pci@e400/...
	/pci@e500/...
	/pci@e600/...
	/pci@e800/ ...
	/pci@e900/ ...
LSB#14	/pci@ea00/...
	/pci@eb00/...
	/pci@ec00/...
	/pci@ed00/...
	/pci@ee00/...
	/pci@f000/...
LSB#15	/pci@f100/...
	/pci@f200/...
	/pci@f300/...
	/pci@f400/...
	/pci@f500/...
	/pci@f600/...
	/pci@f800/...
	/pci@f900/...
	/pci@fa00/...
	/pci@fb00/...
	/pci@fc00/...
	/pci@fd00/...
	/pci@fe00/...

识别基于 WWN 的 SAS2 设备

本附录介绍如何根据 WWN 值识别 SAS2 设备。

- 全球通用名称 (WWN) 语法
- `probe-scsi-all` 命令输出概要
- 使用 `probe-scsi-all` 命令识别磁盘槽
- 识别磁盘槽

B.1 全球通用名称 (WWN) 语法

Oracle Solaris 现在对逻辑设备名称使用全球通用名称 (WWN) 语法。本节介绍如何将一个基于 WWN 的设备名称映射到给定的 SCSI 设备。

以启动设备为例显示以前设备名称 (`tn;` 目标ID) 与基于 WWN 设备名称之间表示法的差异。

表 B-1 设备名称之间表示法的差异

使用 WWN 值的启动设备名称	以前的启动设备名称 (使用目标 ID)
<code>c#tWWNd#</code>	<code>c0t0d0</code>
WWN 是针对此设备的全球唯一十六进制编号。制造商将此编号分配给设备。	

WWN 值不遵照以前的逻辑设备名称结构，因此您无法直接从 `c#tWWNd#` 识别目标设备。

要将一个基于 WWN 的设备名称映射到给定物理设备，请使用 OpenBoot PROM 的 `probe-scsi-all` 命令。有关详情，请参见 "B.3 使用 `probe-scsi-all` 命令识别磁盘槽"。

B.2 probe-scsi-all 命令输出概要

OpenBoot PROM probe-scsi-all 命令的输出可查看系统中所有 SCSI 设备的列表和各设备的基本信息。下表列出了查看的项目。

表 B-2 probe-scsi-all 命令配置

实体名称	说明
Target	分配给各 SAS 设备的唯一目标 ID
SASDeviceName	由制造商分配给 SAS 设备的 WWN 值。 它被 Oracle Solaris 识别。
SASAddress	OpenBoot PROM 固件识别并分配给 SCSI 设备的 WWN 值
PhyNum	目标驱动器上所连控制器端口的十六进制 ID 号
VolumeDeviceName (配置 RAID 卷时)	Oracle Solaris 识别并分配给 RAID 卷的 WWN 值。 取代 RAID 卷中所包括各 SCSI 设备的 SASDeviceName。
VolumeWWID (配置 RAID 卷时)	OpenBoot PROM 固件识别并分配给 RAID 卷的基于 WWN 的值。 取代 RAID 卷中所包括各 SCSI 设备的 SASDeviceName。

B.3 使用 probe-scsi-all 命令识别磁盘槽

本节介绍如何使用 OpenBoot PROM 的 probe-scsi-all 命令识别磁盘槽。这可以将磁盘槽与对应的 WWN 值关联。

B.3.1 使用 probe-scsi-all 命令识别磁盘槽的示例 (SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S)

本节介绍板载 SAS 控制器上所连 PhyNum 与磁盘槽之间的对应关系。

在 SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S 中，SAS 控制器连接到 HDD 底板。下表列出了 HDD 底板 PhyNum 与磁盘槽的对应关系。

表 B-3 PhyNum 和磁盘槽的映射 (SPARC M12-1/M10-1/M10-4/M10-4S)

PhyNum	磁盘槽
0	0
1	1

表 B-3 PhyNum 和磁盘槽的映射 (SPARC M12-1/M10-1/M10-4/M10-4S) (续)

PhyNum	磁盘槽
2	2
3	3
4	4
5	5
6	6
7	7

表 B-4 PhyNum 和磁盘槽的映射 (SPARC M12-2/M12-2S)

PhyNum	SAS 控制器编号	磁盘槽
0	0	0
1		1
2		2
3		3
4	1	4
5		5
6		6
7		7

注 - 有关 SPARC M12-2/M12-2S/M10-1/M10-4/M10-4S 中磁盘槽的物理位置, 请参见服务器的《Service Manual》中的 "Maintaining the Internal Storage"。

probe-scsi-all 命令输出示例

下面介绍在 SPARC M12-2S/M10-1 中安装了八个内部磁盘驱动器时识别磁盘槽的步骤。

1. 执行 **probe-scsi-all** 命令。
在 SPARC M10-1 的以下示例中, 安装在磁盘槽 0 中的内部磁盘驱动器的 PhyNum 为 0。内部磁盘驱动器分配给 Target a, SASDeviceName 值是 50000393c813ae74。

SPARC M10-1 的示例

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0 <---- SAS 控制器

FCCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.57.00

Target a
  Unit 0   Disk   TOSHIBA  MBF2300RC           3706   585937500 Blocks, 300 GB
```

```

SASDeviceName 50000393c813ae74 SASAddress 50000393c813ae76 PhyNum 0
Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81b24ec SASAddress 50000393b81b24ee PhyNum 1
Target c
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81af47c SASAddress 50000393b81af47e PhyNum 2
Target d
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81af3c0 SASAddress 50000393b81af3c2 PhyNum 3
Target e
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81b0f58 SASAddress 50000393b81b0f5a PhyNum 4
Target f
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81b130c SASAddress 50000393b81b130e PhyNum 5
Target 10
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81b2420 SASAddress 50000393b81b2422 PhyNum 6
Target 11
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393b81acc84 SASAddress 50000393b81acc86 PhyNum 7
Target 12
Unit 0 Encl Serv device FUJITSU NBBEXP 0d32
SASAddress 500000e0e04d003d PhyNum 14
{0} ok

```

SPARC M12-2S 的示例

```

{0} ok probe-scsi-all
/pci@8500/pci@4/pci@0/pci@0/scsi@0 <---- SAS 控制器 1

FCode Version 1.00.56, MPT Version 2.00, Firmware Version 20.00.06.00

Target a
Unit 0 Disk TOSHIBA AL13SEB600AL14SE 3702 1172123568 Blocks, 600 GB
SASDeviceName 5000039678332cc5 SASAddress 5000039678332cc6 PhyNum 4
Target b
Unit 0 Disk TOSHIBA AL13SEB600AL14SE 3702 1172123568 Blocks, 600 GB
SASDeviceName 5000039678332ca9 SASAddress 5000039678332caa PhyNum 5
Target c
Unit 0 Disk TOSHIBA AL13SEB600AL14SE 3702 1172123568 Blocks, 600 GB
SASDeviceName 5000039678332c59 SASAddress 5000039678332c5a PhyNum 6
Target d
Unit 0 Disk TOSHIBA AL13SEB600AL14SE 3702 1172123568 Blocks, 600 GB
SASDeviceName 5000039678332c55 SASAddress 5000039678332c56 PhyNum 7
Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e0b0103d PhyNum 14

/pci@8100/pci@4/pci@0/pci@0/scsi@0 <---- SAS 控制器 0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 20.00.06.00

```

```

Target a
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702      1172123568 Blocks, 600 GB
  SASDeviceName 5000039698002565 SASAddress 5000039698002566 PhyNum 0
Target b
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702      1172123568 Blocks, 600 GB
  SASDeviceName 50000396980024b9 SASAddress 50000396980024ba PhyNum 1
Target c
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702      1172123568 Blocks, 600 GB
  SASDeviceName 5000039698002495 SASAddress 5000039698002496 PhyNum 2
Target d
  Unit 0   Disk   TOSHIBA  AL13SEB600AL14SE 3702      1172123568 Blocks, 600 GB
  SASDeviceName 5000039678332cd1 SASAddress 5000039678332cd2 PhyNum 3
Target e
  Unit 0   Encl Serv device FUJITSU  BBEXP          0d32
  SASAddress 500000e0e0b0103d PhyNum 14

```

注 - 上述方法也可以识别 SPARC M12-1/M12-2/M10-4/M10-4S 中的磁盘槽。

B.4 识别磁盘槽

如需执行内部存储器的活动状态更换，您需要知道要安装或移除的设备的物理设备名称或逻辑设备名称。如果系统中的磁盘发生故障，通常您可检查将要故障或者已经故障的磁盘相关信息。此信息也记录在 `/var/adm/messages` 文件中。

在此信息中通常包含了故障磁盘的物理设备名称和逻辑设备名称。根据不同的应用，也可报告磁盘的槽号。

根据 Oracle Solaris 版本，检查 HDD 安装位置信息的步骤有所不同。

- 在 **Oracle Solaris 11** 的情况下
 - 有关详细信息，请参见 ["B.4.1 使用 format 命令 \(Oracle Solaris 11\)"](#) 或 ["B.4.2 使用 diskinfo 命令 \(Oracle Solaris 11\)"](#)。
- 在 **Oracle Solaris 10** 的情况下
 - 有关详细信息，请参见 ["B.4.3 使用 diskinfo 命令 \(Oracle Solaris 10\)"](#)。

B.4.1 使用 format 命令 (Oracle Solaris 11)

1. 执行 `showhardconf` 命令并检查显示安装位置信息的机柜的 **CMUL** 的串行号。

```

XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081238017; Operator_Panel_Switch:Service;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;

```

```

BB#00 Status:Normal; Role:Master; Ver:2044h; Serial:2081238017;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123001Y1 ;
* BB#00 CMUL 序列号
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00321144;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00322957;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
-----略-----
BB#01 Status:Normal; Role:Standby; Ver:2044h; Serial:2081230011;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123203N0 ;
* BB#01 CMUL 序列号
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00320804;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00321030;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
MEM#00A Status:Normal;
+ Code:2c800118KSF1G72PZ-1G6E1 4531-1A94229F;
+ Type:04; Size:8 GB;
-----略-----

```

2. 执行 **format** 命令并查看物理磁盘槽。

在以下的示例中，从 (1) 到 (5) 代表：

- (1): 磁盘的逻辑路径名称
- (2): 磁盘安装在 BB#01 的 HDD00 槽
- (3): 磁盘安装在 BB#01 的 HDD01 槽
- (4): 磁盘安装在 BB#00 的 HDD00 槽
- (5): 磁盘安装在 BB#00 的 HDD01 槽

```

# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
  0. c2t50000394281B5312d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
      /pci@8800/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b5312,0
      /dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD00/disk <-- (2)
* BB#1_CMUL 序列号的最后 4 位
* HDD00

```

```

1. c2t50000394281B59D6d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
    /pci@8800/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b59d6,0
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD01/disk <-- (3)
        * HDD01

2. c0t500003942823C8C6d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w500003942823c8c6,0
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD00/disk <-- (4)
        * BB#0_CMUL 序列号的最后 4 位
        * HDD00

3. c0t50000394281B517Ad0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b517a,0
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD01/disk <-- (5)
        * HDD01

Specify disk (enter its number):

```

B.4.2 使用 diskinfo 命令 (Oracle Solaris 11)

1. 执行 **showhardconf** 命令并检查显示安装位置信息的机柜的 **CMUL** 的串行号。

```

XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081238017; Operator_Panel_Switch:Service;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2044h; Serial:2081238017;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123001Y1 ;
        * BB#00 CMUL 序列号
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00321144;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00322957;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
-----略-----
BB#01 Status:Normal; Role:Standby; Ver:2044h; Serial:2081230011;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123203N0 ;
        * BB#01 CMUL 序列号
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;

```

```

CPU#0 Status:Normal; Ver:4142h; Serial:00320804;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00321030;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
MEM#00A Status:Normal;
+ Code:2c800118KSF1G72PZ-1G6E1 4531-1A94229F;
+ Type:04; Size:8 GB;
-----略-----

```

2. 执行 **diskinfo** 命令并查看物理磁盘槽。

在以下的示例中，从 (1) 到 (4) 代表：

- (1): 安装在 BB#01 的 HDD 0 的磁盘的设备名称和逻辑路径名称
- (2): 安装在 BB#01 的 HDD 1 的磁盘的设备名称和逻辑路径名称
- (3): 安装在 BB#00 的 HDD 0 的磁盘的设备名称和逻辑路径名称
- (4): 安装在 BB#00 的 HDD 1 的磁盘的设备名称和逻辑路径名称

```

# diskinfo
D:devchassis-path                                     c:occupant-compdev
-----
/dev/chassis/SYS/BB0/CMUL/HDD0                        -
/dev/chassis/SYS/BB0/CMUL/HDD1                        -
/dev/chassis/SYS/BB0/CMUL/HDD2                        -
/dev/chassis/SYS/BB0/CMUL/HDD3                        -
/dev/chassis/SYS/BB0/CMUL/HDD4                        -
/dev/chassis/SYS/BB0/CMUL/HDD5                        -
/dev/chassis/SYS/BB0/CMUL/HDD6                        -
/dev/chassis/SYS/BB0/CMUL/HDD7                        -
/dev/chassis/SYS/BB1/CMUL/HDD0                        -
/dev/chassis/SYS/BB1/CMUL/HDD1                        -
/dev/chassis/SYS/BB1/CMUL/HDD2                        -
/dev/chassis/SYS/BB1/CMUL/HDD3                        -
/dev/chassis/SYS/BB1/CMUL/HDD4                        -
/dev/chassis/SYS/BB1/CMUL/HDD5                        -
/dev/chassis/SYS/BB1/CMUL/HDD6                        -
/dev/chassis/SYS/BB1/CMUL/HDD7                        -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD00/disk
c4t50000394281B5312d0 <-- (1)
                                     * BB#01_CMUL 序列号的最后 4 位
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD01/disk
c4t50000394281B59D6d0 <-- (2)
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD02      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD03      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD04      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD05      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD06      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD07      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD00/disk
c2t500003942823C8C6d0 <-- (3)
                                     * BB#00_CMUL 序列号的最后 4 位
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD01/disk

```

```

c2t50000394281B517Ad0 <-- (4)
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD02      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD03      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD04      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD05      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD06      -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD07      -

```

B.4.3 使用 diskinfo 命令 (Oracle Solaris 10)

1. 执行 **diskinfo** 命令并检查物理磁盘槽和逻辑系统板。
在以下的示例中，从 (1) 到 (4) 代表：
 - (1): 安装在 HDD 0 的磁盘的逻辑路径名称。
 - (2): 安装在 LSB#00 的 HDD 0 的磁盘的设备路径
 - (3): 安装在 HDD 1 的磁盘的逻辑路径名称。
 - (4): 安装在 LSB#00 的 HDD 1 的磁盘的设备路径

```

# diskinfo -ap

Enclosure path:      2081210007-physical-hba-0
Chassis Serial Number: 2081210007-physical-hba-0
Chassis Model:      ORCL,SPARC64-X

Enclosure path:      /dev/es/ses0
Chassis Serial Number: 500000e0e06d233f
Chassis Model:      FUJITSU-BBEXP

Label      Disk name      Vendor      Product      Vers
-----
HDD_0      c0t50000393D8289180d0  TOSHIBA    MBF2600RC    3706 <-- (1)
Physical path
-----
0: /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000393D8289180,0<-- (2)
* LSB#0
HDD_1      c0t50000393D82891D0d0  TOSHIBA    MBF2600RC    3706 <-- (3)
Physical path
-----
0: /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000393D82891D0,0<-- (4)
* LSB#0

```

使用 **diskinfo** 命令所显示的磁盘的设备路径符号格式如下。

<SAS 控制器设备路径>/iport@f/disk@wXXXXXXXX,Y:Z

设备路径根据型号或系统配置的不同而有所差异。有关详情，请参见 ["附录 A SPARC M12/M10 系统设备路径列表"](#)。

XSCF Web 页面列表

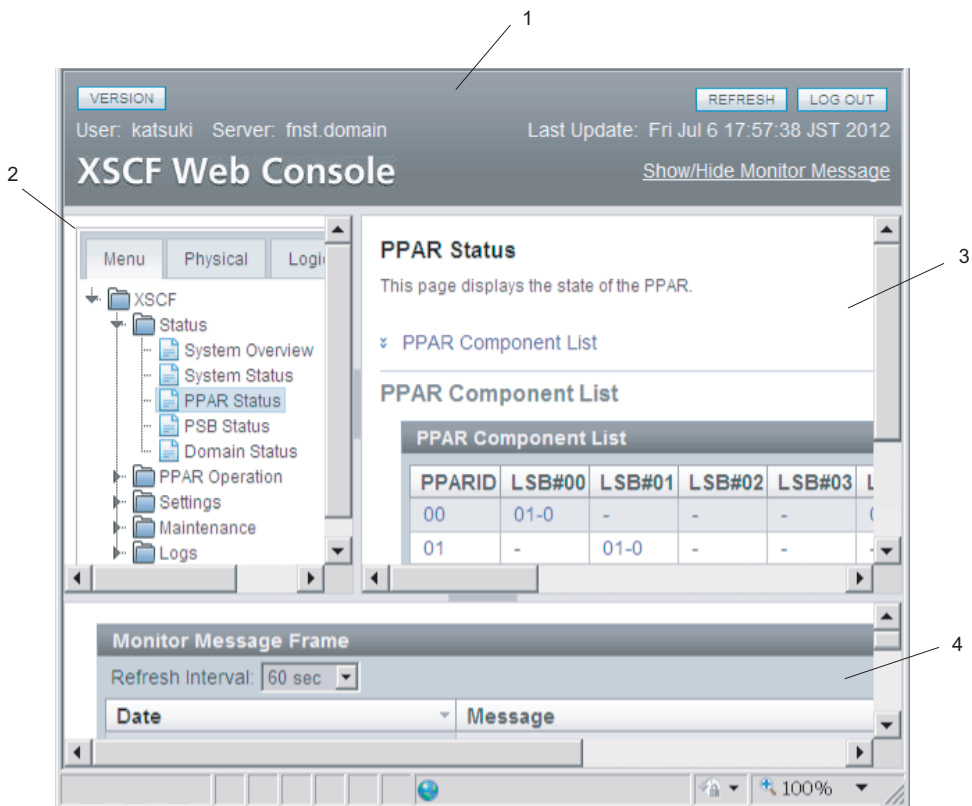
本附录简要介绍了 XSCF Web 的各个页面。
有关如何登录 XSCF Web 和从其注销的详细信息，请参见“[第2章 登录和注销 XSCF](#)”。

- [页面概要](#)
- [了解菜单配置](#)
- [可用页面](#)

C.1 页面概要

[图 C-1](#) 显示了登录后所显示的 XSCF Web 控制台窗口。

图 C-1 XSCF Web 控制台窗口



-
- 1 顶端图文框
 - 2 菜单图文框（树状图文框）
 - 3 主图文框
 - 4 事件图文框
-

登录后显示的 XSCF Web 控制台包括四个图文框。在左图文框上选择一个菜单项目在右图文框中显示它的信息。用户可以操作/管理服务器。

表 C-1 列出了各种类型的 XSCF Web 控制台图文框，并提供了每个图文框的概要。

表 C-1 图文框概要

图文框类型	概要
顶端图文框	窗口顶部的页面（图 C-1 中的 1）。本图文框显示登录时指定的用户帐户名、所连主机的名称以及其它信息。从本图文框中注销后，返回登录页。

表 C-1 图文框概要 (续)

图文框类型	概要
菜单图文框 (树状图文框)	窗口左侧的页面 (图 C-1 中的 2)。 选择一个菜单项目可在右边的主图文框查看相关信息。 共有三个菜单栏。每个菜单以树状格式显示。 - 菜单: 显示各种设置、操作和状态的查看菜单。 - 物理: 系统物理组件配置的查看菜单。 - 逻辑: 每个物理分区的逻辑组件配置的查看菜单。
主图文框	窗口右侧的页面 (图 C-1 中的 3)。 在树状图文框中选择一个菜单项目可查看与其对应的页面。
事件图文框 (监视信息图文框)	窗口底部的页面 (图 C-1 中的 4)。 整个系统中的事件以监视信息形式显示。 图文框被定期刷新。图文框中的间隔时间可更改。默认的刷新间隔时间是 60 秒。

表 C-2 列出了页面功能，并对 XSCF Web 控制台所显示的主页面进行了简要介绍。

表 C-2 主页面概要

页面功能	概要
登录页	这是 XSCF Web 控制台登录页。使用 XSCF 用户帐户从登录页登录。
显示服务器状态	本页面显示整个系统、物理分区和逻辑域的状态。包括 PCI 扩展单元的状态。 从 [Menu] (菜单) 栏中，选择 [Status] (状态)。
操作物理分区	本页面用于操作物理分区和逻辑域。这些操作包括物理分区和系统板 (PSB) 配置管理的电源操作。 从 [Menu] (菜单) 栏中，选择 [PPAR Operation] (PPAR 操作)。
配置服务器	为了使用整个系统和 XSCF，在本页面进行各种设置。 从 [Menu] (菜单) 栏中，选择 [Settings] (设置)。
维护服务器	此页面的操作包括保存/恢复数据、固件更新、XSCF 重新启动、XSCF 切换、远程维护服务以及保存日志。 从 [Menu] (菜单) 栏中，选择 [Maintenance] (维护)。
查看日志	查看的日志包括错误日志、电源日志、事件日志和控制台日志。 从 [Menu] (菜单) 栏中，选择 [Logs] (日志)。
备用端页面	登录到待机 XSCF 时显示本页面。 在本页面进行切换 XSCF、保存日志等。

C.2 了解菜单配置

本节介绍菜单配置。

在菜单图文框选择 [Menu] 栏时，显示如下。

```
Menu
+ XSCF
  + Status
    - System Overview
    - System Status
    - PPAR Status
    - PSB Status
    - Domain Status
  + PPAR Operation
    - PPAR Power
    - PPAR Mode Configuration
    - PPAR Configuration
    - PSB Configuration
    - Domain Configuration
    - PPAR Parameter
    - Verified Boot
  + Settings
    + Network
      - Current
      - Reserve
    + Service
      - Service State
      - HTTPS
      - SSH
      - Telnet
      - NTP
      - SMTP
      - SNMP
      - SNMP Security
    + User Manager
      - Account
      - LDAP
      - LDAP/SSL
      - Active Directory
      - Autologout
      - CoD Reservation
      - CoD Activation
      - Audit
      - Email Reporting
      - Time
      - Power Capping
      - Power Schedule
      - Add-In Card Manager
      - PCIBOX DIO
      - Remote Storage
  + Maintenance
    + Network Tools
      - Ping
      - Traceroute
      - Nslookup
    - Configuration Management
    - Firmware Update
    - Reboot XSCF
```

```
- Switch Over
- Snapshot
- ASR
+ Logs
- Error Log
- Power Log
- Event Log
- Console Log
- Panic Log
- Environment Log
- IPL Message Log
- Monitor Message Log
- Audit Log
```

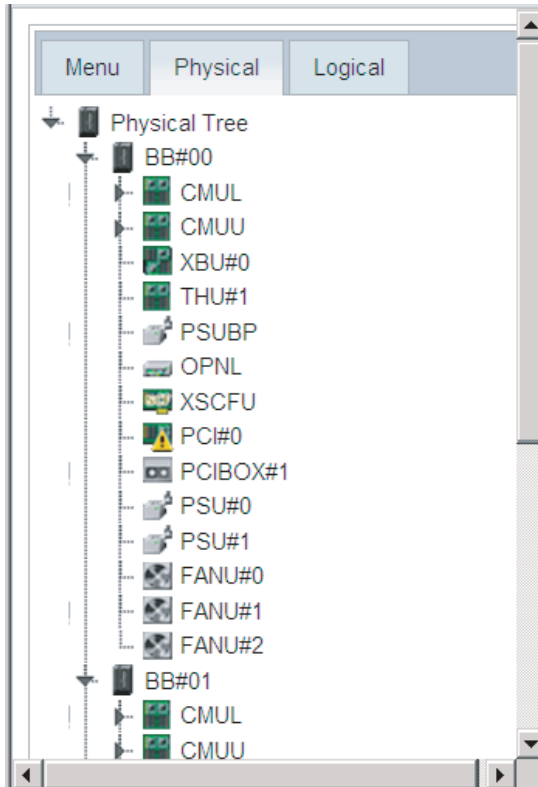
注 - 每个菜单项目会随功能改进或其它原因而变化。根据型号和情况，菜单项目可能不同。

选择一个菜单项目查看主图文框中的对应页面。

对于具有多个 XSCF 的系统，[Switch Over] 可用于在不同系统间切换。有关每个菜单项的目标页面的概要，请参见 "C.3 可用页面"。

图 C-2 显示了在菜单图文框中选择了 [Physical] 栏的画面示例。

图 C-2 物理组件树






注 - 窗口布局和显示的内容只是外观的示例，因功能改进或其他原因可能更改。

选择 [Physical] 栏可以查看系统中用树状形式显示的组件。在树状图文框中选择一个组件可在主图文框显示组件的信息和状态。

选择 [Logical] 栏可以查看用树状形式显示的属于物理分区的逻辑组件。在树状图文框中选择一个逻辑组件可在主图文框查看属于物理分区的逻辑组件的信息和状态。

组件状态显示如下。

表 C-3 组件状态显示

显示	概要
	运行正常
	因故障未运行
	以下的情形 <ul style="list-style-type: none"> - 尽管某些组件已经故障或被降级仍然继续运行 - 尽管组件状态正常，因其他组件故障或被降级，导致本组件降级 - 组件正在维护

C.3 可用页面

本节概括介绍主图文框中可用的页面。每个页面的功能与 XSCF shell 命令的功能相同。有关各功能的详细信息，请参见“第3章 配置系统”、介绍相关命令的章节或《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

C.3.1 本页面显示系统、物理分区和逻辑域的状态

表 C-4 列出了可显示系统信息的功能。选择 [Menu] (菜单) - [Status] (状态) - [System Overview] (系统概览)。

表 C-4 系统信息

项目	概要	相关命令
Product Name (产品名称)	显示服务器产品名称。	showhardconf(8)
Serial Number (序列号)	显示系统序列号。	
System Mode Switch Status (系统模式开关状态)	显示操作面板上模式开关的状态。	
Input power type (输入电源类型)	显示输入供电的类型。	
Power Status (电源状态)	显示输入电源的开闭。	
Power Phase (电源相)	显示系统电源相。	
XSCF Version (XSCF 版本)	显示 XSCF 固件版本。	version(8)
Chassis status (机柜状态)	显示机柜状态，主或备用。	showbbstatus(8)
系统时间	显示系统时间。	showdate(8)
Failed components	显示故障和降级的组件。	showstatus(8)
Temperature (温度)	显示机柜的进气温度。	showenvironment(8)
Exhaust airflow (排气)	显示机柜的排气量。	showenvironment(8)
Power Capping Status (用电封顶状态)	显示用电封顶功能是启用还是禁用，此功能用于降低系统功耗。	showpowercapping(8)

表 C-5 列出了可显示各系统组件状态的功能。选择 [Menu] (菜单) - [Status] (状态) - [System Status] (系统状态)。

表 C-5 组件状态

项目	概要	相关命令
Power Consumption (功耗) Temperature (温度) Voltage (电压) Fan Information (风扇信息)	显示各组件的功耗、排气温度、电压和风扇转速。	showenvironment(8)

表 C-6 列出了可显示各物理分区状态的功能。选择 [Menu] (菜单) - [Status] (状态) - [PPAR Status] (PPAR 状态)。

表 C-6 物理分区状态

项目	概要	相关命令
PPAR configuration list display (显示 PPAR 配置信息)	以表格形式显示与每个 PPAR LSB 号对应的 PSB 号。	showpctl(8)
PPAR Status (PPAR 状态)	显示 PPAR 操作状态和配置策略。	showpctl(8)
PSB Information (PSB 信息)	显示 PSB 信息。	showboards(8)

表 C-7 列出了可显示 PSB 状态的功能。选择 [Menu] (菜单) - [Status] (状态) - [PSB Status] (PSB 状态)。

表 C-7 PSB 状态

项目	概要	相关命令
PSB 状态	列出 PSB 中嵌入的 PPAR ID 及其它详细状态。	showboards(8)

表 C-8 列出了可显示逻辑域状态的功能。选择 [Menu] (菜单) - [Status] (状态) - [Domain Status] (域状态)。

表 C-8 逻辑域状态

项目	概要	相关命令
逻辑域状态	显示属于指定 PPAR 的每个逻辑域的操作状态。	showdomainstatus(8) showpparstatus(8)

C.3.2 操作物理分区的页面

表 C-9 列出了可操作物理分区电源的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [PPAR Power] (PPAR 电源)。

表 C-9 物理分区电源操作

项目	概要	相关命令
System power-on/off (系统电源开启/关闭)	指定是否开启/关闭系统 (所有物理分区) 的电源。	showpparstatus(8) poweron(8) poweroff(8)
PPAR power-on/off or reset (PPAR 电源 开启/关闭或重置)	为指定的 PPAR 执行如下操作: - 系统电源开启/关闭 - 强制关闭电源 - por: PPAR 重置 - panic: 向逻辑域发出崩溃指令 - sir: 逻辑域重置 - xir: CPU 重置 - 发送中断信息	showpparstatus(8) poweron(8) poweroff(8) reset(8) sendbreak(8)

表 C-10 列出了可设置物理分区操作模式的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [PPAR Mode Configuration] (PPAR 模式配置)。

表 C-10 物理分区操作模式

项目	概要	相关命令
PPAR mode display/setting (PPAR 模式显示/设置)	为指定的 PPAR 执行如下显示/设置操作: - 主机 ID - 硬件诊断级别 - 诊断信息级别 - 实时检查功能启用/禁用 - 主机监视程序超时情况下的操作 - 中断信号发送限制 - 逻辑域自动启动功能启用/禁用 - 低功率操作启用/禁用 - I/O 路径重组 - DR 功能即时启用/禁用 - DR 功能下次启动时启用/禁用 - PPAR 以太网地址 (mac 地址)	showpparmode(8) setpparmode(8)

注 - 有关 XSCF 和虚拟机监控程序之间的实时检查功能和 DR 功能的支持信息, 请参见您的服务器的最新《产品说明》。

表 C-11 列出了可配置物理分区的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [PPAR Configuration] (PPAR 配置)。

表 C-11 物理分区设置

项目	概要	相关命令
PPAR configuration list display (显示 PPAR 配置信息)	显示指定 PPAR 系统板 (PSB) 的 PCL。该功能还可用于查看/设置 PPAR 配置策略。 在 SPARC M12-1/M12-2/M10-1/M10-4 上, 该功能仅可显示信息并设置 PPAR-ID 00 的配置策略。	showpcl(8) setpcl(8)

表 C-11 物理分区设置 (续)

项目	概要	相关命令
PCL setting (PCL 设置)	设置 PCL。 本功能将 PPAR LSB 与 PSB 关联，并且为 LSB 设置配置信息。 SPARC M12-1/M12-2/M10-1/M10-4 不支持此功能。	showpcl(8) setpcl(8)
PSB addition, deletion, or setting (添加/删除/配置 PSB)	为 PPAR PSB 配置的以下更改提供指令： - 为 PPAR 预约或并入 PSB (BB) - 从 PPAR 释放 PSB (BB) - 将 PSB (BB) 从一个 PPAR 移到另一个 PPAR 按照《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》中所述的步骤执行上述操作。 SPARC M12-1/M12-2/M10-1/M10-4 不支持此功能。	addboard(8) deleteboard(8)

表 C-12 列出了可设置内存镜像模式的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [PSB Configuration] (PSB 配置)。

表 C-12 系统板设置

项目	概要	相关命令
Memory mirror information display/setting (内存镜像信息查看/设置)	显示/设置系统板 (PSB) 上的 CPU 的内存镜像模式信息。	showfru(8) setupfru(8)

表 C-13 列出了可设置逻辑域配置的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [Domain Configuration] (域配置)。

表 C-13 逻辑域设置

项目	概要	相关命令
Logical domain configuration information display (查看逻辑域配置信息)	查看指定 PPAR 的逻辑域配置信息。配置信息的要素如下： - 配置名称 - 构成逻辑域的数量 - 配置日期 可查看 PPAR 当前运行逻辑域配置的名称以及下次运行的逻辑域配置的名称。	showdomainconfig(8)
Logical domain configuration setting (逻辑域配置设置)	设置逻辑域配置。 可设置在指定的 PPAR 中，下次计划运行的逻辑域配置。	setdomainconfig(8)

表 C-14 列出了可重写物理分区的控制域的 OpenBoot PROM 环境变量的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [PPAR Parameter] (PPAR 参数)。

注 - 有关 [PPAR Parameter] 的支持信息，请参见最新的《产品说明》。

表 C-14 设置 OpenBoot PROM 环境变量

项目	概要	相关命令
Display/setting of PPAR OpenBoot PROM environment variables (查看/设置 PPAR OpenBoot PROM 环境变量)	查看/重写如下 OpenBoot PROM 环境变量， 重写指定 PPAR 的设置。 - use-nvramrc - security-mode - bootscrip	showpparparam(8) setpparparam(8)

表 C-15 列出了可配置各物理分区验证启动的功能。选择 [Menu] (菜单) - [PPAR Operation] (PPAR 操作) - [Verified Boot] (验证启动)。

表 C-15 配置验证启动

项目	概要	相关命令
路由的查看/设置	查看/设置验证启动的启动或模块策略。	showvbootconfig(8) setvbootconfig(8)
系统默认证书查看	查看预装在系统上的 X.509 公共密钥证书。	showvbootcerts(8)
X.509 公共密钥证书的注册/删除/启用/禁用	注册/删除用户指定的 X.509 公共密钥证书。 启用/禁用/查看用户指定的 X.509 公共密钥证书。	addvbootcerts(8) deletevbootcerts(8) showvbootconfig(8) setvbootconfig(8)

C.3.3 配置服务器的页面

XSCF 网络设置

表 C-16 列出了可配置 XSCF 网络的功能。选择 [Menu] (菜单) - [Setting] (设置) - [Network] (网络) - [Current] (当前)。或选择 [Menu] (菜单) - [Setting] (设置) - [Network] (网络) - [Reserve] (预约)。
[Current] (当前) 或 [Reserve] (预约) 菜单可用于设置网络。
[Current] (当前) 菜单显示当前运行 XSCF 网络的信息。您可从 [Reserve] (预约) 菜单确认设置的信息。

在通过 [Current] (当前) 菜单配置网络后，会自动转到 [Reserve] (预约) 菜单。配置网络后，单击 [Reserve] (预约) 菜单中的 [Apply] (应用)，然后单击 [Reboot] (重新启动) 按钮以应用设置。

表 C-16 XSCF 网络设置

菜单	项目	概要	相关命令
[Current] (当前)	XSCF 网络信息/ 状态查看, XSCF 网络设置	查看当前运行 XSCF 网络的信息和状态。您可以设置 XSCF 网络接口的主机名、域名、IP 地址和网络掩码并且启用/禁用它的设置。 单击 [Edit] (编辑) 按钮转到 [Reserve] (预约) 菜单并配置网络设置。您可用 [Reserve] (预约) 菜单确认设置的信息。	shownetwork(8) showhostname(8)
	路由的查看/设置	查看当前的路由。同时用于设置路由。 单击 [Edit] (编辑) 按钮转到 [Reserve] (预约) 菜单并设置路由。您可用 [Reserve] (预约) 菜单确认设置的信息。	shownameserver (8) setnameserver(8)
	DNS 的查看/设置	查看当前名称服务器和搜索路径。同时用于设置名称服务器和搜索路径。 单击 [Edit] (编辑) 按钮转到 [Reserve] (预约) 菜单并配置 DNS。您可用 [Reserve] (预约) 菜单确认设置的信息。	shownameserver (8) setnameserver(8)
[Reserve]	查看 XSCF 网络 设置信息, XSCF 网络设置	查看 XSCF 网络设置信息。您可以设置 XSCF 网络接口的主机名、域名、IP 地址和网络掩码并且启用/禁用它的设置。 您可单击 [Current Status] 按钮转到 [Current], 查看当前信息。	applynetwork(8) setnetwork(8) sethostname(8)
	路由设置信息的 查看/路由设置	查看路由设置信息。 同时用于设置路由。 您可单击 [Current Status] 按钮转到 [Current], 查看当前信息。	applynetwork(8) setroute(8)
	DNS 设置信息的 查看/DNS 设置	查看名称服务器和搜索路径信息。 同时用于设置名称服务器和搜索路径。 您可单击 [Current Status] 按钮转到 [Current], 查看当前信息。	applynetwork(8) setnameserver(8)
	反映网络设置	查看/反映网络设置。 保存设置后, 需要重新启动 XSCF 才能完成此过程。	applynetwork(8) rebootxscf(8)

注 - 使用 XSCF Web 不能设置/查看 SSCP 链接地址。请使用 setsscp 和 showsscp 命令设置/查看此地址。

注 - 使用 XSCF Web 不能设置/查看 IP 数据库筛选规则。请使用 setpacketfilters 和 showpacketfilters 命令设置/查看筛选规则。

个性化服务功能设置

表 C-17 列出了可启用/禁用个性化服务功能的功能。选择 [Settings] (设置) - [Service] (服务) - [Service State] (服务状态)。

表 C-17 个性化服务功能的启用/禁用设置

项目	概要	相关命令
服务功能状态查看 启用/禁用设置	查看下列服务功能的状态。同时启用/禁用服务功能。 - HTTPS 服务 - SNMPv3 服务 - SSH 服务 - Telnet 服务 - NTP 服务器服务 设置启用/禁用 SNMPv3 服务后，转向 SNMP 设置菜单，您可以在此配置 SNMP 代理。 选择 NTP 服务器服务，您可启用/禁用使 XSCF 用作 NTP 服务器的设置。	showhttps(8) sethttps(8) showsnmp(8) setsnmp(8) showssh(8) setssh(8) showtelnet(8) settelnet(8) showntp(8) setntp(8)

表 C-18 列出了可启用/禁用 HTTP 服务功能的功能。选择 [Settings]（设置） - [Service]（服务） - [HTTPS]。

表 C-18 HTTP 服务功能的启用/禁用设置

项目	概要	相关命令
HTTP 服务启用/禁用 设置	查看 HTTP 服务是被启用还是禁用，或启用/禁用该服务。	showhttps(8) sethttps(8)

注 - HTTP 服务被禁用时 XSCF Web 无法使用。要启用 HTTPS 服务，请使用 sethttps 命令。

表 C-19 列出了可启用/禁用 SSH 服务功能的功能。选择 [Settings]（设置） - [Service]（服务） - [SSH]。

表 C-19 SSH 服务功能的启用/禁用设置

项目	概要	相关命令
SSH 服务的启用/禁用 设置	查看 SSH 服务是被启用还是禁用，或启用/禁用该服务。	showssh(8) setssh(8)

注 - XSCF Web 不支持主机密钥生成、用户公共密钥注册/删除和 XSCF shell 超时设置。使用 showssh 和 setssh 命令设置这些功能。

表 C-20 列出了可启用/禁用 Telnet 服务功能的功能。选择 [Settings]（设置） - [Service]（服务） - [Telnet]。

表 C-20 Telnet 服务功能的启用/禁用设置

项目	概要	相关命令
Telnet 服务的启用/禁用 设置	查看 Telnet 服务是被启用还是禁用，或启用/禁用该服务。	showtelnet(8) settelnet(8)

表 C-21 列出了可配置 XSCF NTP 服务功能的功能。选择 [Settings]（设置） -

[Service] (服务) - [NTP]。

表 C-21 NTP 服务功能设置

项目	概要	相关命令
NTP 服务的启用/禁用和查看/设置	查看/设置是否 XSCF 被当做 NTP 服务器被启用或禁用。	showntp(8) setntp(8)
NTP 客户端的启用/禁用和查看/设置	查看/设置是否 XSCF 被当做 NTP 客户端被启用或禁用。	
NTP 服务器设置	查看/设置如下 XSCF 网络使用的 NTP 服务器设置项目： <ul style="list-style-type: none">- NTP 服务器 (最多三台)- 优先级服务器 (首选)- 层次值- 如需完成 XSCF 自身的本地时钟地址设置，需要重新启动 XSCF。 需要重新启动 XSCF 来完成设置过程。	

表 C-22 列出了可配置 XSCF SMTP 服务功能的功能。选择 [Settings] (设置) - [Service] (服务) - [SMTP]。

表 C-22 SMTP 服务功能设置

项目	概要	相关命令
SMTP 服务的查看/设置	查看/设置 SMTP 服务地址、验证算法、POP 服务地址、故障电子邮件的目标电子邮件地址和其他 SMTP 服务信息。	showsmtp(8) setsmtp(8)

表 C-23 列出了可配置 XSCF SNMP 代理功能的功能。选择 [Settings] (设置) - [Service] (服务) - [SNMP]。

表 C-23 SNMP 代理功能设置

项目	概要	相关命令
SNMPv3 代理查看/设置	查看/设置是否 SNMPv3 代理被启用或禁用。同时可用于查看/设置 MIB 定义文件和系统管理信息。	showsnmp(8) setsnmp(8)
SNMPv1/v2c 代理查看/设置	查看/设置是否 SNMPv1/v2c 代理被启用或禁用。还可用于查看/设置团队字符串。	
陷阱主机查看/设置	列表查看 SNMPv1/v2c 和 SNMPv3 陷阱主机。还可用于查看/设置陷阱目标主机名、端口号和其它主机信息。	

表 C-24 列出了可配置 SNMPv3 安全功能的功能。选择 [Settings] (设置) - [Service] (服务) - [SNMP Security] (SNMP 安全)。

表 C-24 SNMP 安全功能设置

项目	概要	相关命令
USM 管理信息查看/设置	查看/设置 USM 管理信息，例如用户验证算法。有关 USM 管理信息的详情，请参见 表 10-5。	showsnmpusm(8) setsnmpusm(8)
SNMPv1/v2c 代理查看/设置	查看/设置 VACM 管理信息，例如访问控制组和访问控制视图。有关 VACM 管理信息的详情，请参见 表 10-5。	showsnmpvacm(8) setsnmpvacm(8)

用户帐户设置

表 C-25 列出了可配置 XSCF 本地用户帐户的功能。选择 [Settings]（设置） - [User Manage]（用户管理） - [Account]（帐户）。

表 C-25 用户帐户设置

项目	概要	相关命令
用户账户信息查看	查看当前已注册用户账户的信息和状态。需要 useradm 权限。	showuser(8)
用户账户添加/删除	添加/删除用户帐户。需要 useradm 权限。	adduser(8) deleteuser(8)
用户账户启用/删除	禁用当前已注册用户账户，然后启用。需要 useradm 权限。	disableuser(8) enableuser(8)
用户账户信息查看/更改	查看特定用户账户的信息、更改密码、用户权限和密码策略。需要 useradm 权限。	showuser(8) password(8) setprivileges(8)
本地用户账户信息查看/更改密码	使用除 useradm 以外的任何权限都可查看本地用户信息和更改密码。	showuser(8) password(8)
系统密码策略查看/设置	查看当前系统密码策略。还可用于设置后续系统密码策略。	showpasswordpolicy(8) setpasswordpolicy(8)

注 - XSCF Web 不支持锁定功能，此功能在 3 次输错登录密码后锁定用户账户。使用 setloginlockout 和 showloginlockout 命令设置 XSCF shell 锁定功能。

LDAP 服务设置

表 C-26 列出了可配置 LDAP 客户端的功能。选择 [Settings]（设置） - [User Manage]（用户管理） - [LDAP]。

表 C-26 LDAP 服务设置

项目	概要	相关命令
LDAP 服务器查看/注册	查看/注册配置为 LDAP 客户端的 XSCF 的 LDAP 服务器。	showldap(8) setldap(8)
证书查看/导入	查看/导入 LDAP 服务器证书。	

LDAP over SSL 服务设置

表 C-27 列出了可配置 LDAP over SSL 客户端的功能。选择 [Settings]（设置） - [User Manage]（用户管理） - [LDAP/SSL]。

表 C-27 LDAP over SSL 服务设置

项目	概要	相关命令
LDAP over SSL 服务器查看/注册	查看/注册配置为 LDAP over SSL 客户端的 XSCF 的 LDAP over SSL 服务器。	showldapssl(8) setldapssl(8)
用户映射查看/设置	查看/设置用户映射。	
证书查看/设置	查看/加载/删除 LDAP over SSL 服务器证书。	
defaultrole 查看/设置	查看/设置通过 LDAP over SSL 验证的所有用户使用的用户权限。	
备选服务器查看/设置	查看/设置最多 5 个备选 LDAP over SSL 服务器。	
组查看/设置	查看/设置管理员组、操作员组和客户组。	
用户域查看/设置	查看/设置最多 5 个用户域。	

Active Directory 服务设置

表 C-28 列出了可配置 Active Directory 客户端的功能。选择 [Settings]（设置） - [User Manage]（用户管理） - [Active Directory]。

表 C-28 Active Directory 服务设置

项目	概要	相关命令
Active Directory 服务器查看/设置	启用/禁用配置为 Active Directory 客户端的 XSCF 的 Active Directory。查看/设置服务器、模式、超时时间、日志、默认设置等。	showad(8) setad(8)
证书查看/设置	查看/加载/删除 Active Directory 服务器证书。	
defaultrole 查看/设置	查看/设置通过 Active Directory 验证的所有用户使用的用户权限。	
备选服务器查看/设置	查看/设置最多 5 个备选 Active Directory 服务器，并查看/加载/删除服务器证书。	
组查看/设置	查看/设置管理员组、操作员组和客户组。	
用户域查看/设置	查看/设置最多 5 个用户域。	
DNS 定位器查询查看/设置	查看/设置最多 5 个 DNS 定位器查询。	

自动注销设置

表 C-29 列出了可设置 XSCF Web 会话超时（自动注销）时间的功能。选择 [Settings]（设置） - [Autologout]（自动注销） - [Account]（帐户）。使用自动注销（分钟）功

能后，登录 XSCF Web 的用户在指定的期间内如果没有访问，用户自动注销。

表 C-29 自动注销设置

项目	概要	相关命令
自动注销时间查看/设置	查看当前设置的自动注销时间（分钟）或设置自动注销时间。 默认值为 10 分钟。指定从 1 到 255 的数值。	仅支持在 XSCF Web 使用。

注 - XSCF Web 不支持 XSCF shell 进程超时的时间设置。请使用 `showautologout` 和 `setautologout` 命令。

CPU 激活设置

表 C-30 列出了可设置 CPU 激活的功能。选择 [Settings]（设置） - [CoD Reservation]（CoD 预约）。

表 C-30 CPU 激活设置

项目	概要	相关命令
CPU 内核资源的使用	查看 CPU 内核资源的使用状况。按以下方式查看： - 资源 (CPU) - 各 PPAR	<code>showcodusage(8)</code>
CPU 激活分配查看/设置	查看各 PPAR 的 CPU 激活分配状况。该功能也指定 PPAR 来增加或减少资源的 CPU 激活数量。	<code>showcod(8)</code> <code>setcod(8)</code>

表 C-31 列出了可注册 CPU 激活密钥的功能。选择 [Settings]（设置） - [CoD Activation]（CoD 激活）。

表 C-31 CPU 激活密钥注册

项目	概要	相关命令
CPU 激活密钥信息查看/设置	查看当前注册的 CPU 激活密钥信息。	<code>showcodactivation(8)</code>
CPU 激活密钥添加/删除	添加/删除 CPU 激活密钥。	<code>addcodactivation(8)</code> <code>deletecodactivation(8)</code>
CPU 激活密钥注册历史	查看关于添加/删除 CPU 激活密钥的历史信息。	<code>showcodactivationhistory(8)</code>

审核设置

表 C-32 列出了可配置 XSCF 审核的功能。选择 [Settings]（设置） - [Audit]（审核）。

表 C-32 审核设置

项目	概要	相关命令
审核日志（审核线索）使用状况/数据存档/数据删除	显示审核日志的使用容量。还可用于存档审核日志 (*1) 和删除次要文件。	showaudit(8) setaudit(8)
审核启用/禁用	查看/设置审核是启用还是禁用。	
审核策略查看/设置	查看/设置审核日志达到满容量 (*2) 时所应用的策略、本地审核日志使用量的警告阈值 (%), 以及警告电子邮件的目标地址。	
全局用户策略查看/设置	查看是否启用/禁用全局用户策略。	
用户审核记录生成策略查看/添加/更改	列表查看指定用户的审核记录生成策略（审核记录生成启用/禁用）。还可用于为用户添加审核记录生成策略。对于已被添加策略的用户，其全局用户策略被禁用。由指定用户启用或禁用审核记录生成策略，同时指定是否启用全局用户策略。	
审核时间/审核类型查看/设置	查看审核时间和审核类别。还用于指定是否启用或禁用审核事件和审核类别。	

*1 当前不支持审核日志存档。

*2 当审核日志达到满容量时，目前仅支持丢弃审核记录的默认审核策略“count”。因此，请勿指定“suspend”。

电子邮件设置

表 C-33 列出了用于进行 XSCF 电子邮件设置的功能。选择 [Settings]（设置） - [Email Reporting]（电子邮件报告）。

表 C-33 电子邮件设置

项目	概要	相关命令
电子邮件通知功能查看/设置	查看/设置电子邮件功能设置信息。您可以启用/禁用电子邮件通知功能和查看/设置发送给系统管理员的目标电子邮件地址。	showemailreport(8) setemailreport(8)

时间设置

表 C-34 列出了可设置系统时间和时区的功能。选择 [Settings]（设置） - [Time]（时间）。

表 C-34 时间设置

项目	概要	相关命令
系统时间查看/设置	查看/设置当前系统时间和时区。设置完成后，重新启动 XSCF。再次登录。在系统时间与 NTP 服务器同步时，不能进行时间设置。	showdate(8) setdate(8) showtimezone(8) settimezone(8)

注 - 使用 XSCF Web 不能设置夏令时。请使用 `showtimezone` 和 `settimezone` 命令设置。

功耗设置

表 C-35 列出了可设置系统功耗限制的功能。选择 [Settings] (设置) - [Power Capping] (用电封顶)。

表 C-35 功耗设置

项目	概要	相关命令
功耗限制查看/设置	查看功耗限制的设置。还用于启用/禁用限制和设置功耗的上限值。	<code>showpowercapping(8)</code> <code>setpowercapping(8)</code>

电源计划设置

表 C-36 列出了可设置电源计划的功能。选择 [Settings] (设置) - [Power Schedule] (电源计划)。

表 C-36 电源计划设置

项目	概要	相关命令
查看电源计划设置状态	列表查看 PPAR 电源计划的状态。	<code>showpowerschedule(8)</code>
电源计划设置	设置电源计划。还用于启用/禁用电源计划和为以下目标进行其他设置： - 各 PPAR - 所有 PPAR	<code>setpowerschedule(8)</code>
电源计划信息查看	查看下次 PPAR 的开机和关机时间。	<code>showpowerschedule(8)</code>
详细的电源计划信息	查看/设置电源计划信息的详细内容。 用于查看/添加/更改/删除如下目标的电源计划： - 各 PPAR - 所有 PPAR	<code>showpowerschedule(8)</code> <code>setpowerschedule(8)</code> <code>addpowerschedule(8)</code> <code>deletepowerschedule(8)</code>

设备设置

表 C-37 列出了可设置 PCI 扩展单元信息和与服务器连接的卡的信息的功能。选择 [Settings] (设置) - [Add-In Card Manager] (外接卡管理器)。

表 C-37 PCI 扩展单元信息设置

项目	概要	相关命令
卡/PCI 扩展单元传感器信息查看	列表查看以下目标的传感器信息： - PCI 卡（连接到服务器） - PCI 扩展单元 - PCI 扩展单元中的 FRU	ioxadm(8)
设备信息查看/电源设置	列表查看 PCI 卡、PCI 扩展单元和链路卡的设备信息。 还用于向 PCI 扩展单元中的电源设备发出关闭/开启的指令。	
监控组件初始化	初始化 PCI 扩展单元的监控组件。	
固件更新	检查、登录和更新 PCI 扩展单元和链路卡固件。	
PCI 扩展单元 LED 状态查看/设置	查看/设置 PCI 扩展单元中 FRU 定位器 LED 的状态。	

注 - 如果 PCI 扩展单元中的两个电源单元均已关闭，PCI 扩展单元无法从 XSCF Web 或 XSCF shell 开启。此时如果需要再次开启电源，必须按下物理电源按钮 (POWER)。

PCI 扩展单元的直接 I/O 功能的设置

表 C-38 列出了可配置 PCI 扩展单元的直接 I/O 功能的功能。选择 [Settings]（设置） - [PCIBOX DIO]。

表 C-38 PCI 扩展单元的直接 I/O 功能的设置

项目	概要	相关命令
启用/禁用直接 I/O 功能	显示/设置是否启用或禁用 SPARC M12/M10 的每个 PCI 插槽的 PCI 扩展单元的直接 I/O 功能。	showpciboxdio(8) setpciboxdio(8)

远程存储设置

表 C-39 列出了可配置远程存储的功能。选择 [Settings]（设置） - [Remote Storage]（远程存储）。

表 C-39 远程存储设置

项目	概要	相关命令
远程存储服务器启动	启动 Java Runtime Environment 以启动远程存储服务器。	无
远程存储连接状态显示/设置	以列表显示远程存储连接信息。 - XSCF-LAN 接口 - XSCF-LAN、IP 地址、子网掩码、网关 - 系统管理终端的连接状态 /IP 地址 对于系统管理终端，也选择 XSCF-LAN 接口、连接到介质/断开介质/指定 IP 地址/配置从 XSCF。	setremotestorage(8) showremotestorage(8)

C.3.4 维护服务器页面

网络连接信息

表 C-40 列出了可显示网络连接信息的功能。选择 [Maintenance]（维护） - [Network Tools]（网络工具）。选定时，[Ping]、[Traceroute] 和 [Nslookup] 菜单分别显示主机响应、主机网络路径和主机名信息。

表 C-40 网络连接信息查看

项目	概要	相关命令
主机响应查看	查看 XSCF 和指定主机之间的网络响应状态。	ping(8)
网络路径查看	查看指定主机或网络设备的网络路径信息。	traceroute(8)
主机名信息查看	查看指定主机名称信息。	nslookup(8)

XSCF 设置信息保存/恢复

表 C-41 列出了可保存/恢复 XSCF 设置信息的功能。选择 [Maintenance]（维护） - [Configuration Management]（配置管理）。

表 C-41 XSCF 设置信息保存/恢复

项目	概要	相关命令
设置信息的保存/恢复	进行 XSCF 设置信息或 CPU 激活密钥的保存/恢复。 使用 [Run] 按钮保存/恢复信息时，XSCF 将重新启动。再次登录。	dumpconfig(8) restoreconfig(8) dumpcodactivation(8) restorecodactivation(8)

固件更新

表 C-42 列出了可更新 XCP 固件的功能。选择 [Maintenance]（维护） - [Firmware Update]（固件更新）。

表 C-42 固件更新

项目	概要	相关命令
版本查看	查看以下固件版本： - XCP 版本 - XSCF 固件版本 - CMU 固件版本	version(8)
XCP 导入	指定如下的固件文件将固件输入到服务器： - XCP 固件文件 - PCI 扩展单元固件文件	getflashimage(8)
固件更新	执行 XCP 升级。 此时，XSCF 重新启动，因此请再次登录到 XSCF。	flashupdate(8)

表 C-42 固件更新 (续)

项目	概要	相关命令
版本匹配 (针对有多个 XSCF 的系统)	在有多个 XSCF 系统中匹配 XCP 固件版本。在 XSCF 单元、CMU、机柜或其他部件更换后使用。	flashupdate(8)

XSCF 重新启动

表 C-43 列出了可重新启动 XSCF 的功能。选择 [Maintenance] (维护) - [Reboot XSCF] (重新启动 XSCF)。

表 C-43 XSCF 重新启动

项目	概要	相关命令
XSCF 重新启动	重新启动本地 XSCF。	rebootxscf(8)
目标 XSCF 重新启动 (对于具有多个 XSCF 的系统)	使用所安装的 XSCF 指定机箱的 BB-ID 来重新启动机箱。 - 所有机柜 - 指定的机柜	showbbstatus(8) rebootxscf(8)

XSCF 切换

表 C-44 列出了可在具有多个 XSCF 的系统中的 XSCF 之间切换的功能。选择 [Maintenance] (维护) - [Switch Over] (切换)。

表 C-44 XSCF 切换

项目	概要	相关命令
XSCF 切换 (针对有多个 XSCF 的系统)	从主 XSCF 切换到备用 XSCF 或从备用 XSCF 切换到主 XSCF。	switchxscf(8)

服务器信息保存

表 C-45 列出了可收集服务器信息并分析/解决系统问题的功能。选择 [Maintenance] (维护) - [Switch Over] (切换)。

表 C-45 服务器信息保存

项目	概要	相关命令
服务器信息保存/目标机柜信息保存 (针对有多个 XSCF 的系统)	指定目标 BB-ID 用于收集数据, 如: 服务器配置、公共系统日志和机柜日志, 并将数据保存到文件中。 - 所有机柜 - 指定的机柜	snapshot(8)

注 - 在具有多个 XSCF 的系统中, 在登录备用 XSCF 以后, 您可以保存页面上显示的服务器信

息。

ASR 功能设置

表 C-46 ASR 功能设置

项目	概要	相关命令
启用/禁用 ASR 功能 (维护标签) (*1)	查看/设置是否维护标签被启用或禁用。	showservicetag(8) setservicetag(8)
实时测试	在 Ops 中心和 ASR 管理器中生成 pseudo 错误, 或查看是否是实时状态。	

*1 ASR 功能是一种远程维护服务, 运行由 Oracle Corporation 公司提供的 Oracle Auto Service Request 软件。有关 ASR 功能的详细信息, 请参见您正在使用的软件版本的《Oracle Auto Service Request Installation and Operations Guide》。

C.3.5 查看日志的页面

表 C-47 列出了可查阅日志信息的功能。选择 [Logs] (日志)。选择所需日志。

表 C-47 日志信息

项目	概要	相关命令
错误日志查看	查看错误日志。您可搜索日志。	showlogs(8) error option
电源日志查看	查看电源日志。您可搜索日志。	showlogs(8) power option
事件日志查看	查看事件日志。您可搜索日志。	showlogs(8) event option
控制台日志查看	查看控制台日志。您可搜索日志。	showlogs(8) console option
崩溃日志查看	查看崩溃日志。您可搜索日志。	showlogs(8) panic option
温度历史日志查看 (环境日志)	指定机柜的 BB-ID 以查看历史日志。您可搜索日志。	showlogs(8) env option
IPL 信息日志查看	指定 PPAR 以查看其 IPL 日志。您可搜索日志。	showlogs(8) ipl option
监视信息日志查看	查看监视信息日志。您可搜索日志。	showlogs(8) monitor option
审核日志查看	查看审核日志。 您可指定时期、日期、用户和类型在日志中查看。	viewaudit(8)

XSCF MIB 信息

本附录概括介绍 XSCF SNMP 代理功能支持的 XSCF 扩展 MIB（管理信息库，Management Information Base）。有关 SNMP 代理功能的详情，请参见“10.3 通过 SNMP 代理监控/管理系统状态”。

- MIB 对象标识
- 标准 MIB
- 扩展 MIB
- 陷阱基本知识

D.1 MIB 对象标识

下面列出 XSCF 所支持 MIB 对象 (OIDs) 标识符的示例。

internet	OBJECT IDENTIFIER ::=	{ iso org(3) dod(6) 1 }
directory	OBJECT IDENTIFIER ::=	{ internet 1 }
mgmt	OBJECT IDENTIFIER ::=	{ internet 2 }
experimental	OBJECT IDENTIFIER ::=	{ internet 3 }
private	OBJECT IDENTIFIER ::=	{ internet 4 }
mib-2	OBJECT IDENTIFIER ::=	{ mgmt 1 }
system	OBJECT IDENTIFIER ::=	{ mib-2 1 }
interfaces	OBJECT IDENTIFIER ::=	{ mib-2 2 }
at	OBJECT IDENTIFIER ::=	{ mib-2 3 }
ip	OBJECT IDENTIFIER ::=	{ mib-2 4 }
icmp	OBJECT IDENTIFIER ::=	{ mib-2 5 }
tcp	OBJECT IDENTIFIER ::=	{ mib-2 6 }

udp	OBJECT IDENTIFIER ::=	{ mib-2 7 }
snmp	OBJECT IDENTIFIER ::=	{ mib-2 11 }
enterprises	OBJECT IDENTIFIER ::=	{ private 1 }
fujitsu	OBJECT IDENTIFIER ::=	{ enterprises 211 }
product	OBJECT IDENTIFIER ::=	{ fujitsu 1 }
solaris	OBJECT IDENTIFIER ::=	{ product 15 }
sparc	OBJECT IDENTIFIER ::=	{ solaris 4 }
xscfSpMIB	OBJECT IDENTIFIER ::=	{ sparc 1 }
scfObjects	OBJECT IDENTIFIER ::=	{ xscfSpMIB 1 }
scfInfo	OBJECT IDENTIFIER ::=	{ scfObjects 1 }
scfState	OBJECT IDENTIFIER ::=	{ scfObjects 2 }
scfMonitorInfo	OBJECT IDENTIFIER ::=	{ scfObjects 3 }
scfSystemInfo	OBJECT IDENTIFIER ::=	{ scfObjects 4 }
scfPPARInfo	OBJECT IDENTIFIER ::=	{ scfObjects 5 }
scfPsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 6 }
scfLsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 7 }
scfBoardInfo	OBJECT IDENTIFIER ::=	{ scfObjects 8 }
scfCpuInfo	OBJECT IDENTIFIER ::=	{ scfObjects 9 }
scfMemoryInfo	OBJECT IDENTIFIER ::=	{ scfObjects 10 }
scfPciBoxInfo	OBJECT IDENTIFIER ::=	{ scfObjects 11 }
scfComponentInfo	OBJECT IDENTIFIER ::=	{ scfObjects 12 }
scfDomainInfo	OBJECT IDENTIFIER ::=	{ scfObjects 13 }
scfMIBTraps	OBJECT IDENTIFIER ::=	{ xscfSpMIB 2 }
scfMIBTrapPrefix	OBJECT IDENTIFIER ::=	{ scfMIBTraps 0 }
scfMIBTrapData	OBJECT IDENTIFIER ::=	{ scfMIBTraps 1 }
scfMIBConformances	OBJECT IDENTIFIER ::=	{ xscfSpMIB 3 }
scfMIBCompliances	OBJECT IDENTIFIER ::=	{ scfMIBConformances 1 }
scfMIBGroups	OBJECT IDENTIFIER ::=	{ scfMIBConformances 2 }
scfMIBObjectGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 1 }
scfMIBNotifGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 2 }

scfHwCtrlMIB	OBJECT IDENTIFIER ::=	{ sparcEnterprise 2 }
scfHwCtrlMIBObjects	OBJECT IDENTIFIER ::=	{ scfHwCtrlMIB 1 }
scfHwCtrlPowerMgmt	OBJECT IDENTIFIER ::=	{ scfHwCtrlMIBObjects 1 }

D.2 标准 MIB

XSCF 支持的标准 MIB 符合以下 RFC（注）。有关标准 MIB 定义文件的详情，请参见通用 RFC 文档。

协议和 RFC 的示例

MIB II	RFC1213
基于用户的安全模型 (USM)	RFC3414
基于视图的访问控制模型 (VACM)	RFC3415
SNMPv2-MIB	RFC3418

注 - RFC: 代表请求注解。RFC 是互联网工程任务组 (IETF) 发布的技术规格，该任务组是一个制订 Internet 相关标准的组织。

D.3 扩展 MIB

SPARC M12/M10 系统中的 XSCF 提供了 XSCF 扩展 MIB 中的以下信息：

- 系统信息、硬件/固件版本和系统配置信息
- 环境信息（温度、电压、风扇转速等）
- 物理分区状态和物理分区配置信息
- 系统中的部件故障信息
- 系统中的功率值信息

注 - 有关如何获取和安装 XSCF 扩展 MIB 定义文件的详细信息，请参见 ["10.3 通过 SNMP 代理监控/管理系统状态"](#)。

D.3.1 XSCF 扩展 MIB 对象

本节介绍 XSCF 扩展 MIB 的主要对象组信息。

scfObjects

- **scfInfo 组**
提供有关 XSCF 的一般信息，如：主 XSCF 和 XSCF-LAN 信息。
- **scfState 组**
提供 XSCF 状态信息、操作面板的开关状态等信息。
- **scfMonitorInfo 组**
提供系统中不同组件的环境信息。如：组件名称、温度、电压和转速。
- **scfSystemInfo 组**
提供以下系统信息：
 - 主机名称、序列号、安装的 CPU 数量，以及其它系统产品信息
 - LED 状态信息
 - 系统环境信息，如：系统功耗、排气和进气温度
- **scfPPARInfo 组**
提供以下物理分区信息：
 - PPAR ID、搭载的 CPU 数量、内存容量，以及其它物理分区硬件信息
 - OpenBoot PROM、POST、管理程序版本
 - Oracle Solaris 信息
 - 物理分区运行操作状态和配置策略
- **scfPsbInfo 组**
该组提供物理分区中 PSB 编号、PSB 电源状态和 PSB 分配/并入状态等 PSB (BB) 信息。
- **scfLsbInfo 组**
提供 LSB 信息，如：LSB 号、LSB 所属 PPAR 的 ID，和 PCL 信息。
- **scfBoardInfo 组**
提供 CMU 信息，如：CPU 内存单元 (CMUL, CMU) 名称、编号和操作状态。
- **scfCpuInfo 组**
提供 CPU 模块信息，如：CPU 编号、CPU 频率和操作状态。
- **scfMemoryInfo 组**
提供信息，如：内存单元编号、容量和操作状态。
- **scfPciBoxInfo 组**
提供 PCI 扩展单元，及其主要组件的信息。典型组件为 I/O 板、PCI 卡、链路卡、电源单元、风扇单元和传感器。有关部件的详情，请参见《PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual》中的 "第2章 Understanding the PCI Expansion Unit Components"。
- **scfComponentInfo 组**
提供有关 FRU 的信息以及系统中所有组件的状态信息。

- `scfDomainInfo` 组
提供逻辑域的信息，如：所属的 PPAR 的 ID、逻辑域名称和逻辑域状态。

D.4 陷阱基本知识

陷阱包含标准陷阱和扩展陷阱。标准陷阱对于设备来说是向 SNMP 确认的一般陷阱。有关标准陷阱，请参见通用文档。在本手册中，识别特定于本系统事件的陷阱称为扩展陷阱。

扩展陷阱在 `scfMIBTRap` 对象中提供不同种类的信息。有关扩展陷阱的概述，请参见"[10.3 通过 SNMP 代理监控/管理系统状态](#)"。

Oracle VM Server for SPARC 的 SPARC M12/M10 系统特定功能

本附录介绍并提供了有关特定于 SPARC M12/M10 系统的 Oracle VM Server for SPARC 的功能的补充信息。

有关管理 Oracle VM Server for SPARC 软件的一般信息，请参见所使用版本的《Oracle VM Server for SPARC Administration Guide》。

- 按顺序关闭逻辑域
- CPU 激活支持
- 检查发生故障的资源
- 自动更换故障的 CPU
- 管理程序转储
- 域控制台日志功能
- CPU 插槽限制条件

E.1 按顺序关闭逻辑域

在 SPARC M12/M10 系统中，可以从 XSCF 执行所有逻辑域的按顺序关闭。有关详情，请参见 "8.7 按顺序关闭逻辑域"。

E.2 CPU 激活支持

SPARC M12/M10 系统支持 CPU 激活。使用 `ldm` 命令可显示 CPU 激活列表。有关详情，请参见 "8.8 检查 CPU 激活信息"。

E.3 检查发生故障的资源

SPARC M12/M10 系统自动检测和降级发生故障的内存和 CPU 资源。使用 `ldm(1M)` 命令可显示内存和 CPU 资源的状态。有关详情，请参见 ["10.6 查看发生故障的硬件资源"](#)。

E.3.1 确认使用 `list-domain` 子命令时是否发生了内存或 CPU 故障

1. 显示物理分区中逻辑域的详细信息，以及是否发生了内存或 **CPU** 故障的信息。

```
primary# ldm list-domain -l -S
```

E.3.2 显示使用 `list-device` 子命令时是否发生了内存或 CPU 故障

1. 显示物理分区中可用内存和可用 **CPU** 的资源信息，以及是否发生了内存或 **CPU** 故障的信息。

```
primary# ldm list-devices -S memory cpu
```

E.4 自动更换故障的 CPU

SPARC M12/M10 系统自动检测故障的 CPU 并将其置于离线状态。您可配置 Oracle VM Server for SPARC，当有空闲 CPU 或可用 CPU 激活时自动更换故障的 CPU。有关详情，请参见 ["10.7 设置故障 CPU 内核的自动更换"](#)。

E.5 管理程序转储

管理程序可能在检测到物理分区不一致时中止。在这种情况下，固件保留了管理程序内存中的内容，并按照出厂默认配置重新启动系统。有关详情，请参见 ["8.13 收集管理程序转储文件"](#)。

E.6 域控制台日志功能

在逻辑域环境中，控制域的控制台输出目的地是 XSCF。所有其他域的控制台输出目的地是启动虚拟控制台终端收集和分配单元 (vcc) 的服务域。在 Oracle Solaris 11.1 及更高版本，服务域支持逻辑域的控制台日志功能。有关详情，请参见 "[8.10 域控制台日志功能](#)"。

E.7 CPU 插槽限制条件

对于具有 Oracle VM Server for SPARC 3.3 或更高版本的 SPARC M12/M10 系统，可以基于物理 CPU 插槽管理逻辑域配置。有关详情，请参见 "[8.14 管理与 CPU 插槽相关联的逻辑域资源](#)"。

SAS2IRCU 实用程序命令示例

本附录包含使用 Broadcom Limited 公司的 SAS-2 集成 RAID 配置实用程序 (SAS2IRCU) (以下称为 SAS2IRCU 实用程序) 14.00.00.00 或更高版本配置和管理 SPARC M12/M10 系统硬件 RAID 卷的典型 SAS2IRCU 实用程序命令的显示示例。

有关 SAS2IRCU 实用程序的详细信息，请参见 "14.2 配置硬件 RAID" 中所述的 Broadcom Limited 公司网站。有关 SAS2IRCU 实用程序以及如何使用的详细信息，请参见相同网站的《SAS-2 Integrated RAID Configuration Utility User Guide》。SAS-2 集成 RAID 配置实用程序 (SAS2IRCU) 的版权归 Broadcom Limited 及其附属公司所有。

- 显示 `sas2ircu` 识别的 SAS 控制器列表
- 查看硬件 RAID 卷的信息
- 添加硬件 RAID 卷
- 查看硬件 RAID 卷的配置状态
- 创建硬件 RAID 卷的热备盘
- 删除硬件 RAID 卷的热备盘
- 删除硬件 RAID 卷
- 识别硬件 RAID 卷的默认磁盘驱动器

F.1 显示 `sas2ircu` 识别的 SAS 控制器列表

如需显示由 `sas2ircu` 识别的 SAS 控制器列表，需使用 `sas2ircu` 的 `list` 命令。以下示例显示 `Adapter Type = SAS2308_2` 是内部 SAS 控制器。检查内部 SAS 控制器显示的索引号。下面是 SPARC M12-2 的示例。

注 - 在 SPARC M12-2/M12-2S 系统或具有多个 SPARC M12-2S/M10-4S 单元的系统配置中，会显示多个 SAS 控制器，但您无法使用索引号来标识其安装位置。SAS 控制器的安装位置可以从 `sas2ircu DISPLAY` 信息中识别。有关 `sas2ircu DISPLAY` 的详细信息，请参见 "F.2 查看硬件 RAID 卷的信息"。

```
# ./sas2ircu LIST
LSI Corporation SAS2 IR Configuration Utility.
Version 20.00.00.00 (2014.09.18)
Copyright (c) 2008-2014 LSI Corporation. All rights reserved.
```

Index	Adapter Type	Vendor ID	Device ID	Pci Address	SubSys Ven ID	SubSys Dev ID
0	SAS2308_2	1000h	87h	00h:03h:00h:00h	10cfh	187eh

Index	Adapter Type	Vendor ID	Device ID	Pci Address	SubSys Ven ID	SubSys Dev ID
1	SAS2308_2	1000h	87h	00h:03h:00h:00h	10cfh	187eh

F.2 查看硬件 RAID 卷的信息

如需查看系统配置的硬件 RAID 卷和磁盘驱动器的信息，请使用 sas2ircu 的 DISPLAY 命令。

以下示例显示了对于索引=1 的 SAS 控制器 (*1) 而言，配备磁盘槽 0 中磁盘驱动器作为 Primary 驱动器和磁盘槽 1 中磁盘驱动器作为 Secondary 驱动器的 RAID 1（镜像）卷，以及磁盘槽 2、3、4 和 5 中未组成硬件 RAID 的磁盘驱动器。

*1 这可以通过 sas2ircu 的 list 命令来检查。请参见 "F.1 显示 sas2ircu 识别的 SAS 控制器列表"。

在以下的示例中，从 (1) 到 (4) 代表：

(1): SAS 控制器的信息

(2): RAID 卷的信息

(2-1): RAID 卷 1 的信息

您可获得如下信息（部分摘录）。

- RAID 卷 ID 是 286
- RAID 卷名称是 RAID1-SYS
- RAID 卷的状态正常 (Okay (OKY))
- RAID 级别是 RAID1（镜像）
- SPARC M12/M10 内部磁盘槽 0 的磁盘 (2:0) 安装在 PHY[0] (Primary)
- SPARC M12/M10 内部磁盘槽 1 的磁盘 (2:1) 安装在 PHY[1] (Secondary)

(3): 物理设备信息

(3-1): SPARC M12/M10 内部磁盘槽 0 (Enclosure#:2,Slot#:0) 的磁盘 (Drive Type=SAS_HDD) 的状态

它被优化为 RAID 卷的一部分。(State:Optimal (OPT))

(3-2): SPARC M12/M10 内部磁盘槽 0 (Enclosure#:2,Slot#:0) 的机壳管理装置 (Device Type= Enclosure services device) 的状态

表明这是一个非硬盘的设备。虽然显示的是 Standby 状态，是正常的显示。

(State:Standby (SBY))

(3-3): SPARC M12/M10 内部磁盘槽 2 (Enclosure#:2,Slot#:2) 的磁盘 (Drive Type=SAS_HDD) 的状态

表明这是一个未在 RAID 配置中的磁盘设备。该状态表明它可以被整合到一个 RAID 卷和热备盘。(State:Ready (RDY))

(4): SPARC M12/M10 机箱信息

(4-1): SAS 控制器的 SAS 地址

注 - 您可以预先在 OBP 上检查 SAS 控制器的 SAS 地址，并将其与 sas2ircu DISPLAY 进行比较，找到 SAS 控制器的设备路径和安装位置。有关如何在 OBP 上获取 SAS 控制器信息的详细信息，请参阅“14.2.4 硬件 RAID 操作前的准备工作”。

```
root# ./sas2ircu 0 DISPLAY
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0
-----
Controller information <-- (1)
-----
Controller type           : SAS2308_2
BIOS version              : 0.00.00.00
Firmware version         : 13.00.66.00
Channel description      : 1 Serial Attached SCSI
Initiator ID              : 0
Maximum physical devices : 255
Concurrent commands supported : 3072
Slot                      : Unknown
Segment                   : 0
Bus                       : 3
Device                    : 0
Function                   : 0
RAID Support              : Yes
-----

IR Volume information <-- (2)
-----
IR volume 1 <-- (2-1)
Volume ID                  : 286
Volume Name                : RAID1-SYS
Status of volume          : Okay (OKY)
Volume wwid                : 0aa6d102f1bf517a
RAID level                 : RAID1
Size (in MB)              : 571250
Physical hard disks       :
PHY[0] Enclosure#/Slot#   : 2:0
PHY[1] Enclosure#/Slot#   : 2:1
-----

Physical device information <-- (3)
-----
Initiator at ID #0

Device is a Hard disk <-- (3-1)
Enclosure #                : 2
```

```
Slot # : 0
SAS Address : 5000039-4-281b-51e2
State : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007NC
GUID : 50000394281b51e0
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Enclosure services device <-- **(3-2)**

```
Enclosure # : 2
Slot # : 0
SAS Address : 500000e-0-e049-073d
State : Standby (SBY)
Manufacturer : FUJITSU
Model Number : NBBEXP
Firmware Revision : 0d32
Serial No : x3625413500
GUID : N/A
Protocol : SAS
Device Type : Enclosure services device
```

Device is a Hard disk

```
Enclosure # : 2
Slot # : 1
SAS Address : 5000039-4-281b-549a
State : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007PT
GUID : 50000394281b5498
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Hard disk <-- **(3-3)**

```
Enclosure # : 2
Slot # : 2
SAS Address : 5000039-4-281a-8ad2
State : Ready (RDY)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007G7
GUID : 50000394281a8ad0
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Hard disk

```
Enclosure # : 2
```

```
Slot # : 3
SAS Address : 5000039-4-281b-5dc2
State : Ready (RDY)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007T3
GUID : 50000394281b5dc0
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Hard disk

```
Enclosure # : 2
Slot # : 4
SAS Address : 5000039-4-281b-58b2
State : Ready (RDY)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007RA
GUID : 50000394281b58b0
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Hard disk

```
Enclosure # : 2
Slot # : 5
SAS Address : 5000039-4-281b-502e
State : Ready (RDY)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007LR
GUID : 50000394281b502c
Protocol : SAS
Drive Type : SAS_HDD
```

Enclosure information <-- (4)

```
Enclosure# : 1
Logical ID : 500000e0:e046ff10 <-- (4-1)
Numslots : 8
StartSlot : 0
Enclosure# : 2
Logical ID : 500000e0:e049073f
Numslots : 9
StartSlot : 0
-----
```

SAS2IRCU: Command DISPLAY Completed Successfully.
SAS2IRCU: Utility Completed Successfully.

F.3 添加硬件 RAID 卷

使用 `sas2ircu` 的 `CREATE` 命令将硬件 RAID 卷添加到系统。

在以下示例中，将为配备有 SPARC M10-1 的磁盘槽 2、3 和 4（磁盘的整个区域）的磁盘驱动器创建名为“RAID1E-VOL”的 RAID1E（镜像扩展）卷。

```
root# ./sas2ircu 0 CREATE RAID1E MAX 2:2 2:3 2:4 RAID1E-VOL
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.
You are about to create an IR volume.
WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES
WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
Please wait, may take up to a minute...
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0          Volume 0 is now , enabled, inactive
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0          Volume 0 is now , enabled, active
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0          Volume 0 is now , enabled, active, data scrub
in progress
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0          Volume 0 is now , enabled, active, background
initialization in progress, data scrub in progress
Jan 20 16:20:15 1S-341-D0 scsi: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 16:20:15 1S-341-D0          Command failed to complete...Device is gone
SAS2IRCUC: Volume created successfully.
SAS2IRCUC: Command CREATE Completed Successfully.
SAS2IRCUC: Utility Completed Successfully.
```

添加硬件 RAID 卷后，使用 `sas2ircu` 的 `DISPLAY` 命令检查硬件 RAID 卷和磁盘驱动器信息。

检查以下信息。

(1): IR 卷的信息

(1-1): 确认新的 RAID 卷（卷 ID:285）已经按照 `sas2ircu CREATE` 命令的定义创建，RAID 卷的状态是 "Okay (OKY)"。

(2): 物理设备信息

(2-1) (2-2) (2-3): 确认新整合的 RAID 卷的磁盘槽 2、3 和 4 的磁盘驱动器的状态是 "Optimal (OPT)"。

■ `sas2ircu` 的 `DISPLAY` 命令的执行结果（部分摘录）

```
root# ./sas2ircu 0 DISPLAY
-----
IR Volume information  <-- (1)
-----
IR volume 1  <-- (1-1)
```



```

Volume ID                : 285
Volume Name              : RAID1E-VOL
Status of volume        : Okay (OKY)
Volume wwid             : 00c354402fc35418
RAID level              : RAID1E
Size (in MB)           : 856875
Physical hard disks    :
PHY[0] Enclosure#/Slot# : 2:2
PHY[1] Enclosure#/Slot# : 2:3
PHY[2] Enclosure#/Slot# : 2:4
IR volume 2
Volume ID                : 286
Volume Name              : RAID1-SYS
Status of volume        : Okay (OKY)
Volume wwid             : 0aa6d102f1bf517a
RAID level              : RAID1
Size (in MB)           : 571250
Physical hard disks    :
PHY[0] Enclosure#/Slot# : 2:0
PHY[1] Enclosure#/Slot# : 2:1

```

Physical device information <-- (2)

Device is a Hard disk <-- (2-1)

```

Enclosure #              : 2
Slot #                  : 2
SAS Address             : 5000039-4-281a-8ad2
State                   : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer            : TOSHIBA
Model Number           : MBF2600RC
Firmware Revision      : 3706
Serial No               : EA25PC7007G7
GUID                   : 50000394281a8ad0
Protocol                : SAS
Drive Type              : SAS_HDD

```

Device is a Hard disk <-- (2-2)

```

Enclosure #              : 2
Slot #                  : 3
SAS Address             : 5000039-4-281b-5dc2
State                   : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer            : TOSHIBA
Model Number           : MBF2600RC
Firmware Revision      : 3706
Serial No               : EA25PC7007T3
GUID                   : 50000394281b5dc0
Protocol                : SAS
Drive Type              : SAS_HDD

```

Device is a Hard disk <-- (2-3)

```

Enclosure #              : 2
Slot #                  : 4
SAS Address             : 5000039-4-281b-58b2
State                   : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567

```

Manufacturer	: TOSHIBA
Model Number	: MBF2600RC
Firmware Revision	: 3706
Serial No	: EA25PC7007RA
GUID	: 50000394281b58b0
Protocol	: SAS
Drive Type	: SAS_HDD

F.4 查看硬件 RAID 卷的配置状态

使用 `sas2ircu` 的 `STATUS` 命令查看创建的硬件 RAID 卷的配置状态。

在以下的示例中，显示了新创建的硬件 RAID 卷 (ID:285) 的配置状态。表明在 `Background Init` 状态，进度是 0.14%。

注 - "`Current Operation:Background Init`" 表明 RAID 卷正在配置过程中。"`Percentage complete`" (进度) 变为 100% 时，配置状态变为 "`Current Operation:None`"，可以安全使用 RAID 卷。

在以下的示例中，从 (1) 到 (2) 代表：

(1): RAID 卷 1 的信息

- RAID 卷 ID 是 285
- 当前 RAID 操作是 `Background Init`，操作进度是 0.14%
- RAID 已启用并优化

(2): RAID 卷 2 的信息

- RAID 卷 ID 是 286
- 当前没有 RAID 操作
- RAID 已启用并优化

```
root# ./sas2ircu 0 STATUS
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Background command progress status for controller 0...

IR Volume 1 <-- (1)
  Volume ID                : 285
  Current operation        : Background Init
  Volume status            : Enabled
  Volume state             : Optimal
  Volume wwid              : 00c354402fc35418
  Physical disk I/Os      : Not quiesced
  Volume size (in sectors) : 1754880000
  Number of remaining sectors : 1752440704
  Percentage complete      : 0.14%

IR Volume 2 <-- (2)
```

```

Volume ID                : 286
Current operation        : None
Volume status            : Enabled
Volume state             : Optimal
Volume wwid              : 0aa6d102f1bf517a
Physical disk I/Os      : Not quiesced
SAS2IRCU: Command STATUS Completed Successfully.
SAS2IRCU: Utility Completed Successfully.

```

F.5 创建硬件 RAID 卷的热备盘

使用 `sas2ircu` 的 `HOTSPARE` 命令创建硬件 RAID 卷的热备盘。

在以下示例中，创建了安装在 SPARC M10-1 的磁盘槽 5 中的磁盘驱动器的热备盘。

```

root# ./sas2ircu 0 HOTSPARE 2:5
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO

Please wait, may take up to a minute...
SAS2IRCU: Hot Spare disk created successfully.
SAS2IRCU: Command HOTSPARE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.

```

创建热备盘后，使用 `sas2ircu` 的 `DISPLAY` 命令查看如下项目。

(1) 物理设备信息

(1-1) 是否磁盘槽 5 的磁盘驱动器的 "State" 是 "HotSpare (HSP)"

■ `sas2ircu` 的 `DISPLAY` 命令的执行结果（部分摘录）

```

root# ./sas2ircu 0 DISPLAY
-----
Physical device information <-- (1)
-----
Device is a Hard disk <-- (1-1)
Enclosure #                : 2
Slot #                     : 5
SAS Address                 : 5000039-4-281b-5022
State                       : Hot Spare (HSP)
Size (in MB)/(in sectors)  : 572325/1172123567
Manufacturer                : TOSHIBA
Model Number                : MBF2600RC
Firmware Revision           : 3706

```

```
Serial No           : EA25PC7007LM
GUID                : 50000394281b5020
Protocol            : SAS
Drive Type          : SAS_HDD
```

F.6 删除硬件 RAID 卷的热备盘

使用 `sas2ircu` 的 `HOTSPARE` 命令删除硬件 RAID 卷的热备盘。

在以下示例中，删除了安装在 SPARC M10-1 的磁盘槽 5 中的磁盘驱动器的热备盘。

```
root# ./sas2ircu 0 HOTSPARE DELETE 2:5
  LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
SAS2IRCUC: Hot Spare disk deleted successfully.
SAS2IRCUC: Command HOTSPARE Completed Successfully.
SAS2IRCUC: Utility Completed Successfully.
```

删除热备盘后，使用 `sas2ircu` 的 `DISPLAY` 命令查看如下项目。

(1) 物理设备信息

(1-1) 是否磁盘槽 5 的磁盘驱动器的 "State" 是 "Ready (RDY)"

■ `sas2ircu` 的 `DISPLAY` 命令的执行结果（部分摘录）

```
root# ./sas2ircu 0 DISPLAY
-----
Physical device information <-- (1)
-----
Device is a Hard disk <-- (1-1)
Enclosure #           : 2
Slot #                : 5
SAS Address            : 5000039-4-281b-5022
State                  : Ready (RDY)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer           : TOSHIBA
Model Number           : MBF2600RC
Firmware Revision      : 3706
Serial No              : EA25PC7007LM
GUID                  : 50000394281b5020
Protocol               : SAS
Drive Type             : SAS_HDD
```

F.7 删除硬件 RAID 卷

使用 sas2ircu 的 DELETEVOLUME 命令将硬件 RAID 卷从系统删除。

以下示例删除了 SPARC M10 上卷 ID:285 的 RAID 卷。

```
root# ./sas2ircu 0 DELETEVOLUME 285
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

You are about to delete an existing RAID Volume on a controller. This command
will delete the specified RAID volume and associated HotSpare drive(s).

WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
Please wait, may take up to a minute...
SAS2IRCU: Volume deleted successfully.
SAS2IRCU: Command DELETEVOLUME Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

删除硬件 RAID 卷后，使用 sas2ircu 的 DISPLAY 命令检查如下硬件 RAID 卷和磁盘驱动器的项目。

(1) IR 卷的信息

(1-1) 是否卷号 ID:285 的 RAID 卷被删除，并且只有卷号 ID:286 的信息存在

(2) 物理设备信息

(2-1) (2-2) (2-3) 是否与被删除卷号 ID:285 一起整合到 RAID 卷的磁盘槽 2、3 和 4 的磁盘驱动器的“State”是“Ready (RDY)”

- sas2ircu 的 DISPLAY 命令的执行结果（部分摘录）

```
root# ./sas2ircu 0 DISPLAY
-----
IR Volume information <-- (1)
-----
IR volume 1 <-- (1-1)
  Volume ID                : 286
  Volume Name              : RAID1-SYS
  Status of volume        : Okay (OKY)
  Volume wwid              : 0aa6d102f1bf517a
  RAID level              : RAID1
  Size (in MB)            : 571250
  Physical hard disks      :
  PHY[0] Enclosure#/Slot# : 2:0
  PHY[1] Enclosure#/Slot# : 2:1
-----
Physical device information <-- (2)
-----
```

```

Device is a Hard disk <-- (2-1)
  Enclosure #           : 2
  Slot #                : 2
  SAS Address           : 5000039-4-281a-8ad2
  State                 : Ready (RDY)
  Size (in MB)/(in sectors) : 572325/1172123567
  Manufacturer          : TOSHIBA
  Model Number          : MBF2600RC
  Firmware Revision     : 3706
  Serial No             : EA25PC7007G7
  GUID                  : 50000394281a8ad0
  Protocol              : SAS
  Drive Type            : SAS_HDD
Device is a Hard disk <-- (2-2)
  Enclosure #           : 2
  Slot #                : 3
  SAS Address           : 5000039-4-281b-5dc2
  State                 : Ready (RDY)
  Size (in MB)/(in sectors) : 572325/1172123567
  Manufacturer          : TOSHIBA
  Model Number          : MBF2600RC
  Firmware Revision     : 3706
  Serial No             : EA25PC7007T3
  GUID                  : 50000394281b5dc0
  Protocol              : SAS
  Drive Type            : SAS_HDD
Device is a Hard disk <-- (2-3)
  Enclosure #           : 2
  Slot #                : 4
  SAS Address           : 5000039-4-281b-58b2
  State                 : Ready (RDY)
  Size (in MB)/(in sectors) : 572325/1172123567
  Manufacturer          : TOSHIBA
  Model Number          : MBF2600RC
  Firmware Revision     : 3706
  Serial No             : EA25PC7007RA
  GUID                  : 50000394281b58b0
  Protocol              : SAS
  Drive Type            : SAS_HDD

```

F.8 识别硬件 RAID 卷的默认磁盘驱动器

如需识别默认硬件 RAID 卷和默认磁盘驱动器，使用 `sas2ircu` 的 `DISPLAY` 命令。

在以下示例中，SPARC M10-1 的磁盘槽 1 的磁盘驱动器出现故障。

在以下的示例中，从 (1) 到 (2) 代表：

(1): RAID 卷的信息

(1-1): RAID 卷 2 的信息

您可获得如下信息（部分摘录）。

- RAID 卷 ID 是 286
 - RAID 卷状态是降级 (Degraded (DGD))
 - RAID 级别是 RAID1 (镜像)
 - SPARC M12/M10 内部磁盘槽 0 的磁盘 (2:0) 安装在 PHY[0] (Primary)
 - PHY[1] (Secondary) 无磁盘信息 (0:0)
- (2): 物理设备信息
- (2-1): 安装位置无信息 (Enclosure#:0,Slot#:0=以前作为 Enclosure#:2,Slot#:1 存在, 执行此命令时无法访问) 的磁盘驱动器 (Drive Type=SAS_HDD) 的状态表明磁盘驱动器处于故障状态。(State:Failed (FLD))

```

root# ./sas2ircu 0 DISPLAY
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0
-----
Controller information
-----
Controller type           : SAS2308_2
BIOS version             : 0.00.00.00
Firmware version        : 13.00.66.00
Channel description     : 1 Serial Attached SCSI
Initiator ID            : 0
Maximum physical devices : 255
Concurrent commands supported : 3072
Slot                    : Unknown
Segment                 : 0
Bus                     : 3
Device                  : 0
Function                 : 0
RAID Support            : Yes
-----

IR Volume information <-- (1)
-----
IR volume 1
Volume ID                : 285
Volume Name              : RAID1E-VOL
Status of volume         : Okay (OKY)
Volume wwid              : 0fd4f41e8cd673de
RAID level                : RAID1E
Size (in MB)             : 856875
Physical hard disks      :
PHY[0] Enclosure#/Slot# : 2:2
PHY[1] Enclosure#/Slot# : 2:3
PHY[2] Enclosure#/Slot# : 2:4

IR volume 2 <-- (1-1)
Volume ID                : 286
Volume Name              : RAID1-SYS
Status of volume         : Degraded (DGD)
Volume wwid              : 0aa6d102f1bf517a
RAID level                : RAID1

```

```
Size (in MB) : 571250
Physical hard disks :
PHY[0] Enclosure#/Slot# : 2:0
PHY[1] Enclosure#/Slot# : 0:0
```

Physical device information <-- (2)

Initiator at ID #0

Device is a Hard disk <-- (2-1)

```
Enclosure # : 0
Slot # : 0
SAS Address : 0000000-0-0000-0000
State : Failed (FLD)
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC700855
GUID : N/A
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Enclosure services device

```
Enclosure # : 2
Slot # : 0
SAS Address : 500000e-0-e049-073d
State : Standby (SBY)
Manufacturer : FUJITSU
Model Number : NBBEXP
Firmware Revision : 0d32
Serial No : x3625413500
GUID : N/A
Protocol : SAS
Device Type : Enclosure services device
```

Device is a Hard disk

```
Enclosure # : 2
Slot # : 0
SAS Address : 5000039-4-281b-6466
State : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007UE
GUID : 50000394281b6464
Protocol : SAS
Drive Type : SAS_HDD
```

Device is a Hard disk

```
Enclosure # : 2
Slot # : 2
SAS Address : 5000039-4-281a-8ad2
State : Optimal (OPT)
```



```

Size (in MB)/(in sectors)      : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                   : MBF2600RC
Firmware Revision              : 3706
Serial No                      : EA25PC7007G7
GUID                           : 50000394281a8ad0
Protocol                       : SAS
Drive Type                     : SAS_HDD

Device is a Hard disk
Enclosure #                    : 2
Slot #                         : 3
SAS Address                    : 5000039-4-281b-5dc2
State                          : Optimal (OPT)
Size (in MB)/(in sectors)     : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                   : MBF2600RC
Firmware Revision              : 3706
Serial No                      : EA25PC7007T3
GUID                           : 50000394281b5dc0
Protocol                       : SAS
Drive Type                     : SAS_HDD

Device is a Hard disk
Enclosure #                    : 2
Slot #                         : 4
SAS Address                    : 5000039-4-281b-502e
State                          : Optimal (OPT)
Size (in MB)/(in sectors)     : 572325/1172123567
Manufacturer                    : TOSHIBA
Model Number                   : MBF2600RC
Firmware Revision              : 3706
Serial No                      : EA25PC7007LR
GUID                           : 50000394281b502c
Protocol                       : SAS
Drive Type                     : SAS_HDD
-----
Enclosure information
-----
Enclosure#                    : 1
Logical ID                    : 500000e0:e046ff10
Numslots                      : 8
StartSlot                    : 0
Enclosure#                    : 2
Logical ID                    : 500000e0:e049073f
Numslots                      : 9
StartSlot                    : 0
-----
SAS2IRCU: Command DISPLAY Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
root#

```

注 - 进行创建或删除 RAID 卷、删除热备盘等操作后，在 Oracle Solaris 显示以下的信息。表

明在 RAID 卷或磁盘驱动器上没有标签信息。这种状态的 RAID 卷或磁盘驱动器不能在 Oracle Solaris 使用。执行 `format` 命令，选择合适的 RAID 卷或磁盘驱动器并做标签后，可在 Oracle Solaris 上使用。

■ 输出信息示例

```
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
```

■ 执行 `format` 命令的示例

```
root@solaris:/root# format
Searching for disks...
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b58b0
(sd3):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b58b0
(sd3):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:08 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 15:55:08 1S-341-D0          Corrupt label; wrong magic number
done
c0t50000394281A8AD0d0: configured with capacity of 558.89GB
c0t50000394281B5DC0d0: configured with capacity of 558.89GB
c0t50000394281B58B0d0: configured with capacity of 558.89GB
AVAILABLE DISK SELECTIONS:
  0. c0t50000394281A8AD0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
    /scsi_vhci/disk@g50000394281a8ad0
    /dev/chassis/SYS/HDD02/disk
  1. c0t50000394281B5DC0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
    /scsi_vhci/disk@g50000394281b5dc0
    /dev/chassis/SYS/HDD03/disk
  2. c0t50000394281B58B0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
    /scsi_vhci/disk@g50000394281b58b0
    /dev/chassis/SYS/HDD04/disk
  3. c0t50000394281B5020d0 <LSI-Logical Volume-3000 cyl 24998 alt 2 hd 16
sec 128>
    /scsi_vhci/disk@g50000394281b5020
```

```
    /dev/chassis/SYS/HDD05/disk
4. c2t3AA6D102F1BF517Ad0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
   sec 557>
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3aa6d102f1bf517a,0
Specify disk (enter its number): 0
[disk formatted]
Disk not labeled.  Label it now? yes
```


SPARC M12-1/M10-1 XSCF 启动模式功能

本附录介绍可减少 SPARC M12-1/M10-1 启动时间的 XSCF 启动模式功能。

- 功能概述
- 限制和注意事项
- 配置步骤

G.1 功能概述

G.1.1 XSCF 启动模式功能是什么？

SPARC M12-1/M10-1 系统的 XCP 2220 及更高版本中引入了 XSCF 启动模式功能。

使用 `xscfstartupmode` 命令可改变启动时 XSCF 的操作。`xscfstartupmode` 命令允许用户选择“正常”（默认）或“快速”模式。

“快速”模式可在开启 (AC ON) 系统输入电源和 XSCF 已经启动后，使 SPARC M12-1/M10-1 系统自动启动物理分区。在“快速”模式下，没有必要输入 XSCF 的 `poweron` 命令来启动物理分区。

对于 XCP 版本早于 XCP 2220 的 SPARC M12-1/M10-1 系统，或 `xscfstartupmode` 命令设置为“正常”模式的 XCP 2220 或更高版本的 SPARC M12-1/M10-1 系统，在系统电源开启 (AC ON) 后，必须使用 XSCF `poweron` 命令启动物理分区。

如需自动启动物理分区，请将启动模式设置为“快速”，设置操作面板模式开关为“锁定”，然后开启系统的输入电源 (AC ON)。如果在操作面板模式开关设置为“维护”时开启 (AC ON) 系统的输入电源，启动模式将恢复为“正常”，因此，物理分区不会自动启动。

若需暂时在“正常”模式下运行，请将操作面板模式开关设置为“维护”，并开启输入电源 (AC ON)。

XSCF 启动模式功能仅是 SPARC M12-1/M10-1 的特定功能，不受 M12-2/M12-2S/M10-4/M10-4S 的支持。

G.1.2 使用状态

使用 XSCF 启动模式功能时的状态如下。

- 如果使用 `xscfstartupmode` 命令将启动模式设置为“快速”模式，并且在操作面板模式开关设置为“锁定”时开启输入电源，则系统将以“快速”模式启动。然而，即使启动模式变更为“快速”，如果在开启输入电源后操作面板模式开关从“维护”变更为“锁定”，系统也将以“正常”模式启动，而不是“快速”模式。
- 当启动模式更改为“快速”时，重新启动 XSCF 不会导致物理分区自动启动。物理分区仅在输入电源开启时自动激活。
- 变更启动模式的配置后，仅执行 `rebootxscf` 命令无法变更系统的启动模式。必须关闭/开启输入电源才可使变更的启动模式设置生效。
- 启动模式的配置保存在主板单元 (MBU) 上的 XSCF 中，但不执行内部备份到 PSU 背板单元 (PSUBP)。如果更换 MBU，启动模式可能变更为默认设置。MBU 更换后，请务必确认启动模式，如果有必要，将启动模式变更为所需的设置。
- 当系统以“快速”模式启动时，请勿变更 XSCF 的配置或执行降级/恢复，或配置 OpenBoot PROM 的环境参数，或保存逻辑域的配置信息。仅可在“正常”模式执行这些操作。系统已经以“快速”模式启动时，如果执行上述操作，配置和变更将保存到 MBU 的 XSCF，但不执行内部备份到 PSUBP。如果更换 MBU，配置信息将不会从 PSUBP 内部备份恢复，并且系统可能无法启动。

除了将 XSCF 启动模式功能设置为“快速”，从将输入电源施加到系统至 Oracle Solaris/Oracle VM Server for SPARC 启动所花费的时间可通过下述进一步降低：

- 使用固态硬盘 (SSD) 内部存储器作为启动设备（而不是 SAS 磁盘）
- 将 POST 诊断级别设置为关闭（从 min 的默认）

注 - 更改 POST 诊断级别时，请确保在确认“[G.2.2 系统操作时的限制和注意事项](#)”的内容后再更改该设置。

G.2 限制和注意事项

G.2.1 系统安装时的限制和注意事项

- 必须在 XSCF 启动模式为“正常”时执行系统安装操作，然后可将 XSCF 启动模式变更为“快速”。使用“[G.3 配置步骤](#)”中介绍的 `xscfstartupmode -d` 命令可以访问启动模式的状态。当 XSCF 启动模式为“快速”时，系统硬件配置信息和 XSCF 配置信息仅保存到 XSCF（不执行内部备份）。如果存储在 XSCF 内的信息与系统硬件信息之间存在差异，可能会发生类似 XSCF 降级和物理分区无法正常操作的问题。
- 如果使用 `setpowerschedule` 命令将系统配置为按预定时间执行电源操作，并且启动模式设置为“快速”，则系统将在预定的时间以“快速”模式启动。

- 如果使用 `setpowerschedule` 命令将电源恢复设置为“关”或“自动”，并且将启动模式设置为“快速”，当施加输入电源时 (AC ON)，系统将忽略“关”或“自动”设置，将以“快速”模式启动。

G.2.2 系统操作时的限制和注意事项

- 在 XSCF 启动模式为“快速”的情况下，登录到 XSCF 的 telnet/ssh 用户帐户限制为最多 10 个。
- `xscfstartupmode` 命令本身不会被审核，但是其他审核不受 XSCF 启动模式设置的影响。
- 当物理分区以“快速”模式启动时，“电源恢复”将被登记在 XSCF 电源日志的“原因”字段。
- 如果 POST 诊断级别设置为“关”，在物理分区电源开启期间，POST 将不执行 CPU、内存和 I/O 诊断。因此，除了 POST 自身停止运行的情况下，POST 诊断期间，将不执行异常检测和故障部件的随之降级。相反，在检测到 CPU、内存或 I/O 异常时，可能发生“管理程序中止”或“操作系统崩溃”。
- 如果将 POST 诊断级别设置为“min/max”，将执行 CPU、内存和 I/O 诊断，但启动时间与诊断操作所花费的时间成比例地增加。
- 当变更 XSCF 的配置信息时，以“正常”启动模式启动 XSCF 后进行上述操作。如需暂时以“正常”模式运行，将操作面板模式开关设置为 "Service"，关闭/开启输入电源，重新启动 XSCF，然后更改 XSCF 的配置信息。
- 在创建或变更逻辑域的配置信息时，以“正常”启动模式启动 XSCF 后进行上述操作。如需暂时以“正常”模式运行，将操作面板模式开关设置为 "Service"，关闭/开启输入电源，重新启动 XSCF，然后在物理分区运行时创建或更改逻辑域的配置信息，并确保执行 `ldm add-spconfig` 命令将逻辑域配置信息保存到 XSCF。

G.2.3 维护时的限制

- 硬件故障可以通过由 `showhardconf` 或 `showstatus XSCF` 命令产生的输出中的故障标记（表示为“*”）进行确认。当将启动模式设置为“快速”，并且检测到系统中的硬件故障时，如果关闭/开启输入电源即使一次，故障部件的所有故障标记（表示为“*”）在下次系统启动时被清除。在更换故障部件之前，请关注使用 `showhardconf` 或 `showstatus XSCF` 命令输出的故障信息。然后，请参阅错误日志中的 FRU 信息来更换部件。
- 当使用 `dumpconfig` 或 `restoreconfig` 命令保存或恢复配置信息时，以“正常”模式启动 XSCF 后进行上述操作。如需暂时以“正常”模式运行，将操作面板模式开关设置为 "Service"，关闭/开启输入电源，重新启动 XSCF，然后执行这些操作。
- 启动模式配置的设置不包含在通过使用 `dumpconfig` 或 `restoreconfig XSCF` 命令获得的已保存或恢复的信息中。因此，更换 MBU 后，应使用 `restoreconfig` 命令恢复配置信息，然后重置启动模式。如果在尚未更换 MBU 的系统上执行 `restoreconfig` 命令，将不会移除现有的配置信息。
- 当系统以“快速”模式启动时，使用 `replacefru` 命令无法更换硬件。采用输入电源关闭的方法更换硬件。在此之后，将操作面板模式开关设置为“维护”，并开启输入电

源，等待，直至 XSCF 已经启动。以这种方式，硬件配置信息和 XSCF 设置信息被保存在 XSCF 中。XSCF 启动后，关闭输入电源并将操作面板模式开关设置“锁定”。然后将输入电源开启时，系统将以“快速”模式启动。

- 当使用 `restoredefaults XSCF` 命令将系统初始化为出厂默认值时，启动模式没有被初始化。执行 `restoredefaults` 命令之前，请确保将启动模式变更为“正常”并关闭/开启输入电源。
- 当更新 XSCF 固件时，以“正常”模式启动 XSCF 后进行上述操作。

G.3 配置步骤

本节介绍配置 XSCF 启动模式功能的步骤。

1. 执行类似更新固件、配置 XSCF 网络和用户、激活 CPU 内核等安装作业。
有关详情，请参见服务器的最新《产品说明》。

注 - 在执行系统安装时，请勿将启动模式设置为“快速”。

注 - 从 XCP 2220 版开始，支持 XSCF 启动模式。如果系统固件版本旧于 XCP 2220，遵循说明书或产品说明采购和更新系统固件。

2. 开启物理分区的电源。
 - a. 使用 `showdomainconfig` 命令确认逻辑域的配置信息是 "factory defaults"。
 - b. 执行 `poweron` 命令启动物理分区。

注 - 在执行系统安装时，请勿将启动模式设置为“快速”。

3. 安装类似于 **Oracle Solaris** 或 **Oracle VM Server for SPARC** 等软件，和/或配置逻辑域。
关于软件安装，请参见 [4.5 连接 DVD 驱动器](#)。有关如何配置逻辑域的详细信息，请参见《Fujitsu SPARC M12 和 Fujitsu M10/SPARC M10 域配置指南》。

注 - 在执行系统安装时，请勿将启动模式设置为“快速”。

注 - 如果已经创建逻辑域的配置信息，请确保通过执行 `ldm add-spconfig` 命令将此信息保存到 XSCF。

4. 使用 `poweroff` 命令关闭物理分区的电源。
5. 将 XSCF 启动模式设置为“快速”模式。
 - a. 使用 `platadm` 用户权限登录 XSCF。
 - b. 查看启动模式的当前值。
有关 `xcscfstartupmode(8)` 命令的详细信息，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。


```
XSCF> xscfstartupmode -d  
Setting Mode: normal  
Current Mode: normal
```

- c. 将启动模式设置为"快速"。

```
XSCF> xscfstartupmode -m fast
```

- d. 确认启动模式已经设置为"快速"。

```
XSCF> xscfstartupmode -d  
Setting Mode: fast [need AC OFF/ON]  
Current Mode: normal
```

6. 将 **POST 诊断级别**设置为"**OFF**"（当非强制选择为开启电源期间跳过 POST 诊断，以便进一步减少系统启动时间时）。

- a. 查看当前 POST 诊断级别。

```
XSCF> showpparmode -p 0  
Host-ID :9007002b  
Diagnostic Level :min  
Message Level :normal  
Alive Check :on  
Watchdog Reaction :reset  
Break Signal :on  
Autoboot (Guest Domain) :on  
Elastic Mode :off  
IOreconfigure :false  
CPU Mode :auto  
PPAR DR (Current) :-  
PPAR DR (Next) :off
```

- b. 将 POST 诊断级别设置为"OFF"。

```
XSCF> setpparmode -p 0 -m diag=off
```

- c. 确认 POST 诊断级别的状态。

```
XSCF> showpparmode -p 0  
Host-ID :9007002b  
Diagnostic Level :off  
Message Level :normal  
Alive Check :on  
Watchdog Reaction :reset  
Break Signal :on  
Autoboot (Guest Domain) :on  
Elastic Mode :off  
IOreconfigure :false
```

CPU Mode	:auto
PPAR DR(Current)	:-
PPAR DR(Next)	:off

7. 关闭输入电源。
8. 将操作面板模式开关设置为"锁定"。
9. 开启输入电源，启动物理分区。
10. 确认启动模式已经设置为"快速"。
有关 `xscfstartupmode(8)` 命令的详细信息，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

```
XSCF> xscfstartupmode -d  
Setting Mode: fast  
Current Mode: fast
```

OpenBoot PROM 环境变量和命令

本附录介绍了 SPARC M12/M10 系统特定的 OpenBoot PROM 命令和 SPARC M12/M10 系统不支持的 OpenBoot PROM 环境变量和命令，以及启用了安全模式的行为。

对于本附录中未说明事项的详细信息，请参见 Oracle Solaris 的参考手册中 `eeeprom` 命令的解释以及 Oracle 公司的《OpenBoot 4.x Command Reference Manual》。

- [SCSI 设备查看](#)
- [不支持的 OpenBoot PROM 环境变量](#)
- [不支持的 OpenBoot PROM 命令](#)
- [启用安全模式的行为](#)

H.1 SCSI 设备查看

如需查看 SCSI 总线上的所有设备，请使用 `probe-scsi-all` 命令。

```
{0} ok probe-scsi-all
```

H.2 不支持的 OpenBoot PROM 环境变量

在 SPARC M12/M10 系统中，无法使用以下 OpenBoot PROM 环境变量。

- `diag-device`
- `diag-file`
- `diag-level`
- `os-root-device`

如需设置/查看适用于 `diag-level` 的电源开启自检 (POST) 诊断级别，请使用 XSCF 固件的 `setpparmode` 命令或 `showpparmode` 命令。

H.3 不支持的 OpenBoot PROM 命令

在 SPARC M12/M10 系统中，无法使用以下 OpenBoot PROM 命令。

- cache-off
- cache-on
- callback
- clear-cache
- ecdatal
- ecdatal@
- ectag!
- ectag@
- eject floppy
- firmware-version
- flush-cache
- help dump
- iomap?
- iomap-page
- iomap-pages
- iopgmap@
- iopgmap!
- map-region
- map-segments
- obdiag
- pgmap?
- rmap!
- rmap@
- sbus
- segmentsize
- smap!
- smap?
- smap@
- test-all
- .ver
- %f0 to %f31

H.4 启用安全模式的行为

当将 OpenBoot PROM 环境变量的安全模式设置为 "command" 或 "full" 时，将 1 到 8 个字符可显示的字符串设置为安全密码时，将启用 OpenBoot PROM 的安全模式，并且命令和操作需要密码。

(1) 当安全模式设置为 "command" 时

boot 命令和 go 命令不需要密码，但所有其他命令都需要密码。请注意，当指定了 "auto-boot?= true" 时，系统将自动启动。

(2) 当安全模式设置为 "full" 时

除 go 命令之外，包括普通操作（如 boot 命令）的任何操作都需要密码来执行。即使指定了 "auto-boot?= true"，启动时也需要密码。

当启用安全模式时，OpenBoot PROM 的提示符从 "ok" 更改为由以下任一操作触发的带 > 的安全提示模式，并且上述情况 (1) 和 (2) 需要密码。

- 执行 logout 命令。
- 在 OpenBoot PROM 正在运行（在 XCP 2340 或更高版本中）时，域控制台断开连接并重新连接。
- 发送中断信号。
- 域重新启动。
- OpenBoot PROM 命令正在运行时发生错误。

有关 OpenBoot PROM 环境变量安全模式的详细信息，请参见 Oracle 的手册。

如何指定启动设备

本附录介绍如何在 SPARC M12/M10 系统中逻辑域的 OpenBoot PROM 上将内置存储器指定为启动设备。

- 内置存储器的设备路径
- 使用 PHY 编号指定的方法
- 使用目标 ID 指定的方法
- 使用 SAS 地址指定的方法
- 使用卷设备名指定的方法

I.1 内置存储器的设备路径

如需将内置存储器指定为启动设备，需将识别磁盘的信息附加到内置存储器设备路径名的末尾。内置存储器的设备路径根据型号或安装的 CPU 的数量而有所不同。有关详情，请参见“附录 A SPARC M12/M10 系统设备路径列表”。

识别内置存储器（即将内置存储器指定为启动设备）有四种方法。表 I-1 介绍了这四种方法。请注意：独立式内置硬盘和内置硬件 RAID 可使用的指定方法不同。

表 I-1 将存储器指定为启动设备的方法

指定方法	摘要	适用的内置存储器类型
使用 PHY 编号	本指定方法使用对应于内置硬盘所安装的磁盘槽的 PHY 编号。本方法在 OpenBoot PROM 上也用作 devalias。	独立式硬盘
使用目标 ID	本指定方法使用唯一分配给内置硬盘的目标 ID。目标 ID 可能会因磁盘安装顺序的不同而不同。	独立式硬盘
使用 SAS 地址	本指定方法使用唯一分配给内置硬盘的 SAS 地址。磁盘更换后，SAS 地址将变更。	独立式硬盘
使用卷设备名	本指定方法使用硬件 RAID 卷名。	硬件 RAID

1.2 使用 PHY 编号指定的方法

此方法使用对应于内置磁盘安装槽的 PHY 编号来识别用作启动设备的磁盘。

在将独立式内置硬盘指定为启动设备时，您可以使用此指定方法。但是，您不能用它来指定内置硬件 RAID。

表 I-2 列出了对应于磁盘槽的 PHY 编号。

表 I-2 对应于磁盘槽的 PHY 编号

磁盘槽	PHY 编号
内置磁盘槽 #0	100 或 0
内置磁盘槽 #1	101 或 1
内置磁盘槽 #2	102 或 2
内置磁盘槽 #3	103 或 3
内置磁盘槽 #4	104 或 4
内置磁盘槽 #5	105 或 5
内置磁盘槽 #6	106 或 6
内置磁盘槽 #7	107 或 7

如需找到启动盘的 PHY 编号，请在 OpenBoot PROM 上执行 probe-scsi-all 命令，并查看 PhyNum 值。

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target a
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
PHY 数

Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1

Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e06d233d PhyNum 14
```

启动设备符号

```
<SAS 控制器的设备路径>/disk@pX,Y:Z
```

此处，对于"disk@p"后的 X，指定对应于安装磁盘槽的 PHY 编号。此外，对于 Y 和 Z 分别指定内置存储器的逻辑单元编号 (LUN) 和切片编号。

注 - 可以省略逻辑单元编号 (LUN) 和切片编号。如果省略, 假定指定 LUN “0” 和切片编号 “a”。如果将内置存储器用作启动设备, 则指定 LUN “0” 和切片编号 “a”, 因此这些数字与省略时具有相同的数值。因此, 在使用示例中, 符号采用省略了 LUN 和切片编号的形式。

使用示例

指定以下内容, 其中“0”是启动盘的 PHY 编号。

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0
```

1.3 使用目标 ID 指定的方法

本方法使用唯一分配给各磁盘的目标 ID 来识别用作启动设备的磁盘。

在将独立式内置硬盘指定为启动设备时, 您可以使用此指定方法。但是, 您不能用它来同样指定内置硬件 RAID。

如需找到启动盘的目标 ID, 请在 OpenBoot PROM 上执行 `probe-scsi-all` 命令, 并查看 Target 值。

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target a
  目标 ID
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e06d233d PhyNum 14
```

启动设备符号

```
<SAS 控制器的设备路径>/disk@X,Y:Z
```

此处, 对于 “disk@” 后的 X, 指定目标 ID。此外, 对于 Y 和 Z 分别指定内置存储器的逻辑单元编号 (LUN) 和切片编号。

注 - 可以省略逻辑单元编号 (LUN) 和切片编号。如果省略, 假定指定 LUN “0” 和切片编号 “a”。如果将内置存储器用作启动设备, 则指定 LUN “0” 和切片编号 “a”, 因此这些数字与省略时具有相同的数值。因此, 在使用示例中, 符号采用省略了 LUN 和切片编号的形式。

使用示例

指定以下内容，其中“a”是启动盘的目标 ID。

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@a
```

1.4 使用 SAS 地址指定的方法

本指定方法使用磁盘驱动器的唯一 SAS 地址来指定启动设备。

对于内置存储器，每个磁盘驱动器都有唯一分配的 SAS 地址，更换磁盘时，SAS 地址也发生变化。磁盘更换后，启动时指定的设备名也因此发生变化。

在将独立式内置硬盘指定为启动设备时，您可以使用此指定方法。但是，您不能用它来同样指定内置硬件 RAID。

如需找到启动盘的 SAS 地址，请在 OpenBoot PROM 上执行 probe-scsi-all 命令，并查看 SASAddress 值。

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target a
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
                                     SAS 地址
Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e06d233d PhyNum 14
```

启动设备符号

```
<SAS 控制器的设备路径>/disk@wXXXXXXXX, Y:Z
```

此处，对于 "disk@w" 后的 XXXXXXXX，指定 SAS 地址。此外，对于 Y 和 Z 分别指定内置存储器的逻辑单元编号 (LUN) 和切片编号。

注 - 可以省略逻辑单元编号 (LUN) 和切片编号。如果省略，假定指定 LUN "0" 和切片编号 "a"。如果将内置存储器用作启动设备，则指定 LUN "0" 和切片编号 "a"，因此这些数字与省略时具有相同的数值。因此，在使用示例中，符号采用省略了 LUN 和切片编号的形式。

使用示例

指定以下内容，其中“50000393d82891d2”是启动盘的 SAS 地址。

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@w50000393d82891d2
```

1.5 使用卷设备名指定的方法

本指定方法使用内置硬件 RAID 的卷设备名来指定启动设备。卷设备名被分配给 RAID 中配置的各卷。

在将内置硬件 RAID 指定为启动设备时，您可以使用此方法。

如需找到启动盘的卷设备名，请在 OpenBoot PROM 上执行 `probe-scsi-all` 命令，并查看 `VolumeDeviceName` 值。

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target 11e Volume 0
Unit 0 Disk LSI Logical Volume 3000 10485760 Blocks, 5368 MB
VolumeDeviceName 3eb2fdbd4c32058f VolumeWWID 0eb2fdbd4c32058f
                    卷设备名
```

在 XCP 2070 和早期版本中，可能不输出 `VolumeDeviceName`。在这种情况下，执行 `show-volumes` 命令，该命令将输出卷 WWID。将第一个 WWID 字符更换为 "3" 获得卷设备名。

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
Name raid1-volume WWID 0eb2fdbd4c32058f
                    RAID 卷的 WWID
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
Disk 1
  Primary Optimal
  Target a TOSHIBA MBF2300RC 3706
Disk 0
  Secondary Optimal
  Target b TOSHIBA MBF2300RC 3706
{0} ok
```

启动设备符号

```
<SAS 控制器的设备路径>/disk@wXXXXXXXX, Y:Z
```

此处，对于 "disk@w" 后的 XXXXXXXX，指定卷设备名。此外，对于 Y 和 Z，分别指定内置硬件 RAID 的逻辑单元编号 (LUN) 和切片编号。

注 - 可以省略逻辑单元编号 (LUN) 和切片编号。如果省略，假定指定 LUN "0" 和切片编号 "a"。如果内置硬件 RAID 用作启动设备，LUN "0" 和切片编号 "a" 被指定，因此这些编号与省略时具有相同的值。因此，在使用示例中，符号采用省略了 LUN 和切片编号的形式。

使用示例

指定以下内容，其中 "3eb2fdbd4c32058f" 是启动设备的卷设备名。

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@w3eb2fdbd4c32058f
```

DVD 驱动器别名列表

本附录将介绍 DVD 驱动器的别名。

- 外部 DVD 驱动器别名
- 远程存储 DVD 驱动器别名

J.1 外部 DVD 驱动器别名

本节列出了 SPARC M12/M10 系统中外部 DVD 驱动器的别名。

J.1.1 SPARC M12-1 外部 DVD 驱动器别名

表 J-1 SPARC M12-1 外部 DVD 驱动器别名

别名	设备路径
cdrom (front)	/pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk@0 (USB2.0/1.1)
cdrom0-30 (后)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom0 (rear)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom1 (front)	/pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk@0 (USB2.0/1.1)

J.1.2 SPARC M12-2 外部 DVD 驱动器别名

对于初始安装时 1-CPU (CMUL) 或 2- CPU 的配置

表 J-2 SPARC M12-2 外部 DVD 驱动器别名 (初始安装时: 单CPU 或 2 个 CPU)

别名	设备路径
cdrom (front)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom00-0-30 (后)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom00-0 (后)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom00-1 (前)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

J.1.3 SPARC M12-2S 外部 DVD 驱动器别名

对于初始安装时 1-CPU (CMUL) 或 2- CPU 的配置

表 J-3 SPARC M12-2S 外部 DVD 驱动器别名 (初始安装时: 单CPU 或 2 个 CPU)

别名	设备路径
cdrom (front)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom00-0-30 (后)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom00-0 (后)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom00-1 (前)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom01-0-30 (后)	/pci@8900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom01-0 (后)	/pci@8900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom01-1 (前)	/pci@8900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom02-0-30 (后)	/pci@9100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)

表 J-3 SPARC M12-2S 外部 DVD 驱动器别名 (初始安装时: 单CPU 或 2 个 CPU) (续)

别名	设备路径
cdrom02-0 (后)	/pci@9100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom02-1 (前)	/pci@9100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom03-0-30 (后)	/pci@9900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom03-0 (后)	/pci@9900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom03-1 (前)	/pci@9900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom04-0-30 (后)	/pci@a100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom04-0 (后)	/pci@a100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom04-1 (前)	/pci@a100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom05-0-30 (后)	/pci@a900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom05-0 (后)	/pci@a900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom05-1 (前)	/pci@a900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom06-0-30 (后)	/pci@b100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom06-0 (后)	/pci@b100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom06-1 (前)	/pci@b100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom07-0-30 (后)	/pci@b900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom07-0 (后)	/pci@b900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom07-1 (前)	/pci@b900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom08-0-30 (后)	/pci@c100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom08-0 (后)	/pci@c100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom08-1 (前)	/pci@c100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

表 J-3 SPARC M12-2S 外部 DVD 驱动器别名（初始安装时：单CPU 或 2 个 CPU）（续）

别名	设备路径
cdrom09-0-30（后）	/pci@c900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom09-0（后）	/pci@c900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom09-1（前）	/pci@c900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom10-0-30（后）	/pci@d100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom10-0（后）	/pci@d100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom10-1（前）	/pci@d100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom11-0-30（后）	/pci@d900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom11-0（后）	/pci@d900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom11-1（前）	/pci@d900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom12-0-30（后）	/pci@e100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom12-0（后）	/pci@e100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom12-1（前）	/pci@e100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom13-0-30（后）	/pci@e900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom13-0（后）	/pci@e900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom13-1（前）	/pci@e900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom14-0-30（后）	/pci@f100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom14-0（后）	/pci@f100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom14-1（前）	/pci@f100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom15-0-30（后）	/pci@f900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom15-0（后）	/pci@f900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@6/disk@0 (USB2.0/1.1)

表 J-3 SPARC M12-2S 外部 DVD 驱动器别名（初始安装时：单CPU 或 2 个 CPU）(续)

别名	设备路径
cdrom15-1（前）	/pci@f900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

J.1.4 SPARC M10-1 外部 DVD 驱动器别名

表 J-4 SPARC M10-1 外部 DVD 驱动器别名

别名	设备路径
cdrom (front)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk@0
cdrom0 (rear)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk@0
cdrom1 (front)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk@0

J.1.5 SPARC M10-4 外部 DVD 驱动器别名

对于初始安装时 2-CPU (CMUL) 或 4- CPU 的配置

表 J-5 SPARC M10-4 外部 DVD 驱动器别名（初始安装时：2 个 CPU 或 4 个 CPU）

别名	设备路径
cdrom (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom00-0 (rear)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom00-1 (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

J.1.6 SPARC M10-4S 外部 DVD 驱动器别名

表 J-6 列出了外部 DVD 驱动器的别名，逻辑系统板 (LSB) 的编号为 0 到 15。

对于初始安装时 2-CPU (CMUL) 或 4- CPU 的配置

表 J-6 SPARC M10-4S 外部 DVD 驱动器别名（初始安装时：2 个 CPU 或 4 个 CPU）

别名	设备路径
cdrom (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom00-0 (rear)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a

表 J-6 SPARC M10-4S 外部 DVD 驱动器别名（初始安装时：2 个 CPU 或 4 个 CPU）(续)

别名	设备路径
cdrom00-1 (front)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom01-0 (rear)	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom01-1 (front)	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom02-0 (rear)	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom02-1 (front)	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom03-0 (rear)	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom03-1 (front)	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom04-0 (rear)	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom04-1 (front)	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom05-0 (rear)	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom05-1 (front)	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom06-0 (rear)	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom06-1 (front)	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom07-0 (rear)	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom07-1 (front)	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom08-0 (rear)	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom08-1 (front)	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom09-0 (rear)	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom09-1 (front)	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom10-0 (rear)	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom10-1 (front)	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom11-0 (rear)	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom11-1 (front)	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom12-0 (rear)	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom12-1 (front)	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom13-0 (rear)	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom13-1 (front)	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom14-0 (rear)	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom14-1 (front)	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom15-0 (rear)	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom15-1 (front)	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

J.2 远程存储 DVD 驱动器别名

本节列出了 SPARC M12/M10 系统中远程存储 DVD 驱动器的别名。

J.2.1 SPARC M12-1 远程存储 DVD 驱动器别名

表 J-7 SPARC M12-1 远程存储 DVD 驱动器别名

别名	设备路径
rcdrom	/pci@8100/pci@4/pci@0/pci@8/usb@0/storage@7/disk@0

J.2.2 SPARC M12-2 远程存储 DVD 驱动器别名

对于初始安装时 1-CPU (CMUL) 或 2- CPU 的配置

表 J-8 SPARC M12-2 远程存储 DVD 驱动器别名（初始安装时：单CPU 或 2 个 CPU）

别名	设备路径
rcdrom	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom00	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

J.2.3 SPARC M12-2S 远程存储 DVD 驱动器别名

对于初始安装时 1-CPU (CMUL) 或 2- CPU 的配置

表 J-9 SPARC M12-2S 远程存储 DVD 驱动器别名（初始安装时：单CPU 或 2 个 CPU）

别名	设备路径
rcdrom	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom00	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom01	/pci@8900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom02	/pci@9100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom03	/pci@9900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom04	/pci@a100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

表 J-9 SPARC M12-2S 远程存储 DVD 驱动器别名（初始安装时：单CPU 或 2 个 CPU）(续)

别名	设备路径
rcdrom05	/pci@a900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom06	/pci@b100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom07	/pci@b900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom08	/pci@c100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom09	/pci@c900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom10	/pci@d100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom11	/pci@d900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom12	/pci@e100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom13	/pci@e900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom14	/pci@f100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom15	/pci@f900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

J.2.4 SPARC M10-1 远程存储 DVD 驱动器别名

表 J-10 SPARC M10-1 远程存储 DVD 驱动器别名

别名	设备路径
rcdrom	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3/disk@0

J.2.5 SPARC M10-4 远程存储 DVD 驱动器别名

对于初始安装时 2-CPU (CMUL) 或 4- CPU 的配置

表 J-11 SPARC M10-4 远程存储 DVD 驱动器别名（初始安装时：2 个 CPU 或 4 个 CPU）

别名	设备路径
rcdrom	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom00	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

J.2.6 SPARC M10-4S 远程存储 DVD 驱动器别名

表 J-12 列出了远程存储 DVD 驱动器的别名，其中逻辑系统板 (LSB) 的编号为 0 到 15。

对于初始安装时 2-CPU (CMUL) 或 4- CPU 的配置

表 J-12 SPARC M10-4S 远程存储 DVD 驱动器别名 (初始安装时: 2 个 CPU 或 4 个 CPU)

别名	设备路径
rcdrom	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom00	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom01	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom02	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom03	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom04	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom05	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom06	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom07	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom08	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom09	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom10	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom11	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom12	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom13	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom14	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom15	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

CPU 激活临时许可证

本附录介绍 CPU 激活临时许可证。CPU 激活临时许可证的使用允许在添加和获得足够数量的 CPU 激活之前，使用额外 CPU 内核资源。

- CPU 激活临时许可证是什么？
- CPU 激活临时许可证的使用条款和注意事项
- 相关命令
- 使用 CPU 激活临时许可证的流程和步骤
- CPU 激活临时许可证的事件通知
- 其他重要注意事项

K.1 CPU 激活临时许可证是什么？

CPU 激活是一种 SPARC M12/M10 功能，可允许您对操作进行优化。

通过在 SPARC M12/M10 上注册额外的 CPU 激活密钥，可以动态添加额外的 CPU 内核，而不会中断您的生产工作负荷。此 SPARC M12/M10 功能可使您优化服务器的投资。

但是，购买 CPU 激活的过程可能需要超过一天的时间，而您现在可能就需要额外的 CPU 内核资源。CPU 激活临时许可证的 SPARC M12/M10 功能解决了此问题。

如需启用 CPU 激活临时许可证，您不需要添加 CPU 激活密钥。启用 CPU 激活临时许可证后，物理分区 (PPAR) 或 SPARC M12/M10 中的所有可用物理内核均可使用 30 天。

CPU 激活临时许可证允许您立即使用所需的 CPU 内核资源，即使没有额外购买 CPU 激活密钥。

K.2 CPU 激活临时许可证的使用条款和注意事项

您可以通过执行 XSCF 固件的命令来使用 CPU 激活临时许可证。表 K-1 显示了每个系统使用 CPU 激活临时许可证所需的 XCP 固件版本。必须在您的系统上安装表 K-1 中列出的固件版本才能使用 CPU 激活临时许可证。

表 K-1 CPU 激活临时许可证支持的型号

型号	XCP 版本	使用条款
SPARC M10-1/M10-4 (*1)	XCP 232x	CPU 激活临时许可证在 SPARC M10-1/M10-4 中仅可使用一次。(*2)
	XCP 2330 或更高版本	在某些条件下，CPU 激活临时许可证可以多次使用。(*3)
SPARC M12-1/M12-2/M12-2S/M10-4S	XCP 2330 或更高版本	CPU 激活临时许可证可用于每个 PPAR。 在某些条件下，CPU 激活临时许可证可以多次使用。(*3)

*1 SPARC M10-1 和 SPARC M10-4 支持在 XCP 2320 及更高版本中使用 CPU 激活临时许可证。但是，我们建议您在 XCP 2330 或更高版本中使用 CPU 激活临时许可证，从而允许您在适当的条件下重新启用 CPU 激活临时许可证。

*2 一旦使用了 CPU 激活临时许可证，即使更新到 XCP 2330 或更高版本后，也不能再次使用该功能。

*3 如需多次使用 CPU 激活临时许可证，您必须首先注册额外购买的 CPU 激活密钥，并进行设置以将购买的 CPU 激活添加到物理分区（对于 SPARC M12-2S/M10-4S）或系统（对于 SPARC M12-1/M12-2/M10-1/M10-4）。如果额外购买的 CPU 激活的注册以及将额外的 CPU 内核资源分配给物理分区（对于 SPARC M12-2S/M10-4S）或系统（对于 SPARC M12-1/M12-2/M10-1/M10-4）的设置由于 CPU 激活临时许可证最后一次已启用而尚未被执行，则无法再次启用 CPU 激活临时许可证。有关详情，请参见“多次启用 CPU 激活临时许可证”。

注意事项

- CPU 激活临时许可证可以使用 30 天。请务必在此期间添加所购买的 CPU 激活密钥。在 Oracle VM Server for SPARC 使用的 CPU 内核数等于或大于已安装的所购买 CPU 激活数量时，如果 CPU 激活临时许可证过期，则 Oracle VM Server for SPARC 将自动删除多余的 CPU 内核。
- 启用 CPU 激活临时许可证时，系统（SPARC M12-2S/M10-4S 时为物理分区）中的所有 CPU 内核都被启用。因此，当 CPU 内核发生故障时，CPU 自动更换功能不起作用。
- 某些类型软件的许可证成本根据所使用 CPU 内核数量而各异。通过使用 CPU 激活临时许可证添加 CPU 内核时，请确认软件的许可证条款。

K.3 相关命令

本节介绍与 CPU 激活临时许可证相关的命令。

K.3.1 使用 CPU 激活临时许可证的命令

表 K-2 列出了使用 CPU 激活临时许可证的 XSCF 命令。

表 K-2 用于 CPU 激活临时许可证的 XSCF 命令

使用	命令
启用/禁用 CPU 激活临时许可证	setinterimpermit(8)
显示 CPU 激活临时许可证的设置信息/状态	showinterimpermit(8)
CPU 激活临时许可证的 CPU 内核使用状况	showinterimpermitusage(8) (*1)

*1 XCP 232x 不支持 showinterimpermitusage(8) 命令。

有关各命令的详情，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual》。

K.3.2 使用 CPU 激活临时许可证时的相关命令

以下命令用于管理（注册/删除）所购买的 CPU 激活或显示 CPU 内核的状态。也可在 CPU 激活临时许可证使用期间根据需要使用。

- addcodactivation
- deletecodactivation
- showcodactivation
- setcod
- showcod
- showcodusage
- showcodactivationhistory

这些命令不显示 CPU 激活临时许可证的设置以及启用了 CPU 激活临时许可证时的临时 CPU 内核资源的使用状态。

当启用 CPU 激活临时许可证时，CPU 激活密钥不用于管理 CPU 内核资源（检查是否发生使用冲突）。但是，即使在这种情况下，也可以通过添加或删除 CPU 激活密钥来更改分配给系统的 CPU 内核数，作为 CPU 激活临时许可证到期的准备。

如需检查启用或禁用 CPU 激活临时许可证的时间，请执行 XSCF 的 showlogs event 命令检查 XSCF 事件日志。

K.4 使用 CPU 激活临时许可证的流程和步骤

本节介绍使用 CPU 激活临时许可证的流程和步骤。使用 CPU 激活临时许可证之前，请仔细阅读本节中流程和步骤的说明。

本节还介绍了在启用 CPU 激活临时许可证的情况下使用 CPU 内核时，到期的情况以及禁用 CPU 激活临时许可证的情况。

K.4.1 XCP 2330 及更高版本的流程和步骤

XCP 2330 及更高版本的操作流程

操作流程如下。

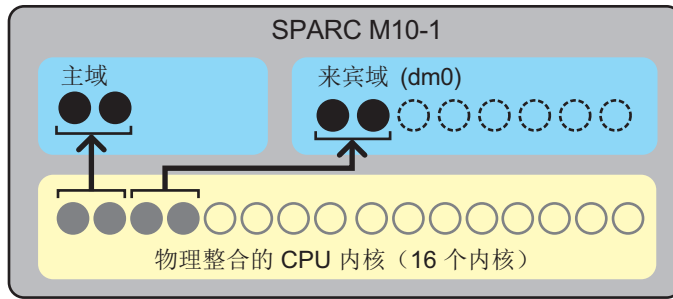
1. 确认是否需要额外的 **CPU** 内核，并启动购买所需 **CPU** 激活的过程。
2. 启用 **CPU** 激活临时许可证。
3. 注册系统获得的 **CPU** 激活密钥。
4. 禁用 **CPU** 激活临时许可证。

配置示例

"[XCP 2330 及更高版本的操作步骤](#)" 中的介绍使用以下配置作为示例。

- 使用具有 16 个物理 CPU 内核的单 CPU 插槽 SPARC M10-1。
- 可激活 4 个 CPU 内核的 CPU 激活已购买并在系统中注册。
- 该系统由两个正在运行的逻辑域组成。
 - 两个 CPU 内核分配给控制域（primary 域）。
 - 两个 CPU 内核分配给来宾域 (dm0)。
- 为了响应负荷增加，来宾域 (dm0) 需要六个以上 CPU 内核。

图 K-1 XCP 2330 或更高版本的配置示例 (SPARC M10-1)



- : 分配给逻辑域的 CPU 内核
- (dashed) : 要分配给逻辑域的 CPU 内核
- (grey) : 通过购买的 CPU 激活密钥启用的 CPU 内核
- (white) : 已物理整合但未通过购买的 CPU 激活密钥启用的 CPU 内核

注 - 系统中注册的 CPU 激活密钥会启用一定数量的 CPU 内核。它们不通过指定 CPU 插槽和每个 CPU 内核的物理位置来启用 CPU 内核。为了易于理解，图 K-1 中启用特定的 CPU 内核并将其分配给逻辑域。

注 - 在 SPARC M12-2S/M10-4S 系统中，对每个 PPAR 启用/禁用 CPU 激活临时许可证。

XCP 2330 及更高版本的操作步骤

操作步骤如下。

1. 确认是否需要额外的 CPU 内核，并启动购买所需 CPU 激活的过程。
在启动购买过程之前，请确认以下内容。
 - a. 根据对 SPARC M12-1/M12-2/M10-1/M10-4 系统时的整个系统或对 SPARC M12-2S/M10-4S 系统时的目标物理分区 (PPAR) 执行的负荷分析或评估，确定是否需要额外的 CPU 内核。
 - b. CPU 激活临时许可证可以使用 30 天。我们建议您提前确认您所在地区收到 CPU 激活密钥需要多少天的时间。有关此信息，请与当地销售代表联系。
2. 启用 CPU 激活临时许可证。
执行以下操作。
 - a. 执行 XSCF 的 `showinterimpermitusage` 命令检查系统 CPU 内核的当前使用情况。

```
XSCF> showinterimpermitusage
```

```
PPAR-ID: 0
```

```

Installed Cores:                16
Purchased Cores Assigned to PPAR: 4
Cores In Use by Ldoms:         4
Interim Assignable Cores:      0
In Use Interim Cores:          0

```

Note:

Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM Server for SPARC ldm command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms" of logical domains.

在 SPARC M12-1/M12-2/M10-1/M10-4 的情况下，仅显示 PPAR-ID 0 的信息。在 SPARC M12-2S/M10-4S 的情况下，显示所有 PPAR 或指定 PPAR 的信息。检查使用 CPU 激活临时许可证的目标 PPAR 的 CPU 内核的使用情况。

表 K-3 列出了使用 showinterimpermitusage 命令所显示的值的含义。

表 K-3 showinterimpermitusage 的含义

列显示	说明	命令示例值的含义
Installed Cores	安装在系统或 PPAR 上的物理 CPU 内核数	"16": 系统有 16 个物理 CPU 内核。
Purchased Cores Assigned to PPAR	已分配给 PPAR 的 CPU 激活的数量	4: 可激活 4 个 CPU 内核的 CPU 激活分配给系统。
Cores In Use by Ldoms	逻辑域中当前使用的 CPU 内核资源的数量	4: 逻辑域中当前使用 4 个 CPU 内核。
Interim Assignable Cores	启用 CPU 激活临时许可证时可用的额外 CPU 内核数	"0": 仍然没有额外的 CPU 内核可用。 参考 - 12: 12 个额外的 CPU 内核已经可用。
In Use Interim Cores	启用 CPU 激活临时许可证时可用的额外 CPU 内核中逻辑域中当前使用的 CPU 内核数	"0": 逻辑域中未使用可用的额外 CPU 内核。

如果 "Purchased Cores Assigned to PPAR" (已分配给 PPAR 的购买的内核) 的数量等于或大于 "Installed Cores" (已安装内核) 的数量，则表明已注册了所有物理并入的 CPU 内核的 CPU 激活密钥。在这种情况下，CPU 激活临时许可证不必需。请勿启用该功能。

- b. 执行 XSCF 的 setinterimpermit 命令启用 CPU 激活临时许可证。
在 SPARC M12-1/M12-2/M10-1/M10-4 的情况下，由 setinterimpermit 命令指定的 PPAR-ID 固定为 0。通过执行此命令，可以使安装在物理分区（固定为 PPAR 0）的 CPU 芯片中的所有 CPU 内核都可用。
在 SPARC M12-2S/M10-4S 系统的情况下，通过指定物理分区 (PPAR) 启用 CPU 激活临时许可证。在这种情况下，构成指定 PPAR 的每个模块化架构 (SPARC M12-2S/M10-4S) 中安装的所有 CPU 芯片中的所有 CPU 内核都可用。

```
XSCF> setinterimpermit -p 0 -c enable
```

Note:

Please add CPU Activation(s) within 30 days of enabling the Interim Permit.

```
The Interim Permit for the PPAR will be changed to enabled.
Continue? [y|n] :y

Completed.
```

- c. 执行 XSCF 的 `showinterimpermitusage` 命令检查通过使用 CPU 激活临时许可证而可用的额外 CPU 内核的数量。

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                16
  Purchased Cores Assigned to PPAR: 4
  Cores In Use by Ldoms:          4
  Interim Assignable Cores:       12
  In Use Interim Cores:           0

Note:
Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
Server for SPARC ldm command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
of logical domains.
```

此示例显示 "Interim Assignable Cores"（临时可分配的内核）为 "12"，这意味着通过启用 CPU 激活临时许可证已经获得 12 个额外的 CPU 内核。在这种情况下，逻辑域中最多可以持续 30 天使用 12 个额外 CPU 内核。

仅将与您计划购买的 CPU 激活的数量相对应的 CPU 内核分配给逻辑域，而不是使用所有可用的额外 CPU 内核。

例如，如果要购买和添加两个 CPU 内核，我们强烈建议仅分配两个额外 CPU 内核给逻辑域。如果将四个 CPU 内核分配给逻辑域，然后购买一个 CPU 激活来仅激活两个额外的 CPU 内核，则总共会减少两个 CPU 内核。禁用 CPU 激活临时许可证后，可能会引起性能问题。

- d. 如果此时执行无选项的 XSCF 的 `showcodusage` 命令，则会显示以下输出。

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-----
PROC          4          16          4 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
-----
0 - PROC          4          16          4 cores
Unused - PROC    0          0          0 cores
```

请注意，如果此时执行 XSCF 的 `showcodusage` 命令，即使通过使用此功能可用 CPU 内核数量已增加，显示内容在启用 CPU 激活临时许可证之前和之后也不会变化。

表 K-4 列出了使用 `showcodusage` 命令所显示的值的含义。

表 K-4 showcodusage 的含义

列显示	说明	命令示例值的含义
In Use	其中的可用 CPU 内核可通过购买的 CPU 激活数量管理的整个系统或每个 PPAR 的逻辑域中目前使用的 CPU 内核数量	"4": 整个系统和 PPAR 0 的逻辑域中当前使用 4 个 CPU 内核。
Installed	安装在整个系统或每个 PPAR 上的物理 CPU 内核数	"16": 整个系统和 PPAR 0 上安装了 16 个物理 CPU 内核。
CoD Permitted	系统中购买和注册的 CPU 激活的数量	4: 可激活 4 个 CPU 内核的 CPU 激活分配给系统。
Status	系统（所有 PPAR）的逻辑域中当前未使用的 CPU 激活的数量（"CoD Permitted" 和 "In Use" 之间的差）	"OK": 从 "CoD Permitted" 的值减去 "In Use" 的值获得的值为 0 或更大，这意味着没有冲突。 参考 - "VIOLATION": 从 "CoD Permitted" 的值减去 "In Use" 的值获得的值小于 0，这意味着发生冲突。
Unused- Assigned	系统（所有 PPAR）的逻辑域中当前未使用的 CPU 激活的数量。负值表示发生冲突的当前使用的 CPU 内核数量。	"0": 当前使用的 CPU 内核与分配给系统（所有 PPAR）的 CPU 激活数相对应。 参考 - "-12": 目前使用的 CPU 内核比已分配的 CPU 激活数多了 12 个 CPU 内核，这意味着发生冲突。

showcodusage 命令用于管理当前在逻辑域中使用的 CPU 内核数量以及已注册（已购买）的 CPU 激活的数量。因此，showcodusage 命令显示的内容不受是否启用/禁用 CPU 激活临时许可证的影响。用于购买和注册的 CPU 激活数量的 "CoD Permitted" 字段和用于逻辑域中使用的 CPU 内核数量的 "In Use" 字段显示它们各自的当前值。

在此示例中，还没有为逻辑域分配额外的 CPU 内核。显示系统中注册的 CPU 激活数量的 "CoD Permitted" 的值为 "4"，显示物理 CPU 内核数量的 "Installed" 的值为 "16"。这意味着 12 个物理 CPU 内核缺少 CPU 激活。但是，由于启用了 CPU 激活临时许可证，12 个 CPU 内核可以使用 30 天。

例如，如果启用 CPU 激活临时许可证时，将 12 个 CPU 内核分配给逻辑域，则 "Status"（状态）将显示 "VIOLATION: 12 cores in excess."（VIOLATION: 12 个内核超出）。在这种情况下，"VIOLATION"（冲突）并不表示紧急状况。此状态警告当 CPU 激活临时许可证过期或被禁用时会发生 CPU 激活冲突。

在 Unused（未使用）行的 Assigned（已分配）字段中，您可以确认系统（所有物理分区 (PPAR)）的逻辑域中相对于购买的 CPU 激活尚未使用的 CPU 内核的数量。在使用中的 CPU 内核发生故障的事件情况下，CPU 自动更换功能会使用这些未使用的 CPU 内核。

- e. 执行 XSCF 的 showinterimpermit 命令确认 CPU 激活临时许可证的状态。以下示例显示 CPU 激活临时许可证已启用，到期前还有 29 天。

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: enabled [29 days remaining]
```

- f. 如需开始在一个或多个逻辑域中使用额外的 CPU 内核，请从控制域（primary 域）执行 ldm add-core 命令。以下示例显示六个 CPU 内核已添加到逻辑域中。

```
# ldm add-core 6 dm0
```

g. 执行 XSCF 的 `showcodusage` 命令。

以下示例显示 "In Use" 的值从 "4" 增加到 "10"，因为逻辑域中添加并使用了六个 CPU 内核。由于 "In Use" 和 "CoD Permitted" 之间的差为六，因此显示 "VIOLATION: 6 cores in excess"（VIOLATION: 6 个内核超出），这意味着六个 CPU 内核暂时发生冲突。如上所述，这个 "VIOLATION"（冲突）并不表示紧急状况。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC      10      16      4 VIOLATION: 6 cores in excess
```

注 - 反映关于逻辑域的 CPU 内核使用情况的信息最多需要 20 分钟。因此，`showcodusage` 命令可能不会显示使用 `ldm` 命令 20 分钟内的结果。

h. 如果需要在更改 CPU 内核分配后立即确认逻辑域中使用的 CPU 内核数，请从控制域执行 `ldm list-permits` 命令。

```
# ldm list-permits CPU CORE
PERMITS (PERMANENT) IN USE REST
16      (16)      10      0
```

i. 如果在所有逻辑域电源关闭时启用了 CPU 激活临时许可证，则将 CPU 内核添加到逻辑域可能不需要 `ldm` 命令。
如果执行 XSCF 的 `showdomainconfig` 命令在 "Booting config" 中显示了 "factory-default"，如下所示，则下次域上电时，所有可用的 CPU 内核将自动用于控制域（primary 域）。这是因为在控制域处于出厂默认模式（显示为 factory-default 模式）的情况下，所有可用的硬件资源都将在电源开启时分配给域。

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :factory-default
(Next)      :factory-default
```

如果 "Booting config" 不是 "factory-default"，则在控制域启动后，执行 `ldm` 命令分配额外的 CPU 内核。执行 `ldm` 命令后，使用 "`ldm add-spconfig`" 命令保存更改后的域配置信息。这样可以确保在域重新启动以后使用最新的逻辑域配置信息。

我们强烈建议使用与当前使用的名称不同的名称作为逻辑域配置名称，如下示例所示。

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :before-IPermit
(Next)      :IPermit-enabled
```

j. 执行 XSCF 的 `showinterimpermitusage` 命令检查 CPU 内核资源的当前使用情况。

```
XSCF> showinterimpermitusage
```

```
PPAR-ID: 0
Installed Cores:                16
Purchased Cores Assigned to PPAR: 4
Cores In Use by Ldoms:         10
Interim Assignable Cores:      12
In Use Interim Cores:          6
```

Note:

```
Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
Server for SPARC ldm command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
of logical domains.
```

此示例显示 "Cores In Use by Ldoms" 显示 "10"，这意味着逻辑域中当前使用的 CPU 内核数量从 4 变为 10。此外，"In Use Interim Cores" 显示 "6"，这意味着目前在逻辑域中额外使用 "Interim Assignable Cores" 中的 12 个可用 CPU 内核中的 6 个。

3. 注册系统获得的 CPU 激活密钥。

执行以下操作。

- a. 在收到新购买的 CPU 激活密钥后，使用 XSCF 中的 `addcodactivation` 命令将其注册到系统中。

```
XSCF> addcodactivation
Product: SPARC M10-1 SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyXTUEFSQy1FbnRlcnByaXNlAA.....
Above Key will be added, Continue?[y|n]: y
XSCF>
```

- b. 使用 `setcod` 命令设置物理分区的 CPU 激活数。

```
XSCF> setcod -p 0 -s cpu -c set 10
PROC Permits assigned for PPAR 1 : 4 -> 10

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y
```



```
Completed.
```

c. 使用 `showcodusage` 命令确认 CPU 内核的状态。

以下示例显示，共有十个 CPU 内核可用，因为已将六个新的 CPU 激活注册并添加到四个 CPU 激活，并对物理分区进行了设置。

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-----
PROC          10         16          10 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
-----
0 - PROC              10          16          10 cores
Unused - PROC         0           0           0 cores
```

d. 执行 XSCF 的 `showinterimpermitusage` 命令检查 CPU 内核资源的当前使用情况。

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                16
  Purchased Cores Assigned to PPAR: 10
  Cores In Use by Ldoms:          10
  Interim Assignable Cores:       6
  In Use Interim Cores:           0

Note:
Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
Server for SPARC ldm command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
of logical domains.
```

您将在步骤 4 中禁用 CPU 激活临时许可证。因此，请仔细确认 "In Use Interim Cores" 为 "0"，这意味着 CPU 激活临时许可证提供的额外 CPU 内核资源不会在逻辑域中使用。

如果 "Cores In Use by Ldoms" 字段中显示的数量大于 "Purchased Cores Assigned to PPAR" 字段中的数量，系统将检测到 CPU 内核冲突。有关在 CPU 激活临时许可证过期或被禁用后检测到冲突时的系统操作的详细信息，请参见 "K.4.3 功能过期或禁用的情况"。

4. 禁用 CPU 激活临时许可证。

执行以下操作。

a. 从 XSCF 执行 `setinterimpermit` 命令禁用 CPU 激活临时许可证。

```
XSCF> setinterimpermit -p 0 -c disable
Interim permit will be disabled.
Continue?[y|n] :y

Completed.
```

b. 执行 `showcodusage` 命令检查 CPU 内核的当前使用情况。

确认 `Status` 字段为 `OK`，这意味着所有使用中的 CPU 内核都允许通过购买的 CPU 激活被使用。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK: 0 cores available
```

c. 执行 XSCF 的 `showinterimpermitusage` 命令检查 CPU 内核资源的当前使用情况。

此示例显示 "Interim Assignable Cores" (临时可分配的内核) 为 "0"，这意味着通过 CPU 激活临时许可证无可用的额外 CPU 内核。

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:          16
  Purchased Cores Assigned to PPAR: 10
  Cores In Use by Ldoms:    10
  Interim Assignable Cores:  0
  In Use Interim Cores:     0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

多次启用 CPU 激活临时许可证

使用 XCP 2330 或更高版本，CPU 激活临时许可证可以多次使用。但是，如需多次启用 CPU 激活临时许可证，必须满足以下所有条件。

条件 1. 即使 CPU 激活临时许可证已启用，也将其禁用。(setinterimpermit(8))

条件 2. 将额外购买的 CPU 激活密钥注册到系统。(addcodactivation(8))

条件 3. 分配要添加到物理分区 (PPAR) 的 CPU 内核资源。(setcod(8))

如果由于启用了最后一次的 CPU 激活临时许可证而尚未执行额外 CPU 激活的注册和 PPAR 的添加设置，则不能再次启用 CPU 激活临时许可证。

注 - 此外，即使满足上述条件 2 和 3，30 天的有效期也不会延长。此处禁用一次 CPU 激活临时许可证。

通过执行 `showinterimpermit-v` 命令可以确认这些条件，如下所述。

- (1) 如果当前启用了 CPU 激活临时许可证，则需要执行 `setinterimpermit(8)` 将其禁用。执行完毕后，由执行 `showinterimpermit-v` 命令显示的 "Status" (状态) 将被更改为 "Interim Permit cannot be enabled again (until more Purchased CPU Activations are installed and Purchased cores are assigned to the PPAR)" (临时

许可证无法再次启用（直到安装了更多购买的 CPU 激活并且将购买的内核分配给 PPAR）。

- (2) 必须增加注册在系统中的购买的 CPU 激活密钥的数量。可以通过执行 `addcodactivation(8)` 命令增加。
通过执行 `showinterimpermit-v` 命令显示的 "Current CPU Activation Information"（当前 CPU 激活信息）的 "Registered CPU Activation Keys (in units of cores)"（注册的 CPU 激活密钥（以内核为单位））的值必须大于 "CPU Activation Information from the last time Interim Permit was enabled"（最后一次临时许可证启用时 CPU 激活信息）的 "Registered CPU Activation Keys (in units of cores)"（注册的 CPU 激活密钥（以内核为单位））的值。
- (3) 必须增加您想要重新启用 CPU 激活临时许可证的 PPAR（适用于 SPARC M12-2S/M10-4S 系统）/系统（适用于 SPARC M12-1/M12-2/M10-1/M10-4 系统）的 CPU 内核资源的数量。可以通过执行 `setcod(8)` 命令增加。
通过执行 `showinterimpermit-v` 命令显示的 "Current CPU Activation Information"（当前 CPU 激活信息）的 "Purchased Cores Assigned to PPAR"（购买的分配给 PPAR 的内核）的值必须大于 "CPU Activation Information from the last time the Interim Permit was enabled"（最后一次临时许可证启用时 CPU 激活信息）的 "Purchased Cores Assigned to PPAR"（购买的分配给 PPAR 的内核）的值。

以下示例显示，"Current CPU Activation Information"（当前 CPU 激活信息）的 "Registered CPU Activation Keys (in units of cores)"（注册的 CPU 激活密钥（以内核为单位））的值增加了 16 个，"Current CPU Activation Information"（当前 CPU 激活信息）的 "Purchased Cores Assigned to PPAR"（购买的分配给 PPAR 的内核）的值增加了 8 个，因此显示 "can be enabled"（可以启用）。这意味着可以重新使用 CPU 激活临时许可证。

```
XSCF> showinterimpermit -v -p 0
PPAR-ID: 0
  Status: Interim Permit is disabled (can be enabled)

CPU Activation Information from the last time Interim Permit was enabled:
  Registered CPU Activation Keys (in units of cores): 16
  Purchased Cores Assigned to PPAR: 8

Current CPU Activation Information:
  Registered CPU Activation Keys (in units of cores): 32
  Purchased Cores Assigned to PPAR: 16
```

如需重新使用 CPU 激活临时许可证，需注册额外的 CPU 激活，并执行 [XCP 2330 及更高版本的操作步骤](#) 中的步骤 3 中所述的相同操作将其添加到 PPAR。

然后，执行 "[XCP 2330 及更高版本的操作步骤](#)" 中的步骤 2 中所述的相同操作启用 CPU 激活临时许可证。

K.4.2 XCP 232x的流程和步骤

使用 XCP 232x版本时，CPU 激活临时许可证只能用于 SPARC M10-1/M10-4 系统。

XCP 232x 的操作流程

操作流程如下。

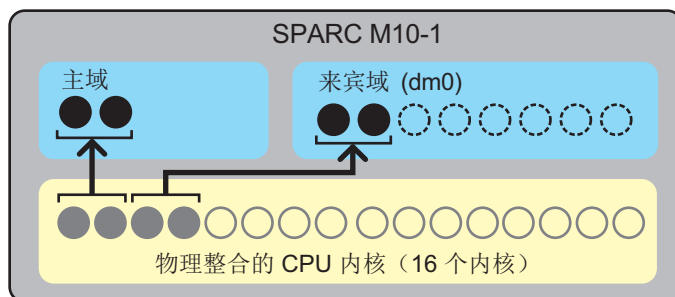
1. 确认需要额外的 **CPU** 内核，并启动购买所需的 **CPU** 激活密钥的过程。
2. 启用 **CPU** 激活临时许可证。
3. 注册系统获得的 **CPU** 激活密钥。
4. 禁用 **CPU** 激活临时许可证。

配置示例

"XCP 232x 的操作步骤" 中的介绍使用以下配置作为示例。

- 使用具有 16 个物理 CPU 内核的单 CPU 插槽 SPARC M10-1。
- 可激活 4 个 CPU 内核的 CPU 激活已购买并在系统中注册。
- 该系统由两个正在运行的逻辑域组成。
 - 两个 CPU 内核分配给控制域（primary 域）。
 - 两个 CPU 内核分配给来宾域（dm0）。
 - 为了响应负荷增加，来宾域（dm0）需要六个以上 CPU 内核。

图 K-2 XCP 232x 的配置示例 (SPARC M10-1)



- : 分配给逻辑域的 CPU 内核
- (虚线) : 要分配给逻辑域的 CPU 内核
- (灰) : 通过购买的 CPU 激活密钥启用的 CPU 内核
- (白) : 已物理整合但未通过购买的 CPU 激活密钥启用的 CPU 内核

注 - 系统中注册的 CPU 激活密钥会启用一定数量的 CPU 内核。它们不通过指定 CPU 插槽和每个 CPU 内核的物理位置来启用 CPU 内核。为了易于理解，图 K-2 中启用特定的 CPU 内核并将其分配给逻辑域。

XCP 232x 的操作步骤

操作步骤如下。

1. 确认需要额外的 CPU 内核，并启动购买所需的 CPU 激活密钥的过程。
在启动购买过程之前，请确认以下内容。
 - a. 根据对系统执行的负荷分析或评估，确定是否需要额外的 CPU 内核。
 - b. CPU 激活临时许可证可以使用 30 天。我们建议您提前确认您所在地区收到 CPU 激活密钥需要多少天的时间。有关此信息，请与当地销售代表联系。
2. 启用 CPU 激活临时许可证。
执行以下操作。
 - a. 执行 XSCF 的 showcodusage 命令检查系统 CPU 内核的当前使用情况。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          4          16          4 OK: 0 cores available
```

表 K-5 列出了使用 showcodusage 命令所显示的值的含义。

表 K-5 showcodusage 的含义

列显示	说明	命令示例值的含义
In Use	其中的可用 CPU 内核可通过购买的 CPU 激活数量管理的整个系统的逻辑域中目前使用的 CPU 内核数量	"4": 整个系统的逻辑域中当前使用 4 个 CPU 内核。
Installed	安装在整个系统上的物理 CPU 内核数	"16": 整个系统上安装了 16 个物理 CPU 内核。
CoD Permitted	系统中购买和注册的 CPU 激活的数量	4: 可激活 4 个 CPU 内核的 CPU 激活分配给系统。
Status	系统的逻辑域中当前未使用的 CPU 激活的数量 ("CoD Permitted" 和 "In Use" 之间的差)	"OK": 从 "CoD Permitted" 的值减去 "In Use" 的值获得的值为 0 或更大，这意味着没有冲突。 参考 - "VIOLATION": 从 "CoD Permitted" 的值减去 "In Use" 的值获得的值小于 0，这意味着发生冲突。
Unused- Assigned	系统的逻辑域中当前未使用的 CPU 激活的数量。负值表示发生冲突的当前使用的 CPU 内核数量。	"0": 当前使用的 CPU 内核与分配给系统的 CPU 激活数相对应。 参考 - "-12": 目前使用的 CPU 内核比已分配的 CPU 激活数多了 12 个 CPU 内核，这意味着发生冲突。

如果 "Installed" 的值等于 "CoD Permitted" 的值，则表明已注册了所有物理并入的 CPU 内核的 CPU 激活密钥。在这种情况下，CPU 激活临时许可证不必需。请勿启用该功能。

- b. 执行 XSCF 的 setinterimpermit 命令启用 CPU 激活临时许可证。通过执行此命

令，可以使安装在系统上的 CPU 芯片中的所有 CPU 内核都可用。

```
XSCF> setinterimpermit -p 0 -c enable
Note:
  Interim Permit can be used only once.
  Please add CPU activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue?[y|n] :y

Completed.
```

c. 执行 XSCF 的 showcodusage 命令检查可用的额外 CPU 内核的数量。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          4          16          4 OK: 0 cores available
```

此示例显示 "Installed" (已安装) 为 "16"。启用 CPU 激活临时许可证之前和之后，此值没有改变。但是，它显示通过启用 CPU 激活临时许可证已经提供 12 个额外的 CPU 内核。在这种情况下，最多 12 个额外 CPU 内核可以在逻辑域 (dm0) 中使用 30 天。

仅将与您计划购买的 CPU 激活的数量相对应的 CPU 内核分配给逻辑域，而不是使用所有可用的额外 CPU 内核。

例如，如果要购买和添加两个 CPU 内核，我们强烈建议仅分配两个额外 CPU 内核给逻辑域。如果将四个 CPU 内核分配给逻辑域，然后购买一个 CPU 激活来仅激活两个额外的 CPU 内核，则总共会减少两个 CPU 内核。禁用 CPU 激活临时许可证后，可能会引起性能问题。

d. 如果此时执行无选项的 XSCF 的 showcodusage 命令，则会显示以下输出。

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-----
PROC          4          16          4 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
-----
0 - PROC          4          16          4 cores
Unused - PROC          0          0          0 cores
```

请注意，如果此时执行 XSCF 的 showcodusage 命令，即使通过使用此功能可用 CPU 内核数量已增加，显示内容在启用 CPU 激活临时许可证之前和之后也不会变化。

showcodusage 命令用于管理当前在逻辑域中使用的 CPU 内核数量以及已注册 (已购买) 的 CPU 激活的数量。因此，showcodusage 命令显示的内容不受是否启用/禁用 CPU 激活临时许可证的影响。用于购买和注册的 CPU 激活数量的 "CoD Permitted" 字段和用于逻辑域中使用的 CPU 内核数量的 "In Use" 字段显示它们各自的当前值。

在此示例中，还没有为逻辑域分配额外的 CPU 内核。显示系统中注册的 CPU 激活数量的 "CoD Permitted" 的值为 "4"，显示物理 CPU 内核数量的 "Installed" 的值为 "16"。这意味着 12 个物理 CPU 内核缺少 CPU 激活。但是，由于启用了 CPU 激活临时许可证，12 个 CPU 内核可以使用 30 天。

例如，如果启用 CPU 激活临时许可证时，将 12 个 CPU 内核分配给逻辑域，则 Status（状态）将显示 VIOLATION: 12 cores in excess.（VIOLATION: 12 个内核超出）。在这种情况下，"VIOLATION"（冲突）并不表示紧急状况。此状态警告当 CPU 激活临时许可证过期或被禁用时会发生 CPU 激活冲突。

在 "Unused"（未使用）行的 "Assigned"（已分配）字段中，您可以确认系统的逻辑域中相对于购买的 CPU 激活尚未使用的 CPU 内核的数量。在使用中的 CPU 内核发生故障的事件情况下，CPU 自动更换功能会使用这些未使用的 CPU 内核。

- e. 执行 XSCF 的 `showinterimpermit` 命令确认 CPU 激活临时许可证的状态。以下示例显示 CPU 激活临时许可证已启用，到期前还有 29 天。

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: enabled [29 days remaining]
```

- f. 如需开始在一个或多个逻辑域中使用额外的 CPU 内核，请从控制域（`primary` 域）执行 `ldm add-core` 命令。以下示例显示六个 CPU 内核已添加到逻辑域中。

```
# ldm add-core 6 dm0
```

- g. 执行 XSCF 的 `showcodusage` 命令。
以下示例显示 "In Use" 的值从 "4" 增加到 "10"，因为逻辑域中添加并使用了六个 CPU 内核。由于 "In Use" 和 "CoD Permitted" 之间的差为六，因此显示 "VIOLATION: 6 cores in excess"（VIOLATION: 6 个内核超出），这意味着六个 CPU 内核暂时发生冲突。如上所述，这个 "VIOLATION"（冲突）并不表示紧急状况。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          4 VIOLATION: 6 cores in excess
```

注 - 反映关于逻辑域的 CPU 内核使用情况的信息最多需要 20 分钟。因此，`showcodusage` 命令可能不会显示使用 `ldm` 命令 20 分钟内的结果。

- h. 如果需要在更改 CPU 内核分配后立即确认逻辑域中使用的 CPU 内核数，请从控制域执行 `ldm list-permits` 命令。

```
# ldm list-permits
```

- i. 如果在所有逻辑域电源关闭时启用了 CPU 激活临时许可证，则将 CPU 内核添加到逻辑域可能不需要 `ldm` 命令。

如果执行 XSCF 的 `showdomainconfig` 命令在 "Booting config" 中显示了 "factory-default"，如下所示，则下次域上电时，所有可用的 CPU 内核将自动用于控制域（primary 域）。这是因为在控制域（"factory-default"（出厂默认））的情况下，所有可用的硬件资源都将在电源开启时分配给域。

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :factory-default
(Next)      :factory-default
```

如果 "Booting config" 不是 "factory-default"，则在控制域启动后，执行 `ldm` 命令分配额外的 CPU 内核。执行 `ldm` 命令后，使用 "`ldm add-spconfig`" 命令保存更改后的域配置信息。这样可以确保在域重新启动以后使用最新的逻辑域配置信息。

我们强烈建议使用与当前使用的名称不同的名称作为逻辑域配置名称，如下示例所示。

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :before-IPermit
(Next)      :IPermit-enabled
```

3. 注册系统获得的 CPU 激活密钥。

执行以下操作。

- a. 在收到新购买的 CPU 激活后，使用 XSCF 中的 `addcodactivation` 命令将其注册到系统中。

```
XSCF> addcodactivation
Product: SPARC M10-1 SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA.....
Above Key will be added, Continue?[y|n]: y
XSCF>
```

- b. 使用 `setcod` 命令设置物理分区的 CPU 激活数。

```
XSCF> setcod -p 0 -s cpu -c set 10
PROC Permits assigned for PPAR 1 : 4 -> 10

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

- c. 使用 `showcodusage` 命令确认 CPU 内核的状态。

以下示例显示，共有十个 CPU 内核可用，因为已将六个新的 CPU 激活注册并添加到四个 CPU 激活，并对物理分区进行了设置。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK: 0 cores available
```

d. 您将在步骤 4 中禁用 CPU 激活临时许可证。因此，请仔细检查在 "CoD Permitted" 中显示的所需要的 CPU 内核数。"In Use" 字段中显示的数量必须等于或小于域运行时的 "CoD Permitted" 字段中的数量。

如果 "In Use" 字段中显示的数量大于 "CoD Permitted" 字段中的数量，系统将检测到 CPU 内核冲突。有关在 CPU 激活临时许可证过期或被禁用后检测到冲突时的系统操作详情，请参见 "K.4.3 功能过期或禁用的情况"。

4. 禁用 CPU 激活临时许可证。

执行以下操作。

a. 从 XSCF 执行 `setinterimpermit` 命令禁用 CPU 激活临时许可证。

```
XSCF> setinterimpermit -p 0 -c disable
Interim permit will be disabled.
Continue?[y|n] :y

Completed.
```

b. 执行 `showcodusage` 命令检查 CPU 内核的当前使用情况。

确认 Status 字段为 OK，这意味着所有使用中的 CPU 内核都允许通过购买的 CPU 激活被使用。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK: 0 cores available
```

K.4.3 功能过期或禁用的情况

本节介绍 CPU 激活临时许可证过期或禁用时要执行的系统操作和应对措施。

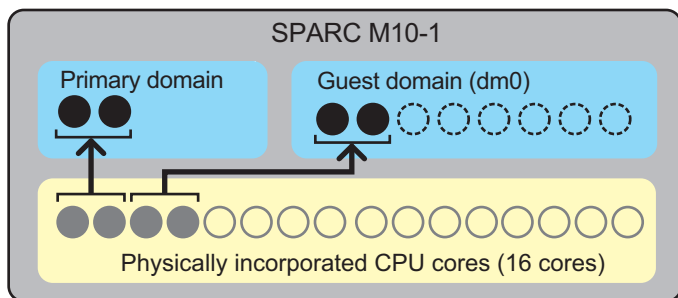
配置示例

此处的介绍使用以下配置作为示例。

- 使用具有 16 个物理 CPU 内核的单 CPU 插槽 SPARC M10-1。
- 可激活 4 个 CPU 内核的 CPU 激活已购买并在系统中注册。
- 该系统由两个正在运行的逻辑域组成。
 - 两个 CPU 内核分配给控制域 (primary 域)。
 - 两个 CPU 内核分配给来宾域 (dm0)。

- 为了响应负荷增加，来宾域 (dm0) 需要六个以上 CPU 内核。
- CPU 激活临时许可证已启用，并且已将六个额外 CPU 内核分配给来宾域 (dm0) 作为临时操作。

图 K-3 功能过期或禁用情况下的配置示例 (SPARC M10-1)



- : CPU core assigned to the logical domain
- (dashed) : CPU core to be assigned to the logical domain
- (gray) : CPU core enabled by a purchased CPU Activation key
- (white) : CPU core physically incorporated but not enabled by a purchased CPU Activation key

注 - 系统中注册的 CPU 激活密钥会启用一定数量的 CPU 内核。它们不通过指定 CPU 插槽和每个 CPU 内核的物理位置来启用 CPU 内核。为了易于理解，图 K-3 中启用特定的 CPU 内核并将其分配给逻辑域。

系统操作和应对措施

无论是否在系统中注册了额外 CPU 激活密钥，CPU 激活临时许可证都将在 30 天后过期。此外，CPU 激活临时许可证可能由于 XSCF 的 `setinterimpermit` 命令而无意中被禁用。一旦禁用了 CPU 激活临时许可证，XCP 232x 版本时就无法再次启用。即使使用 XCP 2330 和更高版本，该功能也无法立即再次启用。

在任何 CPU 内核处于使用冲突状态 "VIOLATION" 时，如果 CPU 激活临时许可证过期或禁用，系统将以下述方式操作。

- 冲突后经历 30 分钟时，会发送给系统一条尝试从逻辑域中删除过多 CPU 内核的通知。
- 冲突后经历 60 分钟时，系统会尝试关闭控制域。
- 冲突后经历 90 分钟时，系统会尝试关闭所有域。

如果在检测到冲突后 30 分钟内执行以下任一操作，系统将不执行上述 a. 至 c. 的操作。

- 减少逻辑域中当前使用的 CPU 内核数
- 通过使用 XSCF 的 `addcodactivation` 命令注册额外购买的 CPU 激活密钥，然后

使用 `setcod` 命令将 CPU 激活数量添加到物理分区。

如果 CPU 激活临时许可证过期，并执行了 XSCF 的 `showinterimpermit` 命令，则将显示 "expired"（过期），如以下示例所示。

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: expired
```

如果 CPU 激活临时许可证过期或禁用，并且您执行 XSCF 的 `showcodusage` 命令，则将显示 CPU 内核的使用情况，如以下示例所示。

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          4 VIOLATION: 6 cores in excess
```

在这种情况下，由于 CPU 激活临时许可证已过期，"Status"（状态）字段中显示 "VIOLATION"（冲突）。此示例显示六个 CPU 内核使用时出现冲突，这实际上警告系统处于紧急情况。在此示例这种情况中，您必须立即总共删除逻辑域中的六个 CPU 内核。

检测到冲突后，系统将尝试从逻辑域中删除 CPU 内核，直到使用的 CPU 内核数量与购买和注册的 CPU 激活密钥的数量相匹配。在此示例中将删除六个 CPU 内核。

系统将从具有最高 CPUID (CID) 值的 CPU 内核开始删除。由于某些原因（例如属于 CPU 内核的 `vcpu` 通过 `pbind` 与特定进程相关联），系统可能无法删除 CPU 内核。在这种情况下，将删除第二个具有高 CID 值的 CPU 内核。

您可以使用 Oracle Solaris 的 `ldm` 命令检查 CID 值，如下所示。

```
# ldm list-domain -o core
NAME
primary
CORE
  CID    CPUSSET
  0      (0, 1)
  4      (8, 9)
-----
NAME
dm0
CORE
  CID    CPUSSET
  8      (16, 17)
  12     (24, 25)
<略>
```

在 CPU 内核数等于或小于购买的 CPU 激活密钥允许使用的 CPU 内核数之后，将不执行上述操作。

如上所述，删除 CPU 内核可能会失败。当 `vcpu` 通过 `pbind` 或以其他方式与特定进程相关联时，或者当要删除的 CPU 内核是逻辑域中的最后一个内核时，会发生删除失败。如果系统无法删除足够的 CPU 内核（本例中为六个 CPU 内核），则将关闭控制域。

如需从上述情况中恢复，请执行以下任一操作。

- 使用 `ldm` 命令删除逻辑域中足够的 CPU 内核，或停止一个或多个逻辑域。
- 使用 XSCF 的 `addcodactivation` 命令注册足够数量的购买的 CPU 激活密钥，然后使用 `setcod` 命令将该数量的 CPU 激活添加到物理分区。

如果由于控制域关闭而无法删除足够的 CPU 内核，则所有逻辑域将被关闭。

如果所有逻辑域都被关闭，可能的恢复方法如下。

- 在启用 CPU 激活临时许可证之前，选择所保存的逻辑域的配置信息文件。使用 XSCF 的 `setdomainconfig` 命令选择逻辑域的旧配置信息文件，如下所示。然后，启动系统。

```
XSCF> setdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :IPermit-enabled
(Next)      :IPermit-enabled
-----
Index       :1
config_name :factory-default
domains     :1
date_created:-
-----
Index       :2
config_name :before-IPermit
domains     :2
date_created:"2015-03-24 19:21:30"
-----
Index       :3
config_name :IPermit-enabled
domains     :2
date_created:"2016-06-16 12:00:30"
Select Index of Using config_name : 2
PPAR-ID of PPARs that will be affected :00
Logical domain config_name will be set to "before-IPermit".
Continue?[y|n] :y
```

- 如果您的目的是恢复控制域，则只需启动控制域，然后删除控制域中必要数量的 CPU 内核资源。

注 - 即使控制域中使用的 CPU 内核数量大于购买的 CPU 激活密钥允许使用的 CPU 内核数量，控制域也始终正常启动。即使 CPU 激活临时许可证已过期或已禁用，也会这样。但是，如果在检测到冲突后 30 分钟内无法删除足够的 CPU 内核，系统将根据上述步骤再次开始自动删除 CPU 内核。成功删除 CPU 内核资源后，使用 `ldm add-spconfig` 命令保存已更正的逻辑域配置信息，以便以后在控制域重新启动时使用。

- 如果您的目的是恢复特定的来宾域，请执行以下步骤。
 - 仅启动控制域。
 - 删除控制域中分配给来宾域的 CPU 内核，并使用 `ldm add-spconfig` 命令保存已更正的逻辑域配置信息。
 - 启动来宾域。

- d. 使用 XSCF 的 `addcodactivation` 命令注册额外购买的 CPU 激活密钥，并使用 `setcod` 命令将该数量的 CPU 激活添加到物理分区。

如果您需要恢复控制域和来宾域，但不使用逻辑域的旧配置信息文件，则上述操作 b. 和 c. 可能都需要。

K.5 CPU 激活临时许可证的事件通知

本节介绍与 CPU 激活临时许可证相关的事件通知。

K.5.1 通知的类型

以下是与 CPU 激活临时许可证相关的四种类型的事件通知。

- a. XSCF 事件日志
使用 XSCF 的 `showlogs event` 命令查阅的事件日志
- b. 域控制台的消息（在 XCP 2330 或更高版本的情况下）
在 `syslog` 中注册并显示在 `primary` 域控制台上的消息
- c. 电子邮件
XSCF 的电子邮件通知功能如果启用时所发送的电子邮件（请参见 ["10.2 故障发生时通过电子邮件接收通知"](#)。）
- d. SNMP 陷阱
如果系统由 XSCF 的 SNMP 代理功能监视所接收到的 SNMP 陷阱（请参见 ["10.3 通过 SNMP 代理监控/管理系统状态"](#)。）

K.5.2 通知示例

在 CPU 激活临时许可证到期之前 14 天开始，每 4 个小时发送一次通知，直到 CPU 激活临时许可证禁用或过期。每个事件的通知均采用以下格式: PPAR-ID 0: Interim Permit due to expire in 14 days（临时许可证 14 天内到期）。

一旦 CPU 激活临时许可证过期，将发送通知。每个事件的通知均采用以下格式: PPAR-ID 0: Interim Permit has expired（临时许可证已过期）。

CPU 激活临时许可证过期或禁用后，发生 CPU 内核使用冲突时，将发送通知。每个事件的通知均采用以下格式: PPAR-ID 0: CoD PROC violation occurred（发生 CoD PROC 冲突）。

此外，当 CPU 内核使用冲突问题解决时，将发送通知。每个事件的通知均采用以下格式: PPAR-ID 0: CoD PROC violation resolved（CoD PROC 冲突已解决）。

以下是事件通知的示例。

此处的说明使用 CPU 激活临时许可证到期 14 天之前的事件示例。

示例 1.XSCF 事件日志

```
XSCF> showlogs event
May 23 18:11:51 JST 2016      PPAR-ID 0: Interim Permit due to expire in 14
days
```

示例 2. 主域控制台上的 syslog 消息（对于 XCP 2330 及更高版本）

■ 消息示例

```
PPAR-ID 0: Interim Permit due to expire in 14 days
```

■ syslog 日志示例

```
Jul 22 01:10:45 4S-441-D0 SC Alert: [ID 695932 daemon.notice]
PPAR-ID 0: Interim Permit due to expire in 14 days
```

示例 3.电子邮件

```
From no-reply@xxxx Mon May 23 18:11:51 2016
Date: Mon, 23 May 2016 18:11:51 +0900
From: no-reply@xxxx
Message-Id: <1463994711.2429@xxxx>
To: administrator@m10.org
Subject: Event: M10-1: M10-1: serial# TZ01111111, PPAR-ID 0: Interim Permit
due to expire in 14 days
Content-Length: 200

TYPE: Event, VER: XCP-2320
MODE-SWITCH: Service
SEVERITY: Event
EVENT-TIME: 05-23-2016 18:11:51 JST
CSN: TZ01111111
SERVER-ID: xxxx
FRU: -
DIAGCODE: -
MSG: PPAR-ID 0: Interim Permit due to expire in 14 days
```

示例 4.SNMP 陷阱

发送了 SNMP 陷阱 OID 1.3.6.1.4.1.211.1.15.4.1.2.0.5。此陷阱包含 .1.3.6.1.4.1.211.1.15.4.1.2.1.1.0 (scfTrapEventType.0)，它是一个指示事件类型的数值对象。

有关 OID 的详情，请参见《Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists》。

K.6 其他重要注意事项

本节介绍使用 CPU 激活临时许可证的注意事项。

K.6.1 PPAR DR 和 CPU 激活临时许可证

CPU 激活临时许可证可以与物理分区动态重新配置 (PPAR DR) 同时使用。

注 - 当使用 `addboard` 或 `deleteboard` 命令执行 PPAR DR 时，更改 CPU 激活临时许可证的模式将失败。换言之，`setinterimpermit` 命令和 `addboard/deleteboard` 命令之间的冲突将导致任一命令失败。

例如，假设您要使用 PPAR DR 将 BB#4 添加到启用了 CPU 激活临时许可证的 PPAR。在这种情况下，当完成 PPAR DR 的添加过程时，搭载在 BB#4 上的所有 CPU 芯片中的所有 CPU 内核都可用。

但是，如果此 PPAR 的逻辑域配置“不”是 `factory-default`（出厂默认），则需要使用 Oracle Solaris 的 `Idm` 命令将添加的 CPU 内核并入到逻辑域中。

相反，假设您要使用 PPAR DR 将 BB#4 从启用了 CPU 激活临时许可证的 PPAR 删除。在这种情况下，搭载在 BB#4 上的所有 CPU 芯片中的所有 CPU 内核都将作为 PPAR DR 删除过程的一部分从 PPAR 中自动删除。因此，必须事先从逻辑域中删除 CPU 内核资源，然后再从 PPAR 中将其删除。

K.6.2 尝试再次使用 CPU 激活临时许可证时（仅适用于 XCP 232x）

如果您尝试使用 XSCF 的 `setinterimpermit` 命令为已使用过 CPU 激活临时许可证功能的系统再次启用 CPU 激活临时许可证，则该命令将失败。

以下示例显示了命令失败的情况。

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: disabled
XSCF> setinterimpermit -p 0 -c enable
Note:
  Interim Permit can be used only once.
  Please add CPU activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue?[y|n] :y

The Interim Permit cannot be enabled because it has already been used once.
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: disabled
```

如果使用了 XCP 232x，这不是缺陷，因为每个系统只能启用一次 CPU 激活临时许可证。

如果以下所有项目都适用于您，请联系当地的销售代表。

- 您对安装了 XCP 232x 的系统使用了 CPU 激活临时许可证。
- 然后，将固件更新为 XCP 2330 或更高版本。
- 您购买了额外 CPU 激活密钥，将其注册在系统中，并将 CPU 内核资源分配给 PPAR。
- 您想再次使用 CPU 激活临时许可证。

K.6.3 移动 CPU 激活密钥（删除/移动）

当 CPU 激活临时许可证启用时，将一个或多个购买的 CPU 激活密钥从一个 SPARC M12/M10 移动（删除和移动）到另一个 SPARC M12/M10 不会影响移动过程。

使用 XSCF 的 `deletecodactivation` 命令进行删除，使用 `addcodactivation` 命令进行添加。

在使用 `deletecodactivation` 命令从 SPARC M12/M10 中删除 CPU 激活密钥之前，请务必使用 `showcodactivation` 命令将 CPU 激活密钥外部保存为文本文件等。

可以使用 `addcodactivation` 命令将保存的 CPU 激活密钥添加到其他 SPARC M12/M10。

CPU 激活临时许可证不受 CPU 激活移动过程的影响。但是请注意，在未启用 CPU 激活临时许可证的系统中，执行移动过程之后，所使用的 CPU 内核数量不得超过已购买的 CPU 激活数量。

CPU 激活临时许可证启用时，可以删除系统中的所有购买的 CPU 激活密钥，即使删除后，系统仍可继续运行。但是，一旦 CPU 激活临时许可证被禁用或过期，系统将不会运行，直到在系统中注册购买的 CPU 激活密钥。

K.6.4 Idm 命令的输出

如果在启用 CPU 激活临时许可证时使用 Oracle Solaris 的 `Idm` 命令，则对于额外的可用 CPU 内核，即使它们实际上不是永久性的，也会显示 "PERMANENT"（永久）。

例如，假设 SPARC M12/M10 的 `primary` 域中有四个 CPU 内核，并且通过所购买的 CPU 激活密钥允许对其进行使用。启用 CPU 激活临时许可证时执行 "`Idm list-domain -l`" 会显示以下信息。

```
# Idm list-domain -l
NAME                STATE      FLAGS    CONS    VCPU    MEMORY    UTIL    NORM    UPTIME
primary             active    -n-c--  UART     8      63744M    0.0%   0.0%   16d 21h
 6m
<略>
CPU CORE
PERMITS (PERMANENT)  IN USE    REST
16      (16)     16       0
<略>
```


实际上，仅四个 CPU 内核是永久可用的（即，通过购买的 CPU 激活密钥可用）。但是，当 CPU 激活临时许可证启用时，物理整合的所有 16 个 CPU 内核在该命令的输出中都会显示为永久性的内核。

索引

A

Active Directory, XSCF 用户帐户, 管理, 67
按顺序关闭, 257

B

保存/恢复 OpenBoot PROM 环境变量, 324
崩溃转储文件, 333
标准 MIB, 295, 559
不间断电源, 411

C

菜单配置, 535
操作模式, 376
操作模式, 切换, 375
磁盘槽, 527
CPU 插槽约束条件, 269
CPU 激活, 209
CPU 激活临时许可证, 611, 612, 614
CPU 激活临时许可证, 事件通知, 633
CPU 激活临时许可证, 相关命令, 613
CPU 激活临时许可证, 注意事项, 635
CPU 激活密钥, 210
CPU 激活密钥, 保存, 224
CPU 激活密钥, 恢复, 224
CPU 激活信息, 221, 258
CPU 激活异常, 225
CPU 激活支持, 563
CPU 激活, 重要注意事项, 226
CPU 内核资源, 删除, 217

CPU 内核资源, 添加, 212
CPU 内核资源, 移动, 219
CPU 运行模式, 240

D

登录, 25
登录 (XSCF shell), 33
登录 (XSCF Web), 37
电子邮件通知功能, 288
动态重新配置策略, 276
DVD 驱动器别名, 601
DVD 驱动器, 连接, 170

F

发生故障的资源, 检查, 564
FAQ, 481
FCode 实用程序, 381
维护模式, 375
服务器, 恢复出厂默认状态, 331

G

功耗, 163
固件版本匹配, 468
固件更新, 441, 444, 447, 462, 473
固件更新, 故障, 472
固件, 更新, 448
故障的 CPU, 自动更换, 564
故障的硬件资源, 查看, 310
故障排除, 477
管理程序转储, 266, 564

管理程序转储文件, 266

H

HTTPS 服务, 117

恢复模式, 设置, 314

I

iSCSI, 使用, 402

J

降级机制, 310

接管 IP 地址, 124, 133

警告和通知信息, 检查, 370

卷设备名, 指定, 方法, 599

K

可用页面, 539

控制台, 切换, 253, 254

扩展 MIB, 295, 559

L

LDAP 服务, 使用, 401

LDAP over SSL, XSCF 用户帐户, 管理, 83

LDAP, XSCF 用户帐户, 管理, 62

逻辑域, 3

逻辑域配置信息, 保存 (XML), 321

逻辑域配置信息, 保存 (XSCF), 318

逻辑域配置信息, 恢复 (XML), 321

逻辑域配置信息, 恢复 (XSCF), 318

逻辑域时间, 265

逻辑域, 崩溃, 329

逻辑域, 重启, 328

逻辑域, 关闭, 256

逻辑域, 关闭, 563

逻辑域, 控制, 251

逻辑域, 配置, 251

逻辑域, 配置更改, 265

逻辑域, 启动, 255

逻辑域, 最大页面大小, 280

M

密码, 52

MIB 定义文件, 295

MIB 对象标识, 557

目标 ID, 指定, 方法, 597

N

内存镜像, 配置, 379

内存配置, 更改, 431

内置存储器, 设备路径, 595

O

OpenBoot PROM, 23

OpenBoot PROM 环境变量, 591

OpenBoot PROM 环境变量, 设置, 259

OpenBoot PROM 命令, 592

Oracle Solaris 内核区, 252

Oracle VM Server for SPARC, 22

P

PCI 扩展单元, 435

PCIe 端点设备, 432

PHY 编号, 指定, 方法, 596

PPAR DR 策略, 如何变更, 279

probe-scsi-all 命令, 524

Q

启动等待时间, 160

启动设备, 指定, 595

全球通用名称 (WWN) 语法, 523

R

RESET 开关, 480

日志, 检查, 355

S

SAN 启动, 使用, 402

SAS 地址, 指定, 方法, 598

SAS 控制器, 列表, 567

SAS2IRCU 实用程序, 381

SCSI 设备, 591

审核, 146

时区, 101

实时检查, 308

双回路供电, 161

SNMP 代理, 293

SPARC M10-1 设备路径, 504
SPARC M10-4 设备路径, 507
SPARC M10-4S 设备路径, 513
SPARC M12-2 设备路径, 488
SPARC M12-2S 设备路径, 494
SSCP, 124, 127, 134
SSH/Telnet 服务, 113
锁定模式, 375

W

外部 DVD 驱动器别名, 601
网络配置, 14
物理分区, 3, 239
物理分区运行模式, 239
物理分区, 查看, 347
物理分区, 重启, 330
物理分区, 关闭, 249
物理分区, 开启, 247
物理分区, 配置, 239
物理分区, 配置更改, 250
WWN, 523

X

X.509 公共密钥证书, 413
XCP 固件, 更新, 441
XCP 映像文件, 448
系统安装, 586
系统管理终端, 25
系统海拔高度, 设置/确认, 157
系统控制网络, 14
系统配置, 429
系统配置, 查看, 335
系统启动, 控制, 158
系统特定功能, 563
系统问题, 482
系统状态, 查看, 335
系统, 重新启动, 236
系统, 管理, 285
系统, 监控, 308
系统, 配置, 41
系统, 启动, 229
系统, 停止, 233
夏令时, 102

陷阱, 561
信息, 检查, 355
XSCF 固件, 4
XSCF 固件设置, 内容, 43
XSCF 扩展 MIB, 560
XSCF MIB 信息, 557
XSCF 启动模式功能, 限制, 586
XSCF 启动模式功能, 注意事项, 586
XSCF 日志文件, 355
XSCF 设置, 41
XSCF 设置信息, 保存, 315
XSCF 设置信息, 恢复, 315
XSCF 时间/日期, 设置, 98
XSCF 网络, 14, 123
XSCF 网络接口, 125
XSCF Web, 533
XSCF Web 页面, 概要, 533
XSCF 用户, 52
XSCF, 故障排除, 288
XSCF, 可能存在的问题, 477
XSCF, 设置项目, 43
XSCF, 设置 (XSCF shell), 47
XSCF, 设置 (XSCF web), 51
虚拟 CPU, 429
虚拟机监控程序, 21

Y

延迟转储, 333
验证启动, 412
硬件 RAID, 381
硬件 RAID 卷, 568, 572
硬件 RAID 卷, 配置状态, 574
硬件 RAID 卷, 热备盘, 575, 576
硬件 RAID 卷, 删除, 577
硬盘, 内容, 保存, 327
硬盘, 内容, 恢复, 327
用户权限, 53
用户网络, 14
域控制台日志功能, 263, 565
预热时间, 159
远程存储, 177
远程存储 DVD 驱动器别名, 607
远程电源管理功能, 402

Z

- 注销(XSCF shell), 37
- 注销 (XSCF Web), 39
- 状态查看, 335
- 组件, 建立冗余配置, 315