SPARC M10 시스템

시스템 적동 및 관리 안내서

FUJITSU

ORACLE

설명서 코드 : C120-E679-02HN
2013 년 3 월

Copyright © 2007, 2013, Fujitsu Limited. All rights reserved.

Oracle 및/또는 그 자회사에서 이 자료에 대한 기술적 정보와 검토 작업을 제공했습니다.

Oracle 및/또는 그 자회사 및 Fujitsu Limited는 본 설명서에 기술된 제품 및 기술과 관련된 지적 재산권을 각각 소유하거나 통제하며, 해당 제품, 기술 및 본 설명서는 저작권법, 특허법 및 기타 지적 재산권법 및 국제 협약에 의해 보호를 받습니다.

본 설명서, 제품 및 관련 기술은 사용, 복사, 배포 및 디컴파일을 제한하는 라이센스에 의거하여 배포됩니다. 해당 제품이나 기술 또는 본 설명서의 어떠한 부분도 Oracle 및/또는 그 자회사 및 Fujitsu Limited와 해당 사용권자의 사전 서면 승인 없이는 어떠한 형태나 수단으로도 재생이 불가능합니다. 본 설명서의 제공으로 인해 해당 제품 또는 기술과 관련하여 명시적이든 묵시적이든 어떤 권리나 라이센스가 제공되는 것은 아닙니다. 또한 본 설명서는 Oracle 또는 Fujitsu Limited 또는 각 자회사의 공약을 포함하거나 표명하지 않습니다.

본 설명서와 본 설명서에 기술된 제품 및 기술에는 소프트웨어 및 글꼴 기술을 포함하여 Oracle 및/또는 그 자회사 및 Fujitsu Limited의 제공업체에 의해 저작권을 취득했거나 그러한 제공업체로부터 라이센스를 취득한 제3자 지적 재산권이 포함되어 있을 수 있습니다.

GPL 또는 LGPL의 조항에 따라, GPL 또는 LGPL에 의해 관리되는 소스 코드 사본(있는 경우)은 최종 사용자의 요청에 따라 사용될 수 있습니다. Oracle 및/또는 그 자회사 또는 Fujitsu Limited에 문의하십시오. 본 배포에는 제3자가 개발한 자료가 포함될 수 있습니다. 제품의 일부는 캘리포니아 대학에서 라이센스를 취득한 Berkeley BSD 시스템 계열일 수 있습니다.

UNIX는 The Open Group의 등록 상표입니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다.

Fujitsu 및 Fujitsu 로고는 Fujitsu Limited의 등록 상표입니다.

SPARC Enterprise, SPARC64, SPARC64로고와 모든SPARC 상표는 미국 및 기타 국가에서SPARC International, Inc.의 상표 또는 등록상표이며 라이선스에 의거하여 사용됩니다.

기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이센스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

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.

보증 부인: 본 설명서 또는 본 설명서에 기술된 제품 또는 기술과 관련하여 Oracle 및 Fujitsu Limited 및/또는 각 자회사가 제공하는 보증은 제공된 제품 또는 기술에 적용되는 라이센스 계약에 명시적으로 기술된 보증에 한합니다.

ORACLE 또는 FUJITSU LIMITED 및/또는 그 자회사는 계약서에 명시적으로 기술된 보증을 제외하고, 있는 그대로 제공되는 해당 제품이나 기술 또는 본 설명서와 관련하여 명시적이든 묵시적이든 어떠한 보증도 표시하거나 보증하지 않습니다. 또한 법률을 위반하지 않는 범위 내에서 상품성, 특정 목적에 대한 적합성 또는 비침해성에 대한 묵시적 보증을 포함하여(이에 국한되지 않음) 모든 명시적 또는 묵시적 조건, 표현 및 보증에 대해 어떠한 책임도 지지 않습니다. 계약서에 명시적으로 기술하지 않는 한, 관련 법률이 허용하는 범위 내에서 Oracle 또는 Fujitsu Limited 및/또는 각 자회사는 어떠한 경우에도 제3자의 자산 또는 수익의 손실, 사용 또는 자료의 손실, 사업 중단 또는 어떤 간접적, 특수, 우발적 또는 결과적 손해에 대해 책임을 지지 않으며, 이는 그러한 손해의 가능성을 미리 알고 있었던 경우에도 마찬가지입니다.

본 설명서는 "있는 그대로" 제공되며 상업성, 특정 목적에 대한 적합성 또는 비침해성에 대한 모든 묵시적 보증을 포함하여 모든 명시적 또는 묵시적 조건, 표현 및 보증에 대해 어떠한 책임도 지지 않습니다. 이러한 보증 부인은 법적으로 허용된 범위 내에서만 적용됩니다.

목차

머리말 xvii
1장 SPARC M10 시스템 개요 이해 1
1.1 SPARC M10 시스템의 기본 정보 1
1.2 XSCF 펌웨어의 기본 정보 4
1.2.1 XSCF 개요 4
1.2.2 XSCF 기능 4
1.2.3 XSCF 기능 9
1.2.4 마스터/슬레이브 XSCF 프레임워크 12
1.2.5 모델 간의 XSCF 구성 차이 13
1.3 하이퍼바이저의 기본 정보 15
1.4 Oracle VM Server for SPARC의 기본 정보 15
1.5 OpenBoot PROM의 기본 정보 16
2장 시스템 연결 구성 이해 17
2.1 개념적 시스템 연결 이미지 17
2.2 시스템 관리 터미널 연결 22
2.2.1 직렬 포트를 통한 연결 22
2.2.2 XSCF-LAN을 통한 연결 24
3장 시스템 시작/정지 27
3.1 시스템 시작 27
3.1.1 입력 전원 공급부터 시스템 시작까지 흐름 27
3.1.2 시스템 전체의 시작 28

3.1.3 물리 분할의 개별 전원 공급 31
3.1.4 논리 도메인 시작 33
3.2 시스템 정지 34
3.2.1 시스템 정지부터 입력 전원 차단까지 흐름 34
3.2.2 종료 순서 지정 35
3.2.3 시스템 전체의 정지 35
3.2.4 물리 분할의 개별 전원 차단 36
3.2.5 논리 도메인 종료 37
3.3 시스템 재설정 38
3.3.1 XSCF 재설정 38
3.3.2 물리 분할 재설정 39
3.3.3 논리 도메인 재설정 40
4장 로그인/로그아웃 43
4.1 XSCF 쉘에 로그인 43
4.1.1 직렬 연결을 위한 터미널 및 작업 44
4.1.2 직렬 연결로 XSCF 쉘에 로그인하는 방법 44
4.1.3 XSCF-LAN을 위한 터미널 및 작업 46
4.1.4 XSCF-LAN을 통해 SSH 연결로 XSCF 쉘에 로그인하는 방법 46
4.1.5 XSCF-LAN을 통해 Telnet 연결로 XSCF 쉘에 로그인하는 방법 47
4.2 XSCF 쉘에서 로그아웃 48
4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환 49
4.3.1 XSCF 쉘에서 제어 도메인 콘솔로 전환하는 방법 49
4.3.2 필요 시 제어 도메인 콘솔에 연결 49
4.4 제어 도메인 콘솔에서 XSCF 쉘로 돌아가기 50
4.4.1 제어 도메인 콘솔에서 XSCF 쉘로 전환하는 방법 50
4.4.2 제어 도메인 콘솔에서 로그아웃 50
4.5 XSCF 웹에 로그인 50
4.5.1 사전에 설정해야 하는 항목 51
4.5.2 지원되는 브라우저 51
4.5.3 브라우저를 위해 활성화되어야 하는 기능 51
4.5.4 XSCF 웹으로 로그인하는 방법 52

4.6 XSCF 웹에서 로그아웃 53
4.7 연결 가능한 사용자 수 54
4.8 XSCF-LAN 포트 번호 및 기능과 방화벽 54
5장 잠금/서비스 모드로 전환 55
5.1 잠금 모드와 서비스 모드 간의 차이 이해 55
5.2 작동 모드 전환 56
6장 SPARC M10 시스템 일일 관리 59
7장 XSCF 펌웨어에서 항상 설정하는 항목과 항목 흐름에 대한 이해 61
7.1 XSCF 설정을 위한 예비 작업 61
7.1.1 설정 전 초기 작업 61
7.1.2 최신 지원 정보 확인 62
7.1.3 구성을 위한 사용자 인터페이스와 액세스 방법 62
7.2 XSCF 쉘에서 설정 63
7.3 XSCF 웹에서 설정 67
8장 XSCF 펌웨어 구성 69
8.1 XSCF의 원활한 설정 69
8.2 XSCF 펌웨어 설정 이해 70
8.2.1 XSCF를 사용하기 위한 설정 항목 70
8.2.2 마스터 XSCF 확인 71
8.2.3 스탠바이 XSCF에서 실행 가능한 기능 72
8.2.4 설명서 페이지를 사용한 명령의 옵션 세부 사항 확인 73
8.3 XSCF 사용자 생성/관리 73
8.3.1 XSCF 사용자 계정 73
8.3.2 암호 및 암호 정책 74
8.3.3 사용자 권한 유형 74
8.3.4 XSCF 사용자 계정과 관련된 설정 항목 및 명령의 확인 76
8.3.5 XSCF 사용자 계정 등록 흐름 76
8.3.6 암호 정책 확인/변경 77
8.3.7 XSCF 사용자 계정 추가/삭제 및 암호 구성 78
8.3.8 사용자 권한 설정 79
8.3.9 사용자 계정 활성화/비활성화 80

8.3.10 로그인 잠금 기능 활성화/비활성화 81
8.4 XSCF 시간/날짜 설정 82
8.4.1 논리 도메인의 시간 관리 정책 82
8.4.2 각 제어 도메인과 XSCF 간의 시간 관계 이해 83
8.4.3 시간과 관련된 설정 항목 및 명령의 확인 83
8.4.4 표준 시간대 구성 84
8.4.5 서머 타임 구성 84
8.4.6 시스템 시간 구성 85
8.4.7 제어 도메인 시간과 XSCF 시간의 동기화 86
8.4.8 NTP 서버로서 XSCF 지정 89
8.4.9 NTP 클라이언트로서 XSCF 지정 90
8.4.10 XSCF에 사용되는 NTP 서버 구성 90
8.4.11 NTP 서버에서 선호 지정/지정 해제 92
8.4.12 XSCF의 계층 값 구성 93
8.4.13 XSCF 로컬 클록의 클록 주소 변경 93
8.5 XSCF 네트워크 구성 95
8.5.1 XSCF 네트워크를 사용한 서비스 이용 96
8.5.2 XSCF 네트워크 인터페이스 이해 96
8.5.3 XSCF 네트워크 인터페이스 구성 97
8.5.4 SSCP에서 IP 주소 설정 이해 100
8.5.5 네트워크 그룹 서브넷 이해 101
8.5.6 XSCF 네트워크와 관련된 설정 항목 및 명령의 확인 102
8.5.7 XSCF 네트워크 구성 흐름 103
8.5.8 XSCF 네트워크의 활성화/비활성화와 XSCF-LAN IP 주소 및 네트워크 마스크의 구성 104
8.5.9 인계 IP 주소 구성 105
8.5.10 SSCP IP 주소 구성 106
8.5.11 XSCF 호스트 이름 및 도메인 이름 구성 108
8.5.12 XSCF 라우팅 설정 구성 108
8.5.13 XSCF의 DNS 설정 구성 110
8.5.14 XSCF 네트워크에 IP 패킷 필터링 규칙 구성 112

8.5.15 XSCF 네트워크 설정 적용 113
8.5.16 XSCF 네트워크 연결의 상태 확인 115
8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성 116
8.6.1 SSH 및 Telnet과 관련된 설정 항목 및 명령의 확인 117
8.6.2 SSH 및 Telnet 서비스의 활성화/비활성화 118
8.6.3 SSH 서비스 호스트 키 구성 119
8.6.4 SSH 서비스를 위한 사용자 공개 키 등록/삭제 120
8.6.5 SSH/Telnet 서비스 시간 초과 시간의 구성 121
8.7 XSCF에 로그인하기 위한 HTTPS 서비스 구성 121
8.7.1 외부 또는 인트라넷 인증 기관의 사용 흐름 122
8.7.2 자치 인증 기관의 사용 흐름 122
8.7.3 HTTPS와 관련된 설정 항목 및 명령의 확인 123
8.7.4 HTTPS 서비스의 활성화/비활성화 123
8.7.5 외부 또는 인트라넷 인증 기관을 사용한 웹 서버 인증서 가져오기 124
8.7.6 자치 인증 기관 구성 및 웹 서버 인증서 생성 125
8.8 XSCF 보안 강화를 위한 감사 구성 126
8.8.1 감사 용어 이해 127
8.8.2 감사 데이터 기록 이해 127
8.8.3 감사 설정과 관련된 설정 항목 및 명령의 확인 128
8.8.4 감사의 활성화/비활성화 128
8.8.5 감사 파일의 데이터 삭제 129
8.8.6 감사 정책 구성 130
8.8.7 감사 로그 보기 131
9장 시스템 구성 133
9.1 시스템 고도 설정/확인 133
9.1.1 시스템 고도 설정 133
9.1.2 시스템 고도 확인 134
9.2 시스템 활성화 제어 135
9.2.1 웜업 시간 설정/확인 135
9.2.2 시작 대기 시간 설정/확인 137

9.3 이중 전원 공급 활성화/비활성화 138
9.3.1 이중 전원 공급 활성화 138
9.3.2 이중 전원 공급 비활성화 139
9.3.3 이중 전원 공급 설정 확인 140
9.4 소비 전력 최소화 141
9.4.1 소비 전력의 상한 구성 141
9.4.2 비정상 온도/전압 해결 143
9.5 DVD 드라이브 연결 143
9.5.1 USB를 통해 연결되는 외부 DVD 드라이브 사용 143
10장 물리 분할 제어 145
10.1 물리 분할 구성 145
10.2 물리 분할 작동 모드 설정 145
10.3 물리 분할의 전원 공급 146
10.4 물리 분할의 전원 차단 146
10.5 물리 분할 재설정 146
10.6 물리 분할의 구성 변경 147
11장 논리 도메인 제어 149
11.1 논리 도메인 구성 149
11.2 제어 도메인용 OpenBoot PROM 환경 변수 설정 149
11.2.1 XSCF 펌웨어에 의해 설정되는 OpenBoot PROM 환경 변수 150
11.2.2 제어 도메인용 OpenBoot 환경 변수 설정 150
11.2.3 제어 도메인용으로 설정된 OpenBoot PROM 환경 변수의 표시 151
11.2.4 제어 도메인용으로 설정된 OpenBoot PROM 환경 변수의 삭제 152
11.3 논리 도메인의 구성 변경 153
11.4 논리 도메인의 시간 구성 154
11.5 논리 도메인에서 패닉 발생 154
11.5.1 게스트 도메인에서 패닉 발생 154
11.5.2 제어 도메인에서 패닉 발생 155
12장 고 신뢰성 시스템 구성 157

12.1 메모리 미러링 구성 157
12.1.1 메모리 미러링 개요 157
12.1.2 메모리 미러링 구성 158
12.2 하드웨어 RAID 구성 159
12.2.1 하드웨어 RAID의 기본 정보 159
12.2.2 FCode 유틸리티 명령 161
12.2.3 하드웨어 RAID 작동 전 준비 161
12.2.4 하드웨어 RAID 볼륨 생성 163
12.2.5 하드웨어 RAID 볼륨 삭제 165
12.2.6 디스크 드라이브 상태 확인 166
12.2.7 고장인 디스크 드라이브 확인 167
12.2.8 하드웨어 RAID 볼륨 재활성화 167
12.2.9 디스크 슬롯 번호 169
12.3 SAN 부팅 사용 171
12.4 iSCSI 사용 171
12.5 SPARC M10 시스템과 I/O 장치의 전원 공급 연동 171
12.5.1 SPARC M10 시스템 전원 공급 연동 기능의 기본 정보 171
12.5.2 전원 공급 연동의 연결 모드 이해 172
12.5.3 전원 공급 연동의 메커니즘 174
12.5.4 전원 공급 연동의 설정 흐름 176
12.5.5 전원 공급 연동의 설정 상태 확인 178
12.5.6 전원 공급 연동 설정 초기화 178
12.5.7 전원 공급 연동 기능 활성화/비활성화 179
12.5.8 관리 파일 생성 179
12.5.9 전원 공급 연동 그룹의 설정 정보 가져오기 180
12.5.10 전원 공급 연동 그룹 설정 180
12.6 이중 전원 공급 사용 181
12.7 무정전 전원 공급 장치 사용 181
13장 시스템 구성 확장 183
13.1 가상 CPU의 구성 변경 183
13.2 메모리 구성 변경 185

13.3 PCI 확장 장치 사용 187
13.3.1 PCI 확장 장치 확인 187
13.3.2 PCI 확장 장치의 전원 제어 187
13.4 SPARC M10-4S 확장 188
14장 필요 시 용량 제공(CoD) 189
14.1 필요 시 용량 제공(CoD)의 기본 정보 189
14.2 CPU 코어 활성화의 기본 정보 189
14.3 CPU 코어 활성화 키의 기본 정보 190
14.3.1 CPU 코어 활성화 키 및 사용 가능한 CPU 190
14.4 CoD 자원 추가 191
14.4.1 CoD 자원 추가까지 흐름 191
14.4.2 CPU 코어 활성화의 구입 191
14.4.3 CPU 코어 활성화 키의 확인 191
14.4.4 CPU 코어 활성화 키의 추가 192
14.4.5 물리 분할에 CoD 자원 할당 193
14.4.6 논리 도메인에 CoD 자원 할당 194
14.4.7 CPU 코어 활성화 키의 삭제 194
14.5 CoD 정보 표시 195
14.5.1 CoD 정보 표시 195
14.5.2 CoD 로그 확인 196
14.5.3 CPU 코어 활성화 키 정보 표시 196
14.5.4 CoD 자원 사용 상태 표시 197
14.6 CoD 오류에 대한 대응 조치 198
14.6.1 사용되는 CPU의 수가 CPU 코어 활성화에서 허용되는 수를 초과하는 경우 198
14.6.2 고장으로 인해 CoD 자원 수가 CPU 코어 활성화 수 미만인 경우 199
14.7 CoD 사용 시 유의 사항 199
15장 고장 대응 201
15.1 고장 대응 조치 및 기능 이해 201
15.2 고장 발생 시 이메일을 통한 알림 수신 202

15.2.1 이메일 알림 기능의 특징 202
15.2.2 고장 알림 세부 사항 203
15.2.3 이메일 알림과 관련된 설정 항목 및 명령의 확인 205
15.2.4 이메일 알림 설정의 흐름 205
15.2.5 호스트 이름, 포트 번호, 회신 대상 이메일 주소 및 SMTP 서버의 인증 방법 설정 206
15.2.6 대상 이메일 주소 및 이메일 알림 기능의 활성화/비활성화 여부 설정 207
15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리 207
15.3.1 SNMP의 기본 정보 208
15.3.2 SNMP 용어 209
15.3.3 MIB 정의 파일의 기본 정보 209
15.3.4 확장 MIB의 전원 정보 참조/전원 정보 설정 210
15.3.5 트랩의 기본 정보 211
15.3.6 SNMP 에이전트와 관련된 설정 항목 및 명령의 확인 212
15.3.7 SNMP 에이전트 설정의 흐름 213
15.3.8 SNMP 에이전트의 시스템 관리 정보 설정 및 SNMP 에이전트의 활성화/비활성화 여부 지정 215
15.3.9 SNMPv3 트랩 설정 216
15.3.10 SNMPv3의 대상 호스트로 트랩 비활성화 217
15.3.11 SNMPv1 및 SNMPv2c 통신 활성화/비활성화 217
15.3.12 SNMPv1 및 SNMPv2c 트랩 설정 218
15.3.13 SNMPv1 및 SNMPv2c의 대상 호스트로 트랩 비활성화 219
15.3.14 기본값으로 SNMP 설정 복귀 219
15.3.15 USM 관리 정보 설정 220
15.3.16 VACM 관리 정보 설정 221
15.4 시스템 모니터링 222
15.4.1 하트비트 기능/활성 모니터링의 메커니즘 이해 222
15.4.2 모니터링 및 서버 작동 제어 223
15.5 고장 성능 저하 메커니즘 이해 224
15.6 중복 구성요소 구성 224

15.7 XSCF 설정 정보 저장/복원 225
15.7.1 XSCF 설정 정보의 저장/복원 방법 이해 225
15.7.2 XSCF 설정 정보 저장 226
15.7.3 XSCF 설정 정보 복원 227
15.8 논리 도메인 구성 정보 저장/복원 228
15.8.1 논리 도메인 구성 정보 저장/표시 228
15.8.2 논리 도메인 구성 정보 복원 229
15.9 하드 디스크 내용 저장/복원 231
15.10 하이퍼바이저의 덤프 파일 수집 232
15.10.1 하이퍼바이저 덤프의 기본 정보 232
15.10.2 하이퍼바이저 덤프 기능에 사용되는 명령 232
15.10.3 하이퍼바이저 덤프 사용 시 주의 사항 234
15.11 공장 기본 상태로 서버 복귀 234
15.11.1 초기화 명령 이해 235
15.11.2 서버 초기화 235
16장 시스템 상태의 확인 237
16.1 시스템 구성/상태의 확인 237
16.1.1 시스템 구성/상태와 관련된 항목 및 명령의 확인 237
16.1.2 시스템에 장착된 구성요소의 확인 238
16.1.3 시스템 환경의 확인 240
16.1.4 고장/성능 저하된 구성요소의 확인 243
16.1.5 PCI 확장 장치 상태 표시 244
16.2 물리 분할 확인 247
16.2.1 물리 분할 및 논리 도메인 구성/상태와 관련된 항목 및 명령의 확인 247
16.2.2 물리 분할 구성의 확인 248
16.2.3 물리 분할 작동 상태의 확인 250
16.2.4 시스템 보드 설정의 확인 251
16.2.5 시스템 보드 상태의 확인 253
16.2.6 논리 도메인 상태의 확인 254
17장 로그 및 메시지 확인 255

17.1 XSCF로 저장된 로그 확인 255
17.1.1 로그 유형 및 참조 명령의 확인 255
17.1.2 로그 참조 258
17.1.3 오류 로그 확인 259
17.1.4 모니터 메시지 로그의 확인 261
17.1.5 전원 로그 확인 261
17.1.6 이벤트 로그 확인 263
17.1.7 콘솔 로그 확인 263
17.1.8 패닉 로그 확인 264
17.1.9 IPL 로그 확인 265
17.1.10 감사 로그 확인 265
17.1.11 CoD 로그 확인 267
17.1.12 온도 이력 로그 확인 268
17.1.13 스냅샷으로 파일에 로그 저장 268
17.1.14 로컬 USB 장치로 로그 저장 269
17.2 경고 및 알림 메시지의 확인 270
17.2.1 메시지 유형 및 참조 방법의 확인 270
17.2.2 보고된 메시지 처리 272
18장 펌웨어/소프트웨어 업데이트 275
18.1 XCP 펌웨어 업데이트 275
18.1.1 펌웨어 업데이트의 기본 정보 275
18.1.2 펌웨어 업데이트 전 278
18.1.3 펌웨어 업데이트 281
18.1.4 펌웨어 업데이트 중 문제 289
18.1.5 펌웨어 업데이트와 관련된 FAQ 289
18.2 Oracle Solaris 및 Oracle VM Server for SPARC 업데이트 290
19장 XSCF/시스템 문제 해결 291
19.1 XSCF 문제 해결 291
19.2 질문과 대답/FAQ 294
19.3 XSCF가 있는 시스템 문제 해결 296
부록 A WWN을 지원하는 SAS2 장치의 식별 299

A.1 WWN(World Wide Name) 구문 299
A.2 probe-scsi-all 명령 출력 요약 299
A.3 probe-scsi-all 명령을 사용한 디스크 슬롯의 식별 300
A.4 probe-scsi-all 명령을 사용한 디스크 슬롯의 식별 예(SPARC M10-1/M10-4/M10-4S) 300
부록 B XSCF 웹 페이지 목록 303
B.1 페이지 요약 303
B.2 메뉴 구성 이해 306
B.3 사용 가능한 페이지 309
B.3.1 시스템, 물리 분할 및 논리 도메인의 상태를 표시하는 페이지 309
B.3.2 물리 분할을 작동하는 페이지 311
B.3.3 서버를 구성하는 페이지 313
B.3.4 서버를 유지 관리하는 페이지 322
B.3.5 로그를 보는 페이지 324
부록 C XSCF MIB 정보 325
C.1 MIB 개체 식별 325
C.2 표준 MIB 327
C.3 확장 MIB 327
C.3.1 XSCF 확장 MIB 개체 328
C.4 트랩의 기본 정보 329
부록 D SPARC M10 시스템용 Oracle VM Server for SPARC의 특징 331
D.1 도메인의 지정된 종료 331
D.1.1 도메인 테이블(ldomTable) 332
D.1.2 도메인 정보(ldom_info) 자원 332
D.2 필요 시 용량 제공 지원 333
D.2.1 필요 시 용량 제공 허가 정보의 나열 방법 333
D.3 고장인 자원 보기 334
D.3.1 모든 도메인에 대한 자원 상태의 생성 방법 334
D.3.2 사용 가능한 자원에 대한 상태 생성 방법 334
D.4 고장인 CPU의 자동 교체 334
D.4.1 자동 교체 정책의 수정 방법 335

D.4.2 최대 재시도 카운터 및 재시도 간격의 수정 방법 336
D.5 하이퍼바이저 덤프 수집 336
D.5.1 하이퍼바이저 덤프 수집의 비활성화 방법 336
D.5.2 하이퍼바이저 덤프 수집의 활성화 방법 336
D.5.3 덤프 수집 후 자동 재부팅의 활성화 방법 337
D.5.4 덤프 수집 후 자동 재부팅의 비활성화 방법 337
D.5.5 덤프 수집 프로세스의 수동 시작 방법 337
D.6 도메인 콘솔 로깅 338
D.6.1 콘솔 로깅의 비활성화 방법 338
D.6.2 콘솔 로깅의 활성화 방법 338
D.6.3 서비스 도메인 요구 사항 339
D.6.4 가상 콘솔 그룹 테이블(ldomVconsTable) 339
D.6.5 콘솔(콘솔) 자원 339
색인 341

머리말

본 설명서에는 Oracle 또는 Fujitsu SPARC M10 시스템 설치 후의 설정 및 관리 방법이 설명되어 있습니다. SPARC M10 시스템을 작동할 때 필요한 부분을 읽어보시기 바랍니다.
『SPARC M10 시스템 빠른 안내서』를 읽어보시면 본 설명서의 내용을 보다 쉽게 이해하실 수 있습니다.

이 머리말에는 다음 절이 포함되어 있습니다.

- 대상
- 관련 설명서
- 텍스트 규약
- 안전 주의 사항
- 명령줄 인터페이스(Command-Line Interface, CLI) 구문
- 설명서 피드백

대상

본 설명서는 컴퓨터 네트워크와 Oracle Solaris에 대한 고급 지식을 지니고 있는 시스템 관리자를 대상으로 합니다.

관련 설명서

서버에 대한 모든 설명서는 다음 위치에서 온라인으로 사용 가능합니다.

- Sun Oracle 소프트웨어 관련 설명서(Oracle Solaris 등)
  http://www.oracle.com/documentation/
- Fujitsu 설명서
  http://www.fujitsu.com/global/services/computing/server/sparc/downloads/manual/

다음 표에는 SPARC M10 시스템과 관련된 설명서가 나열되어 있습니다.

관련된 **SPARC M10** 시스템 설명서
『SPARC M10 시스템 시작 안내서』 *
『SPARC M10 시스템 빠른 안내서』
『SPARC M10 Systems Important Legal and Safety Information』 *
『Software License Conditions for SPARC M10 Systems』
『SPARC M10 Systems Safety and Compliance Guide』
『SPARC M10 Systems Security Guide』
『SPARC M10 시스템 설치 안내서』
『SPARC M10-1 Service Manual』
『SPARC M10-4/M10-4S Service Manual』
『PCI Expansion Unit for SPARC M10 Systems Service Manual』
『SPARC M10 시스템 시스템 작동 및 관리 안내서』
『SPARC M10 시스템 도메인 구성 안내서』
『SPARC M10 Systems XSCF Reference Manual』
『SPARC M10 시스템 제품 노트』
『SPARC M10 Systems Glossary』

* 인쇄된 설명서입니다.

텍스트 규약

이 설명서는 다음과 같은 글꼴과 기호를 사용하여 특정 유형의 정보를 표현합니다.

글꼴/기호	의미	예
AaBbCc123	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 대조됩니다. 이 글꼴은 프레임의 명령 입력 예를 나타냅니다.	`XSCF> adduser jsmith`

`AaBbCc123`	명령, 파일 및 디렉토리 이름, 컴퓨터 화면 출력입니다.
	이 글꼴은 명령 출력 예를 나타냅니다.
		`XSCF> showuser -P`
		`User Name: jsmith`
		`Privileges: useradm`
		`auditadm`

『 』	참조 설명서 이름, 변수 또는 사용자 대체 텍스트를 나타냅니다.	『SPARC M10 시스템 설치 안내서』를 참조하십시오.
" "	장, 절, 항목, 버튼 또는 메뉴 이름을 나타냅니다.	"2장 네트워크 연결"을 참조하십시오.

텍스트의 명령 구문

XSCF 명령에 (8) 또는 (1)의 절 번호가 있지만 텍스트에서는 생략되어 있습니다. Oracle Solaris 명령은 (1M)과 같은 절 번호가 텍스트에 있습니다. 사용자가 절 번호를 참조하라고 프롬프트를 표시할 때 각 명령마다 명령 이름에 절 번호가 있게 됩니다.

안전 주의 사항

SPARC M10 시스템을 사용하거나 처리하기 전에 다음 설명서 전체를 읽으십시오.

- 『SPARC M10 Systems Important Legal and Safety Information』
- 『SPARC M10 Systems Safety and Compliance Guide』

명령줄 인터페이스(Command-Line Interface, CLI) 구문

해당 명령의 구문은 다음과 같습니다.

- 값 입력이 필요한 변수는 기울임꼴로 표시되어야 합니다.
- 선택적 요소는 [ ]로 묶어야 합니다.
- 선택적 키워드에 대한 옵션 그룹은 [ ]로 묶고, |로 구분되어야 합니다.

설명서 피드백

본 설명서와 관련된 의견이나 요청이 있으면 다음 웹 사이트로 이동하십시오.

- 일본 사이트:
  http://jp.fujitsu.com/platform/server/unix/manual/
- 글로벌 사이트:
  http://www.fujitsu.com/global/services/computing/server/sparc/downloads/manual/

1장

SPARC M10 시스템 개요 이해

이 장에는 SPARC M10 시스템과 이 시스템에 사용되는 소프트웨어 및 펌웨어의 요약이 설명되어 있습니다.

- SPARC M10 시스템의 기본 정보
- XSCF 펌웨어의 기본 정보
- 하이퍼바이저의 기본 정보
- Oracle VM Server for SPARC의 기본 정보
- OpenBoot PROM의 기본 정보

1.1 SPARC M10 시스템의 기본 정보

이 절에는 SPARC M10 시스템의 요약이 설명되어 있습니다.

SPARC M10 시스템은 빌딩 블록 시스템이 사용되는 UNIX 서버입니다. 이 서버는 기본 장치인 캐비닛을 조합하여 활용도 또는 비즈니스 규모에 따라 시스템이 유연하게 구성될 수 있도록 합니다. 이 서버는 클라우드 시스템이나 웹 서버 및/또는 응용 프로그램 서버가 많은 양을 처리해야 할 때 데이터 센터에 최적인 데이터베이스 서버로서 다양한 방법으로 적용됩니다.

다음 유형의 SPARC M10 시스템이 다양한 활용을 지원하도록 제공됩니다.

- SPARC M10-1
  이는 공간을 절약하고 성능이 뛰어난 단일 1-CPU 캐비닛으로 구성된 컴팩트 모델입니다.
- SPARC M10-4
  이는 단일 4-CPU 캐비닛으로 구성된 모델입니다.
- SPARC M10-4S
  이는 빌딩 블록(BB) 시스템 방식의 서로 연결된 4-CPU 캐비닛으로 구성된 모델입니다. 연결되는 SPARC M10-4S 캐비닛의 수는 필요한 성능에 맞춰 조정할 수 있습니다. SPARC M10-4S 캐비닛을 상호 연결하여 최대 4개 BB까지 구성을 설정할 수 있습니다. 더욱이 크로스바 박스를 사용하면 최대 16개 BB까지 구성이 지원되고 최대 64개 CPU까지 확장성이 보장됩니다.

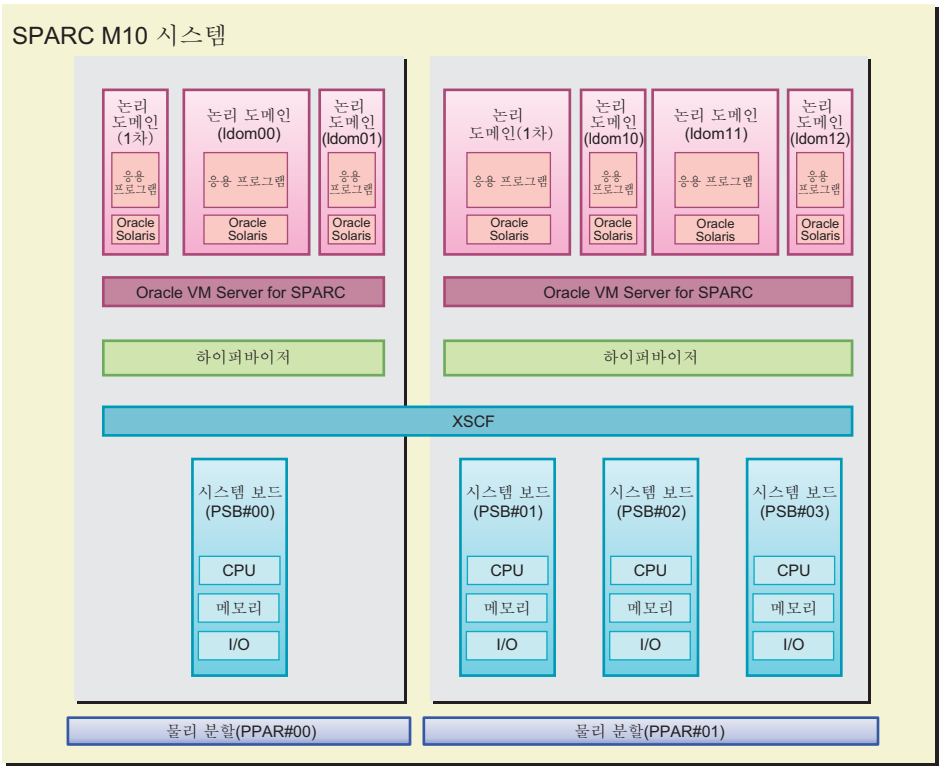
SPARC M10 시스템의 하드웨어 시스템 구성과 사양은『SPARC M10 시스템 빠른 안내서』를 참조하십시오.

소프트웨어 측면에서 본 시스템 구성

이 절에는 펌웨어 및 소프트웨어 측면에서 본 SPARC M10 시스템 구성이 설명되어 있습니다.

필요한 펌웨어 및 소프트웨어를 사용하여 SPARC M10 시스템을 설치하고 시스템을 구성하면 그림 1-1에 나타난 것과 같은 시스템 구성이 설정됩니다. 그림 1-1에는 2개 이상의 SPARC M10-4S가 빌딩 블록 시스템으로 연결된 시스템 구성의 예가 나타나 있습니다.
각 SPARC M10-4S는 소프트웨어 용도의 1개 시스템 보드(PSB)로서 인식됩니다. 1개 이상의 시스템 보드를 연결 조합하여 물리 분할(PPAR)을 구성합니다.
CPU, 메모리 모듈 및 I/O 장치와 같은 구성된 물리 분할에서 구현된 하드웨어 자원을 논리 도메인에 할당하면 시스템이 구성됩니다.
각 논리 도메인은 1개 독립 UNIX 서버로서 처리됩니다. 각 논리 도메인에서는 독립적으로 Oracle Solaris를 설치하고 비즈니스 응용 프로그램을 실행할 수 있습니다.

그림 1-1 SPARC M10 시스템 구성 예



다음 하위 절에는 시스템 구성의 주요 요소인 "물리 분할"과 "논리 도메인"이 설명되어 있습니다.

물리 분할 구성

시스템 구성의 경우 먼저 빌딩 블록 시스템으로 연결된 SPARC M10-4S를 조합하여 물리 분할을 구성합니다. 물리 분할 구성을 분할이라고 하며 구성된 것을 물리 분할(PPAR)이라고 합니다. 물리 분할은 시스템 관리 펌웨어인 XSCF 펌웨어를 사용하여 구성합니다.

물리 분할을 구성할 때 각 SPARC M10-4S 캐비닛은 1개 시스템 보드(PSB)로서 처리됩니다. 물리 분할은 시스템 보드를 기반으로 구성됩니다.

그림 1-1에 나타난 예에서 SPARC M10 시스템의 시스템 보드 가운데 하나인 시스템 보드 PSB#00은 물리 분할 PPAR#00으로서 구성됩니다. 유사하게 시스템 보드 PSB#01, PSB#02 및 PSB#03도 물리 분할 PPAR#01로서 구성됩니다.

물리 분할의 구성 후 CPU, 메모리 모듈 및 I/O 장치와 같은 물리 분할의 하드웨어 자원은 논리 도메인으로 할당됩니다.
유의할 점으로, SPARC M10-1/M10-4는 1개 물리 분할만 구성되는 단일 캐비닛으로 이루어진 모델입니다.

논리 도메인 구성

CPU, 메모리 모듈 및 I/O 장치와 같은 물리 분할(PPAR)의 하드웨어 자원은 논리 도메인으로 할당됩니다. 논리 도메인은 Oracle VM Server for SPARC 소프트웨어를 사용하여 구성합니다.

구성된 논리 도메인은 1개 소프트웨어 UNIX 시스템으로서 각각 처리됩니다. Oracle Solaris 및/또는 응용 프로그램은 논리 도메인에 별도 설치할 수 있으며 개별 비즈니스에 적용됩니다. 그림 1-1에 나타난 예에서 논리 도메인 primary, ldom00 및 ldom01은 물리 분할 PPAR#00의 하드웨어 자원 할당으로 구성됩니다.
유사하게 물리 분할 PPAR#01의 경우 논리 도메인 primary, ldom10, ldom11 및 ldom12가 구성됩니다.

물리 분할에 할당된 논리 도메인 가운데 하나는 모든 논리 도메인을 제어하는 데 사용됩니다. 이를 제어 도메인이라고 합니다. 논리 도메인 컨트롤러인 제어 도메인은 물리 분할과 논리 도메인 간의 통신을 처리하는 데도 사용됩니다.

SPARC M10 시스템에 필요한 펌웨어 및 소프트웨어

SPARC M10 시스템의 시스템 구성에 필요한 물리 분할과 논리 도메인은 그 이름이 각각 XSCF 펌웨어 및 Oracle VM Server for SPARC인 다른 펌웨어와 소프트웨어로 구현됩니다. 시스템 전체의 모니터링 및 관리 면에서 XSCF 펌웨어와 Oracle VM Server for SPARC 간의 통신은 시스템 내부에서 처리됩니다. 사용자는 주의를 기울이지 않아도 됩니다.

SPARC M10 시스템의 경우 XSCF 펌웨어와 Oracle VM Server for SPARC 간의 인터페이스는 그 이름이 하이퍼바이저인 펌웨어에 의해 구현됩니다.

다음 절에는 SPARC M10 시스템에 사용되는 소프트웨어와 펌웨어의 요약이 설명되어 있습니다.

1.2 XSCF 펌웨어의 기본 정보

이 절에는 XSCF 펌웨어의 요약과 기능이 설명되어 있습니다.

1.2.1 XSCF 개요

XSCF 펌웨어는 SPARC M10 시스템에서 구현되는 시스템 제어 설비입니다. XSCF 펌웨어는 서버의 프로세서와 독립적으로 전용 프로세서(서비스 프로세서) 상에서 실행됩니다. SPARC M10-1, SPARC M10-4 및 SPARC M10-4S 시스템 각각의 캐비닛에 1개 XSCF 펌웨어가 위치하여 논리 도메인과의 통신을 보장하고 시스템 전체를 관리합니다. 빌딩 블록(BB)으로 구성된 SPARC M10-4S 시스템의 경우 XSCF 펌웨어가 SPARC M10-4S 캐비닛 각각과 각 크로스바 박스(XBBOX)에 있습니다.

작동 전원이 서버에 공급되면 논리 도메인이 작동하지 않거나 물리 분할로의 전원이 차단되더라도 XSCF 펌웨어가 실행되어 서버가 제대로 작동하는지 모니터링할 수 있습니다. XSCF는 서버 구성을 변경하거나 서버 전원을 공급/차단할 수도 있습니다.

또한 XSCF 펌웨어는 사용자와 인터페이스되어 시스템 관리자의 일일 관리 활동을 지원하기도 합니다.

본 설명서에서는 XSCF 펌웨어를 XSCF라고도 합니다. XSCF 펌웨어가 실행되는 서비스 프로세서를 포함하는 보드를 XSCF 장치라고도 합니다.

1.2.2 XSCF 기능

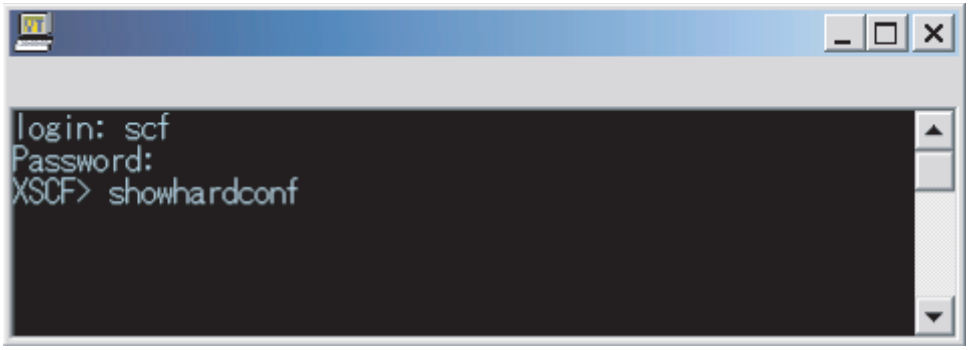
일일 서버 작동 및 유지 관리에 사용 가능한 사용자 인터페이스

명령줄 또는 웹 브라우저에서 XSCF에 액세스하여 서버 상태를 파악하고 서버를 작동하며 서버를 서비스할 수 있습니다.

- **XSCF 쉘(명령줄 인터페이스)**
  직렬 케이블로 사용자 PC를 서버에 직접 연결하거나 XSCF LAN에 이더넷 연결하여 SSH 서비스 또는 Telnet 서비스를 사용할 수 있습니다. 이를 통해 PC를 XSCF 쉘 터미널로 사용하고 XSCF 쉘 명령을 실행할 수 있습니다. XSCF 쉘에서 제어 도메인을 작동할 수 있도록 하는 콘솔로 전환할 수 있습니다(이후 제어 도메인 콘솔이라고 함).

  그림 1-2에는 XSCF 쉘 터미널의 예가 나타나 있습니다.

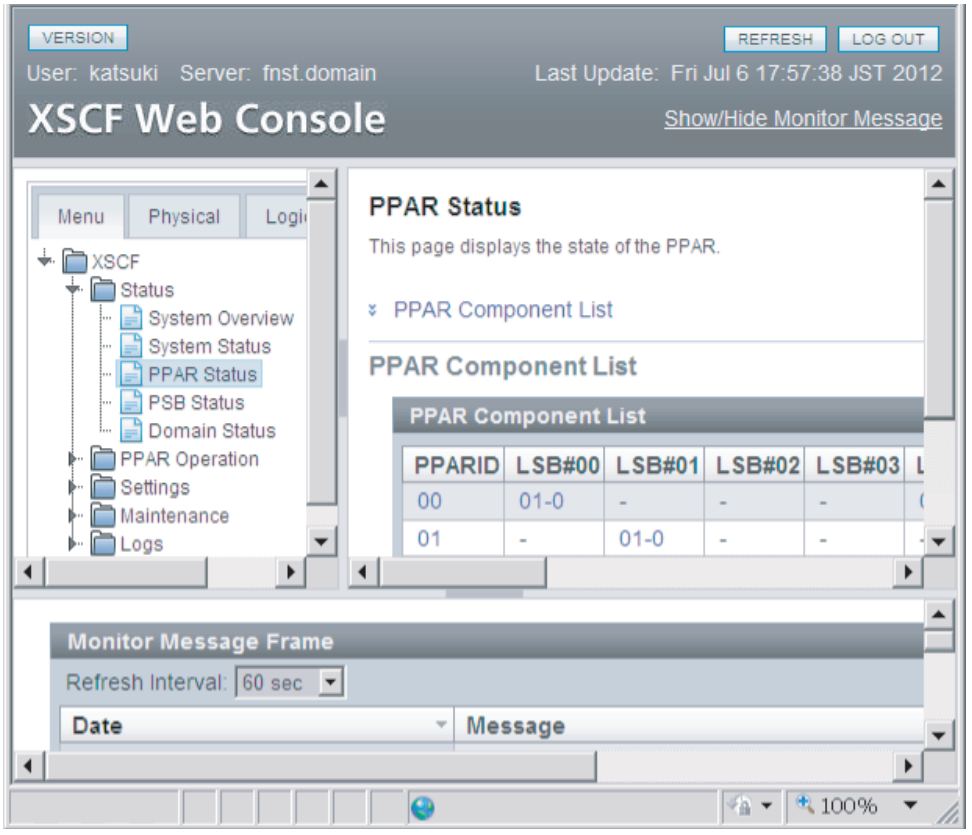
그림 1-2 XSCF 쉘 터미널의 예



- **XSCF 웹(**브라우저 사용자 인터페이스**)**
  이에 따라 이더넷을 통해 PC를 XSCF LAN에 연결하고 HTTPS 프로토콜 또는 SSL/TLS 프로토콜을 사용할 수 있습니다. XSCF용 PC에서 웹 브라우저를 사용하고 이를 통해 XSCF 웹 콘솔을 사용할 수 있습니다. XSCF 웹의 경우 구성요소를 계층 보기로 표시하고 원하는 작동 메뉴를 찾으며 기타 편리한 명령을 수행하고 작동 부담을 줄이며 서버 관리 비용을 절감할 수 있습니다.

  그림 1-3에는 XSCF 웹 콘솔의 사용 예가 나타나 있습니다.

그림 1-3 XSCF 웹 콘솔의 예



다중 XSCF 구성

빌딩 블록으로 구성된 시스템의 경우 각 SPARC M10-4S 캐비닛 및 크로스바 박스(XBBOX)마다 1개 XSCF가 있습니다. XSCF를 개별 캐비닛에 배치하면 신뢰성 높은 시스템이 구현됩니다.

그림 1-4에는 4BB 구성의 SPARC M10-4S 시스템 예가 나타나 있습니다.

그림 1-4 SPARC M10-4S 시스템 -1에서의 XSCF 구성 예

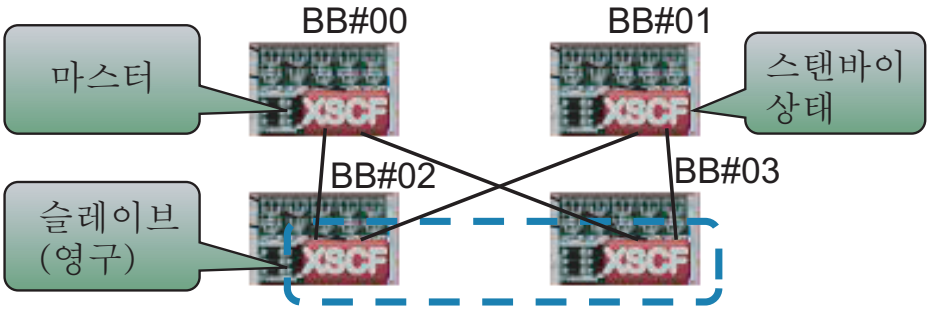
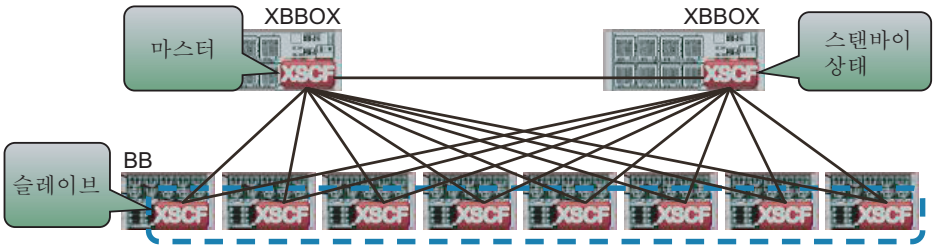


그림 1-5에는 8BB 구성의 SPARC M10-4S 시스템 예가 나타나 있습니다.

그림 1-5 SPARC M10-4S 시스템 -2에서의 XSCF 구성 예



빌딩 블록으로 구성된 시스템의 경우 다중 구성의 XSCF는 서비스 프로세서 간 통신(SP 대 SP 통신 프로토콜(SSCP))으로 서로 모니터링합니다.

XSCF는 다음 2개 유형으로 분류됩니다.

- 마스터 XSCF: 서버 전체를 관리 및 제어합니다. 마스터 XSCF의 백업 역할을 하는 스탠바이 성격의 또 다른 중복 XSCF가 있습니다.
- 슬레이브 XSCF: XSCF가 구현되는 SPARC M10-4S 캐비닛 또는 크로스바 박스를 관리합니다.

이 마스터 및 슬레이브 XSCF와 관련된 자세한 내용은 "1.2.4 마스터/슬레이브 XSCF 프레임워크"를 참조하십시오.

외부 인터페이스

SPARC M10 시스템 캐비닛 및 크로스바 박스에는 다음의 XSCF 관련 커넥터(포트)와 LED가 있습니다. XSCF 펌웨어를 통해 사용자, 시스템 관리자 및 현장 엔지니어는 서버를 모니터링 및 작동할 수 있습니다. 각 인터페이스 위치와 각 연결 방법의 자세한 내용은 『SPARC M10 시스템 설치 안내서』의 "5장 캐비닛에 케이블 연결"을 참조하십시오.

- 직렬 포트
  직렬 포트는 서버를 구성하고 XSCF 쉘로 서버 상태를 보는 데 사용됩니다. 직렬 포트(RS-232C 포트)는 RJ-45 커넥터입니다. 직렬 포트와 PC는 RS-232C 직렬 크로스 케

이블로 연결합니다. LAN 케이블만 있는 경우 RJ-45/RS-232C 변환 케이블 또는 변환 커넥터를 사용해야 합니다.

- XSCF-LAN 포트 x 2(이더넷 포트)
  XSCF-LAN 포트는 시스템 관리자가 이더넷을 통해 서버를 작동할 수 있도록 하는 LAN 커넥터입니다. XSCF-LAN 포트를 통해 시스템 관리자는 서버를 구성하고 XSCF 쉘 또는 XSCF 웹을 사용하여 서버 상태를 볼 수 있습니다. 2개 XSCF-LAN 포트를 사용할 수 있습니다. 두 포트 모두 RJ-45 커넥터를 사용합니다. 이 포트는 10Base-T, 100Base-TX 및 1000Base-T를 지원합니다.

- USB 포트
  USB 장치와 연결하도록 1개 USB 포트(유형-A)가 전면 패널에 있고 2개 USB 포트가 후면 패널에 있습니다.
  DVD 장치를 USB 포트 가운데 하나에 연결하여 Oracle Solaris를 설치하는 등의 목적에 이 USB 포트를 사용합니다. 후면 패널의 XSCF 전용 USB 포트는 USB1.1 인터페이스를 지원하며 XSCF 하드웨어 정보를 저장 및 복원하고 로그 정보를 수집하는 데 사용됩니다.

- 서비스 프로세서 간 통신 포트(SSCP 포트)
  빌딩 블록으로 구성된 다중 XSCF 시스템의 경우 SSCP 구현을 위해 다음 커넥터(포트)가 SPARC M10-4S 캐비닛 및 크로스바 박스 각각에 장착되어 있습니다. SSCP 케이블 연결과 관련된 자세한 내용은 『SPARC M10 시스템 설치 안내서』의 "4장 빌딩 블록 연결 구성"을 참조하십시오.

  - SPARC M10-4S측
    XSCF DUAL 제어 포트: 1. 마스터 및 스탠바이 XSCF를 연결합니다.
    XSCF BB 제어 포트: 3. 마스터 및 스탠바이 XSCF를 슬레이브 XSCF에 연결합니다.
  - 크로스바 박스측
    XSCF DUAL 제어 포트: 1. 마스터 및 스탠바이 XSCF를 연결합니다.
    XSCF BB 제어 포트: 19. 마스터 및 스탠바이 XSCF를 슬레이브 XSCF에 연결합니다.

- LED
  다음 LED는 XSCF 및 XSCF-LAN과 관련됩니다.

  - READY LED
    READY LED는 녹색으로 켜집니다. 입력 전원이 켜지면 READY LED가 점멸됩니다. 점멸은 XSCF가 활성화 및 초기화 중임을 나타냅니다. XSCF 초기화가 끝나면 LED가 점멸을 멈추고 켜짐 상태를 유지합니다.
  - CHECK LED
    CHECK LED는 황갈색으로 켜집니다. 서버 입력 전원이 켜진 직후 CHECK LED가 켜집니다. XSCF가 정상적으로 실행되는 동안 CHECK LED가 꺼짐 상태로 유지됩니다. XSCF에서 오류 또는 고장이 발생하는 경우 켜집니다. XSCF 쉘 명령은 CHECK LED가 점멸되도록 할 수 있습니다. 시스템에 오류 또는 고장이 없더라도 CHECK LED로 빌딩 블록 및/또는 크로스바 박스를 식별할 수 있습니다.
  - MASTER LED(SPARC M10-4S 시스템에만 해당)
    MASTER LED는 녹색으로 켜집니다. MASTER LED는 2개 이상의 XSCF가 장착된 SPARC M10-4S 시스템에서 마스터 XSCF가 위치한 캐비닛 또는 크로스바 박스를 나타냅니다. 이는 마스터 XSCF에서 켜지고 스탠바이 XSCF 및 슬레이브 XSCF에서는 꺼짐 상태로 유지됩니다.
  - 링크 속도 LED

링크 속도 LED는 XSCF-LAN 포트에서 구현되며 녹색 또는 황갈색으로 켜집니다. 링크 속도 LED는 1,000Mbps LAN 연결에서 황갈색으로 켜지고 100Mbps LAN 연결에서는 녹색으로 켜집니다. 이 LED는 10Mbps LAN 연결에서는 켜지지 않습니다.

- ACT LED
  ACT LED는 XSCF-LAN 포트에서 구현되며 녹색으로 켜집니다. 이는 통신이 링크 업 상태에 있는 동안 켜짐 상태로 유지되고 통신이 링크 다운 상태에 있는 동안에는 꺼짐 상태로 유지됩니다. 또한 이 LED는 LAN 연결이 설정되고 데이터가 전송되는 동안 점멸됩니다. 따라서 빈번히 켜지고 켜질 때 LED가 점멸되는 것으로 나타납니다.

물리 분할(PPAR) 및 시각화 제어

XSCF는 캐비닛별로 CPU, 메모리 및 I/O 시스템 자원을 관리합니다. 시스템에 빌딩 블록 구성이 있는 경우 XSCF는 1개 빌딩 블록 캐비닛(1 BB)을 1개 논리적 시스템 보드(PSB)로 간주하고 1개 이상의 시스템 보드를 물리 분할(PPAR)이라고 하는 1개 가상 블록으로서 구성합니다.

XSCF는 시스템 전체를 물리 분할로 나누어 경우에 따라 필요한 시스템 자원에만 전원을 공급하고 시스템 보드를 추가/제거하거나 시스템 보드를 물리 분할 사이에서 이동합니다. 이는 시스템 자원의 효율적인 적용에 사용됩니다.

하이퍼바이저를 통해 논리 도메인과의 연결

SPARC M10-4S 시스템의 경우 최대 16개 물리 분할까지 구성할 수 있습니다. 물리 분할의 시스템 자원은 논리 도메인에 사용됩니다. Oracle VM Server for SPARC 소프트웨어를 통한 관리로 2개 이상의 논리 도메인을 구성할 수 있습니다. 논리 도메인의 상태를 관리하도록 하이퍼바이저 펌웨어가 각 물리 분할마다 있습니다. 하이퍼바이저 펌웨어와의 연결을 통해 XSCF 펌웨어는 논리 도메인이 사용하는 메모리, CPU 및 I/O 자원을 모니터링합니다.

1.2.3 XSCF 기능

XSCF 쉘 및 XSCF 웹

XSCF는 사용자가 서버 상태를 보고 서버를 작동하며 물리 분할의 상태를 보고 분할을 작동하며 콘솔을 표시할 수 있도록 하는 XSCF 쉘과 XSCF 웹을 제공합니다.

시스템 초기화 및 초기 진단

XSCF는 입력 전원이 켜지거나 XSCF가 재설정될 때 초기 자가 진단을 수행하여 오류를 찾아내며 오류가 있을 때 이를 사용자에게 알립니다. XSCF는 초기 하드웨어 설정을 구성하고 Oracle Solaris를 활성화하는 데 필요한 하드웨어를 초기화하기도 합니다.

시스템 구성 인식 및 물리 분할 구성 관리

XSCF는 시스템 구성의 상태를 표시하고 물리 분할 구성의 정의를 생성 및 변경합니다. XSCF는 XSCF가 주로 제어하는 논리 도메인 활성화/비활성화 기능을 제공하기도 합니다.
SPARC M10 시스템의 경우 사용자는 CPU, 메모리 및 I/O 장치로 구성된 1개 시스템 보

드(PSB)로 물리 분할을 구성할 수 있습니다.

사용자는 물리 분할과 물리 분할로부터 참조할 수 있는 수의 논리적 시스템 보드(LSB)를 PSB에 할당하여 물리 분할 구성을 관리할 수 있습니다.

Oracle VM Server for SPARC 관리에서 1개 이상의 논리 도메인을 1개 물리 분할에 할당합니다.

노트 - SPARC M10-1/M10-4 시스템에는 물리 분할 구성 관리 기능을 사용할 수 없습니다. SPARC M10-1/M10-4 시스템은 1개 또는 4개 CPU가 장착된 1개 PSB로만 구성되며 1개 물리 분할에서만 실행됩니다.

고장 최소화 및 RAS 기능에 대한 모니터링

XSCF는 배치 서버 제어 및 모니터링을 수행하여 시스템이 안정되게 작동하도록 합니다. 시스템 고장이 감지되면 이는 즉시 하드웨어 로그 수집을 시작하여 분석하고 고장 위치를 식별하며 고장 상태를 결정합니다. XSCF는 서버 상태를 표시하고 필요에 따라 부품의 성능 저하, 물리 분할의 성능 저하 및 시스템 재설정을 수행하여 또 다른 고장의 발생을 방지합니다. XSCF는 시스템 전체의 높은 신뢰성, 가용성 및 유용성(RAS)을 보장합니다.

XSCF는 다음과 같이 모니터링을 수행합니다.

- 하드웨어 구성을 모니터링 및 관리합니다.
- 네트워크 구성을 모니터링합니다.
- 팬 장치와 같은 냉각 장치 및 주변 온도를 모니터링합니다.
- 물리 분할 및 논리 도메인의 상태를 모니터링합니다.
- 주변 장치의 전원 공급/차단과 이 장치의 오류/고장을 모니터링합니다.

시스템 관리자에게 고장 정보 알림 기능

XSCF는 항상 시스템 작동을 모니터링합니다. XSCF는 캐비닛 내부 네트워크 기능으로 서버에 액세스하여 다음을 수행합니다.

- Oracle Solaris가 실행되지 않는 동안 그 상태에 대한 서버 모니터링 기능 서비스를 제공합니다.
- 원격지에서 서버를 원격 제어할 수 있도록 합니다.
- 발생한 고장 보고서를 지정된 이메일 주소로 전송합니다.
- SNMP 에이전트 기능을 사용하여 트랩 알림을 생성합니다.

메시징 및 로깅

XSCF는 시스템 고장 관련 정보를 수집하여 저장합니다. 하드웨어 고장 정보의 경우 오류 및 고장 위치가 식별되고 사용자를 위해 서버 고장 예측 및 고장 정보가 즉시 올바르면서도 이해가 쉽도록 제공됩니다. 오류 메시지 및 로깅된 메시지와 관련된 자세한 내용은 "17장 로그 및 메시지 확인"을 참조하십시오.

다음 유형의 메시지가 표시됩니다.

- 시스템 활성화 시의 초기 진단 메시지

- 네트워크 구성 모니터링 시의 구성 오류 감지 메시지
- 전원 공급 장치, 팬, 시스템 보드, 메모리, CPU 및 기타 구성요소의 모니터링 시에 발견된 고장 감지 메시지
  이 정보를 통해 시스템 관리자는 즉시 교체하는 부품을 알 수 있습니다.
- 서버 온도 및 CPU 온도 모니터링 시의 온도 오류 감지 메시지
  이 유형의 메시지는 온도 상승에 따른 시스템 불안정을 방지하는 데 사용됩니다.

다음 유형의 로그가 수집됩니다.

- 오류 로그
- 모니터 메시지 로그
- 전원 로그
- 이벤트 로그
- 콘솔 로그
- 패닉 로그
- IPL 로그
- 감사 로그
- CoD 로그
- 온도 이력 로그

XSCF 사용자 계정 관리

XSCF는 XSCF를 사용하기 위한 사용자 계정을 관리합니다. XSCF가 관리하는 사용자 계정의 주요 권한 유형은 아래 나열된 바와 같습니다. 작동 가능한 XSCF 쉘 및 XSCF 웹은 사용자 계정 유형(사용자 권한이라고 함)에 따라 제공됩니다.

- 시스템 관리자
- 물리 분할(PPAR) 관리자
- 운영자
- 현장 엔지니어

보안

XSCF는 SSH/SSL에 따른 암호화 및 감사 기능을 제공합니다. 이는 시스템이 실행되는 동안 작동 오류와 유효하지 않은 액세스를 로깅합니다. 시스템 관리자는 로그를 사용하여 시스템 고장 또는 유효하지 않은 액세스의 원인을 조사할 수 있습니다.

부품 활성 교체 지원

XSCF는 부품 활성 교체 시 XSCF 쉘을 사용하여 유지 관리 작업을 지원합니다. 유지 관리 명령을 실행하면 서비스 메뉴가 표시되며 이를 통해 사용자는 메뉴에 따라 유지 관리 작업을 수행할 수 있습니다.

콘솔 리디렉션 기능

XSCF는 각 물리 분할마다 Oracle Solaris의 OS 콘솔(제어 도메인 콘솔)로 가는 출력 생성 기능을 제공합니다. 이는 SSH(보안 쉘) 또는 Telnet을 XSCF에 연결하여 OS 콘솔 역할을 할 수 있습니다.

필요 시 용량 제공 기능

필요 시 용량 제공(CoD) 기능은 서버 전용 CPU 자원을 구입할 수 있도록 합니다. 서버가 작동하려면 먼저 1개 이상 CPU에 대해 CPU 자원을 구입해야 합니다.

XSCF는 CPU의 추가 또는 감소가 필요할 때 CPU 자원의 추가 또는 삭제를 지원합니다. CoD 자원 구입과 관련된 자세한 내용은 "14장 필요 시 용량 제공(CoD)"을 참조하십시오.

펌웨어 업데이트 기능

XSCF 웹 및 XSCF 쉘 명령을 사용하여 물리 분할의 전원 차단 없이도 새 펌웨어 이미지(XSCF 펌웨어, OpenBoot PROM 펌웨어, POST 펌웨어 및 하이퍼바이저 펌웨어)를 다운로드할 수 있습니다. 또한 다른 물리 분할의 전원 차단 없이 펌웨어 업데이트를 적용할 수도 있습니다. 유의할 점으로, OpenBoot PROM 펌웨어, POST 펌웨어 및 하이퍼바이저 펌웨어의 업데이트는 물리 분할의 재부팅으로 적용합니다. 펌웨어 업데이트와 관련된 자세한 내용은 "18.1 XCP 펌웨어 업데이트"를 참조하십시오.

그린 IT 기능

Oracle Solaris, 하이퍼바이저 및 XSCF는 작동하지 않는 구성요소로의 전원 공급을 중단하고 전력 소비를 억제합니다. 또한 XSCF는 전력 소비의 허용 상한을 제어하여 시스템 전력 소비를 억제할 수도 있습니다. 상한을 초과하면 XSCF는 즉시 시스템 전원 공급 상태를 파악하여 전원을 종료 또는 차단합니다.

시간 제어

SPARC M10 시스템은 시스템 기준 시간으로서 XSCF 클록을 설정합니다. SPARC M10 시스템의 물리 분할은 물리 분할의 활성화 시에 XSCF 클록과의 시간 동기화를 수행합니다. XSCF는 하이퍼바이저 펌웨어와 함께 제어 도메인과의 시간 차이를 관리합니다.

1.2.4 마스터/슬레이브 XSCF 프레임워크

SPARC M10-4S가 빌딩 블록 시스템에 의해 연결되는 경우 각 SPARC M10-4S 캐비닛 및 각 크로스바 박스마다 1개 XSCF가 위치합니다. XSCF는 역할에 따라 2개 유형으로 분류됩니다.

- 마스터 XSCF
  마스터 XSCF는 시스템 전체를 모니터링 및 관리합니다. 시스템 전체의 모니터링 및 관리 외에 마스터 XSCF는 그 설치 위치인 SPARC M10-4S 또는 크로스바 박스를 관리하기도 합니다. 시스템에는 마스터 XSCF가 하나만 있습니다.

- 슬레이브 XSCF
  슬레이브 XSCF는 비 마스터 XSCF입니다. 슬레이브 XSCF는 그 설치 위치인 SPARC M10-4S 또는 크로스바 박스만 모니터링 및 관리합니다.

슬레이브 XSCF 가운데 하나는 마스터 XSCF의 스탠바이 XSCF로서 기능합니다. 마스터 XSCF와 스탠바이 XSCF는 서로를 모니터링합니다. 마스터 XSCF에 고장이 발생하는 경우 마스터 XSCF가 스탠바이 XSCF로 전환되어 비즈니스 중단이 없는 시스템 작동과 관리가 보장됩니다.

마스터 XSCF는 SP 대 SP 통신 프로토콜(SSCP)이라고 하는 XSCF 전용 프로토콜에 따

라 전용 케이블을 통해 슬레이브 XSCF에 연결됩니다. 마스터 XSCF에 대해 구성된 설정이 SSCP를 통해 슬레이브 XSCF에 반영됩니다. 특정 물리 분할에 대해 구성된 설정은 대상 PPAR에 속한 XSCF에만 반영됩니다.

1.2.5 모델 간의 XSCF 구성 차이

이 절에는 SPARC M10 시스템의 각 모델 구성에서 XSCF의 구성 방법과 시스템의 모니터링 및 관리 방법이 설명되어 있습니다.

단일 장치 구성의 SPARC M10-1/M10-4 및 SPARC M10-4S

단일 장치 구성의 SPARC M10-1/M10-4 및 SPARC M10-4S는 XSCF를 하나만 사용합니다. 스탠바이 XSCF 또는 슬레이브 XSCF는 구현되지 않습니다.

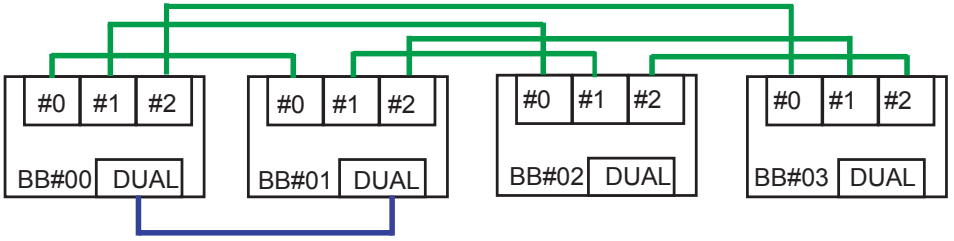
빌딩 블록 구성의 SPARC M10-4S(크로스바 박스 없음)

빌딩 블록 구성의 SPARC M10-4S(크로스바 박스 없음)는 최대 4개의 SPARC M10-4S 캐비닛으로 구성되어 이에 따라 XSCF가 최대 4개까지 구성됩니다. 이 구성에서 BB#00 캐비닛은 마스터 XSCF 역할을 하고 BB#01 캐비닛은 스탠바이 XSCF 역할을 합니다. 마스터 XSCF에서 오류가 발생하면 스탠바이 XSCF가 마스터 XSCF로 전환됩니다. BB#02 및 BB#03 캐비닛은 슬레이브 XSCF로서 안정적으로 고정됩니다.

- 연결 모드
  마스터 XSCF(BB#00)는 각 슬레이브 XSCF의 네트워크 ID가 0인 XSCF BB 커넥터(그림 1-6에서 BB#01 ~ BB#03의 #0 포트)에 연결됩니다. 스탠바이 XSCF(BB#01)는 각 슬레이브 XSCF의 네트워크 ID가 1인 XSCF BB 커넥터(그림 1-6에서 BB#02 및 BB#03의 #1 포트)에 연결됩니다. 마스터 XSCF 및 스탠바이 XSCF는 그 이름이 DUAL인 전용 포트를 통해 연결됩니다. 슬레이브 XSCF는 마스터 XSCF 및 스탠바이 XSCF에만 연결됩니다.

- XSCF 제어 흐름
  마스터 XSCF는 모든 XSCF를 모니터링 및 관리합니다. XSCF의 설정은 원칙적으로 마스터 XSCF에서 구성됩니다. 마스터 XSCF에 의해 구성된 설정은 SSCP 네트워크를 통해 스탠바이 XSCF를 포함한 모든 XSCF에 반영됩니다. 특정 SPARC M10-4S 캐비닛의 설정 또한 대상인 SPARC M10-4S 캐비닛의 스탠바이 XSCF 및 슬레이브 XSCF에 반영됩니다.

그림 1-6 XSCF 연결(빌딩 블록 구성의 SPARC M10-4S(크로스바 박스 없음))

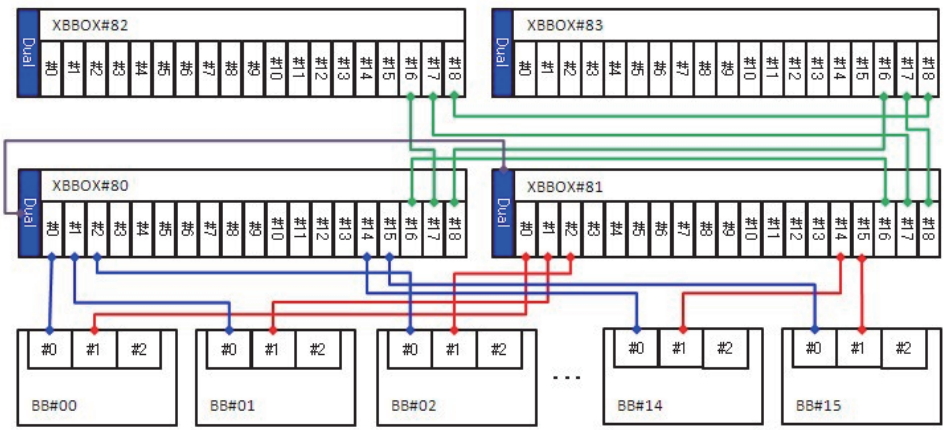


빌딩 블록 구성의 SPARC M10-4S(크로스바 박스 있음)

빌딩 블록 구성의 SPARC M10-4S(크로스바 박스 있음)는 최대 16개 XSCF로 구성됩니다. 이 구성에서 XBBOX#80 크로스바 박스의 XSCF는 마스터 XSCF로서 구성되고 XBBOX#81 크로스바 박스의 XSCF는 스탠바이 XSCF로서 구성됩니다. XBBOX#82 및 XBBOX#83 크로스바 박스와 모든 SPARC M10-4S 캐비닛의 XSCF는 슬레이브 XSCF에 안정적으로 고정됩니다.

- 연결 모드
  - 크로스바 박스에 연결:
    마스터 XSCF(XBBOX#80)는 각 슬레이브 XSCF의 네트워크 ID가 16인 XSCF BB 커넥터(그림 1-7에서 XBBOX#81 ~ XBBOX#83의 #16 포트)에 연결됩니다. 스탠바이 XSCF(XBBOX#81)는 각 슬레이브 XSCF의 네트워크 ID가 17인 XSCF BB 커넥터(그림 1-7에서 XBBOX#82 및 XBBOX#83의 #17 포트)에 연결됩니다. 슬레이브 XSCF에 고정된 XSCF(XBBOX#82 및 XBBOX#83)는 네트워크 ID#18의 상호 XSCF BB 커넥터(그림 1-7에서 XBBOX#82 및 XBBOX#83의 #18 포트)에 연결됩니다. 마스터 XSCF 및 스탠바이 XSCF는 그 이름이 DUAL인 전용 포트를 통해 연결됩니다. 슬레이브 XSCF는 마스터 XSCF 및 스탠바이 XSCF를 제외한 모든 XSCF에 연결되지 않습니다.
  - SPARC M10-4S에 연결:
    마스터 XSCF(XBBOX#80)는 각 슬레이브 XSCF의 네트워크 ID가 0인 XSCF BB 커넥터(그림 1-7에서 BB#00 ~ BB#15의 #0 포트)에 연결됩니다. 스탠바이 XSCF(XBBOX#81)는 각 슬레이브 XSCF의 네트워크 ID가 1인 XSCF BB 커넥터(그림 1-7에서 BB#00 ~ BB#15의 #1 포트)에 연결됩니다. 슬레이브 XSCF는 마스터 XSCF 및 스탠바이 XSCF에만 연결됩니다. 슬레이브 XSCF에 고정된 XSCF(BB#00 ~ BB#15)는 마스터 XSCF 및 스탠바이 XSCF에만 연결됩니다.
- XSCF 제어 흐름
  마스터 XSCF는 모든 XSCF를 모니터링 및 관리합니다. XSCF의 설정은 원칙적으로 마스터 XSCF에서 구성됩니다. 마스터 XSCF에 의해 구성된 설정은 SSCP 네트워크를 통해 스탠바이 XSCF를 포함한 모든 XSCF에 반영됩니다. 특정 SPARC M10-4S 캐비닛의 설정 또한 대상인 SPARC M10-4S 캐비닛의 스탠바이 XSCF 및 슬레이브 XSCF에 반영됩니다.

그림 1-7 XSCF 연결(빌딩 블록 구성의 SPARC M10-4S(크로스바 박스 있음))



1.3 하이퍼바이저의 기본 정보

이 절에는 SPARC M10 시스템에 장착된 하이퍼바이저 펌웨어의 요약이 설명되어 있습니다.

하이퍼바이저 펌웨어는 시각화를 구현합니다. 이는 CPU 메모리 장치에 장착됩니다.

SPARC M10 시스템의 경우 논리 도메인에 설치된 시스템 전체와 Oracle Solaris를 모니터링 및 관리하는 XSCF 펌웨어와 같은 다양한 소프트웨어와 펌웨어가 실행됩니다. XSCF 펌웨어와 Oracle Solaris 사이 중간에 위치한 하이퍼바이저 펌웨어는 인터페이스로서 기능하여 XSCF에서 논리 도메인으로 설정 정보를 게시하고 XSCF에 논리 도메인의 상태를 알려줍니다.

하이퍼바이저 펌웨어의 주요 기능은 아래 설명된 바와 같습니다.

- XSCF가 관리하는 물리 분할과 Oracle VM Server for SPARC가 관리하는 논리 도메인 간의 정보 전송
  XSCF에서 제어 도메인으로 게시한 PPAR 구성 정보(PCL)에 따라 Oracle VM Server for SPARC는 논리 도메인을 구성합니다. 또한 논리 도메인 구성 정보와 재구성된 하드웨어 자원 정보도 하이퍼바이저를 통해 XSCF 펌웨어로 게시됩니다.
- 논리 도메인의 끊김 또는 장애와 관련된 정보 전송
  논리 도메인에 끊김 또는 장애가 발생하는 경우 하이퍼바이저는 논리 도메인의 상태를 XSCF로 게시합니다.
- XSCF 및 논리 도메인 날짜/시간과 관련된 정보 전송
  논리 도메인에 구성된 시간이 하이퍼바이저에 의해 XSCF로 게시됩니다. XSCF는 논리 도메인의 시간을 구성된 시간과의 차이로서 시스템 전체에 저장합니다.

1.4 Oracle VM Server for SPARC의 기본 정보

이 절에는 Oracle VM Server for SPARC 소프트웨어의 요약이 설명되어 있습니다.

Oracle VM Server for SPARC 소프트웨어는 논리 도메인 환경을 구성하는 데 사용됩니다. 이는 Oracle Solaris 환경에 설치되어 사용됩니다.

논리 도메인은 XSCF 펌웨어가 구성하는 물리 분할의 CPU, 메모리 및 I/O 장치와 같은 하드웨어 자원을 유연하게 분산하고 가상 하드웨어 환경으로서 자원을 할당하여 구성합니다. 구성된 각 논리 도메인에서 Oracle Solaris가 설치되어 비즈니스 응용 프로그램 소프트웨어를 실행합니다. 1개 SPARC M10 시스템에서 2개 이상의 가상 하드웨어 환경을 구성하면 이러한 서버 통합에 따른 서버 가용성 향상과 비용 절감이 구현됩니다.

일반적인 논리 도메인은 다른 논리 도메인과 비즈니스 운영 용도의 게스트 도메인을 제어하는 데 전용인 제어 도메인입니다. SPARC M10 시스템의 경우 물리 분할에 구성된

다른 논리 도메인을 관리하도록 1개 제어 도메인이 물리 분할에 의해 구성됩니다. 제어 도메인에서 실행되는 Oracle VM Server for SPARC는 게스트 도메인을 구성 및 관리하는 데 사용됩니다.
제어 도메인은 펌웨어로서 장착된 하이퍼바이저를 통해 논리 도메인 정보를 XSCF 펌웨어에 알려주는 역할을 하기도 합니다. 하이퍼바이저 펌웨어를 통해 XSCF에서 제어 도메인으로 설정 정보가 게시되기도 합니다.

논리 도메인이 구성되어 비즈니스 운영에 사용되었더라도 논리 도메인의 작동 상태에 따라 CPU, 메모리, I/O 장치 및 기타 하드웨어 자원을 재구성할 수 있습니다. 하드웨어 자원 재구성은 Oracle VM Server for SPARC에 의해서도 구현됩니다. 일시적 부하 증가를 일으키는 비즈니스에 하드웨어 자원을 추가하면 하드웨어 자원 가용성이 높아지고 비즈니스 작업의 오버플로가 방지될 수 있습니다.

SPARC M10 시스템에서 Oracle VM Server for SPARC를 사용한 논리 도메인의 구성 및 재구성은『SPARC M10 시스템 도메인 구성 안내서』를 참조하십시오. Oracle VM Server for SPARC와 관련된 자세한 내용은 사용 버전의『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

1.5 OpenBoot PROM의 기본 정보

이 절에는 OpenBoot PROM의 요약이 설명되어 있습니다.

OpenBoot PROM은 Oracle Solaris 활성화에 필요한 기본 기능을 제공합니다.

OpenBoot PROM 환경에서 ok 프롬프트가 콘솔 화면에 표시됩니다. OpenBoot PROM 환경 변수의 정의로 Oracle Solaris 활성화 기능을 구성할 수 있습니다. OpenBoot PROM 환경 변수는 다음 명령 가운데 하나로 정의할 수 있습니다.

- OpenBoot PROM 환경에서 setenv 명령을 실행(ok 프롬프트 시)
- Oracle Solaris 환경에서 eeprom 명령을 실행

OpenBoot PROM 환경 변수를 설정하려면 XSCF 펌웨어 setpparparam 명령을 사용합니다.
setpparparam 명령의 자세한 내용은 setpparparam(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

2장

시스템 연결 구성 이해

이 장에는 시스템 작동을 위한 네트워크 연결 이미지와 시스템 관리를 위한 터미널 연결 구성이 설명되어 있습니다.

- 개념적 시스템 연결 이미지
- 시스템 관리 터미널 연결

2.1 개념적 시스템 연결 이미지

이 절에는 시스템 작동을 위한 네트워크 연결 개요가 설명되어 있습니다.

시스템은 2개 주요 네트워크로 구성되어 있습니다. 하나는 사용자 네트워크이고 다른 하나는 시스템 제어 네트워크입니다.

- 사용자 네트워크
  사용자 네트워크는 비즈니스를 위해 구성된 시스템을 적용하는 데 사용됩니다. 사용자 네트워크는 비즈니스에 필요한 다른 서버, PC 및 주변 장치에 연결됩니다.

  해당 시 방화벽 또는 기타 안전 조치가 적용됨에 따라 사용자 네트워크는 외부 인터넷에 연결 가능한 보안 네트워크 환경을 구성할 수 있습니다.

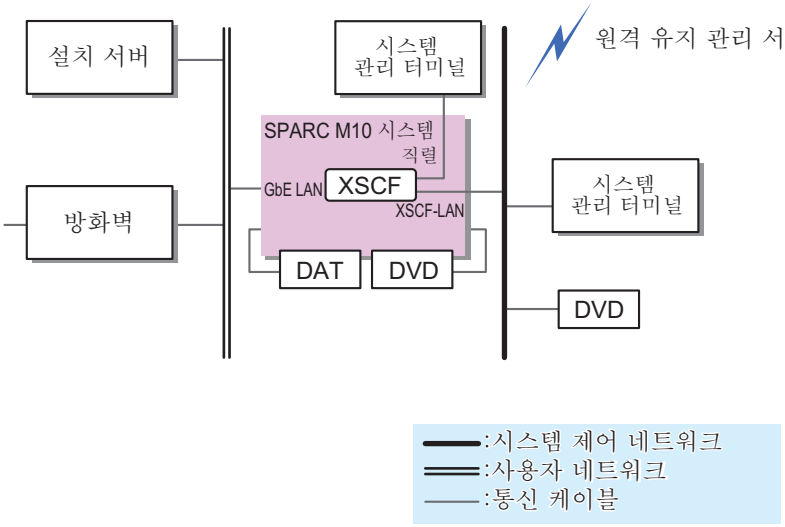
- 시스템 제어 네트워크
  시스템 제어 네트워크는 시스템의 유지 관리에 사용됩니다. 이 네트워크는 시스템의 모니터링 및 관리 용도인 XSCF 펌웨어를 작동하는 데 사용됩니다. 이 네트워크는 전원 공급/차단, 구성요소 교체 작업 및 기타 시스템 처리에도 사용됩니다. 원격 시스템 모니터링 작동의 구현을 위해 시스템 제어 네트워크의 설정 환경이 구성됩니다.

  시스템 제어 네트워크는 방화벽과 같은 보안 조치를 취해 시스템 제어 네트워크의 유효하지 않은 외부 액세스를 방지하도록 사용자 네트워크에 연결될 수도 있습니다.

  시스템 유지 관리에 사용되는 터미널(시스템 관리 터미널)은 상황에 따라 직렬 또는 LAN 연결이 가능합니다. 시스템 관리 터미널 연결은 "2.2 시스템 관리 터미널 연결"을 참조하십시오.

다음에는 각 시스템 구성의 연결 이미지가 나타나 있습니다.

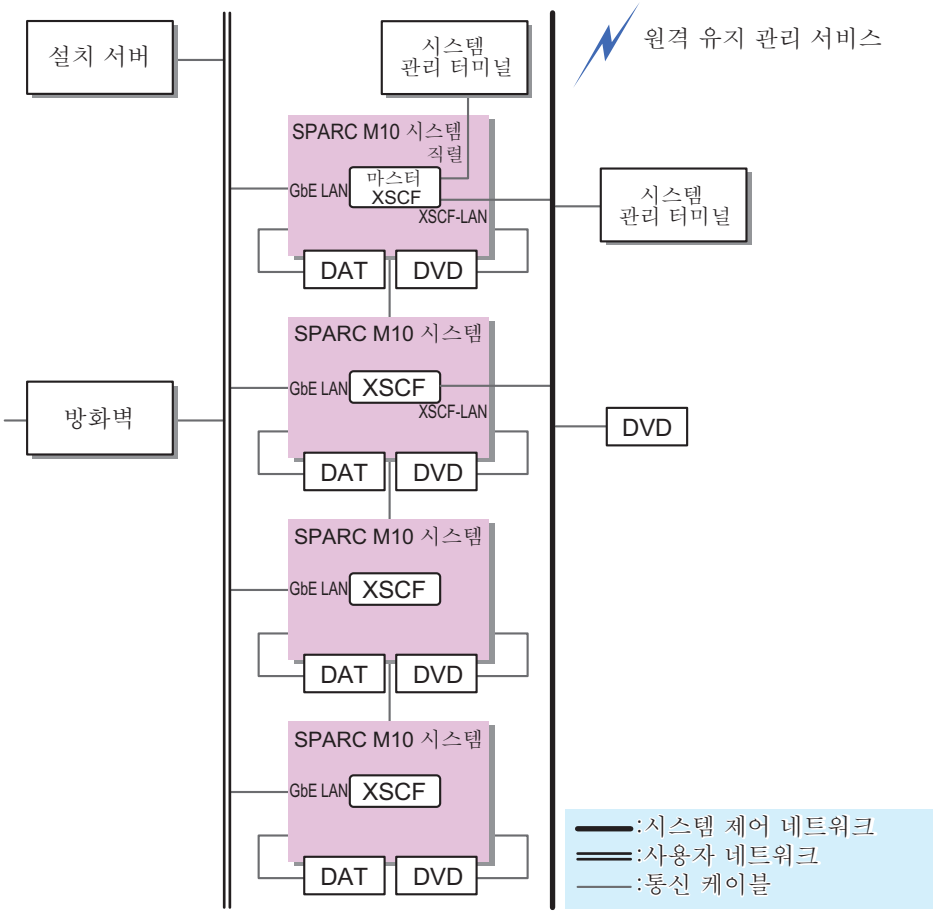
그림 2-1 SPARC M10-1/M10-4/M10-4S용 1개 캐비닛 구성의 연결 이미지



이는 1개 SPARC M10-1/M10-4/M10-4S 캐비닛의 활용 이미지입니다.

직렬 포트 또는 XSCF-LAN 포트를 통해 시스템 제어 네트워크에 연결되고 GbE LAN 포트를 통해 사용자 네트워크에 연결됩니다. 또한 SAS 포트와 DAT가 연결되고 외부 DVD 연결을 위한 USB 포트와 DVD가 연결됩니다.

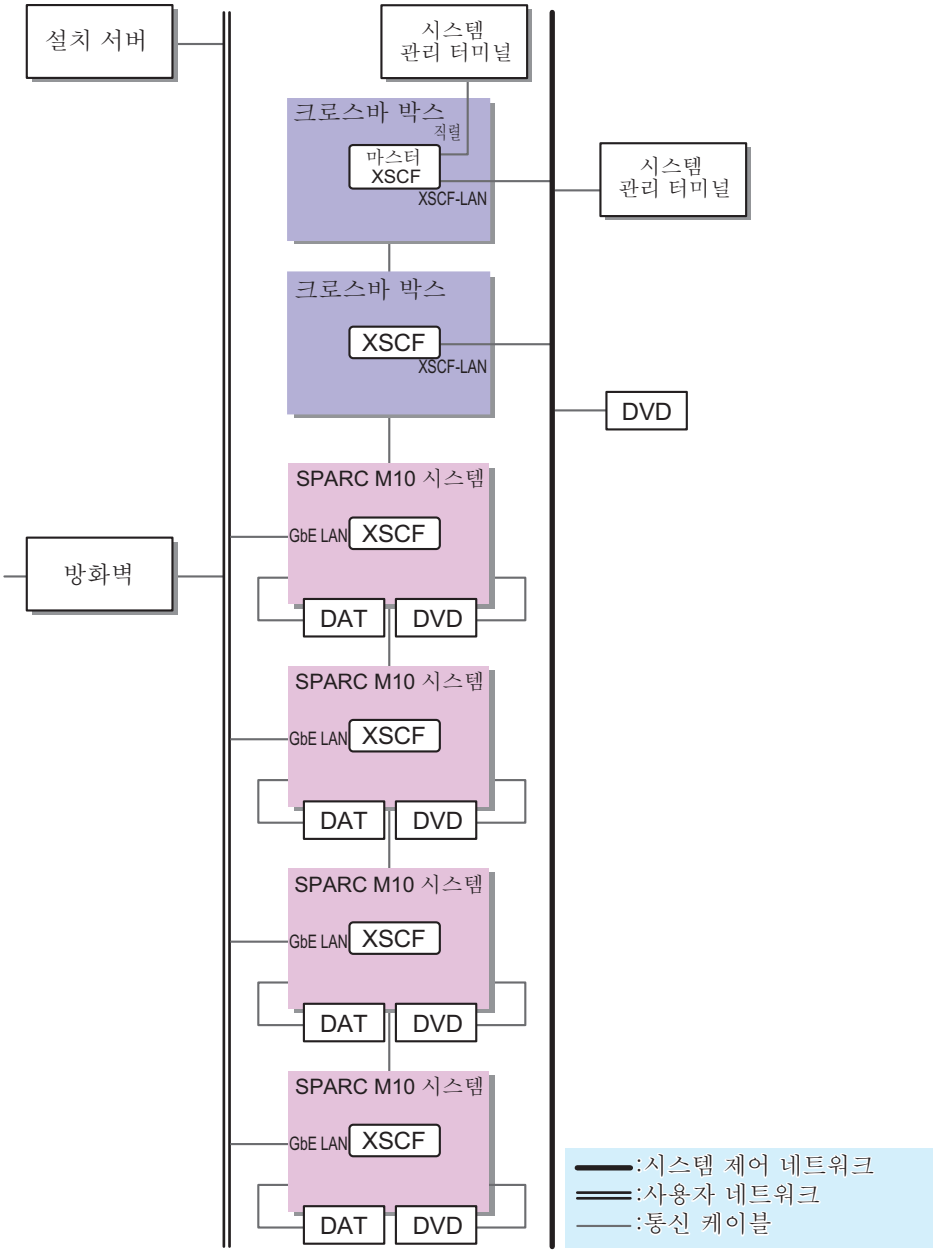
그림 2-2 SPARC M10-4S 연결 이미지(크로스바 박스 없음)



이 이미지에는 전기 케이블로 연결된 4개 SPARC M10-4S 캐비닛의 활용이 나타나 있습니다.

마스터 XSCF는 직렬 포트 또는 XSCF-LAN 포트를 통해 시스템 제어 네트워크에 연결되고 4개 캐비닛의 GbE LAN 포트를 통해 사용자 네트워크에 연결됩니다. 또한 SAS 포트와 DAT가 연결되고 외부 DVD 연결을 위한 USB 포트와 DVD가 연결됩니다.

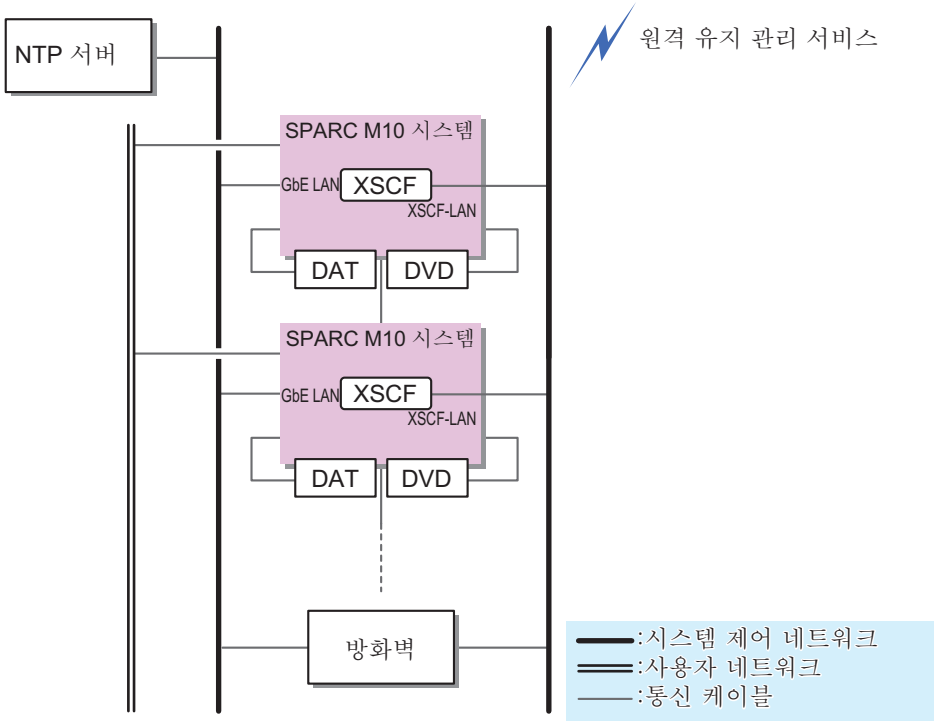
그림 2-3 SPARC M10-4S 연결 이미지(크로스바 박스 있음)



이 이미지에는 크로스바 박스를 통해 광 케이블로 연결된 2개 이상 SPARC M10-4S 캐비닛의 활용이 나타나 있습니다.

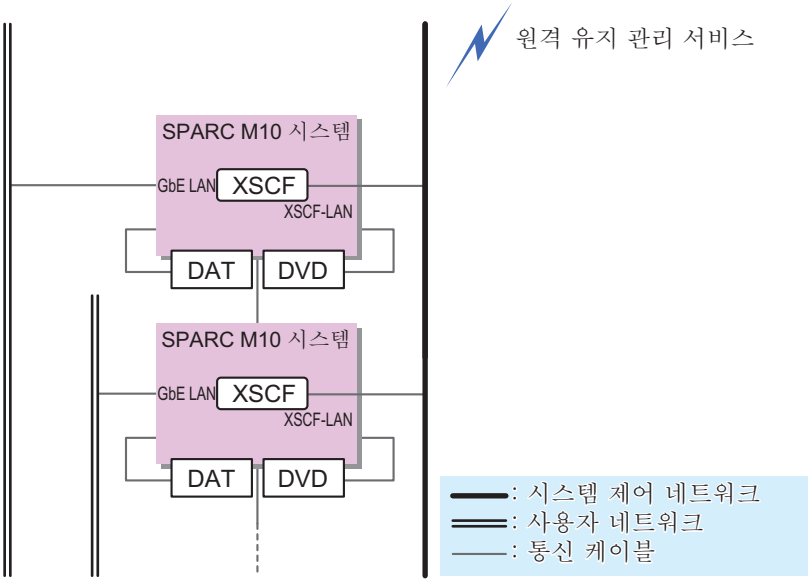
크로스바 박스의 마스터 XSCF는 직렬 포트 또는 XSCF-LAN 포트를 통해 시스템 제어 네트워크에 연결되고 SPARC M10-4S 캐비닛의 GbE LAN 포트 및 크로스바 박스를 통해 사용자 네트워크에 연결됩니다. 또한 SAS 포트와 DAT가 연결되고 외부 DVD 연결을 위한 USB 포트와 DVD가 연결됩니다.

그림 2-4 시스템 제어 네트워크가 인터넷에 연결된 구성



이는 GbE LAN 포트를 통해 사용자 네트워크와 다른 네트워크에 연결하기 위한 구성입니다. 예를 들어 NTP 서버를 사용하여 시간을 조절하는 경우 이 네트워크를 통해 NTP 서버에 연결됩니다. 이 구성의 경우 XSCF-LAN 포트를 통해 라우팅된 시스템 제어 네트워크에 방화벽을 설정하면 XSCF가 도메인으로부터 보호됩니다.

그림 2-5 사용자 네트워크가 분리된 구성



이 구성의 경우 대상 사용자 네트워크가 각 SPARC M10-4S마다 분리됩니다. 이 구성 유형은 각 도메인마다 보안을 보장할 수 있습니다.

2.2 시스템 관리 터미널 연결

이 절에는 시스템 제어 네트워크에서의 시스템 관리 터미널 연결 구성이 설명되어 있습니다. 실제 연결 방법은 "4.1.1 직렬 연결을 위한 터미널 및 작업"을 참조하십시오.

시스템 제어 네트워크는 연결된 사용되는 포트에 따라 다음 2개 연결 구성으로 분류됩니다.

- 직렬 연결
  직렬 케이블이 직렬 포트에 연결됩니다.
- LAN 연결
  LAN 케이블이 XSCF-LAN 포트에 연결됩니다.

시스템 관리 터미널은 대개 XSCF 펌웨어 초기 설정을 구성하도록 직렬 포트에 연결됩니다. XSCF 네트워크 설정 구성을 마쳤으면 직렬 연결 또는 LAN 연결을 선택할 수 있습니다.

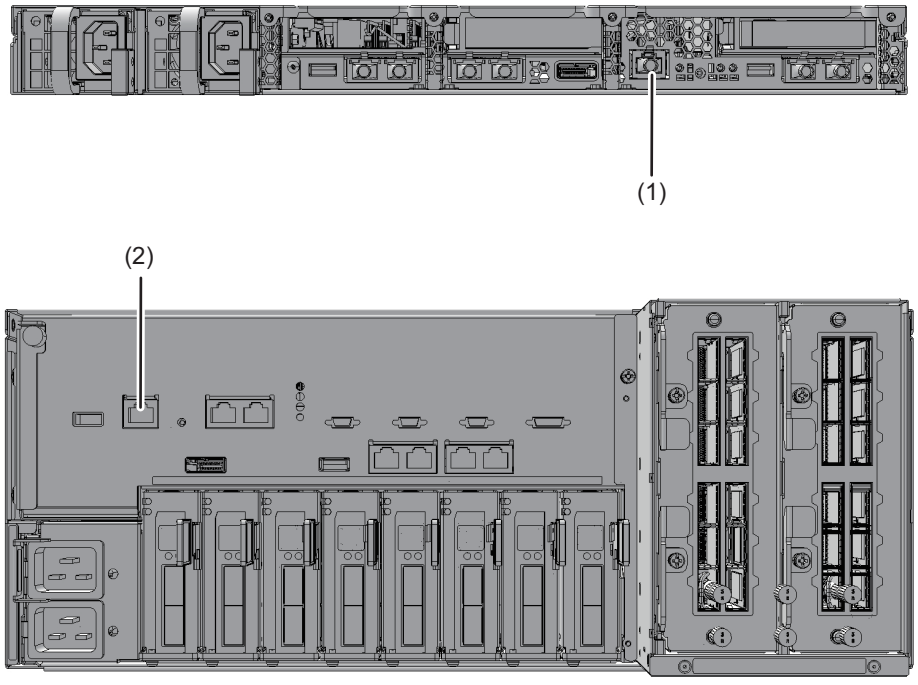
후속 절에는 연결 구성의 특징이 설명되어 있습니다.

2.2.1 직렬 포트를 통한 연결

직렬 연결은 서버에서 구현된 직렬 포트가 연결되는 연결 구성입니다. 빌딩 블록 구성

의 M10-4S인 경우 마스터 XSCF가 위치하는 캐비닛에 연결됩니다. 시스템 관리 터미널과 마스터 XSCF는 보안 환경에서 1대1로 연결됩니다. 시스템 관리 터미널로 직렬 연결이 설정된 경우 마스터 XSCF로의 로그인 화면이 표시됩니다.

그림 2-6 SPARC M10 시스템의 직렬 포트



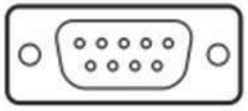
번호	구성요소
1	직렬 포트(SPARC M10-1)
2	직렬 포트(SPARC M10-4/M10-4S)

XSCF에 로그인하면 XSCF 쉘을 사용할 수 있습니다. XSCF 명령을 실행하여 시스템을 모니터링 및 관리할 수 있습니다. 논리 도메인을 모니터링 및 관리해야 하는 경우 XSCF 쉘을 제어 도메인 콘솔로 전환할 수 있습니다. 전환 방법은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

직렬 연결에는 아래 설명된 준비가 필요합니다.

- 직렬 케이블의 준비
  제공된 D-Sub 9핀 RS-232C 케이블을 곁에 준비합니다. 터미널에 사용 가능한 직렬 포트가 없는 경우 RJ-45/RS-232C 변환 케이블 또는 변환 커넥터를 사용해야 합니다.

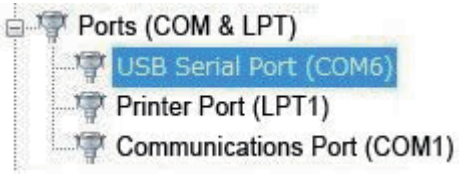
그림 2-7 RC232C D-Sub 9핀 커넥터



- 연결용 터미널 소프트웨어의 준비
- 인식된 직렬 포트의 확인
  직렬 케이블을 터미널에 연결한 후 인식된 직렬 포트를 확인합니다. 연결할 때 인식된 직렬 포트를 연결 포트로서 지정합니다.

  다음 예에는 COM6으로서 인식된 직렬 포트가 나타나 있습니다.

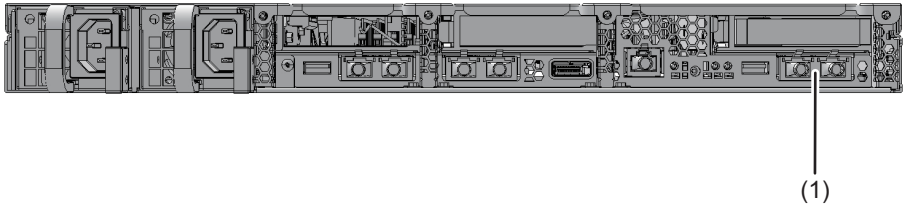
그림 2-8 직렬 포트 확인(장치 관리자를 사용)

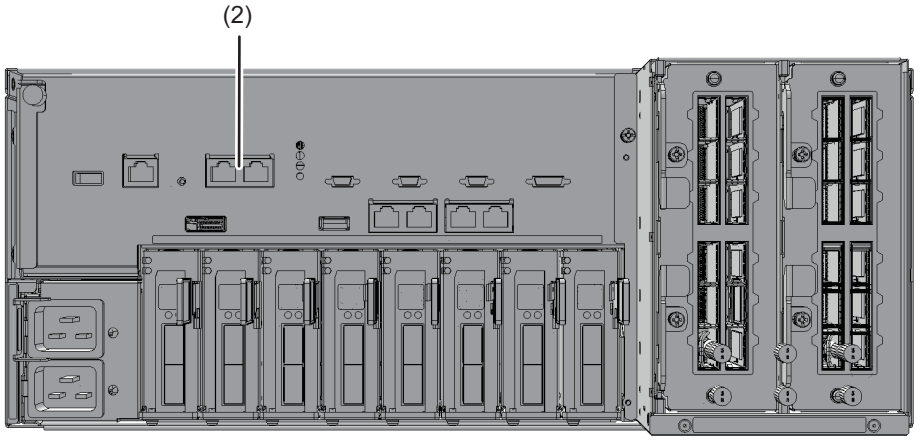


2.2.2 XSCF-LAN을 통한 연결

LAN 케이블로 XSCF-LAN 포트에 연결할 수 있습니다. 빌딩 블록 구성의 SPARC M10-4S인 경우 마스터 XSCF가 위치하는 캐비닛에 연결됩니다. LAN 케이블 연결 후 SSH 또는 Telnet을 통해 시스템 관리 터미널에 연결하면 마스터 XSCF 로그인 화면이 표시됩니다.

그림 2-9 SPARC M10 시스템의 XSCF-LAN 포트





번호	구성요소
1	XSCF-LAN 포트(SPARC M10-1)
2	XSCF-LAN 포트(SPARC M10-4/M10-4S)

XSCF-LAN으로 연결된 시스템 관리 터미널의 경우 XSCF 쉘을 사용할 수 있습니다. 또한 웹 브라우저를 구성하여 XSCF 웹을 사용할 수도 있습니다. XSCF 명령 또는 XSCF 웹을 사용하여 XSCF 설정을 구성할 수 있습니다.

XSCF 네트워크를 구성하고 XSCF-LAN을 통해 시스템 관리 터미널을 연결하면 네트워크 환경을 필요로 하는 다음 기능을 사용할 수 있습니다.

- 이메일 알림
- SNMP
- 로그 아카이브
- 원격 유지 관리 서비스
- 외부 NTP 서버 연결/동기화
- 원격 제어에 의한 XSCF 모니터링/관리

구현된 2개 XSCF-LAN 포트가 있습니다. 시스템 작동에 따라 두 포트 가운데 하나만 사용하거나 둘 모두를 사용할 수 있습니다. 예를 들어 인트라넷에 포트 하나를 사용하고 인터넷에 다른 포트 하나를 사용할 수 있습니다.

XSCF에 로그인하면 XSCF 쉘이 열립니다. XSCF 명령을 사용하여 서버를 모니터링 및 관리합니다. 논리 도메인을 모니터링 및 관리해야 하는 경우 XSCF 쉘을 제어 도메인 콘솔로 전환할 수 있습니다. 전환 방법은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

XSCF-LAN을 통한 시스템 관리 터미널 연결에는 아래 설명된 준비가 필요합니다.

- LAN 케이블의 준비
  카테고리 5 이상의 LAN 케이블이 필요합니다.
- XSCF 네트워크 구성

XSCF 네트워크, SSH, Telnet 및 기타 서비스를 구성해야 합니다. 자세한 내용은 "8.5 XSCF 네트워크 구성"을 참조하십시오.

- 웹 브라우저의 준비(XSCF 웹을 사용하는 경우)
  XSCF 웹을 지원하는 웹 브라우저를 준비합니다. XSCF 웹을 지원하는 웹 브라우저는 최신『제품 노트』를 참조하십시오.
- 연결용 터미널 소프트웨어의 준비

3장

시스템 시작/정지

이 장에는 SPARC M10 시스템의 시작 및 정지 시퀀스와 작동 방법이 설명되어 있습니다.

- 시스템 시작
- 시스템 정지
- 시스템 재설정

3.1 시스템 시작

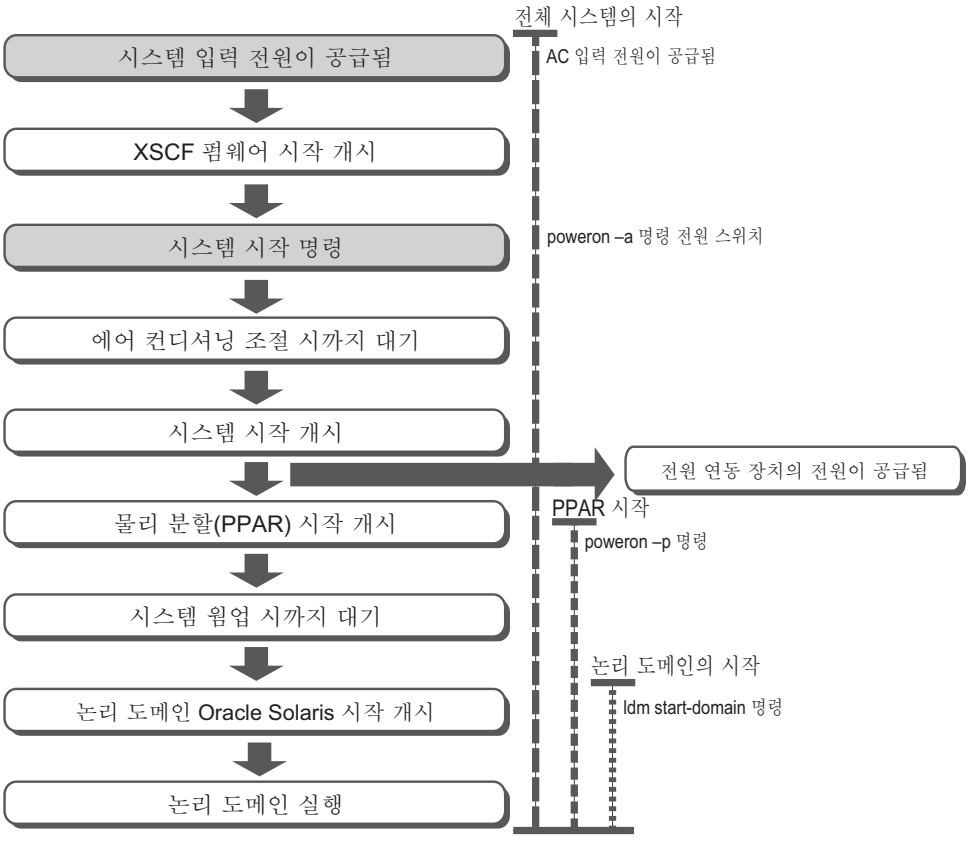
이 절에는 시스템 시작 흐름과 작동 방법이 설명되어 있습니다.

3.1.1 입력 전원 공급부터 시스템 시작까지 흐름

이 절에는 전원 공급부터 논리 도메인 시작까지 흐름이 설명되어 있습니다.

시스템 전체의 시작에 사용되는 명령, 물리 분할의 시작에 사용되는 명령 및 논리 도메인의 시작에 사용되는 명령이 유효 범위와 함께 설명되어 있습니다.
후속 절에는 단계별 시작 절차가 설명되어 있습니다.

그림 3-1 입력 전원 공급부터 시스템 시작까지 흐름



3.1.2 시스템 전체의 시작

아래 설명된 방법을 사용하여 시스템 전체를 시작할 수 있습니다. 마스터 XSCF 캐비닛에서 다음 방법 가운데 하나를 수행합니다.

- 운영 패널의 POWER 스위치를 사용
- XSCF 펌웨어의 poweron 명령을 사용

POWER 스위치의 사용

마스터 XSCF가 구성된 캐비닛에서 운영 패널의 POWER 스위치를 누릅니다. POWER 스위치를 누르면 해당 순서에 따라 시스템의 모든 물리 분할로 전원 공급이 시작됩니다. 그런 다음 해당 순서에 따라 물리 분할의 모든 논리 도메인이 시작됩니다.

노트 - 마스터 XSCF 캐비닛의 POWER 스위치만 작동할 수 있습니다. 다른 캐비닛의 POWER 스위치는 전원 공급 기능을 하지 않습니다.

노트 - XSCF 펌웨어 setpparparam 명령에 의해 자동 부팅이 억제되는 제어 도메인이 있는 경우 제어 도메인이 시작되지 않습니다. 또한 setpparmode 명령에 의해 자동 부팅이 억제되는 물리 분할 및/또는 논리 도메인이 있는 경우 논리 도메인이 시작되지 않습니다. setpparparam 및 setpparmode 명령의 자세한 내용은 setpparparam(8) 및 setpparmode(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

마스터 XSCF 캐비닛은 모델에 따라 다릅니다.

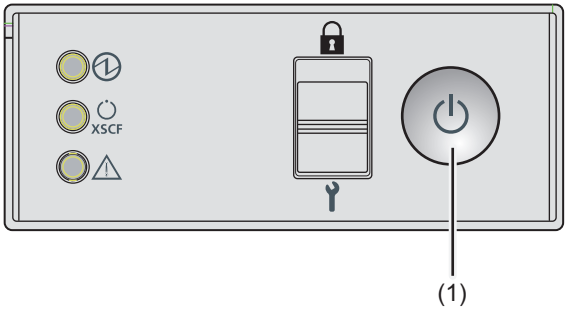
- SPARC M10-1
  SPARC M10-1의 POWER 스위치
- SPARC M10-4
  SPARC M10-4의 POWER 스위치
- SPARC M10-4S(크로스바 박스 없음)
  SPARC M10-4S의 POWER 스위치(BB#00)
- SPARC M10-4S(크로스바 박스 있음)
  크로스바 박스의 POWER 스위치(XBBOX#80)

운영 패널 스위치와 LED의 자세한 내용은 사용 모델에 맞는『서비스 설명서』의 "2장 시스템 구성요소 이해"를 참조하십시오.

그림 3-2 운영 패널(SPARC M10-1)

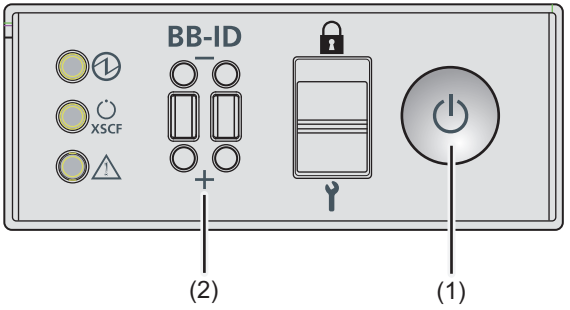
번호	구성요소
1	POWER 스위치

그림 3-3 운영 패널(SPARC M10-4)



번호	구성요소
1	POWER 스위치

그림 3-4 운영 패널(SPARC M10-4S/크로스바 박스)



번호	구성요소
1	POWER 스위치
2	BB-ID 스위치

작동 절차

1. 마스터 **XSCF**가 구성된 캐비닛에서 운영 패널의 **POWER** 스위치를 누릅니다**.**
   시스템에서 모든 물리 분할이 시작됩니다. 그런 다음 물리 분할의 모든 논리 도메인이 시작됩니다.

poweron 명령의 사용

XSCF 펌웨어 poweron 명령을 사용하여 시스템 전체를 시작합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

```
XSCF> poweron -a
```

시스템 전체를 시작하려면 -a 옵션이 지정된 poweron 명령을 실행합니다. 명령을 실행하면 확인 메시지가 표시되며 이때 "y"를 입력합니다.

명령이 실행되면 해당 순서에 따라 시스템의 모든 물리 분할에 전원이 공급됩니다. 그런 다음 해당 순서에 따라 물리 분할의 모든 논리 도메인이 시작됩니다.

poweron 명령의 자세한 내용은 poweron(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

노트 - XSCF 펌웨어 setpparparam 명령에 의해 자동 부팅이 억제되는 제어 도메인이 있는 경우 제어 도메인이 시작되지 않습니다. 또한 setpparmode 명령에 의해 자동 부팅이 억제되는 물리 분할 및/또는 논리 도메인이 있는 경우 논리 도메인이 시작되지 않습니다. setpparparam 및 setpparmode 명령의 자세한 내용은 setpparparam(8) 및 setpparmode(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **poweron -a** 명령을 실행하여 시스템 전체에 전원을 공급합니다. 확인 메시지에 **"y"**를 입력합니다.

```
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 "showlogs
power".
XSCF>
```

   시스템에서 모든 물리 분할에 전원이 공급됩니다. 그런 다음 물리 분할의 모든 논리 도메인이 시작됩니다.

3. **showlogs power** 명령을 실행하여 시스템의 모든 물리 분할에 전원이 공급되었는지 확인합니다.

```
XSCF> showlogs power
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

3.1.3 물리 분할의 개별 전원 공급

물리 분할에 개별적으로 전원을 공급하려면 XSCF 펌웨어 poweron 명령을 사용합니다. 이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 물리 분할에 대해 pparadm 또는 pparmgr 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

```
XSCF> poweron -p ppar_id
```

물리 분할을 지정하려면 -p ppar_id 옵션을 지정합니다. Ppar_id의 경우 시작되는 물리 분할의 PPAR-ID를 0 ~ 15의 값으로 지정할 수 있습니다.
명령을 실행하면 확인 메시지가 표시되며 이때 "y"를 입력합니다.

노트 - SPARC M10-1/M10-4의 경우 0만 PPAR-ID에 지정할 수 있습니다.

명령이 실행되면 지정된 물리 분할에 전원이 공급됩니다. 그런 다음 물리 분할의 모든 논리 도메인이 시작됩니다. 먼저 제어 도메인이 시작된 후 다른 도메인이 해당 순서에 따라 시작됩니다.

poweron 명령의 자세한 내용은 poweron(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

노트 - XSCF 펌웨어 setpparparam 명령에 의해 자동 부팅이 억제되는 제어 도메인이 있는 경우 제어 도메인이 시작되지 않습니다. 또한 setpparmode 명령에 의해 자동 부팅이 억제되는 물리 분할 및/또는 논리 도메인이 있는 경우 논리 도메인이 시작되지 않습니다. setpparparam 및 setpparmode 명령의 자세한 내용은 setpparparam(8) 및 setpparmode(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

1. 대상 물리 분할에 대해 관리 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **poweron** 명령을 실행하여 지정된 물리 분할에 전원을 공급합니다.
   다음에는 PPAR-ID 00 전원 공급의 예가 나타나 있습니다.

```
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 "showlogs
power".
XSCF>
```

   PPAR-ID 00의 물리 분할에 전원이 공급됩니다. 물리 분할의 모든 논리 도메인이 시작됩니다.
3. **showlogs power** 명령을 실행하여 지정된 물리 분할에 전원이 공급되었는지 확인합니다.

```
XSCF> showlogs power
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

3.1.4 논리 도메인 시작

논리 도메인을 개별적으로 시작하려면 Oracle VM Server for SPARC의 ldm start-domain 명령을 사용합니다.

노트 - 이 작동은 루트 사용자 또는 ldomadm 역할의 사용자만 실행할 수 있습니다.

```
primary# ldm start-domain ldom
```

ldom의 경우 시작하려는 논리 도메인의 이름을 지정합니다.
ldm(1M) 명령의 자세한 내용은 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

작동 절차

1. **XSCF** 콘솔을 대상 논리 도메인이 속한 제어 도메인 콘솔로 전환합니다.
제어 도메인 콘솔로의 전환 방법과 관련된 자세한 내용은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

   대상 제어 도메인 콘솔로 이미 전환했으면 다음 단계로 이동합니다.

2. **ldm start-domain** 명령을 실행하여 도메인 상태를 확인합니다.
다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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
```

3. **ldm start-domain** 명령을 실행하여 지정된 도메인을 시작합니다.
다음에는 ldom2의 시작 예가 나타나 있습니다.

```
primary# ldm start-domain ldom2
```

4. **ldm list-domain** 명령을 실행하여 도메인 상태를 확인합니다.
다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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
```

논리 도메인 ldom2가 성공적으로 시작되었음을 알 수 있습니다.

3.2 시스템 정지

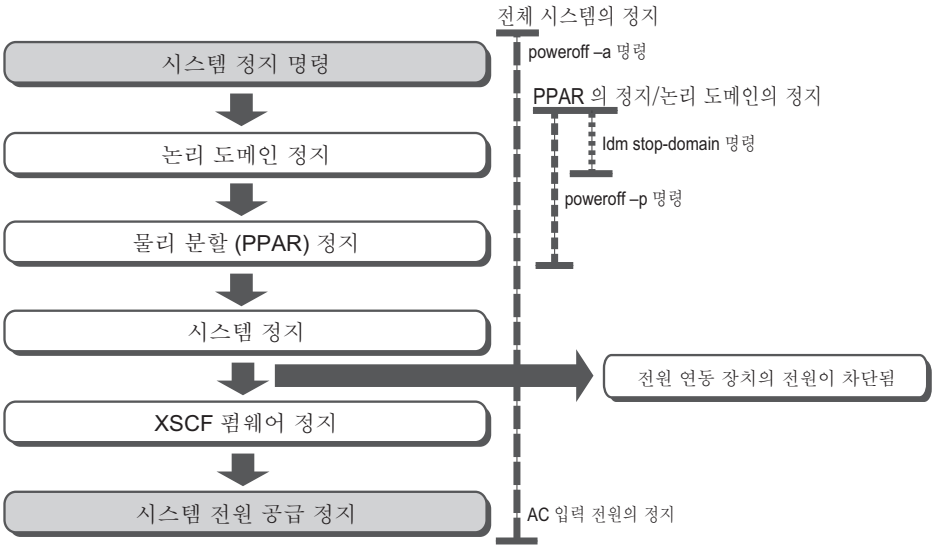
이 절에는 시스템 정지 흐름과 정지 방법이 설명되어 있습니다.

3.2.1 시스템 정지부터 입력 전원 차단까지 흐름

이 절에는 시스템 정지부터 입력 전원 차단까지 흐름이 설명되어 있습니다.

시스템 전체의 정지에 사용되는 명령, 물리 분할의 정지에 사용되는 명령 및 논리 도메인의 정지에 사용되는 명령이 유효 범위와 함께 설명되어 있습니다.
후속 절에는 단계별 정지 절차가 설명되어 있습니다.

그림 3-5 시스템 정지부터 입력 전원 차단까지 흐름



3.2.2 종료 순서 지정

시스템 전원을 차단하려면 대상 물리 분할의 모든 논리 도메인을 종료해야 합니다. 논리 도메인의 종료 순서는 확연하거나 제어 도메인을 제외한 도메인이 먼저 종료된 후 제어 도메인이 마지막에 종료되어야 합니다.

SPARC M10 시스템은 사용자가 위에 설명된 논리 도메인의 종료 순서에 주의를 기울이지 않아도 되게끔 해당 순서에 따라 도메인이 종료되도록 하고 물리 분할을 정지하는 지정된 종료라고 하는 기술을 지원합니다.

지정된 종료의 경우 논리 도메인에 대해 그룹의 종료 순서를 나타내는 번호가 사전에 정의됩니다. 정의된 순서는 XSCF 관리 중이더라도 종료 순서가 보장되도록 XSCF에 저장됩니다.

지정된 종료의 자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』의 "4.6 종료 순서 지정"을 참조하십시오.

3.2.3 시스템 전체의 정지

XSCF 펌웨어 poweroff 명령을 사용하여 시스템 전체를 정지합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

노트 - 잠금 모드에서는 마스터 XSCF 캐비닛 운영 패널의 POWER 스위치를 사용하여 전원을 차단할 수 없습니다. 잠금 모드의 자세한 내용은 "5장 잠금/서비스 모드로 전환"을 참조하십시오.

```
XSCF> poweroff -a
```

시스템 전체를 정지하려면 -a 옵션이 지정된 poweroff 명령을 실행합니다. 명령을 실행하면 확인 메시지가 표시되며 이때 "y"를 입력합니다.

명령이 실행되면 각 물리 분할의 논리 도메인이 지정된 종료 규칙에 따라 종료됩니다. 그런 다음 물리 분할의 전원 공급이 차단됩니다.

poweroff 명령의 자세한 내용은 poweroff(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **poweroff -a** 명령을 실행하여 시스템 전체의 전원을 차단합니다. 확인 메시지에 **"y"**를 입력합니다.

```
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 "showlogs
power".
XSCF>
```

각 물리 분할에 대해 모든 논리 도메인이 종료된 후 모든 물리 분할의 전원이 차단됩니다.

3. **showlogs power** 명령을 실행하여 모든 물리 분할의 전원이 차단되었는지 확인합니다.

```
XSCF> showlogs power
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

3.2.4 물리 분할의 개별 전원 차단

물리 분할을 개별적으로 정지하려면 XSCF 펌웨어 poweroff 명령을 사용합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 물리 분할에 대해 pparadm 또는 pparmgr 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

```
XSCF> poweroff -p ppar_id
```

물리 분할을 지정하려면 -p ppar_id를 지정합니다. Ppar_id의 경우 전원이 차단되는 물리 분할의 PPAR-ID를 시스템 구성에 따른 0 ~ 15의 값으로 지정할 수 있습니다.
명령을 실행하면 확인 메시지가 표시되며 이때 "y"를 입력합니다.

명령이 실행되면 각 물리 분할의 논리 도메인이 지정된 종료 규칙에 따라 종료됩니다. 그런 다음 물리 분할의 전원 공급이 차단됩니다.

poweroff 명령의 자세한 내용은 poweroff(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

1. 대상 물리 분할에 대해 관리 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **poweroff** 명령을 실행하여 지정된 물리 분할의 전원을 차단합니다.
   다음에는 PPAR-ID 00 전원 차단의 예가 나타나 있습니다.

```
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 "showlogs
power".
XSCF>
```

   물리 분할에서 모든 논리 도메인이 종료된 후 PPAR-ID 00 물리 분할의 전원이 차단됩니다.

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

3.2.5 논리 도메인 종료

논리 도메인을 개별적으로 종료하려면 Oracle VM Server for SPARC의 ldm stop-domain 명령을 사용합니다. 이 작동은 루트 사용자 또는 ldomadm 역할의 사용자만 실행할 수 있습니다.

```
primary# ldm stop-domain ldom
```

ldom의 경우 종료하려는 논리 도메인의 이름을 지정합니다.
ldm(1M) 명령의 자세한 내용은 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

작동 절차

1. **XSCF** 콘솔에서 대상 논리 도메인이 속한 물리 분할의 제어 도메인 콘솔로 전환합니다.
   제어 도메인 콘솔로의 전환 방법과 관련된 자세한 내용은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

   대상 제어 도메인 콘솔로 이미 전환했으면 다음 단계로 이동합니다.

2. **ldm list-domain** 명령을 실행하여 도메인 상태를 확인합니다.
   다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타

나 있습니다.

```
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       34%   17h 48m
ldom3             active     -n----  5003    16    4G 1     7%    17h 48m
```

3. **ldm stop-domain** 명령을 실행하여 지정된 도메인을 종료합니다.
   다음에는 ldom2의 종료 예가 나타나 있습니다.

```
primary# ldm stop-domain ldom2
```

4. **ldm list-domain** 명령을 실행하여 도메인 상태를 확인합니다.
   다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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
```

도메인 종료를 마치면 상태가 자원 바운드 상태(바운드)로 변경됩니다.

3.3 시스템 재설정

이 절에는 시스템 재설정 방법이 설명되어 있습니다.

3.3.1 XSCF 재설정

XSCF 펌웨어 rebootxscf 명령을 사용하여 XSCF를 재설정합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

다음 XSCF 설정을 구성한 경우 XSCF를 재설정하면 구성된 설정이 적용됩니다.

- XSCF에 구성된 XSCF 네트워크 적용(applynetwork)
- 시스템 고도(setaltitude)
- NTP 설정(setntp)

```
XSCF> rebootxscf -a | -b bb_id | -s
```

시스템에서 모든 XSCF를 재설정하려면 -a를 지정합니다. 지정된 SPARC M10-4S의 XSCF를 재설정하려면 -b bb_id를 지정합니다. -a 및 -b는 마스터 XSCF에서만 실행 가능합니다. 처리 중인 XSCF를 재설정하려면 -s를 지정합니다.

XSCF를 재설정하면 SSH 및 Telnet에 의한 연결처럼 XSCF 연결이 분리됩니다. 다시 연결합니다.

노트 - XSCF 펌웨어 setdate 명령에 의한 XSCF 재설정이 취소되는 경우 rebootxscf 명령을 사용하여 XSCF를 재설정하면 설정이 적용되지 않습니다. setdate 명령을 다시 실행해야 합니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오. 위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. 해당 시 **XSCF** 명령을 실행합니다.
   다음에는 setaltitude 명령의 실행 예가 나타나 있습니다. 명령을 실행하여 모두를 재설정할 수 있습니다.

```
XSCF> setaltitude -s altitude=1000
1000m
```

3. **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다. 확인 메시지에 **"y"**를 입력합니다.
   다음에는 모든 XSCF의 재설정 예가 나타나 있습니다.

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

3.3.2 물리 분할 재설정

XSCF 펌웨어 reset 명령을 사용하여 지정된 물리 분할을 재설정합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 물리 분할에 대해 pparadm 또는 pparmgr 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

노트 - reset 명령은 지정된 물리 분할을 강제 재설정하여 디스크 또는 다른 구성요소에 고장을 일으킬 수도 있습니다. 끊김 시의 Oracle Solaris 복구와 같은 비상 목적으로만 이 명령을 사용합니다.

```
XSCF> reset -p ppar_id por | xir
```

ppar_id의 경우 재설정되는 물리 분할의 PPAR-ID를 지정합니다. 시스템 구성에 따라 0

~ 15 가운데 1개 값만 지정할 수 있습니다.
물리 분할 자체를 재설정하고 por을 지정하거나 물리 분할의 모든 CPU를 재설정하려면 xir을 지정합니다.

setpparparam 명령에 의해 구성된 제어 도메인 자동 부팅 기능이 비활성화될 때 reset 명령이 실행되면 Oracle Solaris의 시작 전에 처리가 정지됩니다.

작동 절차

1. 대상 물리 분할에 대해 관리 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **reset** 명령을 실행하여 지정된 물리 분할을 재설정합니다. 확인 메시지에 **"y"**를 입력합니다.
   다음에는 PPAR-ID 00의 재설정 예가 나타나 있습니다.

```
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 "showlogs
power".
XSCF>
```

3. **showlogs power** 명령을 실행하여 지정된 물리 분할이 재설정되었는지 확인합니다.

```
XSCF> showlogs power
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

3.3.3 논리 도메인 재설정

XSCF 펌웨어 reset 명령을 사용하여 지정된 논리 도메인을 재설정합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 논리 도메인이 속한 물리 분할의 경우 pparadm 또는 pparmgr 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

노트 - reset 명령은 지정된 물리 분할을 강제 재설정하여 디스크 또는 다른 구성요소에 고장을 일으킬 수도 있습니다. 끊김 시의 Oracle Solaris 복구와 같은 비상 목적으로만 이 명령을 사용합니다.

```
XSCF> reset -p ppar_id -g hostname sir | panic
```

ppar_id의 경우 재설정되는 논리 도메인이 속한 물리 분할의 PPAR-ID를 지정합니다. 시스템 구성에 따라 0 ~ 15 가운데 1개 값만 지정할 수 있습니다.
Hostname의 경우 재설정되는 논리 도메인의 호스트 이름을 지정합니다.
Sir을 지정하여 논리 도메인 자체를 재설정하거나 panic을 지정하여 논리 도메인의 Oracle Solaris가 패닉이 되도록 합니다.

setpparmode 명령에 의해 구성된 자동 부팅 기능이 비활성화될 때 reset 명령이 실행되면 Oracle Solaris의 시작 전에 처리가 정지됩니다.

작동 절차

1. 대상 물리 분할에 대해 관리 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **reset** 명령을 실행하여 지정된 논리 도메인을 재설정합니다. 확인 메시지에 **"y"**를 입력합니다.
   다음에는 PPAR-ID 00의 게스트 도메인 ldom1에 대한 재설정 예가 나타나 있습니다.

```
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>
```

3. **showdomainstatus** 명령을 실행하여 지정된 논리 도메인이 재설정되었는지 확인합니다.
   다음 예에서는 PPAR-ID 0의 논리 도메인 상태를 확인합니다.

```
XSCF> showdomainstatus -p 0
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

4장

로그인/로그아웃

이 장에는 XSCF 쉘 또는 XSCF 웹을 사용하여 XSCF에 로그인하는 방법이 설명되어 있습니다.

XSCF에 로그인하기 전에 터미널을 서버의 XSCF 전용 LAN 포트(이후 XSCF-LAN 포트라고 함) 또는 직렬 포트에 연결해야 합니다.

직렬 연결의 경우 XSCF 쉘에 로그인하고 XSCF-LAN 연결의 경우에는 XSCF 쉘 및 XSCF 웹에 로그인할 수 있습니다. XSCF 기능은 직렬 포트와 XSCF-LAN 포트에서 동일하게 사용할 수 있습니다.

- XSCF 쉘에 로그인
- XSCF 쉘에서 로그아웃
- XSCF 쉘에서 제어 도메인 콘솔로 전환
- 제어 도메인 콘솔에서 XSCF 쉘로 돌아가기
- XSCF 웹에 로그인
- XSCF 웹에서 로그아웃
- 연결 가능한 사용자 수
- XSCF-LAN 포트 번호 및 기능과 방화벽

4.1 XSCF 쉘에 로그인

이 절에는 XSCF 쉘을 사용하여 XSCF에 로그인하는 방법이 설명되어 있습니다.

로그인 인증을 위해 만든 새 사용자 계정과 처음 로그인할 때의 기본 사용자 계정을 사용합니다. 기본 로그인 인증은『SPARC M10 시스템 설치 안내서』의 "6장 시스템의 초기 진단 구현"을 참조하십시오. 새 계정의 구성 방법은 "8장 XSCF 펌웨어 구성"을 참조하십시오.

4.1.1 직렬 연결을 위한 터미널 및 작업

터미널을 직렬 포트에 연결하면 XSCF 쉘과 제어 도메인용 콘솔(제어 도메인 콘솔)을 사용할 수 있습니다. XSCF 웹은 사용할 수 없습니다.

표 4-1에는 직렬 연결을 위한 터미널 및 콘솔과 사용 가능한 기능이 설명되어 있습니다.

표 4-1 직렬 연결을 위한 터미널 및 콘솔과 사용 가능한 기능

터미널 유형	작업	케이블
XSCF 쉘 터미널	■ 직렬 포트에 연결한 직후 XSCF 쉘 터미널을 사용할 수 있습니다. ■ console 명령을 사용하여 제어 도메인 콘솔 화면으로 전환할 수 있습니다. ■ 로그인 후 지정된 시간 동안 쉘을 사용하지 않으면 강제 로그아웃됩니다. XSCF 세션 시간 초과 설정은 setautologout(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』를 참조하십시오.	RS-232C 직렬 크로스 케이블이 필요합니다. LAN 케이블만 있는 경우 PC측에 9핀 변환 케이블이 필요합니다.
제어 도메인 콘솔(RW 콘솔)	■ 이는 입력/출력에 사용 가능한 OS 콘솔입니다. XSCF 쉘 터미널에서 console 명령으로 물리 분할과 쓰기 가능 콘솔을 지정하여 RW 콘솔을 열 수 있습니다. ■ 1개 물리 분할에서 한 번에 한 사용자(1개 연결)만 RW 콘솔을 사용할 수 있습니다. ■ 제어 도메인 콘솔의 비작동 시간에 대해 세션 시간 초과를 설정하는 방법은 사용 버전의『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.	
제어 도메인 콘솔(RO 콘솔)	■ 이는 보기 전용 OS 콘솔입니다. XSCF 쉘 터미널에서 console 명령으로 물리 분할과 보기 전용 콘솔을 지정하여 RO 콘솔을 열 수 있습니다. ■ SPARC M10 시스템에서 동시 액세스할 수 있는 RW/RO 콘솔의 최대 수는 다음과 같습니다. - SPARC M10-1: 20개 콘솔 - SPARC M10-4: 40개 콘솔 - SPARC M10-4S(크로스바 박스 없음): 40개 콘솔 - SPARC M10-4S(크로스바 박스 있음): 70개 콘솔	

4.1.2 직렬 연결로 XSCF 쉘에 로그인하는 방법

다음에는 직렬 포트를 통해 터미널에 연결하고 XSCF 쉘에 로그인하는 방법이 설명되어 있습니다.

1. 직렬 케이블이 마스터 **XSCF**의 직렬 포트 슬롯에 연결되고 사용하는 **PC/**워크스테이션으로 연결이 올바로 설정되었는지 확인합니다**.**
2. 터미널 소프트웨어를 사용하여 다음 값을 지정했는지 확인합니다**.**
   전송 속도: 9,600bps
   데이터 길이: 8bit

패리티: 없음

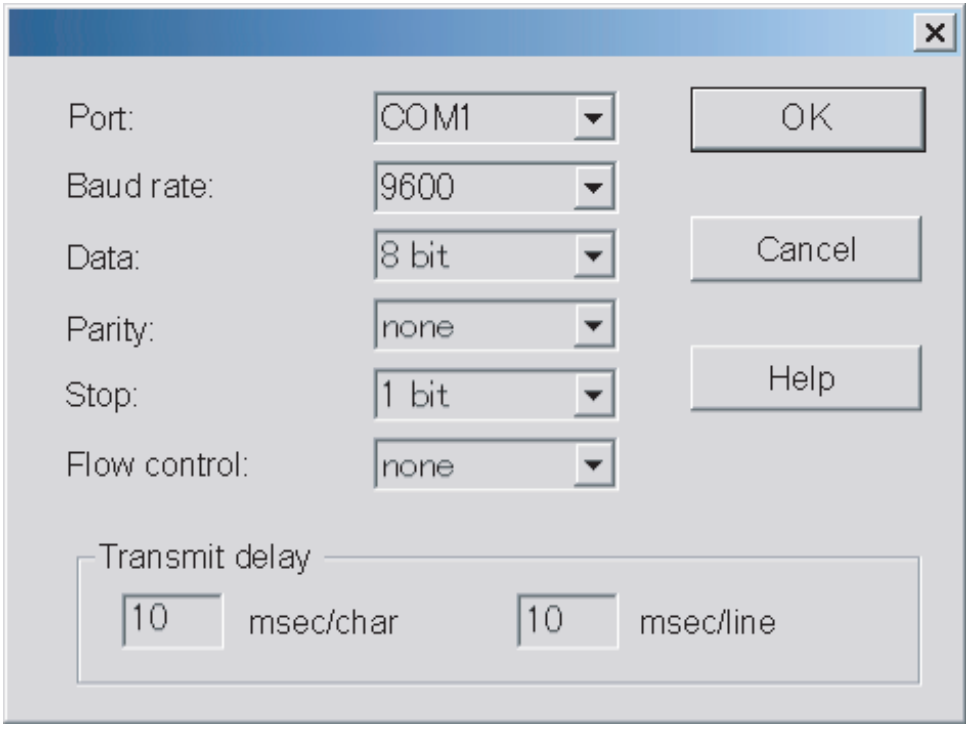
정지 비트: 1bit

흐름 제어: 없음

전송 지연: 0이 아님

그림 4-1에는 터미널 소프트웨어에서의 설정 구성 예가 나타나 있습니다. 연결할 수 없으면 지연 값을 증가시킵니다.

그림 4-1 터미널 소프트웨어에서의 설정 구성 예



3. 직렬 연결을 하고 **[Enter]** 키를 누릅니다.
   터미널이 XSCF 터미널로서 설정되고 로그인 프롬프트가 표시됩니다.

4. **XSCF** 사용자 계정과 암호를 입력하여 **XSCF**에 로그인합니다.

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

5. **XSCF** 쉘 프롬프트**(XSCF>)**가 나타나는지 확인합니다.
   이제 XSCF 쉘을 사용할 수 있습니다.

```
XSCF>
```

4.1.3 XSCF-LAN을 위한 터미널 및 작업

XSCF-LAN에 연결된 터미널에서 SSH 또는 Telnet을 통해 XSCF 쉘과 제어 도메인 콘솔을 사용할 수 있습니다.

XSCF-LAN을 통해 액세스하면 이메일 알림 기능, SNMP 기능, 원격 유지 관리 서비스 기능 및 외부 NTP 서버에 의한 시간 동기화를 사용할 수 있습니다. 또한 브라우저 설정을 구성하면 XSCF 웹에도 사용할 수 있습니다.

표 4-2에는 XSCF-LAN 연결을 위한 터미널 및 콘솔과 사용 가능한 기능이 설명되어 있습니다.

표 4-2 XSCF-LAN 연결을 위한 터미널 및 콘솔과 사용 가능한 기능

터미널 유형	작업	포트 번호/케이블
XSCF 쉘 터미널	• SSH 또는 Telnet 연결을 통해 XSCF 쉘을 사용할 수 있습니다. • 직렬 포트에서처럼 제어 도메인 콘솔 화면으로 전환할 수 있습니다. • 로그인 후 지정된 시간 동안 쉘을 사용하지 않으면 직렬 포트에서처럼 강제 로그아웃됩니다.	SSH:22 Telnet:23 LAN 케이블이 필요합니다.
제어 도메인 콘솔(RW 콘솔)	직렬 포트에서와 동일함.	
제어 도메인 콘솔(RO 콘솔)	직렬 포트에서와 동일함.	
XSCF 웹 콘솔	XSCF 웹 콘솔은 브라우저에서 URL을 지정하여 사용할 수 있습니다.	HTTPS:443 LAN 케이블이 필요합니다.

4.1.4 XSCF-LAN을 통해 SSH 연결로 XSCF 쉘에 로그인하는 방법

이 절에 설명된 절차에서는 "8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성"에 설명된 SSH 서비스가 활성화된 것으로 가정합니다.

다음에는 XSCF-LAN 포트를 통해 SSH를 사용하여 XSCF 쉘에 로그인하는 방법이 설명되어 있습니다.

1. **LAN** 케이블이 마스터 **XSCF**의 **XSCF-LAN** 포트 슬롯에 연결되고 사용하는 **PC/**워크스테이션으로 연결이 올바로 설정되었는지 확인합니다**.**
2. **SSH**로 로그인하기 전에 저장된 지문을 사전에 확인합니다**.**
   지문이 저장되어 있지 않으면 직렬 포트를 통해 연결하고 showssh 명령을 실행한 후 호스트 공개 키의 지문을 기록합니다.
3. **SSH** 클라이언트를 시작하고 **XSCF IP** 주소 또는 호스트 이름과 포트 번호를 필요

한 경우 지정하여 **SSH** 연결을 합니다.
XSCF가 2개 이상인 시스템의 경우 인계 IP 주소를 지정합니다.

4. **XSCF** 사용자 계정과 암호를 입력하여 **XSCF** 쉘에 로그인합니다.
5. 호스트 공개 키의 지문이 표시된 후 올바른지 그 여부와 관련된 확인이 표시되면 지문을 확인하고 올바른 **XSCF**에 연결되었는지 확인한 후 **"yes"**를 입력합니다.
6. **XSCF** 쉘 프롬프트**(XSCF>)**가 나타나는지 확인합니다.
이제 XSCF 쉘을 사용할 수 있습니다.

다음에는 로그인 예가 나타나 있습니다.

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

사용자 키를 사용하여 SSH 연결을 하려면 XSCF로 사용자 공개 키를 사전에 등록합니다. 사용자 공개 키의 등록 방법은 "8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성"을 참조하십시오.

다음에는 사용자 공개 키를 사용한 로그인 예가 나타나 있습니다.

```
[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>
```

노트 - SSH 시작은 SSH 설명서를 참조하십시오.

4.1.5 XSCF-LAN을 통해 Telnet 연결로 XSCF 쉘에 로그인하는 방법

이 절에 설명된 절차에서는 "8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성"에 설명된 Telnet 서비스가 활성화된 것으로 가정합니다.

다음에는 XSCF-LAN 포트를 통해 Telnet을 사용하여 XSCF 쉘에 로그인하는 방법이 설명되어 있습니다.

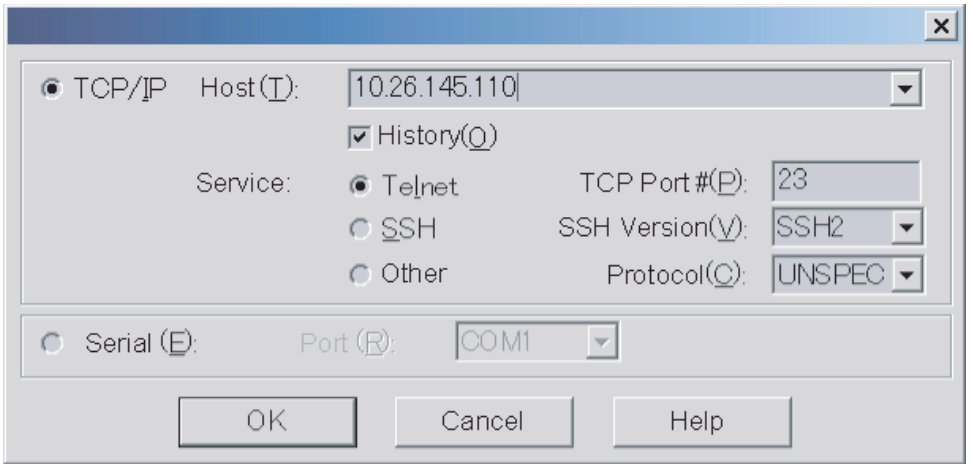
1. **LAN** 케이블이 마스터 **XSCF**의 **XSCF-LAN** 포트 슬롯에 연결되고 사용하는 **PC/**워

크스테이션으로 연결이 올바로 설정되었는지 확인합니다.

2. 터미널 에뮬레이터를 시작하고 **XSCF IP** 주소 또는 호스트 이름과 포트 번호 **23**을 지정하여 **Telnet** 연결을 합니다.
   XSCF가 2개 이상인 시스템의 경우 인계 IP 주소를 지정합니다.

그림 4-2에는 터미널 에뮬레이터의 설정 구성 예가 나타나 있습니다.

그림 4-2 터미널 에뮬레이터의 설정 구성 예



3. **XSCF** 사용자 계정과 암호를 입력하여 **XSCF** 쉘에 로그인합니다.
4. **XSCF** 쉘 프롬프트**(XSCF>)**가 나타나는지 확인합니다.
   이제 XSCF 쉘을 사용할 수 있습니다.

   다음에는 성공적인 로그인 예가 나타나 있습니다.

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

4.2 XSCF 쉘에서 로그아웃

XSCF 웹에서 로그아웃하는 절차는 아래 설명된 바와 같습니다.

1. **exit** 명령을 실행하여 로그아웃합니다.

```
XSCF> exit
```

XSCF에서 로그아웃되고 XSCF 세션이 분리됩니다.

로그인 후 지정된 시간 동안 쉘을 사용하지 않으면 강제 로그아웃됩니다. XSCF 세션 시간 초과 설정은 setautologout(8) 명령 설명서 페이지와 『SPARC M10 Systems XSCF

Reference Manual』을 참조하십시오.

4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환

XSCF 터미널에서 XSCF 쉘로 로그인한 후 console 명령을 실행하면 제어 도메인 콘솔을 사용할 수 있습니다.

명령을 사용하여 XSCF 쉘을 제어 도메인 콘솔로 전환하는 기능을 XSCF 콘솔 리디렉션 기능이라고 합니다. SPARC M10 시스템의 경우 시스템 보드가 XSCF에 바로 직렬 연결됩니다. 사용자가 console 명령을 실행하면 XSCF는 유효한 제어 도메인으로 가는 경로를 자동 선택하고 제어 도메인 콘솔로 전환합니다.

4.3.1 XSCF 쉘에서 제어 도메인 콘솔로 전환하는 방법

PC 또는 워크스테이션에 XSCF-LAN 또는 직렬 연결이 설정된 경우 XSCF 쉘과 제어 도메인 콘솔을 한 화면에서만 작동할 수 있습니다. 다음에는 전환 방법이 설명되어 있습니다.

1. **XSCF** 쉘 터미널 화면에서 **console** 명령을 실행하여 제어 도메인 콘솔로 전환합니다.
   아래 예에서는 물리 분할 0이 지정됩니다.

```
XSCF> console -p 0
```

2. 제어 도메인 콘솔 화면으로 전환되었는지 확인합니다.

```
#
```

   물리 분할당 1개 RW 콘솔만 연결될 수 있습니다. 물리 분할에 대해 platadm 또는 pparadm의 사용자 권한이 있는 사용자가 다른 RW 콘솔에 강제 연결하면 현재 연결 중인 RW 콘솔이 분리됩니다.

4.3.2 필요 시 제어 도메인 콘솔에 연결

처리하는 물리 분할의 전원이 차단되면 제어 도메인 콘솔로 전환할 수 없습니다.
다음에는 물리 분할에 전원을 공급하고 제어 도메인 콘솔에 연결하는 방법이 설명되어 있습니다.

1. **XSCF** 쉘 터미널에서 물리 분할을 지정하고 **poweron** 명령을 실행하여 물리 분할에 전원을 공급합니다.
2. 다른 창에서 제어 도메인 콘솔을 표시하려면 **"4.1 XSCF 쉘에 로그인"**을 참조하여 다른 **XSCF** 쉘 터미널을 설정한 후 로그인합니다.
3. **console** 명령을 실행합니다.

4. 지정된 제어 도메인 콘솔로 전환되었는지 확인합니다.

4.4 제어 도메인 콘솔에서 XSCF 쉘로 돌아가기

제어 도메인 콘솔에서 작동을 마친 후 키를 눌러 XSCF 쉘로 돌아갈 수 있습니다.

4.4.1 제어 도메인 콘솔에서 XSCF 쉘로 전환하는 방법

다음에는 제어 도메인 콘솔에서 XSCF 쉘로 다시 전환하는 방법이 설명되어 있습니다.

1. 제어 도메인 콘솔에서 **XSCF** 쉘로 돌아가려면 **[Enter]** 키에 이어 **[#]** 키**(**이스케이프 문자의 기본값**)** 및 **[.] (**마침표**)** 키를 누릅니다**.**
   기본값과 다른 이스케이프 문자를 설정하려면 옵션을 지정하고 console 명령을 실행합니다.

   이는 현재 세션에서 유효합니다.

   아래 예에서는 이스케이프 문자가 [|]로 변경됩니다.

```
XSCF> console -d 0 -s "|"
Console contents may be logged.
Connect to DomainID 0?[y|n] :y
```

   이스케이프 문자 유형의 자세한 내용은 console(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

2. **XSCF** 쉘 프롬프트**(XSCF>)**가 터미널에 나타나는지 확인합니다**.**

4.4.2 제어 도메인 콘솔에서 로그아웃

도메인의 로그아웃 없이 도메인 콘솔에서 XSCF 쉘로 돌아가거나 도메인의 로그아웃 없이 XSCF 쉘을 종료하는 경우 도메인에서 자동 로그아웃됩니다. 이 경우 도메인 콘솔에서 시작된 백그라운드 프로그램으로 종료 신호가 전송될 수 있습니다.

도메인 콘솔의 비작동 시간에 대해 세션 시간 초과를 설정하는 방법은 Oracle Solaris 관련 설명서를 참조하십시오.

4.5 XSCF 웹에 로그인

이 절에는 XSCF 웹을 사용하여 XSCF에 로그인하는 방법이 설명되어 있습니다.

XSCF-LAN에 연결된 PC에서 브라우저를 구성하면 이를 XSCF 웹에 사용할 수 있습니다. 이는 직렬 포트에서는 연결할 수 없습니다.

XSCF-LAN을 통해 액세스하면 이메일 알림 기능, SNMP 기능, 원격 유지 관리 서비스 기능 및 외부 NTP 서버에 의한 시간 동기화를 사용할 수 있습니다.

XSCF 웹은 HTTPS 프로토콜 및 SSL/TLS 프로토콜로 사용자 네트워크를 통해 연결된 서버에 연결되며 서버 상태 표시, 작동 장치 제어 및 설정 정보 찾아보기의 웹 기반 지원을 제공합니다.

클라이언트 터미널에서 웹 브라우저를 사용하여 등록된 사용자를 XSCF 웹에 연결하고 XSCF에 로그인하면 사용 가능한 트리 색인과 페이지가 표시됩니다. XSCF 웹 페이지의 정보는 "부록 B XSCF 웹 페이지 목록"을 참조하십시오.

4.5.1 사전에 설정해야 하는 항목

기본적으로 XSCF 웹에서는 설정이 비활성화되어 있습니다. XSCF 웹을 사용하려면 다음 설정을 사전에 구성해야 합니다.

- XSCF 사용자 계정의 등록
- XSCF 웹을 사용하기 위한 HTTPS 서비스의 활성화
- HTTPS 서비스 설정을 사용한 웹 서버 인증서의 등록
- 이메일 알림 설정의 구성(고장 시에 권장됨)

HTTPS 서비스의 활성화 방법은 "8.7 XSCF에 로그인하기 위한 HTTPS 서비스 구성"을 참조하십시오.

4.5.2 지원되는 브라우저

XSCF 웹은 표 4-3에 나열된 웹 브라우저를 지원합니다.

표 4-3 지원되는 브라우저

브라우저 이름	버전
Microsoft Internet Explorer	8.0
Firefox	3.6 이상

사용 가능한 웹 브라우저와 관련된 최신 정보는 『SPARC M10 시스템 제품 노트』의 최신 버전을 참조하십시오.

4.5.3 브라우저를 위해 활성화되어야 하는 기능

웹 브라우저에 사용되도록 다음 기능 설정을 활성화합니다.

- Secure Socket Layer Protocol(SSL) 버전 3

- Transport Layer Security(TLS) 버전 1
- JavaScript
- Cookie(세션 관리용)

4.5.4 XSCF 웹으로 로그인하는 방법

다음에는 XSCF 웹을 사용하여 XSCF에 로그인하는 방법이 설명되어 있습니다.

1. **LAN** 케이블이 마스터 **XSCF**의 **XSCF-LAN** 포트 슬롯에 연결되고 사용하는 **PC/**워크스테이션으로 연결이 올바로 설정되었는지 확인합니다**.**
2. 웹 브라우저 **URL**의 경우 **XSCF**의 **IP** 주소 또는 호스트 이름을 지정하고 **XSCF**에 연결합니다**.**

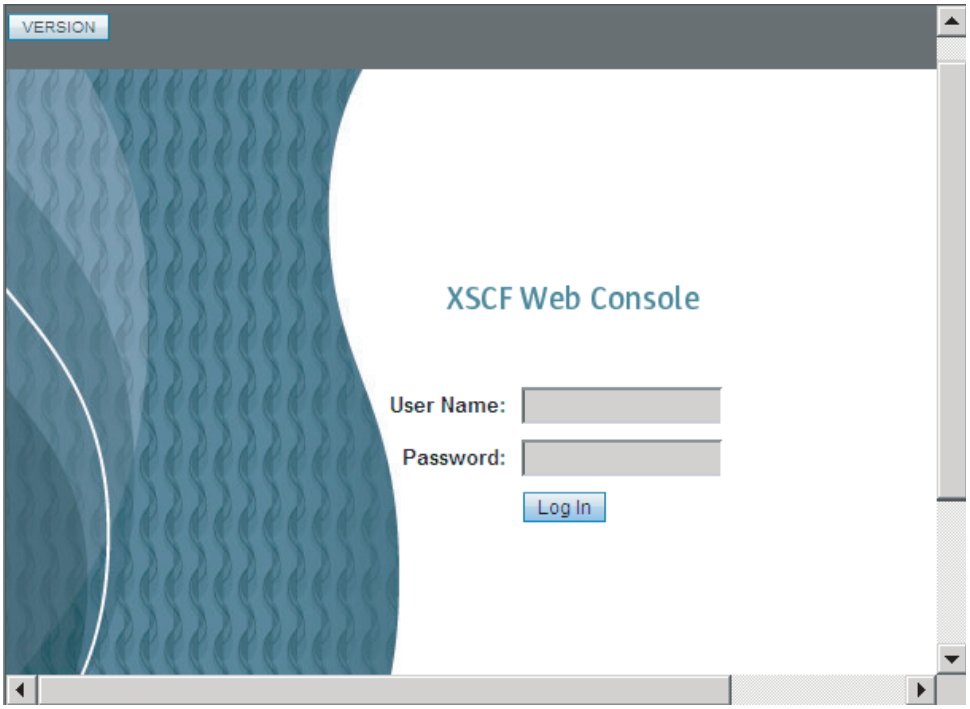
   <웹 브라우저의 URL 입력 이미지>

```
URL https://192.168.111.111 (XSCF IP 주소<숫자>입력)/
또는,
https://XSCF-host-name (참고: 도메인 호스트 이름이 아님)/
```

노트 **-** 통신 시작 시 인증서 확인 질문이 나타날 수도 있습니다. 인증서를 확인하여 적용합니다. HTTPS 연결 시 웹 브라우저는 인증서 설치를 마칠 때까지 경고를 계속 표시합니다.

3. 로그인 페이지에서 **XSCF** 사용자 계정과 암호를 입력하여 **XSCF**에 로그인합니다**.** 그림 4-3에는 로그인 페이지의 예가 나타나 있습니다.

그림 4-3 XSCF 웹 로그인 페이지의 예



성공적으로 로그인하면 하나 또는 여러 페이지를 선택할 수 있도록 트리 보기를 표시하는 기본 페이지가 나타납니다.

로그인에 실패하는 경우

로그인에 실패하면 로그인 실패 메시지가 나타납니다. 또한 실패한 로그인 시도가 이벤트 로그와 감사 로그에 로깅됩니다.

4.6 XSCF 웹에서 로그아웃

XSCF 웹에서 로그아웃하는 절차는 아래 설명된 바와 같습니다.

1. **XSCF** 웹 페이지에서 **[LOG OUT]** 버튼을 클릭하여 로그아웃합니다.
   XSCF 웹 로그인 페이지로 XSCF에서 로그아웃됩니다.

상태 모니터링 액세스

XSCF 웹은 로그인하는 XSCF 사용자 계정의 활용 상태를 모니터링합니다. XSCF 웹은 로그인했지만 지정된 시간 동안 액세스하지 않은 계정을 인증이 만료된 것으로 결정합니다. 따라서 인증이 만료된 계정으로 XSCF 웹에 액세스하는 경우 인증 만료를 알려주는 대화 상자가 표시되고 맨 위 페이지로 돌아갑니다. XSCF 웹을 계속 사용하려면 다시 로그인합니다.

XSCF 웹 페이지에서 인증 만료의 결정 시간을 변경할 수 있습니다. 인증 만료의 결정 시간은 10분으로 디폴트됩니다. 지정 가능한 시간 범위는 1 ~ 255분입니다. [Menu] -> [Settings] -> [Autologout]으로 시간 설정을 구성할 수 있습니다.

4.7 연결 가능한 사용자 수

XSCF에 연결 가능한 사용자 수는 아래 설명된 바와 같습니다. who 명령을 실행하면 XSCF에 로그인하는 사용자 계정이 나열됩니다.

- SPARC M10-1 시스템
  최대 20명 사용자. 20명 사용자가 XSCF에 동시 연결하는 경우 21번째 사용자로서 액세스를 시도하는 사용자는 거부됩니다.
- SPARC M10-4/M10-4S 시스템
  최대 70명 사용자. 70명 사용자가 XSCF에 동시 연결하는 경우 71번째 사용자로서 액세스를 시도하는 사용자는 거부됩니다.

4.8 XSCF-LAN 포트 번호 및 기능과 방화벽

표 4-4에는 XSCF에 사용되는 XSCF-LAN 포트와 기능을 사용하기 위한 포트 번호가 나타나 있습니다. 유효하지 않은 XSCF 액세스 또는 XSCF 공격이 없도록 외부 네트워크에 연결이 허용될 때 방화벽을 구성하는 것이 좋습니다. 방화벽을 구현하는 경우 필요에 따라 패킷이 포트를 통과할 수 있도록 해야 합니다.

표 4-4 XSCF-LAN 포트 번호, 기능 및 연결 방향

포트 번호/프로토콜	기능	연결 방향
22/TCP	XSCF 쉘(SSH)	외부 네트워크 →XSCF
22/TCP	펌웨어 업데이트 기능	XSCF→외부 네트워크
23/TCP	XSCF 쉘(Telnet)	외부 네트워크 →XSCF
25/TCP	이메일 알림 및 원격 유지 관리 서비스	XSCF→외부 네트워크
53/TCP 53/UDP	DNS	XSCF→외부 네트워크
110/TCP	POP 서버에 의한 인증	XSCF→외부 네트워크
123/UDP	NTP에 의한 시간 동기화(외부 서버를 사용하는 경우)	XSCF→외부 네트워크
161/UDP	SNMP 기능	외부 네트워크 →XSCF
162/UDP	SNMP 트랩 기능	XSCF→외부 네트워크
443/TCP	XSCF 웹(HTTPS)	외부 네트워크 →XSCF

5장

잠금/서비스 모드로 전환

이 장에는 유지 관리 작업에 사용되는 서비스 모드와 잠금 모드 간의 차이 및 모드 전환 방법이 설명되어 있습니다.

- 잠금 모드와 서비스 모드 간의 차이 이해
- 작동 모드 전환

5.1 잠금 모드와 서비스 모드 간의 차이 이해

SPARC M10 시스템은 2개 작동 모드를 제공합니다. 잠금 모드 및 서비스 모드.

- 잠금 모드
  잠금 모드는 정기적인 작동 전용 모드입니다. 모드 스위치가 "잠금"으로 설정됩니다.

  XSCF에서 구성된 사용자 계정이 작업 동안 사용됩니다. 사용 가능한 작업 범위는 사용자 계정 유형에 따라 변경됩니다.

  잠금 모드에서 전원은 실수로 인한 잘못된 분리로부터 전원 공급을 보호하도록 쉽게 꺼지지 않게 구현됩니다. 운영 패널의 POWER 스위치는 전원 공급에 사용할 수 있지만 전원 차단에는 사용할 수 없습니다.

- 서비스 모드
  서비스 모드는 유지 관리 작업 전용 모드입니다. 모드 스위치가 "서비스"로 설정됩니다. 서비스 모드에서 시스템 전체가 정지한 동안 유지 관리를 수행해야 합니다.

  서비스 모드의 경우 전용 사용자 계정이 사용됩니다.

잠금 모드와 서비스 모드에서의 전원 공급 및 차단 제어는 POWER 스위치 작동은 물론 원격 전원 제어, 자동 전원 제어 등에도 영향을 미칩니다. 표 5-1에는 전원 제어 면에서의 두 모드 간 차이가 나타나 있습니다.

표 5-1 전원 제어 면에서의 잠금 모드와 서비스 모드 간 차이

항목	작동 모드	
	잠금 모드	서비스 모드
POWER 스위치에 의한 전원 공급	설정에 따라 다름 (기본적으로 전원 공급이 허용됨)	전원 공급이 허용됨

표 5-1 전원 제어 면에서의 잠금 모드와 서비스 모드 간 차이 (계속)

항목	작동 모드	
	잠금 모드	서비스 모드
POWER 스위치에 의한 전원 차단	전원 차단이 허용되지 않음	전원 차단이 허용됨 길게 누르면 전원 차단 시퀀스가 시작됨(4초 이상)
브레이크 신호	설정에 따라 다름 (기본적으로 활성화됨)	제어 도메인으로 전송됨
정전 복구 후 전원 공급	전원이 공급됨	전원이 공급되지 않음
활성화 확인	설정에 따라 다름 (기본적으로 활성화됨)	비활성화됨
호스트 와치독 시간 초과 시의 반응	설정에 따라 다름 (기본값은 PPAR 재설정임)	설정에 따라 다름 (기본값은 PPAR 재설정임)
자동 예약 전원 공급	전원 공급이 허용됨	전원 공급이 허용되지 않음
자동 예약 전원 차단	전원 차단이 허용됨	전원 차단이 허용되지 않음
원격 전원 제어	사용 가능	사용 불가능

"설정에 따라 다름"이라고 표시된 잠금 모드 및 서비스 모드 제어 항목은 XSCF 펌웨어의 setpparmode 명령을 사용하여 구성할 수 있습니다.

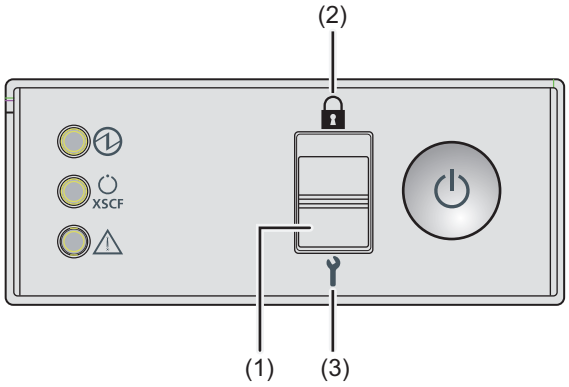
5.2 작동 모드 전환

SPARC M10 시스템의 작동 모드를 전환하려면 운영 패널의 모드 스위치를 사용합니다.

그림 5-1 운영 패널(SPARC M10-1)

번호	구성요소
1	모드 스위치
2	잠금 모드
3	서비스 모드

그림 5-2 운영 패널(SPARC M10-4)

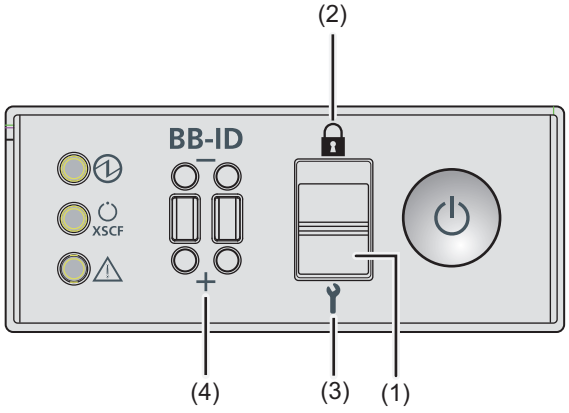


번호	구성요소
1	모드 스위치
2	잠금 모드
3	서비스 모드

빌딩 블록 구성의 SPARC M10-4S에서는 SPARC M10-4S 운영 패널의 모드 스위치를 돌려 마스터 XSCF와 스탠바이 XSCF로서 설정합니다. 마스터 XSCF의 경우 크로스바 박스가 사용되지 않을 때 BB#00이 기본적으로 설정되고 크로스바 박스가 사용될 때는 XBBOX#80이 기본적으로 설정됩니다.

노트 - 빌딩 블록 구성의 SPARC M10-4S에서는 마스터 XSCF와 스탠바이 XSCF의 모드 스위치를 동일하게 설정합니다.

그림 5-3 운영 패널(SPARC M10-4S)/크로스바 박스



번호	구성요소
1	모드 스위치
2	잠금 모드
3	서비스 모드
4	BB-ID 스위치

노트 - SPARC M10-4에는 BB-ID 스위치가 없습니다. BB-ID 스위치는 다른 것과 조합 형태로 구성 가능한 캐비닛의 BB-ID를 설정하는 데 사용됩니다.

다음에는 잠금 모드에서 서비스 모드로 전환하고 서비스 모드에서 잠금 모드로 전환하는 방법이 설명되어 있습니다.

서비스 모드로 전환

SPARC M10 시스템에서 콜드 시스템 유지 관리 작업을 수행하거나 XSCF 초기 설정을 구성하려면 서비스 모드를 설정합니다.

잠금 모드에서 서비스 모드로 전환하는 절차는 아래 설명된 바와 같습니다.

1. **운영 패널에서 모드 스위치를 서비스( )로 돌립니다.**

잠금 모드로 전환

SPARC M10 시스템의 경우 서비스 모드에서 잠금 모드로 전환하는 절차는 아래 설명된 바와 같습니다.

1. **운영 패널에서 모드 스위치를 잠금( )으로 돌립니다.**

6장

SPARC M10 시스템 일일 관리

이 장에는 SPARC M10 시스템의 일일 관리 작업이 설명되어 있습니다.

XSCF 설정 정보의 백업

마스터 XSCF에 저장된 XSCF 설정 정보를 주기적으로 백업합니다. 마스터 XSCF를 포함한 FRU의 고장으로 FRU를 교체한 후 백업으로 저장한 XSCF 설정 정보를 복원하여 수행한 시스템 작동을 보호할 수 있습니다.

자세한 내용은 "15.7 XSCF 설정 정보 저장/복원"을 참조하십시오.

논리 도메인 설정 정보의 백업

Oracle VM Server for SPARC가 구성한 논리 도메인 설정 정보를 주기적으로 백업합니다. 제어 도메인에서 도메인으로 백업합니다. 백업은 명령 실행 시에 지정되는 파일 이름과 XML 형식으로 저장됩니다. 도메인 구성의 변경 시마다 최신 설정 정보를 백업합니다. 디스크 고장 시 중복 백업 파일을 다른 매체에 저장하는 것이 좋습니다.

자세한 내용은 "15.8 논리 도메인 구성 정보 저장/복원"을 참조하십시오.

내부 디스크 드라이브의 백업

내부 디스크 드라이브의 데이터를 주기적으로 백업합니다. 백업 방법은 드라이브 유형에 따라 다릅니다.

최신 펌웨어로 펌웨어 업데이트

SPARC M10 시스템 관리용 XSCF 펌웨어는 OpenBoot PROM, 하이퍼바이저 및 POST와 함께 XCP 패키지로서 제공됩니다. 새로운 기능 및/또는 버그 픽스가 추가된 최신 버전의 XCP 패키지가 정기적으로 배포됩니다. 공개되면 바로 최신 XCP 패키지를 적용하는 것이 좋습니다.

최신 펌웨어로의 업데이트 방법과 관련된 자세한 내용은 "18.1 XCP 펌웨어 업데이트"를 참조하십시오.

XCP 패키지의 새로운 기능과 변경 사항은 새 XCP 버전의 『SPARC M10 시스템 제품 노트』에 언급되어 있습니다. 읽어보시기 바랍니다.

CPU 코어 활성화 키의 백업

SPARC M10 시스템의 CPU는 필요 시 용량 제공(CoD) 형태로 제공됩니다. SPARC M10 시스템에 장착된 CPU의 사용 라이센스를 구입할 때 제공되는 CPU 코어 활성화 키는 SPARC M10 시스템에 등록한 후 안전한 곳에 저장합니다. CPU 코어 활성화 키가 등록된 디스크가 고장이더라도 CPU 코어 활성화 키를 다시 등록하면 비즈니스에 미치는 부정적인 영향이 최소화됩니다.

CoD의 자세한 내용은 "14장 필요 시 용량 제공(CoD)"을 참조하십시오.

7장

XSCF 펌웨어에서 항상 설정하는 항목과 항목 흐름에 대한 이해

이 장에는 XSCF를 사용하는 데 필요한 시스템의 설정 방법이 설명되어 있습니다.

- XSCF 설정을 위한 예비 작업
- XSCF 쉘에서 설정
- XSCF 웹에서 설정

7.1 XSCF 설정을 위한 예비 작업

이 절에는 XSCF를 설정하기 전에 확인 및 수행해야 하는 것이 설명되어 있습니다.

이 절에서는 캐비닛 설치, 케이블 연결, 시스템 초기 진단 및 기타 필요한 설치 작업이 수행된 것으로 가정합니다.

7.1.1 설정 전 초기 작업

XSCF 설정을 시작하기 전에 직렬 연결 또는 인터넷 연결을 가능케 하는 터미널을 사용하여 XSCF에 연결할 수 있도록 케이블 연결, 초기 서버 로그인, 인증 및 기타 필요한 작업을 마쳐야 합니다.

시스템 관리자와 현장 엔지니어는 다음 작업을 마친 후 XSCF 설정을 시작해야 합니다.

표 7-1 XSCF 설정을 시작하기 전에 수행하는 작업

작업	참조
XSCF 기본 사용자 계정을 사용하여 XSCF 초기 로그인 인증을 거칩니다.	『SPARC M10 시스템 설치 안내서』의 "6.3 XSCF에 로그인"
platadm 또는 useradm 사용자 권한이 있는 사용자 계정을 적어도 하나 등록합니다.	"8.3 XSCF 사용자 생성/관리"

정기적인 작동 동안 모드 스위치를 잠김으로 설정합니다.

7.1.2 최신 지원 정보 확인

설정을 시작하기 전에『SPARC M10 시스템 제품 노트』를 읽어 최신 제품 지원 정보를 확인합니다.

7.1.3 구성을 위한 사용자 인터페이스와 액세스 방법

PC를 마스터 XSCF에 연결하여 XSCF를 설정합니다. 필요한 설정을 구성하려면 명령줄 인터페이스인 XSCF 쉘을 사용하거나 브라우저 사용자 인터페이스인 XSCF 웹을 사용하여 XSCF에 액세스합니다.

표 7-2 사용자 인터페이스와 XSCF 액세스 방법

사용자 인터페이스	**XSCF** 액세스
XSCF 쉘 (명령줄 인터페이스)	직렬 포트에 연결된 PC에서 로그인합니다. SSH 또는 Telnet 서비스를 사용하여 XSCF 전용 LAN 포트(XSCF-LAN)에 연결된 PC에서 로그인합니다.
XSCF 웹 (브라우저 사용자 인터페이스)	HTTPS 서비스를 사용하여 웹 브라우저가 설치 및 XSCF-LAN에 연결된 PC에서 로그인합니다.

사용 가능한 기능은 인터페이스에서 동일합니다. 하지만 XSCF 웹을 사용하려면 먼저 XSCF 쉘을 사용하여 설정을 구성합니다. 또한 XSCF 웹은 일부 기능을 지원하지 않습니다. 지원되지 않은 기능은 XSCF 쉘을 사용하여 구성합니다. XSCF 웹이 지원하는 기능은 "부록 B XSCF 웹 페이지 목록"을 참조하십시오.

설정 절차

절차는 사용하는 사용자 인터페이스에 따라 다릅니다.

- XSCF 쉘을 사용하는 경우
  "7.2 XSCF 쉘에서 설정"를 참조하십시오.
- XSCF 웹을 사용하는 경우
  "7.3 XSCF 웹에서 설정"를 참조하십시오.

설정 정보

XSCF 구성 후 구성된 정보는 XSCF와 PSU 백플레인 또는 크로스바 백플레인 장치에 자동 저장됩니다. 따라서 XSCF가 구성되면 일일 관리가 필요하지 않습니다. 하지만 XSCF 정보를 저장 및 복원할 수 있습니다. XSCF 설정 정보의 저장 및 복원 방법은 "15.7 XSCF 설정 정보 저장/복원"을 참조하십시오.

설명서 페이지

XSCF 쉘 명령, 옵션 및 사용자 권한의 자세한 설명은『SPARC M10 Systems XSCF Reference Manual』또는 XSCF의 설명서 페이지를 참조하십시오. 설명서 페이지는 XSCF에서 man 명령을 실행하여 참조할 수 있습니다. 설명서 페이지는『SPARC M10 Systems XSCF Reference Manual』과 동일한 설명을 제공합니다.

7.2 XSCF 쉘에서 설정

이 절에는 XSCF 쉘을 사용하여 시스템을 설정하는 방법 흐름이 설명되어 있습니다.

단계의 자세한 내용은 제목에 큰 따옴표가 붙은 절을 참조하십시오. (옵션) 항목은 표준 구성에서 권장되지만 필수는 아닌 설정입니다. 환경에 따라 설정을 활성화 또는 비활성화합니다.

1. 직렬 연결을 가능케 하는 터미널에서 **XSCF** 쉘에 연결합니다.
   서버와 직렬 연결된 보안 환경을 설정합니다.

   자세한 내용은 "4.1.2 직렬 연결로 XSCF 쉘에 로그인하는 방법"을 참조하십시오.

2. **XSCF** 쉘에 로그인합니다.
   초기 로그인 인증 시에 구성되는 새 사용자 계정을 사용하여 XSCF 쉘에 로그인합니다.

   로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   초기 로그인 인증 시에 새 사용자 계정을 생성하려면 "8.3 XSCF 사용자 생성/관리"를 참조하십시오.

3. 암호 정책을 구성합니다.
   유효한 암호 조건 및 XSCF 사용자 계정의 허용 문자 수와 같은 암호 특성을 지정합니다.

   자세한 내용은 "8.3 XSCF 사용자 생성/관리"을 참조하십시오.

4. **XSCF** 사용자 계정을 구성합니다.
   환경에 적합하도록 서버로 XSCF 사용자 계정을 로컬 등록합니다.

   - 사용자 계정을 추가하려면 -l 옵션을 사용하여 `showuser` 명령을 실행하고 사용자 계정 목록에 유효하지 않은 사용자 계정이 없는지 확인합니다.
   - 유지 관리 작업을 고려하여 fieldeng 사용자 권한이 있는 현장 엔지니어(FE)용 사용자 계정을 구성합니다.

   자세한 내용은 "8.3 XSCF 사용자 생성/관리"을 참조하십시오.

5. 감사 설정(옵션)을 구성합니다.
   감사 기능은 XSCF 로그인, 로그아웃 및 기타 이벤트를 감사 로그에 기록합니다. 감사 기능은 기본적으로 활성화됩니다. 감사 설정의 경우 auditadm 사용자 권한이 필요합니다.

   자세한 내용은 "8.8 XSCF 보안 강화를 위한 감사 구성"을 참조하십시오.

6. 시간 설정을 구성합니다.
   시스템 표준 시간인 XSCF 시간 설정을 구성합니다. 시스템 시간이 업데이트되면 XSCF 재설정이 수행되고 XSCF 세션이 분리됩니다. 다시 로그인합니다.

   자세한 내용은 "8.4 XSCF 시간/날짜 설정"을 참조하십시오.

노트 - 이 설정은 초기 시작 시에 설정됩니다. 설정을 변경해야 하는 경우 설정을 다시 구성하십시오.

---

7. **SSH/Telnet** 서비스를 구성합니다.

SSH와 Telnet은 동시 활성화가 가능합니다. 하지만 Telnet 연결은 보안 프로토콜을 기반으로 하지 않습니다. SSH를 활성화하는 경우 Telnet을 비활성화하는 것이 좋습니다.

SSH 및 Telnet 서비스는 기본적으로 비활성화됩니다.

자세한 내용은 "8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성"을 참조하십시오.

8. **XSCF 호스트 공개 키를 확인합니다.**
XSCF-LAN 연결에서 SSH를 사용하는 경우 showssh 명령을 실행하고 지문을 기록합니다. 호스트 공개 키의 텍스트 데이터를 클라이언트 디렉토리의 파일로 복사합니다.

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

자세한 내용은 "8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성"을 참조하십시오.

9. 사용자 공개 키를 등록합니다.
XSCF-LAN 연결을 통해 SSH 사용자 키를 사용하는 경우 사용자 비밀 키와 사용자 공개 키를 클라이언트의 등록된 XSCF 사용자 계정에 생성하고 사용자 공개 키를 XSCF에 등록합니다.

자세한 내용은 "8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성"을 참조하십시오.

10. **XSCF 전용 네트워크를 구성합니다.**
XSCF-LAN IP 주소 및 SSCP와 같은 XSCF 네트워크 설정을 구성합니다. SSH, Telnet 또는 HTTPS를 사용하여 2명 이상의 사용자가 XSCF에 동시 액세스할 수 있

습니다.

applynetwork 명령을 실행하여 네트워크 구성을 적용합니다. 그런 다음 네트워크 구성이 완료되도록 rebootxscf 명령을 실행하여 XSCF를 재설정합니다. XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.

자세한 내용은 "8.5 XSCF 네트워크 구성"을 참조하십시오.

11. **XSCF-LAN(옵션) 연결을 가능케 하는 터미널에서 XSCF 쉘에 연결합니다.**
이 단계에서 XSCF-LAN 연결을 사용하여 설정을 구성할 수 있습니다. XSCF-LAN에 연결된 PC에서 IP 주소를 지정하고 XSCF에 연결한 후 다시 로그인합니다.

XSCF-LAN 연결로 전환하지 않고 직렬 연결에서 설정을 구성하려면 12단계로 이동합니다.

Telnet 연결은 보안 프로토콜을 기반으로 하지 않습니다. SSH를 사용하는 것이 좋습니다. SSH 로그인의 경우 호스트 공개 키의 지문 유효성이 조회됩니다. 지문이 8단계에서 기록한 지문과 동일한지 확인하고 "yes"로 응답합니다. 지문이 일치하지 않으면 대상의 IP 주소가 올바르고 고유한지 다시 확인합니다. 이는 "가장"을 의미하는 것일 수도 있습니다.

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

사용자 키 인증으로 SSH를 사용하고 암호가 구성된 경우 암호를 입력합니다.

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

12. **NTP 설정(옵션)을 구성합니다.**
XSCF가 NTP 서버로서 작동하거나 XSCF가 NTP 클라이언트로서 작동하도록 설정을 구성합니다. 특정된 경우 도메인 구성 후에 NTP 설정을 구성할 수 있습니다.

자세한 내용은 "8.4 XSCF 시간/날짜 설정"을 참조하십시오.

13. **SMTP 설정(옵션)을 구성합니다.**
XSCF 이메일 알림 기능을 사용하도록 설정을 구성합니다.

자세한 내용은 "15.2 고장 발생 시 이메일을 통한 알림 수신"을 참조하십시오.

14. **SNMP 설정(옵션)을 구성합니다.**
자세한 내용은 "15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리"을 참조하십시오.

15. **원격 유지 관리 서비스(옵션)를 사용하도록 설정을 구성합니다.**
본 설명서에는 원격 유지 관리 서비스 기능이 자세히 언급되어 있지 않습니다. 원격 유지 관리 서비스 기능과 관련된 정보는 『SPARC M10 시스템 제품 노트』를 참조하십시오.

다음 단계에서는 전체 시스템 하드웨어의 관리 설정을 구성합니다.

16. **고도 설정을 구성합니다.**
자세한 내용은 "9.1 시스템 고도 설정/확인"을 참조하십시오.

노트 - 이 설정은 초기 시작 시에 설정됩니다. 설정을 변경해야 하는 경우 설정을 다시 구성하십시오.

17. 전원 캡핑 설정(옵션)을 구성합니다.
    자세한 내용은 "9.4 소비 전력 최소화"을 참조하십시오.

18. 시스템 보드 설정(옵션)을 구성합니다.
    메모리 미러 모드에서 시스템 보드를 구성합니다.

    자세한 내용은 "12.1 메모리 미러링 구성"을 참조하십시오.

19. 이중 전원 공급 설정(옵션)을 구성합니다.
    이중 전원 공급 설정을 활성화 또는 비활성화합니다.

    자세한 내용은 "9.3 이중 전원 공급 활성화/비활성화"을 참조하십시오.

노트 - 이 설정은 초기 시작 시에 설정됩니다. 설정을 변경해야 하는 경우 설정을 다시 구성하십시오.

20. 에어 컨디셔닝 대기 시간(옵션)을 구성합니다.
    룸 온도가 에어 컨디셔닝 장비에 의해 조절될 때까지 전원 공급 시퀀스의 대기 시간을 구성합니다.

    자세한 내용은 "9.2.2 시작 대기 시간 설정/확인"을 참조하십시오.

다음 단계에서는 물리 분할(PPAR) 설정을 구성합니다.

21. 물리 분할 설정(옵션)을 구성합니다.
    도메인 구성 관리 정보를 구성합니다.

    자세한 내용은 "16.2 물리 분할 확인" 및 『SPARC M10 시스템 도메인 구성 안내서』를 참조하십시오.

22. 물리 분할 모드 설정(옵션)을 구성합니다.
    자세한 내용은 "10.2 물리 분할 작동 모드 설정" 및 『SPARC M10 시스템 도메인 구성 안내서』의 "3장 물리 분할 구성"을 참조하십시오.

23. **CoD** 설정을 구성합니다.
    자세한 내용은 "14장 필요 시 용량 제공(CoD)"을 참조하십시오.

24. 웜업 시간(옵션)을 구성합니다.
    서버 전원 공급 프로세스 시퀀스의 시작 후 Oracle Solaris가 시작되기 직전, 지정된 시간이 경과할 때까지 전원 공급 프로세스의 지연 시간을 구성합니다. 이 설정은 서버가 웜업되고 주변 장치에 전원이 공급될 때까지 대기하는 데 사용됩니다.

    또한 setpowercapping 명령으로 소비 전력의 상한을 설정하는 경우 한 번에 모든 물리 분할이 시작될 때 이 상한을 초과할 수 있습니다. 이를 피하도록 이 설정을 사용하여 각 물리 분할을 시작할 때 시간 차이를 설정할 수도 있습니다.

    자세한 내용은 "9.2.1 웜업 시간 설정/확인"을 참조하십시오.

25. 전원 예약(옵션)을 구성합니다.
    각 물리 분할마다 전원 예약 정보를 구성합니다.

    전원 예약을 구성하려면 XSCF 펌웨어 setpowerschedule, addpowerschedule 및 deletepowersched 명령을 사용합니다. 명령의 자세한 내용은 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

7.3 XSCF 웹에서 설정

이 절에는 XSCF 웹을 사용하여 시스템을 설정하는 방법 흐름이 설명되어 있습니다. 단계의 자세한 내용은 제목에 큰 따옴표가 붙은 절을 참조하십시오.

XSCF 웹을 사용하려면 사전에 XSCF 쉘을 사용하여 HTTPS 서비스를 활성화하도록 설정을 구성해야 합니다.

1. 직렬 연결을 가능케 하는 터미널에서 **XSCF** 쉘에 연결합니다.
   자세한 내용은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
2. **"7.2 XSCF** 쉘에서 설정**"**의 **2 ~ 11**단계를 수행합니다**. XSCF** 쉘을 사용하여 **7.2**절의 **2 ~ 11**단계를 이미 수행한 경우 이 절에서 아래 **3**단계로 이동합니다**.**
3. **HTTP** 설정**(**옵션**)**을 구성합니다**.**
   "8.7 XSCF에 로그인하기 위한 HTTPS 서비스 구성"를 참조하십시오.
4. 웹 브라우저부터 **XSCF**까지 연결합니다**.**
   XSCF-LAN에 연결되고 웹 브라우저가 실행 중인 PC에서 XSCF 웹에 연결하기 위한 호스트 이름 또는 IP 주소를 지정합니다.

```
<웹 브라우저의 URL 입력 이미지>
URL https://192.168.111.111 (XSCF IP 주소<숫자>입력)/
또는,
https://XSCF host name (참고: 도메인 호스트 이름이 아님)/
```

5. **XSCF** 웹 콘솔에서 **XSCF**에 로그인합니다**.**
   이미 구성된 사용자 계정으로 로그인합니다.

```
<웹 브라우저의 로그인 인증 입력 이미지>
login:yyyy
Password:xxxxxxxx
```

   XSCF 웹 브라우저 창을 XSCF 웹 콘솔이라고도 합니다.

   자세한 내용은 "4.5 XSCF 웹에 로그인"을 참조하십시오.

6. 설정 항목은 **XSCF** 쉘에서의 설정 항목과 동일합니다**. "7.2 XSCF** 쉘에서 설정**"**의 **12**단계 및 후속 단계에서 수행한 것과 동일한 방법으로 **XSCF** 웹 콘솔을 사용하여 설정을 구성합니다**.**

노트 **-** 고도 설정 및 이중 전원 공급 설정과 같이 XSCF 웹 메뉴에 포함되지 않은 항목을 구성하려면 XSCF 쉘을 사용하십시오.

8장

XSCF 펌웨어 구성

이 장에는 XSCF를 설정하는 방법이 자세히 설명되어 있습니다.

- XSCF의 원활한 설정
- XSCF 펌웨어 설정 이해
- XSCF 사용자 생성/관리
- XSCF 시간/날짜 설정
- XSCF 네트워크 구성
- XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성
- XSCF에 로그인하기 위한 HTTPS 서비스 구성
- XSCF 보안 강화를 위한 감사 구성

8.1 XSCF의 원활한 설정

이 절에는 XSCF 설정을 시작하기 전에 이해해야 할 내용이 설명되어 있습니다.

많은 경우 기본 값과 설정으로 시스템이 실행될 수 있습니다. 하지만 환경에 적합하도록 서버를 구성해야 합니다. 『SPARC M10 시스템 설치 안내서』에 따라 이미 수행한 작업과 결정할 항목을 사전에 확인하여 구성 시간을 줄일 수 있습니다. 설정 구성을 시작하기 전에 다음을 고려합니다.

- 있다면 초기 시작 시에 이미 구성된 항목 모두를 나열합니다. 나중에 설명되는 항목의 경우 항목에 구성된 설정 정보를 표시하고 재구성이 필요하지 않은지 확인합니다.
- 유지 관리, 시스템 관리자 및 물리 분할 등에 맞게 필요한 사용자 계정이 구성되었는지 확인합니다.
- 서버 구성을 다시 확인합니다. 네트워크 주소, 도메인 구성, CPU 코어 활성화 수와 같은 필요한 모든 항목이 중복 또는 누락 설정 없이 구성되었는지 확인합니다. 환경에 부적합한 설정이 있는 경우 네트워크 주소를 다시 구성하거나 기타 조치를 취해야 합니다.
- XSCF 네트워크에 연결하면 다양한 서비스를 사용할 수 있습니다. 호스트 액세스 제한, 알림 등과 관련된 원격 유지 관리 서비스 및 표준 시간 설정에서 유효하지 않은 액세스에 사용하는 조치를 사전에 결정합니다.

- 절전 구현의 경우 서버 작동 환경을 조심스럽게 살핍니다. 서버가 위치하는 룸의 면적 및 주변 온도와 같은 설치 환경 요소에 적합하도록 시작 전의 서버 대기 시간을 결정합니다. 또한 최대 소비 전력 값과 기타 필요한 값을 결정합니다.

8.2 XSCF 펌웨어 설정 이해

이 절에는 XSCF 펌웨어를 설정하는 절차가 자세히 설명되어 있습니다.

8.2.1 XSCF를 사용하기 위한 설정 항목

XSCF의 다양한 설정이 주로 다음 용도로 사용됩니다.

- XSCF 펌웨어를 사용하기 위한 설정
- 물리 분할(PPAR)과 논리 도메인을 구성하기 위한 설정
- 시스템 하드웨어를 관리 및 제어하기 위한 설정
- 이벤트 알림과 기타 기능을 위한 설정

이 절에는 XSCF 펌웨어를 사용하기 위한 설정이 설명되어 있습니다. 물리 분할과 논리 도메인 구성 설정은 10장 및『SPARC M10 시스템 도메인 구성 안내서』를 참조하십시오. CoD 설정, 전원 설정 및 기타 하드웨어 관리/제어 설정은 "9장 시스템 구성" 및 "13장 시스템 구성 확장"을 참조하십시오. 기타 설정은 관련 장/절을 참조하십시오.

표 8-1에는 XSCF 펌웨어를 사용하기 위한 설정 항목이 설명되어 있습니다. 각 항목의 자세한 내용은 표에 나타난 절을 참조하십시오.

표 8-1 XSCF를 사용하기 위한 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	서비스가 기본적으로 활성화 또는 비활성화되는지 여부	참조:
사용자 관리	필수	활성화됨	8.3
시간	필수	활성화됨	8.4
네트워크	필수	활성화됨	8.5
SSH/Telnet 서비스	옵션	비활성화됨	8.6
HTTPS 서비스	옵션	비활성화됨	8.7
감사	옵션	활성화됨	8.8

8.2.2 마스터 XSCF 확인

2개 이상의 XSCF가 구현되는 시스템에서 사용자는 마스터 XSCF 또는 스탠바이 XSCF에만 액세스할 수 있습니다. 마스터 XSCF에서 XSCF 설정을 구성합니다. 마스터 XSCF는 원칙적으로 빌딩 블록 구성의 크로스바 박스 80 또는 81이나 ID(BB-ID)가 0 또는 1인 캐비닛에 구현됩니다. 스탠바이 XSCF는 위 번호대로 구현됩니다.

시스템이 실행되는 동안 마스터 XSCF가 스탠바이 XSCF로 전환되면 마스터 XSCF의 위치 또한 0에서 1로 변경되고 스탠바이 XSCF는 1에서 0으로 변경됩니다.

XSCF가 2개 이상인 시스템의 경우 마스터 XSCF와 스탠바이 XSCF의 구성요소 위치 번호는 아래 설명된 바와 같습니다.

- SPARC M10-4S 시스템(크로스바 박스 없음)
  마스터 XSCF: BB#00

  스탠바이 XSCF: BB#01
- SPARC M10-4S 시스템(크로스바 박스 있음)
  마스터 XSCF: XBBOX#80

  스탠바이 XSCF: XBBOX#81

XSCF가 하나만 있는 시스템의 경우 연결 대상 XSCF가 마스터 XSCF입니다. XSCF가 2개 이상인 시스템의 경우 다음 절차에 따라 마스터 XSCF를 확인하고 연결합니다.

- MASTER LED를 확인하고 직렬 연결을 합니다.

전원이 SPARC M10-4S 또는 크로스바 박스로 공급되고 마스터 XSCF가 초기화된 후 XSCF 장치의 후면 패널에서 MASTER LED가 켜집니다. PC를 동일 패널의 직렬 포트에 연결합니다. 마스터 XSCF에 로그인할 수 있습니다.

- 인계 IP 주소 또는 마스터 XSCF IP 주소를 지정하고 연결합니다.

마스터 XSCF 및 스탠바이 XSCF에는 각각 XSCF LAN#0과 LAN#1 포트가 있습니다. LAN#0 포트와 LAN#1 포트는 중복을 위해 동일 서브넷을 통해 서로 연결됩니다.

마스터 XSCF에 연결하려면 LAN#0 인계 IP 주소 또는 LAN#1 인계 IP 주소를 지정합니다. 마스터와 스탠바이 간의 전환 후라도 동일한 인계 IP 주소를 지정하면 마스터 XSCF로의 연결이 설정됩니다.

또는 마스터 XSCF LAN#0 또는 LAN#1 IP 주소를 지정하고 마스터 XSCF에 연결합니다. 시스템에 XSCF가 하나만 있거나 유지 관리로 인해 스탠바이 XSCF에 액세스할 수 없는 경우 이를 수행합니다.

지정된 IP 주소로 마스터 XSCF를 연결하여 로그인한 후 showhardconf 명령을 실행합니다. 어떤 SPARC M10-4S의 캐비닛 또는 크로스바 박스가 마스터 XSCF인지 확인할 수 있습니다.

다음 예에는 BB-ID 0이 마스터 XSCF인 것으로 나타나 있습니다.

```
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 ;
:
```

다음 예에는 크로스바 박스 80이 마스터 XSCF인 것으로 나타나 있습니다.

```
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 ;
:
```

노트 - 마스터 XSCF에 구성된 설정이 스탠바이 XSCF에 적용됩니다.

8.2.3 스탠바이 XSCF에서 실행 가능한 기능

스탠바이 XSCF에서 사용 가능한 기능과 실행 가능한 명령은 아래 설명된 바와 같습니다.

- XSCF 종료: exit 명령
- 설명서 페이지 표시: man 명령
- XSCF 재설정: rebootxscf 명령
- 사용자 권한 설정: setprivileges 명령
- 캐비닛 상태 표시: showbbstatus 명령
- 명령의 끝 상태 표시: showresult 명령
- 사용자 정보 표시: showuser 명령
- 펌웨어 덤프: snapshot 명령
- XSCF 전환: switchscf 명령
- 감사 보기: viewaudit 명령
- 로그인 사용자 표시: who 명령

명령의 자세한 내용은 설명서 페이지 및 『SPARC M10 Systems XSCF Reference

Manual』을 참조하십시오.

8.2.4 설명서 페이지를 사용한 명령의 옵션 세부 사항 확인

XSCF를 구성할 때 XSCF에서 man (1) 명령을 실행하면 피연산자, 옵션 등의 설명과 더불어 XSCF 명령의 설명서 페이지가 표시됩니다. 설명서 페이지는『SPARC M10 Systems XSCF Reference Manual』과 동일한 자세한 명령 설명을 제공합니다.

```
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.
:
```

8.3 XSCF 사용자 생성/관리

이 절에는 XSCF 로그인에 사용되는 로컬 사용자 계정, 암호, 사용자 권한, 암호 정책의 생성 및 관리 방법이 설명되어 있습니다.

8.3.1 XSCF 사용자 계정

XSCF 사용자 계정의 사용

XSCF 사용자 계정은 SSH, Telnet 또는 XSCF 웹을 통해 XSCF 쉘에 로그인하는 데 사용됩니다.

사용자 계정이 로그인 인증 통과에 실패하면 지정된 시간 동안 사용자 계정이 잠길 수 있습니다. 계정 잠금 기능을 XSCF 사용자 계정 잠금 기능이라고 합니다. 시스템 관리자는 사용하는 XSCF 사용자 계정을 비활성화 또는 활성화할 수 있습니다.

XSCF 사용자 계정을 등록할 수 있는 사용자

XSCF 사용자 계정을 등록하려면 useradm 사용자 권한이 있는 사용자 계정을 사용하여

로그인합니다.

사용 가능한 XSCF 사용자 계정 이름

다음 XSCF 사용자 계정 이름은 시스템을 위해 예약된 이름이며 사용자가 사용할 수 없습니다.

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

사용 가능한 문자의 자세한 내용은 adduser(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

사용자 계정 수

지정 가능한 사용자 계정 수는 100개이며 평균 사용자 계정당 10자가 사용되는 것으로 가정합니다. adduser 명령을 사용하여 등록한 사용자 계정의 경우 UID라고 하는 ID가 자동 할당됩니다. UID는 수동으로 지정할 수도 있습니다. UID의 지정 가능한 범위는 100 ~ 60000입니다.

8.3.2 암호 및 암호 정책

XSCF 사용자 계정을 등록하는 경우 암호도 등록합니다. 새로 생성한 사용자 계정의 경우에는 암호가 구성되지 않습니다. 따라서 이는 password 명령을 사용하여 암호를 설정하거나 보안 쉘(SSH)을 사용하여 공개 키를 사용자로 설정할 때까지 로그인하는 데 사용할 수 없습니다.

암호와 관련하여 길이, 문자 유형 등과 같은 제한이 있습니다. 암호 특성은 암호 정책이라고 하는 규칙 세트에 부합되어야 합니다. 생성된 사용자 계정과 관련하여 현재 암호 정책이 생성된 사용자 계정에 적용됩니다. 암호 정책이 다시 구성되면 암호 정책이 나중에 추가되는 사용자에 적용됩니다. showpasswordpolicy 명령을 사용하여 현재 암호 정책을 확인할 수 있습니다.

암호 정책 항목의 자세한 내용은 setpasswordpolicy(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

8.3.3 사용자 권한 유형

XSCF 사용자 계정을 추가하는 경우 사용자 권한을 계정에 할당해야 합니다. 사용자 권한은 다음과 같도록 사용자 계정에 할당됩니다.

- 시스템 관리자가 서버 전체에 대한 작동 권한을 갖도록 합니다.
- 작동이 특정 또는 지정된 물리 분할로 제한되는 사용자 계정을 관리합니다.
- 사용자 계정을 관리합니다.
- 감사를 구성합니다.
- 현장 엔지니어에 허용 가능한 서버 작동을 제한합니다.

1개 사용자 계정에 2개 이상의 사용자 권한을 지정할 수 있습니다. 사용자의 환경과 활용에 따라 사용자 권한을 계정에 할당합니다. 표 8-2에는 사용자 권한이 나열되어 있습

니다.

표 8-2 사용자 권한

사용자 권한	요약	설명
pparop@n	1개 전체 PPAR n의 상태를 참조함.	• 1개 PPAR n에 장착된 하드웨어의 모든 상태를 참조할 수 있음. • 1개 PPAR n의 모든 상태를 참조할 수 있음.
pparmgr@n	전원 작동과 1개 PPAR n만의 상태를 참조함.	• 전원을 공급/차단하고 1개 PPAR n을 재부팅할 수 있음. • 1개 PPAR n에 장착된 하드웨어의 모든 상태를 참조할 수 있음. • 1개 PPAR n의 모든 상태를 참조할 수 있음.
pparadm@n	1개 PPAR n만 관리함.	• 1개 PPAR n에 장착된 하드웨어에서 모든 작동을 수행할 수 있음. • 1개 PPAR n에 장착된 하드웨어의 모든 상태를 참조할 수 있음. • 1개 PPAR n에서 모든 작동을 수행할 수 있음. • 1개 PPAR n의 모든 상태를 참조할 수 있음.
platop	전체 시스템의 상태를 참조함.	서버의 모든 상태를 참조할 수 있지만 상태를 변경할 수는 없음.
platadm	전체 시스템을 관리함.	• 시스템 하드웨어에서 모든 작동을 수행할 수 있음. • useradm 및 XSCF 감사 권한이 필요한 경우를 제외하고 모든 XSCF 설정을 구성할 수 있음. • 하드웨어를 PPAR에 추가/삭제할 수 있음. • PPAR 전원 작동을 수행할 수 있음. • 모든 서버 상태를 참조할 수 있음.
useradm	사용자 계정을 관리함.	• 사용자 계정을 생성, 삭제, 활성화 및 비활성화할 수 있음. • 사용자 암호와 암호 프로파일을 변경할 수 있음. • 사용자 권한을 변경할 수 있음.
auditop	감사 상태를 참조함.	XSCF 참조 상태와 감사 방법을 참조할 수 있음.
auditadm	감사를 제어함.	• XSCF 감사를 제어할 수 있음. • XSCF 감사 방법을 삭제할 수 있음.
fieldeng	현장 엔지니어가 사용함.	현장 엔지니어만 유지 관리 작동 및 구성 변경을 수행할 수 있음.

대상 물리 분할에 대한 사용자 권한의 경우 "@PPAR-number"를 사용자 권한 이름에 추가합니다. (예를 들어 PPAR-ID 01에 대한 pparadm이 pparadm@1이어야 함)

1개 사용자 계정에 대상 물리 분할을 포함한 2개 이상의 물리 분할에 대한 권한이 있을 수 있습니다. 사용자 권한 설정의 자세한 내용은 setprivileges(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

8.3.4 XSCF 사용자 계정과 관련된 설정 항목 및 명령의 확인

표 8-3에는 XSCF 사용자 계정과 관련된 설정 항목 및 해당 XSCF 쉘 명령이 나타나 있습니다.

표 8-3 XSCF 사용자 계정과 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
사용자 계정의 추가/삭제	필수	showuser(8), adduser(8), deleteuser(8)
사용자 계정의 활성화/비활성화	필수	enableuser(8), disableuser(8)
암호 정책의 구성	옵션	setpasswordpolicy(8), showpasswordpolicy(8)
암호의 구성	필수	password(8)
사용자 권한의 할당	필수	setprivileges(8), showuser(8)
잠금 기능의 구성	옵션	setloginlockout(8), showloginlockout(8)

8.3.5 XSCF 사용자 계정 등록 흐름

XSCF 제공 시에 구성되는 기본 사용자 계정이 아닌 사용자 계정을 등록합니다.

사용자 계정 "기본"에는 다음 권한이 있습니다.

- "기본"의 권한: useradm 및 platadm

초기 시작 시에 기본 계정을 사용하여 로그인하는 경우 useradm 및 platadm 사용자 권한이 있는 사용자 계정을 적어도 하나는 등록합니다. 기본 사용자 계정으로 로그인 인증은 『SPARC M10 시스템 설치 안내서』를 참조하십시오.

등록 흐름

시스템 관리자는 다음 단계를 수행하여 사용자 계정을 등록해야 합니다. 단계의 자세한 내용은 나타난 절을 참조하십시오.

1. **useradm 권한이 있는 사용자 계정으로 로그인합니다(8.3.6절 참조).**
   기본 사용자 계정 "기본"에는 useradm 권한이 있습니다.
2. 등록된 사용자를 확인합니다**(8.3.6절의 showuser(8) 설명 참조).**
   사용자 계정을 추가하는 경우 -l 옵션을 사용하여 showuser 명령을 실행하고 사용자 계정 목록에 유효하지 않은 사용자 계정이 없는지 확인합니다.
3. 암호 정책을 확인 또는 변경합니다**(8.3.6절의 showpasswordpolicy(8) 및 setpasswordpolicy(8) 설명 참조).**

4. 사용자 계정을 등록합니다(8.3.7절의 **adduser(8)** 설명 참조).
adduser 명령을 사용하여 사용자 환경에 적합하도록 사용자 계정을 등록합니다.
5. 암호를 확인합니다(8.3.7절의 **password(8)** 설명 참조).
6. 사용자 권한을 등록합니다(8.3.8절의 **setprivileges(8)** 설명 참조).
명령의 자세한 내용은 설명서 페이지 및 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

8.3.6 암호 정책 확인/변경

암호 정책이 구성되면 암호 정책이 이후 추가되는 사용자에 적용됩니다.
showpasswordpolicy 및 setpasswordpolicy 명령을 사용하여 현재 암호 정책을 확인하고 필요에 따라 변경합니다.

1. **useradm** 권한이 있는 사용자 계정으로 로그인합니다.

```
login: xxxxxxxxxx
Password: xxxxxxxxxxx
XSCF>
```

2. **showuser** 명령을 실행하여 모든 로컬 사용자 계정과 관련된 정보를 표시합니다.

```
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
```

3. **showpasswordpolicy** 명령을 실행하여 암호 정책을 확인합니다.

```
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
```

4. **setpasswordpolicy** 명령을 실행하여 암호 정책을 구성합니다.
   다음 예에서 재시도 카운트: 3, 암호 문자 수: 2개 이상의 숫자를 포함하여 8, 유효 기간: 60일 및 만료 경고 시작일: 15일 전으로 지정됩니다.

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

5. **showpasswordpolicy** 명령을 실행하여 설정을 확인합니다.

```
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
```

노트 - 사용자 피연산자에서 다른 사용자를 지정하여 암호를 변경할 때 시스템 암호 정책이 적용되지 않습니다. 다른 사용자의 암호를 변경하는 경우 시스템 암호 정책에 부합되는 암호를 지정하십시오.

8.3.7 XSCF 사용자 계정 추가/삭제 및 암호 구성

사용 가능한 사용자 계정 이름은 "사용 가능한 XSCF 사용자 계정 이름"을 참조하십시오.

1. **useradm** 권한이 있는 사용자 계정으로 로그인합니다.

```
login: xxxxxxxxxx
Password: xxxxxxxxxxx
XSCF>
```

2. **showuser** 명령을 실행하여 모든 로컬 사용자 계정과 관련된 정보를 표시합니다.

```
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
```

3. **adduser** 명령을 실행하여 사용자 계정을 추가합니다.
   다음에는 사용자 계정 이름의 지정 예가 나타나 있습니다.

```
XSCF> adduser jsmith
```

다음에는 UID를 지정하여 사용자 계정을 추가하는 예가 나타나 있습니다.

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

4. **password** 명령을 실행하여 암호를 지정합니다.

```
XSCF> password jsmith
Changing password for platadm
(current) XSCF password:
New XSCF password: xxxxxx
BAD PASSWORD: is too similar to the old one
New XSCF password: xxxxxx
BAD PASSWORD: it is too simplistic/systematic
New XSCF password: xxx
BAD PASSWORD: it's WAY too short
New XSCF password: xxxxxx
Retype new XSCF password: xxxxxx
XSCF>
```

다음에는 유효 기간: 60일 및 만료 경고 시작일: 15일 전으로 지정된 예가 나타나 있습니다.

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

8.3.8 사용자 권한 설정

사용자 권한 유형은 표 8-2를 참조하십시오.

1. **useradm** 권한이 있는 사용자 계정으로 로그인합니다.

```
login: xxxxxxxxxx
Password: xxxxxxxxxx
XSCF>
```

2. **showuser** 명령을 실행하여 활성화된 사용자 계정과 관련된 정보를 표시합니다.

```
XSCF> showuser -a
User Name:            jsmith
Status:               Enabled
Minimum:              0
Maximum:              99999
Warning:              7
Inactive:             -1
Last Change:          Aug 22, 2012
Password Expires:     Never
Password Inactive:    Never
Account Expires:      Never
```

3. **setprivileges** 명령을 실행하여 사용자 권한을 사용자 계정에 할당합니다.
   다음에는 useradm 및 auditadm을 사용자 계정에 지정하는 예가 나타나 있습니다.

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

4. **showuser** 명령을 실행하여 사용자 권한을 확인합니다.

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

8.3.9 사용자 계정 활성화/비활성화

adduser 명령을 사용하여 등록한 사용자 계정이 활성화됩니다. 등록된 XSCF 사용자 계정을 다시 비활성화 또는 활성화할 수 있습니다.

1. **useradm** 권한이 있는 사용자 계정으로 로그인합니다.

```
login: xxxxxxxxxx
Password: xxxxxxxxxxxx
XSCF>
```

2. **showuser** 명령을 실행하여 활성화된 사용자 계정과 관련된 정보를 표시합니다.

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

3. **disableuser** 명령을 실행하여 사용자 계정을 비활성화합니다.
   다음에는 사용자 계정의 비활성화 예가 나타나 있습니다.

```
XSCF> disableuser jsmith
```

4. 사용자 계정을 다시 사용하는 경우 **enableuser** 명령을 실행하여 계정을 활성화합니다.
   다음에는 사용자 계정의 활성화 예가 나타나 있습니다.

```
XSCF> enableuser jsmith
```

5. **showuser** 명령을 실행하여 활성화된 사용자 계정과 관련된 정보를 표시합니다.

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

8.3.10 로그인 잠금 기능 활성화/비활성화

잠금 기능을 비활성화하려면 잠금 시간을 0분으로 설정합니다. 잠금 기능을 활성화하려면 잠금 시간을 0분 초과로 설정합니다. 기본값은 잠금 비활성화로 설정됩니다.

로그인에 3회 연속 실패하면 지정된 시간 동안 잠금이 설정됩니다. 잠금 시간은 0 ~ 1,440분입니다.

1. **useradm** 권한이 있는 사용자 계정으로 로그인합니다.

```
login: xxxxxxxxxx
Password: xxxxxxxxxxx
XSCF>
```

2. **showloginlockout** 명령을 실행하여 잠금 기능 설정을 표시합니다.

```
XSCF> showloginlockout
```

3. **setloginlockout** 명령을 실행하여 잠금 기능을 구성합니다.
   다음에는 20분으로 잠금 시간을 설정하고 잠금 기능을 활성화하는 예가 나타나 있습니다.

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

다음에는 잠금 기능의 비활성화 예가 나타나 있습니다.

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

설정된 잠금 시간은 다음 로그인부터 적용됩니다. 0분이 지정되고 사용자가 사용자 계정으로 로그인에 성공하면 잠금 기능이 비활성화됩니다.

잠금 기능은 마스터와 스탠바이 XSCF 둘 모두에서 활성화됩니다. 잠금이 활성화되면 메시지가 감사 로그에 로깅됩니다.

잠금 기능이 비활성화되면 사용자는 시도 수의 제한 없이 로그인할 수 있습니다. 잠금 시간이 만료되기 전에 잠긴 사용자 계정에 액세스해야 하는 경우 시스템 관리자에게 잠금 기능의 비활성화를 요청합니다. 사용자 계정에 성공적으로 로그인한 후 시스템 관리자는 잠금 시간을 구성하고 잠금 기능을 다시 활성화해야 합니다.

8.4 XSCF 시간/날짜 설정

이 절에는 시스템 날짜/시간 설정의 구성 방법이 설명되어 있습니다. 시스템은 기준 클록으로서 XSCF 클록을 모든 물리 분할에 사용합니다.

NTP 서버 및 NTP 클라이언트로서 XSCF가 실행되도록 하기 위한 설정을 구성할 수도 있습니다. XSCF가 NTP 클라이언트로서 구성되지 않으면 XSCF는 setdate 명령에 의해서만 기능하는 내부 실시간 클록(RTC)에 따라 작동합니다.

노트 - 시스템 사용자는 NTP 서버의 작동 방식을 결정해야 합니다. NTP의 자세한 내용은 NTP 관련 설명서를 참조하십시오.

8.4.1 논리 도메인의 시간 관리 정책

논리 도메인에는 개별 시간 관리 정책이 있을 수 있습니다. 다양한 시간 관리 설정이 논리 도메인별로 적용됩니다. 도메인 시간 관리 정책의 자세한 내용은 아래 설명된 바와 같습니다.

- 논리 도메인은 외부 NTP 서버에 대한 NTP 클라이언트로서 구성할 수 있습니다. 이 구성에서 Oracle Solaris의 초기 시간은 XSCF로부터 얻습니다.
- Oracle Solaris에서 시간 설정이 구성되지 않는 경우(논리 도메인이 NTP 클라이언트로서 구성되지 않고 Oracle Solaris `date(1M)` 명령을 사용하여 논리 도메인 시간 설정을 구성하지 않는 경우) 논리 도메인이 XSCF에서 초기 시간을 가져옵니다.
- 논리 도메인은 NTP 서버로서 구성된 XSCF에 대한 NTP 클라이언트로서 구성할 수 있습니다. 이 경우 XSCF를 NTP 서버로서 구성해야 합니다. 이 구성의 경우 논리 도메인은 XSCF(NTP 서버)에서 초기 시간을 가져오고 논리 도메인이 XSCF 장치와 동

기화됩니다.

- Oracle Solaris date(1M) 명령을 사용하여 논리 도메인에서 시간 설정을 구성하는 경우 논리 도메인과 물리 분할 간의 시간 차이가 재부팅 후에도 그대로 유지됩니다.

노트 - NTP를 사용하여 시간을 동기화하는 경우 동일 물리 분할의 논리 도메인에 대해 동일한 NTP 서버를 지정하십시오. NTP 서버를 도메인에 지정하는 방법은 Oracle Solaris 설명서를 참조하십시오.

8.4.2 각 제어 도메인과 XSCF 간의 시간 관계 이해

각 제어 도메인과 XSCF 간의 시간 차이

XSCF는 제어 도메인과의 시간 차이를 유지합니다(물리 분할과의 시간 차이).

이에 따라 제어 도메인의 재부팅후라도 제어 도메인과 XSCF 간의 시간 차이가 보장됩니다. date(1M) 명령이 실행되어 제어 도메인이 재부팅된 후라도 XSCF와 제어 도메인 간의 시간 차이가 보장됩니다.

물리 분할의 전원이 차단 또는 공급된 후라도 XSCF는 제어 도메인과의 시간 차이를 가져 제어 도메인 시간의 정확도가 보장됩니다.

물리 분할 시간과 XSCF 시간의 동기화

모든 제어 도메인(모든 물리 분할)의 시간과 XSCF의 시간을 동기화하려면 XSCF에서 resetdateoffset 명령을 실행합니다. 이 명령은 모든 제어 도메인과 XSCF 간의 시간 차이를 삭제하며 시작 후 물리 분할의 시간이 XSCF의 시간과 동기화됩니다.

제어 도메인과 XSCF 간의 시간 차이 삭제는 "8.4.7 제어 도메인 시간과 XSCF 시간의 동기화"를 참조하십시오.

8.4.3 시간과 관련된 설정 항목 및 명령의 확인

표 8-4에는 시간과 관련된 설정 항목 및 해당 XSCF 쉘 명령이 나타나 있습니다.

표 8-4 시간과 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
표준 시간대	옵션	settimezone(8), showtimezone(8)
서머 타임	옵션	settimezone(8), showtimezone(8)
시스템 시간	필수	setdate(8), showdate(8)
물리 분할(제어 도메인)과 XSCF 간의 시간 동기화	옵션	resetdateoffset(8), showdateoffset(8)

표 8-4 시간과 관련된 설정 항목 (계속)

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
NTP 서버	옵션	setad(8), showad(8)
선호, 계층	옵션	setad(8), showad(8)
로컬 클록	옵션	setad(8), showad(8)

8.4.4 표준 시간대 구성

표준 구성으로 구성되는 표준 시간대는 POSIX 표준을 준수합니다. 표준 시간대 목록은 매년 수정될 수 있습니다.

1. **showtimezone** 명령을 실행하여 표준 시간대를 표시합니다.

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

2. **settimezone** 명령을 실행하여 **XSCF** 표준 시간대를 구성합니다.
   -a 옵션을 지정하여 지정 가능한 표준 시간대를 나열합니다. -a 옵션을 사용하려면 platadm 사용자 권한이 필요합니다.
   다음에는 표준 시간대의 나열 예가 나타나 있습니다.

```
XSCF> settimezone -c settz -a
Africa/Abidjan
Africa/Accra
:
```

   다음에는 표준 시간대의 구성 예가 나타나 있습니다.

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

   구성된 표준 시간대는 명령 실행 직후 적용됩니다.

3. **showtimezone** 명령을 실행하여 설정을 확인합니다.

8.4.5 서머 타임 구성

1. **showtimezone** 명령을 실행하여 표준 시간대를 표시합니다.
   다음에는 표준 시간대의 표시 예가 나타나 있습니다.

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

다음에는 서머 타임 정보의 표시 예가 나타나 있습니다. 이 예에서 표준 시간대 약어가 JST로, GMT와의 시차가 +9시간으로, 서머 타임 이름이 JDT로, 서머 타임이 1시간 앞당겨진 것으로 설정되었습니다. 기간은 3월 마지막 일요일 2:00시(JST)부터 10월 마지막 일요일 2:00시(JDT)까지인 것으로 설정되었습니다.

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

2. **settimezone** 명령을 실행하여 **XSCF** 서머 타임 정보를 구성합니다.
   다음에는 서머 타임 정보의 구성 예가 나타나 있습니다. 이 예에서 표준 시간대 약어가 JST이고 GMT와의 시차가 +9시간이며 서머 타임 이름이 JDT이고 GMT 서머 타임과의 시차가 +10시간입니다. 기간은 4월 첫 번째 일요일 0:00시(JST)부터 9월 첫 번째 일요일 0:00시(JDT)까지입니다.

```
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
```

다음에는 현재 구성된 서머 타임 정보의 삭제 예가 나타나 있습니다.

```
XSCF> showtimezone -c dst -m customsettimezone -c deldst -b JST -o
GMT-9
```

-c adddst 또는 c deldst 옵션을 사용하여 변경한 서머 타임 정보를 적용하려면 로그아웃했다가 다시 로그인합니다.

3. **showtimezone** 명령을 실행하여 설정을 확인합니다.

8.4.6 시스템 시간 구성

XSCF 클록 날짜와 시간을 현지 시간 또는 UTC로 설정합니다. 설정은 모든 물리 분할의 전원이 차단된 경우에만 구성할 수 있습니다. 설정을 구성하면 XSCF가 재설정됩니다.

노트 - 시스템 시간은 초기 시작 시에 구성됩니다.

1. **showdate** 명령을 실행하여 **XSCF** 시간 설정을 표시합니다.
   다음에는 현지 시간인 현재 시간의 표시 예가 나타나 있습니다.

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

다음에는 UTC인 현재 시간의 표시 예가 나타나 있습니다.

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

2. **setdate** 명령을 실행하여 시간 설정을 구성합니다.
   다음에는 현지 시간인 2012년 1월 27일 오후 4시 59분으로 현재 시간을 구성하는 예가 나타나 있습니다.

```
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
```

   다음에는 UTC인 2012년 1월 27일 오전 7시 59분으로 현재 시간을 지정하는 예가 나타나 있습니다.

```
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
```

   시간을 구성하면 XSCF가 재설정됩니다. XSCF 세션이 분리됩니다. XSCF에 재연결하고 다시 로그인합니다.

노트 - 유지 관리 작업을 수행하도록 입력 전원이 꺼진 경우 입력 전원을 켠 후 showdate 명령을 사용하여 XSCF 시간을 확인하십시오. 이 시간이 현재 시간과 일치하지 않으면 setdate 명령을 실행하여 현재 시간으로 설정하십시오.

8.4.7 제어 도메인 시간과 XSCF 시간의 동기화

date(1M) 명령을 사용하여 제어 도메인 시간을 구성한 후 다음 3개 방법 가운데 하나로 제어 도메인 시간과 XSCF 시간을 동기화할 수 있습니다.

- 제어 도메인을 위한 NTP 서버로서 XSCF 설정
- 제어 도메인과 XSCF를 위한 동일 NTP 서버 설정
- resetdateoffset 명령 실행

제어 도메인을 위한 NTP 서버로서 XSCF 설정

1. **XSCF**를 **NTP** 서버로서 설정합니다.
   자세한 내용은 "8.4.8 NTP 서버로서 XSCF 지정"을 참조하십시오.
2. **console** 명령을 실행하여 대상 물리 분할의 제어 도메인 콘솔로 전환합니다.

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

3. 제어 도메인을 위한 **NTP** 서버로서 **XSCF**를 지정합니다.
Oracle Solaris의 NTP 서버 설정과 관련된 자세한 내용은 Oracle Solaris 관련 설명서를 참조하십시오.
4. 제어 도메인을 재부팅합니다.
5. **Oracle Solaris date(1M)** 명령을 실행하여 제어 도메인의 시간을 표시합니다.
6. 물리 분할의 제어 도메인 콘솔에서 **.#**을 누르거나 **escape** 명령을 다시 실행하여 **XSCF** 쉘로 돌아갑니다.
7. **showdate** 명령을 실행하여 **XSCF** 시간을 표시하고 대상 물리 분할의 제어 도메인 시간이 **XSCF**의 시간과 동일한지 확인합니다.

제어 도메인과 XSCF를 위한 동일 NTP 서버 지정

1 **XSCF**를 **NTP** 클라이언트로서 설정합니다.
자세한 내용은 "8.4.9 NTP 클라이언트로서 XSCF 지정"을 참조하십시오.

2 외부 **NTP** 서버를 **XSCF**에 등록합니다.
XSCF의 NTP 서버 설정과 관련된 자세한 내용은 "8.4.10 XSCF에 사용되는 NTP 서버 구성"을 참조하십시오.

3 **console** 명령을 실행하여 대상 물리 분할의 제어 도메인 콘솔로 전환합니다.

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

4. 제어 도메인과 **XSCF**를 위한 동일 외부 **NTP** 서버를 지정합니다.
Oracle Solaris의 NTP 서버 설정과 관련된 자세한 내용은 Oracle Solaris 관련 설명서를 참조하십시오.
5. 제어 도메인을 재부팅합니다.
6. **Oracle Solaris date(1M)** 명령을 실행하여 제어 도메인의 시간을 표시합니다.
7. 물리 분할의 제어 도메인 콘솔에서 **.#**을 누르거나 **escape** 명령을 다시 실행하여 **XSCF** 쉘로 돌아갑니다.
8. **showdate** 명령을 실행하여 **XSCF** 시간을 표시하고 대상 물리 분할의 제어 도메인 시간이 **XSCF**의 시간과 동일한지 확인합니다.

노트 - 게스트 도메인을 위한 제어 도메인과 XSCF로서 동일 NTP 서버를 지정하는 경우 모든 도메인의 시간을 XSCF와 동기화할 수 있습니다.

---

resetdateoffset 명령을 실행하여 제어 도메인과 XSCF 간의 시간을 동기화합니다.

1 **showdate** 명령을 실행하여 **XSCF** 시간을 표시합니다.

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

2. **showdateoffset** 명령을 실행하여 **XSCF**와 모든 제어 도메인**(**물리 분할**)** 간의 시간

차이를 확인합니다.

```
XSCF> showdateoffset -a
PID             Domain Date Offset
00              128 sec
01              0 sec
02              -1024 sec
03              -9999999 sec
:
```

3. **poweroff -p** 명령을 실행하여 대상 물리 분할의 전원을 차단합니다. 이 작동은 물리 분할의 논리 도메인 역시 정지시킵니다.

```
XSCF> poweroff -p xx
PPAR-IDs to power off: xx
Continue? [y|n] :y
xx : Powering off

*Note*
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showlogs
power".
XSCF>
```

4. **resetdateoffset** 명령을 실행하여 대상 물리 분할과 **XSCF** 간의 시간 차이를 재설정합니다.

```
XSCF> resetdateoffset -p xx
Clear the offset of PPAR-ID xx? [y|n] :y
```

setdate 명령을 사용하여 XSCF 시간을 구성한 경우 재부팅 후에 제어 도메인의 시간을 동일하게 동기화할 수 있습니다.

예를 들어 유지 관리 작업으로 인해 XSCF 시간과의 시간 차이가 발생할 경우 resetdateoffset -a 명령을 실행하여 모든 물리 분할과의 시간 차이를 재설정합니다. 이 명령은 모든 제어 도메인의 시간을 동기화합니다.

5. **poweron** 명령을 실행하여 대상 물리 분할에 전원을 공급합니다.

```
XSCF> poweron -p xx
DomainIDs to power on: xx
Continue? [y|n] :y
xx :Powering on

*Note*
This command only issues the instruction to power-on.
The result of the instruction can be checked by the "showlogs
power".
XSCF>
```

6. **showdateoffset** 명령을 실행하여 **XSCF**와 대상 물리 분할 간에 시간 차이가 없는지 확인합니다.

```
XSCF> showdateoffset -a
PID             Domain Date Offset
00              0 sec
01              0 sec
02              0 sec
03              0 sec
:
```

7. **console** 명령을 실행하여 제어 도메인 콘솔로 전환합니다.
8. **Oracle Solaris date(1M)** 명령을 실행하여 논리 도메인의 시간을 표시합니다.
9. 물리 분할의 제어 도메인 콘솔에서 **.#**을 누르거나 **escape** 명령을 다시 실행하여 **XSCF** 쉘로 돌아갑니다.
10. **showdate** 명령을 실행하여 **XSCF** 시간을 표시하고 대상 물리 분할의 논리 도메인 시간이 **XSCF**의 시간과 동일한지 확인합니다.

8.4.8 NTP 서버로서 XSCF 지정

NTP 서버로서 다른 클라이언트를 위한 NTP 서비스를 제공하도록 XSCF를 구성합니다. XSCF는 기본적으로 NTP 서버로서 다른 클라이언트를 위한 NTP 서비스를 제공하지 않습니다.

1. **shownntp** 명령을 실행하여 **XSCF**의 **NTP** 서비스 상태를 표시합니다.

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

2. **XSCF**용 **NTP** 서버로서 다른 클라이언트를 위한 서비스를 제공하도록 **setntp** 명령을 실행합니다.

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

3. **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

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

XSCF 세션이 분리됩니다. XSCF에 재연결하고 다시 로그인합니다.

4. **shownntp** 명령을 실행하여 **XSCF**가 **NTP** 서버로서 구성되었는지 확인합니다.

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

8.4.9 NTP 클라이언트로서 XSCF 지정

XSCF가 NTP 서버를 사용하는 경우 NTP 클라이언트로서 작동하도록 설정을 구성합니다. 기본적으로 XSCF는 NTP 서버로부터 시간을 가져오는 NTP 클라이언트로서 구성되지 않습니다.

1. **showntp** 명령을 실행하여 **NTP** 클라이언트로서 **XSCF**의 상태를 표시합니다.

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

2. **setntp** 명령을 실행하여 **NTP** 클라이언트로서 **XSCF**를 구성합니다.

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

3. **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

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

   XSCF 세션이 분리됩니다. XSCF에 재연결하고 다시 로그인합니다.

4. **showntp** 명령을 실행하여 **XSCF**가 **NTP** 클라이언트로서 구성되었는지 확인합니다.

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

8.4.10 XSCF에 사용되는 NTP 서버 구성

XSCF 시간을 상위 NTP 서버에서 가져오는 경우 NTP 서버를 최대 3개까지 등록할 수 있습니다. XSCF를 NTP 클라이언트로서 구성해야 합니다. XSCF를 NTP 클라이언트로서 구성하는 방법은 "8.4.9 NTP 클라이언트로서 XSCF 지정"을 참조하십시오.

NTP 서버가 등록되면 기존 구성이 삭제되고 지정된 NTP 서버의 구성이 덮어쓰기가 됩니다. NTP 서버가 호스트 이름으로 지정되는 경우 DNS 서버가 서버 이름을 분석할 수 있어야 합니다.

1. **showntp** 명령을 실행하여 **XSCF** 네트워크에 사용되는 **NTP** 서버를 표시합니다.

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

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

2. **showntp** 명령을 실행하여 동기화를 확인하고 상태를 표시합니다.

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

3. **setntp** 명령을 실행하여 **NTP** 서버를 추가합니다.
   다음에는 XSCF용 NTP 서버를 위한 3개 IP 주소 192.168.1.2, 130.34.11.111 및 130.34.11.117의 추가 예가 나타나 있습니다.

```
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.
```

   다음에는 XSCF용 NTP 서버를 위한 2개 호스트 이름 ntp1.red.com 및 ntp2.blue.com2의 추가 예가 나타나 있습니다.

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

4. **setntp** 명령을 실행하여 **XSCF** 네트워크용 **NTP** 서버를 삭제합니다.
   다음에는 XSCF용 NTP 서버인 ntp2.example.com의 삭제 예가 나타나 있습니다.

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

5. 구성된 설정을 적용하려면 **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

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

   XSCF 세션이 분리됩니다. XSCF에 재연결하고 다시 로그인합니다.

6. **showntp** 명령을 실행하여 **NTP** 서버를 확인합니다.

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

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

8.4.11 NTP 서버에서 선호 지정/지정 해제

선호를 지정하면 setntp 명령으로 맨 처음 지정한 NTP 서버에 최고 우선순위가 부여됩니다. 기본값으로서 최상위에 선호가 지정됩니다.

1. **showntp** 명령을 실행하여 선호 설정을 표시합니다.

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

2. **setntp** 명령을 실행하여 선호 설정을 구성합니다.
   다음에는 NTP 서버의 선호 지정 예가 나타나 있습니다.

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

   다음에는 NTP 서버의 선호 지정 해제 예가 나타나 있습니다.

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

3. 구성된 설정을 적용하려면 **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

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

   XSCF 세션이 분리됩니다. XSCF에 재연결하고 다시 로그인합니다.

4. **showntp** 명령을 실행하여 선호 설정을 확인합니다.
   다음에는 선호 지정의 지정 해제 예가 나타나 있습니다.

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

   다음에는 신호 미지정 예가 나타나 있습니다.

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

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

8.4.12 XSCF의 계층 값 구성

XSCF로 설정되도록 계층 값을 지정합니다. 1 ~ 15의 값을 지정합니다. 기본 값은 5입니다.

1. **showntp** 명령을 실행하여 **XSCF** 네트워크에 지정되는 계층 값을 표시합니다.

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

2. **setntp** 명령을 실행하여 계층 값을 변경합니다.
   다음에는 XSCF 네트워크에 사용되는 계층 값에 7을 구성하는 예가 나타나 있습니다.

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

3. 구성된 설정을 적용하려면 **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

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

   이때 세션이 분리됩니다. 새 인터페이스를 사용하여 세션을 재연결하고 다시 로그인합니다.

4. **showntp** 명령을 실행하여 계층 값을 확인합니다.
   다음에는 선호 지정의 지정 해제 예가 나타나 있습니다.

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

8.4.13 XSCF 로컬 클록의 클록 주소 변경

XSCF의 로컬 클록 주소를 구성합니다. 로컬 클록 주소의 LSB(최하위 비트)인 경우 0 ~ 3의 값을 지정할 수 있습니다. 기본 로컬 클록 주소는 127.127.1.0입니다.

1. **showntp** 명령을 실행하여 **XSCF**의 로컬 클록 주소를 표시합니다.

```
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. **setntp** 명령을 실행하여 **XSCF**의 로컬 클록 주소를 변경합니다.
   다음에는 클록 주소의 LSB를 1로 구성하는 예가 나타나 있습니다.

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

3. 구성된 설정을 적용하려면 **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

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

   이때 세션이 분리됩니다. 새 인터페이스를 사용하여 세션을 재연결하고 다시 로그인합니다.

4. **showntp** 명령을 실행하여 **XSCF**의 로컬 클록 주소를 표시합니다.

```
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 서버가 로컬 클록을 참조하는 경우의 유의 사항

XSCF가 참조하는 NTP 서버가 서버 자체의 시스템 시간(로컬 클록)을 참조하고 주소 "127.127.1.0"이 로컬 클록으로 설정되는 경우 XSCF가 시간을 동기화하지 못할 수도 있습니다.

XSCF 자체의 로컬 클록 주소는 주소 "127.127.1.0"에 고정됩니다. 반면, XSCF가 참조하는 NTP 서버의 로컬 클록 주소가 "127.127.1.0"으로 설정되는 경우에는 클록 소스(refid)의 주소가 XSCF 자체가 갖는 로컬 클록과 동일한 값을 갖습니다. 이러한 NTP 서버는 XSCF 시간 동기화로부터 설정됩니다.

showntp -l 명령을 실행하면 XSCF가 구성하는 NTP 서버의 클록 소스 주소와 XSCF 자체의 로컬 클록 주소를 표시할 수 있습니다.

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

2개 NTP 서버 출력(192.168.1.2) 가운데 첫 번째는 setntp 명령을 사용하여 구성하는 NTP 서버입니다. Refid가 LOCAL(0)로 설정되기 때문에 주소 "127.127.1.0"의 로컬 클록이 NTP 서버의 클록 소스로 구성됩니다. 두 번째는 XSCF 자체의 로컬 클록입니다. XSCF 자체의 로컬 클록 주소는 주소 "127.127.1.0"에 고정됩니다. 이에 따라 NTP 서버(192.168.1.2)가 XSCF 시간 동기화로부터 설정되어 XSCF가 로컬 클록과 시간 동기화됩니다.

문제가 없도록 다음 조치를 취하면 setntp 명령으로 구성하는 NTP 서버와의 올바른 시간 동기화가 보장됩니다.

- XSCF를 위해 구성되는 NTP 서버의 클록 소스를 변경합니다.
  showntp -l 명령을 사용하여 XSCF를 위해 구성되는 NTP 서버의 클록 소스를 확인합니다. Refid가 LOCAL(0)인 NTP 서버의 경우 주소 "127.127.1.0"의 로컬 클록이 참조되므로 다른 클록 소스를 참조하도록 변경합니다. NTP 서버의 클록 소스가 변경되는 경우 변경이 다른 NTP 클라이언트에 영향을 미치지 않는지 사전에 확인합니다.
- NTP 서버의 로컬 클록 주소를 변경합니다.
  XSCF가 참조하는 NTP 서버의 로컬 클록 주소를 "127.127.1.1," "127.127.1.2," 또는 "127.127.1.3"으로 변경합니다. Oracle Solaris의 /etc/inet/ntp.conf를 수정합니다. 변경 사항을 적용하려면 NTP 데몬을 다시 시작합니다. NTP 서버의 로컬 클록 주소가 변경되는 경우 변경이 다른 NTP 클라이언트에 영향을 미치지 않는지 사전에 확인합니다.
- NTP 서버의 계층 값을 변경합니다.
  XSCF가 참조하는 NTP 서버의 계층 값을 1로 변경합니다. 계층 값이 1인 NTP 서버는 refid가 없는 최상위 클록 소스로서 구성됩니다. 따라서 주소가 XSCF 자체의 로컬 클록 주소와 절대 동일하지 않습니다. NTP 서버의 계층 값이 변경되는 경우 변경이 다른 NTP 클라이언트에 영향을 미치지 않는지 사전에 확인합니다.
- XSCF 자체의 로컬 클록 주소를 변경합니다.
  setntp -m localaddr=value 명령을 사용하여 XSCF 자체의 로컬 클록 주소를 변경합니다. 값의 경우 로컬 클록 주소 "127.127.1.x"의 최하위 바이트를 지정합니다. 0 ~ 3의 값을 지정할 수 있습니다. 값으로 1 ~ 3의 값을 지정하면 로컬 클록을 참조하는 NTP 서버의 주소가 XSCF 내부 로컬 클록의 주소와 더 이상 일치하지 않아 로컬 클록을 참조하는 서버라도 XSCF용 NTP 서버로서 구성될 수 있습니다.

8.5 XSCF 네트워크 구성

이 절에는 시스템을 위한 XSCF 네트워크의 구성 방법이 설명되어 있습니다.

XSCF 네트워크 구성은 XSCF-LAN 및 서비스 프로세서 간 통신 프로토콜(SSCP)과 같은 XSCF 네트워크 인터페이스 설정, 라우팅 설정, DNS 설정이 구성되어야 합니다.

8.5.1 XSCF 네트워크를 사용한 서비스 이용

XSCF 네트워크에 연결하여 XSCF 쉘 및 XSCF 웹 인터페이스를 통해 다양한 서버 정보와 서비스를 사용할 수 있습니다. 서비스는 아래 나열된 절을 참조하십시오.

- 서버 작동, 상태 표시 및 구성 변경(15장 및 16장 참조)
- NTP 서비스(8.4절 참조)
- Telnet 서비스(8.6절 참조)
- SSH 서비스(8.6절 참조)
- HTTPS 서비스(8.7절 참조)
- SMTP 서비스(15.2절 참조)
- SNMP 서비스(15.3절 참조)
- 원격 유지 관리 서비스(『SPARC M10 시스템 제품 노트』 참조)

8.5.2 XSCF 네트워크 인터페이스 이해

XSCF 이더넷 포트

각 SPARC M10 시스템 캐비닛 및 크로스바 박스마다 2개 XSCF 이더넷 포트가 있습니다. 이 포트는 그 이름이 각각 XSCF-LAN#0 및 XSCF-LAN#1입니다.

둘 모두 RJ-45 커넥터를 사용하고 10Base-T/100Base-TX/1000Base-T를 지원합니다. XSCF-LAN 포트는 시스템 관리자가 작동을 수행할 수 있도록 하는 데 사용되는 LAN 연결 포트입니다. 작동에는 서버 상태 보기, 도메인 작동 및 XSCF 쉘 또는 XSCF 웹을 사용한 콘솔 표시가 포함됩니다.

XSCF 네트워크에 연결하려면 이더넷 포트의 IP 주소를 지정합니다. 2개 LAN 경로를 사용하여 사용자는 서버를 유지 관리할 수 있습니다.

XSCF가 2개 이상인 시스템의 경우 마스터 XSCF 또는 스탠바이 XSCF의 XSCF-LAN만 사용됩니다. 슬레이브 XSCF의 경우를 제외하고 XSCF-LAN이 사용되지 않습니다.

마스터 XSCF와 스탠바이 XSCF 간의 인계 IP 주소

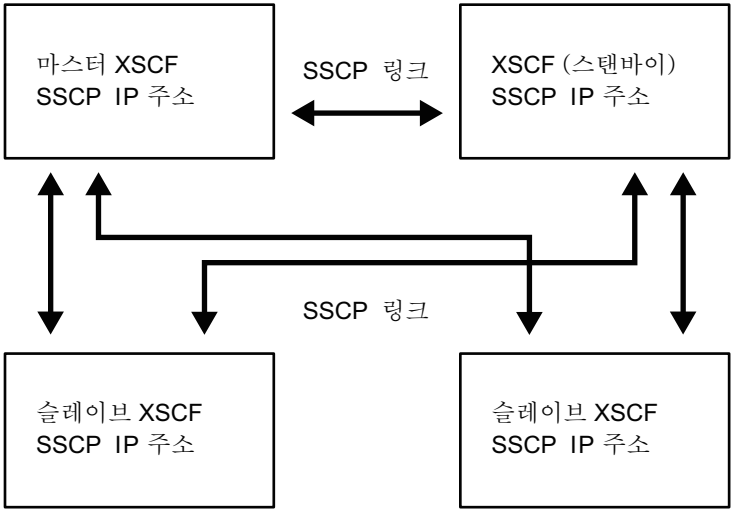
XSCF가 2개 이상인 시스템의 경우 마스터 XSCF 및 스탠바이 XSCF의 XSCF-LAN#0 포트와 XSCF-LAN#1 포트를 각각 그룹화하고 1개 가상(인계) IP 주소를 그룹에 할당할 수 있습니다. 이를 통해 마스터와 스탠바이 간의 전환이 이루어지더라도 XSCF-LAN 간에 IP 주소를 인계할 수 있습니다. 사용자는 마스터와 스탠바이의 IP 주소에 주의를 기울일 필요 없이 동일한 인계 IP 주소로 전환된 마스터 XSCF에 액세스할 수 있습니다.

서비스 프로세서 간 통신 프로토콜(SSCP)

XSCF가 2개 이상인 시스템의 경우 XSCF 간 네트워크가 구성됩니다. XSCF 간 네트워크 인터페이스 프로토콜을 서비스 프로세서 간 통신 프로토콜(SSCP) 또는 SSCP 링크 네트워크라고 합니다. 통신 경로를 통해 XSCF는 상호 연결하고 상태를 상호 모니터링하며 시스템 정보를 교환할 수 있습니다.

그림 8-1에는 4BB 구성인 SPARC M10-4S 시스템의 SSCP 링크 네트워크가 나타나 있습니다.

그림 8-1 SSCP 링크 네트워크



SSCP 링크를 구성하려면 케이블을 사용하여 마스터 XSCF를 슬레이브 XSCF에, 스탠바이 XSCF를 슬레이브 XSCF에, 마스터 XSCF를 스탠바이 XSCF에 연결합니다. 마스터 XSCF와 스탠바이 XSCF 사이에 DUAL 제어 포트를 연결합니다. 마스터를 슬레이브에, 스탠바이를 슬레이브에 연결하는 SSCP 포트를 XSCF BB 제어 포트라고 합니다. 슬레이브의 XSCF는 상호 연결되지 않습니다. SSCP 구성을 위한 케이블 연결의 자세한 내용은 『SPARC M10 시스템 설치 안내서』의 "4장 빌딩 블록 연결 구성"을 참조하십시오.

SSCP의 IP 주소는 기본적으로 구성됩니다. IP 주소를 변경하는 경우 시스템 초기 구성 시에 SSCP의 IP 주소를 구성해야 합니다. SSCP IP 주소의 자세한 내용은 "8.5.4 SSCP에서 IP 주소 설정 이해"를 참조하십시오.

8.5.3 XSCF 네트워크 인터페이스 구성

다음의 XSCF 네트워크 인터페이스가 구현됩니다.

- 사용자가 XSCF에 액세스하기 위한 LAN(XSCF-LAN)
- XSCF 간 통신(SSCP)을 위한 LAN(XSCF가 2개 이상인 시스템)

단일 XSCF 구성의 SPARC M10 시스템인 경우 일반적으로 XSCF-LAN에서 2개 IP 주소가 구성됩니다. XSCF-LAN은 1개 LAN 포트만 사용할 수 있습니다.

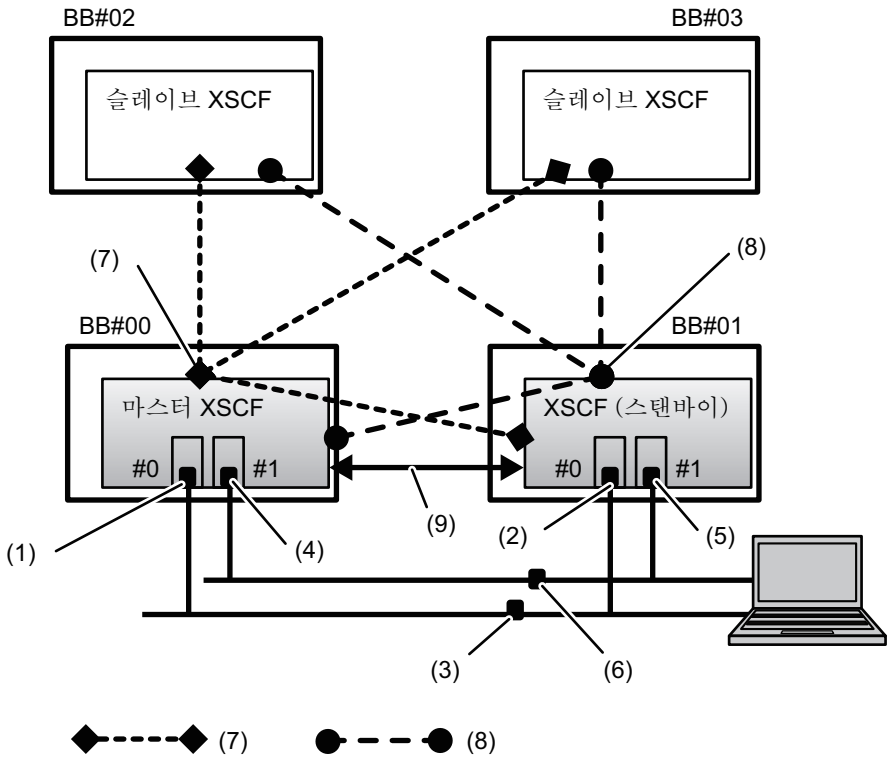
4-BB 구성의 SPARC M10-4S 시스템인 경우 일반적으로 XSCF-LAN용 4개 IP 주소, 인계 IP 주소용 2개 IP 주소 및 SSCP용 10개 IP 주소 또는 총 최대 16개의 IP 주소가 구성됩니다.

16BB 구성 및 최대 4-XBBOX 구성의 SPARC M10-4S 시스템인 경우 일반적으로 XSCF-LAN용 4개 IP 주소, 인계 IP 주소용 2개 IP 주소 및 SSCP용 44개 IP 주소 또는 총 최대 50개의 IP 주소가 구성됩니다.

노트 - XSCF가 2개 이상인 시스템의 경우 마스터 XSCF에서만 모든 XSCF 설정을 구성하는 명령을 실행하십시오. 마스터 XSCF와 스탠바이 XSCF 둘 모두에서 명령을 실행하지 않아도 됩니다. XSCF 설정은 스탠바이 XSCF로 구성할 수 없습니다.

그림 8-2에는 4BB 구성의 SPARC M10-4S 시스템에서 XSCF 네트워크를 구성하는 데 필요한 네트워크 인터페이스가 나타나 있습니다.

그림 8-2 4BB 구성의 XSCF 네트워크

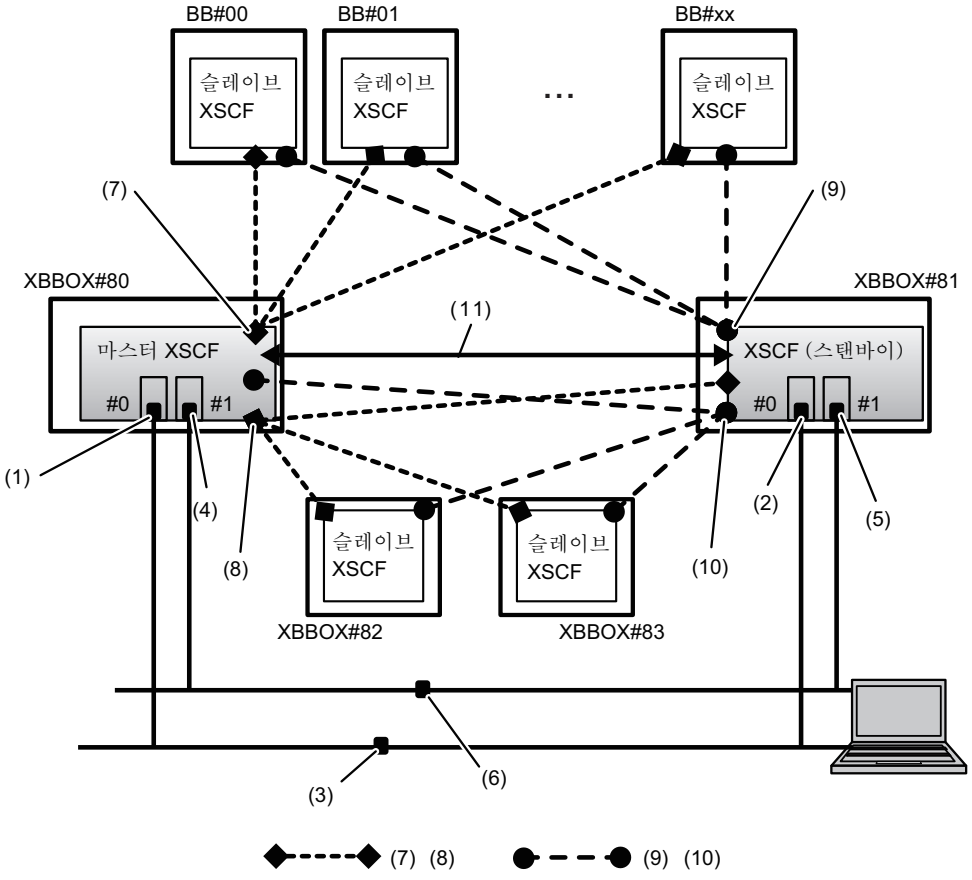


번호	주소 설정	번호	주소 설정
1	XSCF-LAN#0 주소(마스터 XSCF측)	6	XSCF 간 LAN#1 인계 IP 주소
2	XSCF-LAN#0 주소(스탠바이 XSCF 측)	7	SSCP 주소(BB#xx의 마스터 XSCF 및 XSCF): 4개 주소

번호	주소 설정	번호	주소 설정
3	XSCF 간 LAN#0 인계 IP 주소	8	SSCP 주소(BB#xx의 스탠바이 XSCF 및 XSCF): 4개 주소
4	XSCF-LAN#1 주소(마스터 XSCF측)	9	중복 SSCP 주소(마스터 XSCF 및 스탠바이 XSCF): 2개 주소
5	XSCF-LAN#1 주소(스탠바이 XSCF 측)		

그림 8-3에는 크로스바 박스가 있는 SPARC M10-4S 시스템에서 XSCF 네트워크를 구성하는 데 필요한 XSCF 네트워크 인터페이스의 예가 나타나 있습니다.

그림 8-3 크로스바 박스가 있는 시스템 구성의 XSCF 네트워크



번호	주소 설정	번호	주소 설정
1	XSCF-LAN#0 주소(마스터 XSCF측)	7	SSCP 주소(BB#xx의 마스터 XSCF 및 XSCF): 17개 주소
2	XSCF-LAN#0 주소(스탠바이 XSCF 측)	8	SSCP 주소(XBBOX#xx의 마스터 XSCF 및 XSCF): 4개 주소

번호	주소 설정	번호	주소 설정
3	XSCF 간 LAN#0 인계 IP 주소	9	SSCP 주소(BB#xx의 스탠바이 XSCF 및 XSCF): 17개 주소
4	XSCF-LAN#1 주소(마스터 XSCF측)	10	SSCP 주소(XBBOX#xx의 스탠바이 XSCF 및 XSCF): 4개 주소
5	XSCF-LAN#1 주소(스탠바이 XSCF 측)	11	중복 SSCP 주소(마스터 XSCF 및 스탠바이 XSCF): 2개 주소
6	XSCF 간 LAN#1 인계 IP 주소		

8.5.4 SSCP에서 IP 주소 설정 이해

SSCP를 위해 구성되는 IP 주소는 다음 그룹으로 분류됩니다. 이 그룹은 SSCP 링크 네트워크 ID로 구별할 수 있습니다. SSCP 포트당 3개 이상의 IP 주소를 설정해야 합니다. (그림 8-2 및 그림 8-3 참조)

- BB의 마스터 XSCF 및 XSCF 그룹(그림 8-2, 7번, 그림 8-3, 7번)
- BB의 스탠바이 XSCF 및 XSCF 그룹(그림 8-2, 8번, 그림 8-3, 9번)
- XBBOX의 마스터 XSCF 및 XSCF 그룹(그림 8-3, 8번)
- XBBOX의 스탠바이 XSCF 및 XSCF 그룹(그림 8-3, 10번)
- 마스터 XSCF 및 스탠바이 XSCF 그룹(그림 8-2, 9번, 그림 8-3, 11번)

단일 XSCF 구성의 SPARC M10-1/M10-4 시스템에는 SSCP 설정이 없습니다.

표 8-5에는 4BB 구성의 SPARC M10-4S 시스템에서 구성하는 SSCP IP 주소의 위치, SSCP IP 주소의 수, ID 및 기본 값이 나타나 있습니다. showsscp 명령을 실행하여 현재 구성된 IP 주소를 확인합니다.

표 8-5 SSCP IP 주소(4BB 구성)

위치	수	**SSCP** 링크 네트워크 **ID**	기본 **IP** 주소
BB#xx의 마스터 XSCF와 XSCF 간 연결	4	0	
BB#00(마스터)			169.254.1.1
BB#01			169.254.1.2
BB#02			169.254.1.3
BB#03			169.254.1.4
스탠바이 XSCF와 BB#xx 간 연결	4	1	
BB#00			
BB#01(스탠바이)			169.254.1.9
BB#02			169.254.1.10
BB#03			169.254.1.11
			169.254.1.12
마스터 XSCF와 스탠바이 XSCF 간 중복 연결	2	2	
BB#00(마스터)			
BB#01(스탠바이)			169.254.1.17
			169.254.1.18

표 8-5 SSCP IP 주소(4BB 구성) (계속)

위치	수	SSCP 링크 네트워크 ID	기본 IP 주소
총계	10		

표 8-6에는 최대 구성(16개 BB 및 4개 XBBOX)의 SPARC M10-4S 시스템에서 구성하는 SSCP IP 주소의 위치, SSCP IP 주소의 수, ID 및 기본 값이 나타나 있습니다.

표 8-6 SSCP IP 주소(16개 BB 및 4개 XBBOX 구성)

위치	수	SSCP 링크 네트워크 ID	기본 IP 주소
BB#xx의 마스터 XSCF와 XSCF 간 연결	17	0	
XBBOX#80(마스터)			169.254.1.1
BB#00 ~ BB#15			169.254.1.2 ~ 169.254.1.17
BB#xx의 스탠바이 XSCF와 XSCF 간 연결	17	1	
XBBOX#81(스탠바이)			169.254.1.33
BB#00 ~ BB#15			169.254.1.34 ~ 169.254.1.49
XBBOX#xx의 마스터 XSCF와 XSCF 간 연결	4	2	
XBBOX#80(마스터)			
XBBOX#81			169.254.1.65
XBBOX#82			169.254.1.66
XBBOX#83			169.254.1.67
			169.254.1.68
XBBOX#xx의 스탠바이 XSCF와 XSCF 간 연결	4	3	
XBBOX#80			
XBBOX#81(스탠바이)			169.254.1.73
XBBOX#82			169.254.1.74
XBBOX#83			169.254.1.75
			169.254.1.76
마스터 XSCF와 스탠바이 XSCF 간 중복 연결	2	4	
XBBOX#80(마스터)			
XBBOX#81(스탠바이)			169.254.1.81
			169.254.1.82
총계	44		

8.5.5 네트워크 그룹 서브넷 이해

다음 XSCF 네트워크 연결의 그룹 IP 주소는 다양한 서브넷 주소로 구성되어야 합니다.

- XSCF-LAN#0
- XSCF-LAN#1
- 마스터 XSCF와 BB 간 SSCP 링크
- 스탠바이 XSCF와 BB 간 SSCP 링크

- XBBOX의 마스터 XSCF와 XSCF 간 SSCP 링크
- XBBOX의 스탠바이 XSCF와 XSCF 간 SSCP 링크
- 마스터 XSCF와 스탠바이 XSCF 간 SSCP 링크(DUAL)

최대 4BB 구성인 SPARC M10-4S 시스템의 한 시스템에 3개 유형의 SSCP 서브넷이 있습니다(SSCP 링크 네트워크 ID 0 ~ 2).

그림 8-2에 7, 8 및 9번으로 나타난 SSCP 링크는 다양한 서브넷으로 구성되어야 합니다.

크로스바 박스가 있는 시스템의 경우 최대 5개 유형의 서브넷이 사용됩니다(SSCP 링크 네트워크 ID 0 ~ 4).

그림 8-3에 7 ~ 11번으로 나타난 SSCP 링크는 다양한 서브넷으로 구성되어야 합니다.

8.5.6 XSCF 네트워크와 관련된 설정 항목 및 명령의 확인

표 8-7에는 XSCF 네트워크와 관련된 설정 항목 및 해당 XSCF 쉘 명령이 나타나 있습니다.

네트워크 설정의 구성을 완료하려면 XSCF를 재설정합니다. rebootxscf 명령을 사용하여 XSCF를 재설정합니다. XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.

표 8-7 XSCF 네트워크와 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
XSCF 네트워크의 IP 주소 ● XSCF-LAN ● 인계 IP 주소 ● SSCP	필수	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
네트워크의 활성화/비활성화	옵션	setnetwork(8), shownetwork(8)
네트워크 마스크	옵션	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
호스트 이름/도메인 이름	옵션	sethostname(8), showhostname(8)
네트워크 경로 추가/삭제 ● 대상 IP 주소 ● 게이트웨이 ● 네트워크 마스크	옵션	setroute(8), showroute(8)
DNS 추가/삭제 ● 이름 서버 ● 검색 경로	옵션	setnameserver(8), shownameserver(8)
IP 패킷 필터링 규칙	옵션	setpacketfilters(8), showpacketfilters(8)
네트워크 적용	필수	applynetwork(8)

8.5.7 XSCF 네트워크 구성 흐름

이 절에는 XSCF 네트워크의 구성 흐름이 설명되어 있습니다. 단계에서 자세한 내용을 참조할 수 있는 위치가 나타나 있습니다.

1. 이더넷**(XSCF-LAN) IP** 주소를 구성합니다**.**
   네트워크 구성에 따라 2개 XSCF-LAN 포트를 사용할 수 있습니다.

   XSCF가 1개인 시스템의 경우 다음 IP 주소 가운데 하나 또는 둘 모두를 구성합니다.

   - BB#00의 XSCF-LAN#0(마스터 XSCF)
   - BB#00의 XSCF-LAN#1(마스터 XSCF)

   XSCF가 2개 이상인 시스템의 경우 마스터 XSCF측 주소를 구성한 후 스탠바이 XSCF에서 XSCF-LAN의 IP 주소를 구성합니다(shownetwork(8), setnetwork(8) 참조).

   XSCF 장애 조치 시 두 XSCF 모두를 연결할 수 있도록 XSCF에서 번호가 동일한 LAN 포트에 동일 서브넷 주소를 구성합니다.

   XSCF-LAN#0 및 XSCF-LAN#1의 IP 주소를 다양한 서브넷 주소로 구성해야 합니다.

2. **XSCF**가 **2**개 이상인 시스템의 경우 인계 **IP** 주소를 지정합니다**.**
   인계 IP 주소를 구성하면 XSCF 장애 조치 시 마스터가 스탠바이로 전환된 후 IP 주소를 인계할 수 있습니다. 사용자는 항상 XSCF 전환에 주의를 기울일 필요 없이 인계 IP 주소에 액세스하여 마스터 XSCF에 연결할 수 있습니다.

   XSCF-LAN#0 및 XSCF-LAN#1의 각 IP 주소를 구성한 후 중복인 XSCF-LAN#0 및 XSCF-LAN#1의 LAN 포트 각각마다 1개 인계 IP 주소를 구성합니다 (shownetwork(8), setnetwork(8) 참조).

3. **XSCF**가 **2**개 이상인 시스템의 경우 **SSCP IP** 주소를 지정합니다**.**
   SSCP는 중복 XSCF 간 네트워크에 사용되므로 IP 주소를 구성해야 합니다. SSCP IP 주소는 기본적으로 구성됩니다(표 8-5, 표 8-6 참조).

   구성된 XSCF-LAN IP 주소가 SSCP 기본 서브넷 주소와 충돌하는 경우 SSCP IP 주소를 다른 주소로 구성해야 합니다. SSCP IP 주소는 동일 그룹의 동일 서브넷 안에 있거나 그룹 밖 다른 서브넷 주소가 되어야 합니다. 서브넷은 "8.5.5 네트워크 그룹 서브넷 이해"를 참조하십시오. 사용자는 SSCP 네트워크에 액세스할 수 없습니다 (showsscp(8), setsscp(8) 참조).

4. 호스트 이름**,** 라우팅 및 **DNS** 설정을 구성합니다**.**
   XSCF가 2개 이상인 시스템의 경우 마스터 XSCF측에서 이를 구성한 후 스탠바이 XSCF측에서 호스트 이름과 라우팅 설정을 구성합니다(showhostname(8), sethostname(8), showroute(8), setroute(8), shownameserver(8) 및 setnameserver (8) 참조).

5. **IP** 패킷 필터링 규칙을 구성합니다**.**
   XSCF-LAN의 경우 IP 패킷 필터링 규칙을 구성합니다(showpacketfilters(8), setpacketfilters(8) 참조).

6. 구성된 네트워크 설정을 적용합니다**.**
   네트워크 설정의 구성을 완료하려면 설정을 적용하고 XSCF를 재설정해야 합니다. XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다(applynetwork (8), rebootxscf(8) 참조).

노트 - 모든 XSCF 설정의 구성 명령이 실행되는 동안 XSCF가 재설정되거나 장애 조치가 수행되는 경우 일부 설정이 성공적으로 수행되지 않을 수도 있습니다. 마스터 XSCF에 다시 로그인하고 설정이 올바로 적용되었는지 확인합니다. 그렇지 않으면 설정을 다시 구성합니다.

8.5.8 XSCF 네트워크의 활성화/비활성화와 XSCF-LAN IP 주소 및 네트워크 마스크의 구성

1. **shownetwork** 명령을 실행하여 모든 **XSCF** 네트워크 인터페이스의 정보를 표시합니다.

```
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. **XSCF-LAN#0** 또는 **XSCF-LAN#1**의 정보를 표시합니다.
다음에는 BB#00(마스터 XSCF) XSCF-LAN#1 네트워크 인터페이스 정보의 표시 예가 나타나 있습니다.

```
XSCF> shownetwork bb#00-lan#1
bb#00-lan#1
          Link encap:Ethernet HWaddr 00:00:00:12:34:57 PM
          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. **setnetwork** 명령을 실행하여 네트워크 인터페이스 정보를 지정합니다.
다음에는 IP 주소 192.168.1.10 및 네트워크 마스크 255.255.255.0을 BB#00의 XSCF-LAN#0으로 설정하여 활성화하는 예가 나타나 있습니다.

```
XSCF> setnetwork bb#00-lan#0 -m 255.255.255.0 192.168.1.10
```

다음에는 BB#00의 XSCF-LAN#1을 비활성화하는 예가 나타나 있습니다.

```
XSCF> setnetwork bb#00-lan#1 -c down
```

다음에는 BB#00의 XSCF-LAN#1로 구성된 IP 주소 및 네트워크 마스크의 삭제 예가 나타나 있습니다.

```
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. 구성된 **XSCF** 네트워크 인터페이스 설정을 적용하려면 **applynetwork** 및 **rebootxscf** 명령을 실행합니다.
   XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.
5. **shownetwork** 명령을 실행하여 **XSCF** 네트워크 인터페이스의 정보를 확인합니다.

8.5.9 인계 IP 주소 구성

1. **shownetwork** 명령을 실행하여 모든 **XSCF** 네트워크 인터페이스의 정보를 표시합니다.

```
XSCF> shownetwork -a
```

2. **XSCF-LAN#0** 또는 **XSCF-LAN#1**의 인계 **IP** 주소 정보를 표시합니다.
   다음에는 XSCF-LAN#0 인계 IP 주소의 정보 표시 예가 나타나 있습니다.

```
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. **XSCF-LAN#0** 또는 **XSCF-LAN#1** 인계 **IP** 주소를 구성합니다.
   다음에는 XSCF-LAN#0의 인계 IP 주소 192.168.11.10 및 네트워크 마스크 255.255.255.0을 설정하는 예가 나타나 있습니다.

```
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.11.10
```

4. 구성된 **XSCF** 네트워크 인터페이스 설정을 적용하려면 **applynetwork** 및 **rebootxscf** 명령을 실행합니다.
   XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.
5. **shownetwork** 명령을 실행하여 **XSCF** 네트워크 인터페이스의 정보를 확인합니다.

8.5.10 SSCP IP 주소 구성

1. **shownetwork** 명령을 실행하여 모든 **XSCF** 네트워크 인터페이스의 정보를 표시합니다.

```
XSCF> shownetwork -a
```

2. **showsscp** 명령을 실행하여 **SSCP** 주소의 정보를 표시합니다.
   다음에는 4BB 구성의 SPARC M10-4S 시스템에서 모든 SSCP 주소의 정보 표시 예가 나타나 있습니다.

```
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#1 169.254.1.10
bb#01-if#1 169.254.1.9
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
```

다음에는 마스터 XSCF측 SSCP 설정의 정보 표시 예가 나타나 있습니다.

```
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
```

다음에는 스탠바이 XSCF측 SSCP 설정의 정보 표시 예가 나타나 있습니다.

```
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
```

다음에는 마스터 및 스탠바이 중복에 대한 SSCP 링크 설정의 정보 예가 나타나 있습니다.

```
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. **SSCP IP** 주소를 구성합니다.
   다음에는 대화형 모드에서 4BB 구성인 SPARC M10-4S 시스템의 SSCP 링크 네트워크 SSCP 주소와 네트워크 마스크를 구성하는 예가 나타나 있습니다.

```
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. 구성된 **IP** 주소 및 네트워크 마스크 설정을 적용하려면 **applynetwork** 및

rebootxscf 명령을 실행합니다.
XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.

5. **showsscp** 명령을 실행하여 **SSCP** 주소의 정보를 확인합니다.

8.5.11 XSCF 호스트 이름 및 도메인 이름 구성

1. **showhostname** 명령을 실행하여 호스트 이름을 표시합니다.

```
XSCF> showhostname -a
bb#00: scf-hostname0.company.com
bb#01: scf-hostname1.company.com
```

2. **sethostname** 명령을 실행하여 호스트 이름을 구성합니다.
다음에는 호스트 이름 scf0-hostname을 BB#00으로 구성하는 예가 나타나 있습니다.

```
XSCF> sethostname bb#00 scf0-hostname
```

다음에는 도메인 이름 company.com을 마스터 XSCF 및 스탠바이 XSCF로 구성하는 예가 나타나 있습니다.

```
XSCF> sethostname -d company.com
```

3. **sethostname** 명령을 실행하고 **applynetwork** 및 **rebootxscf** 명령을 실행하여 구성된 호스트 이름과 도메인 이름을 적용합니다.
XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.
4. **showhostname** 명령을 실행하여 호스트 이름과 도메인 이름을 확인합니다.

8.5.12 XSCF 라우팅 설정 구성

다음에는 XSCF가 2개 이상인 시스템에서 각 서브넷의 라우팅 데이터 예가 나타나 있습니다.

<예 1> 1개 기본 게이트웨이를 구성하는 경우

BB#00의 XSCF BB#01의 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]

대상	게이트웨이	네트워크 마스크	인터페이스
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

노트 - XSCF 인터페이스 라우팅의 결정 방법은 설치 위치의 네트워크 환경에 따라 달라집니다. 네트워크 환경은 시스템 작동에 적합하도록 구현되어야 합니다.

노트 - 인계 IP 주소에 대해서는 경로 설정을 구성할 수 없습니다.

<예 2> 2개 기본 게이트웨이를 구성하는 경우

BB#00의 XSCF BB#01의 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]

대상	게이트웨이	네트워크 마스크	인터페이스
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[default]	[192.168.11.1]	[0.0.0.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[default]	[192.168.11.1]	[0.0.0.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

노트 - 2개 기본 게이트웨이를 구성하는 경우 게이트웨이 가운데 하나가 자동 선택됩니다. 이 구성의 경우 게이트웨이가 기본 게이트웨이로서 올바로 작동하도록 네트워크가 구성되어야 합니다.

작동 절차

1. **showroute** 명령을 실행하여 라우팅 설정을 표시합니다.

```
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. **setroute** 명령을 실행하여 네트워크 인터페이스 라우팅을 지정합니다.
   다음에는 BB#00의 XSCF-LAN#0에 대해 대상 192.168.11.0이 지정되고 네트워크 마스크 255.255.255.0이 지정되는 라우팅 설정의 추가 예가 나타나 있습니다.

```
XSCF> setroute -c add -n 192.168.11.0 -m 255.255.255.0 bb#00-lan#0
```

   다음에는 BB#00의 XSCF-LAN#1에 대해 기본 게이트웨이 10.12.108.1이 지정되는 라우팅 설정의 추가 예가 나타나 있습니다.

```
XSCF> setroute -c add -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

   다음에는 BB#00의 XSCF-LAN#0에 대해 대상 192.168.11.0으로 가는 라우팅 설정의 삭제 예가 나타나 있습니다.

```
XSCF> setroute -c del -n 192.168.11.0 bb#00-lan#0
```

3. **applynetwork** 및 **rebootxscf** 명령을 실행하여 **setroute** 명령으로 구성한 설정을 적용합니다.
   XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.
4. **showroute** 명령을 실행하여 라우팅 설정을 확인합니다.

8.5.13 XSCF의 DNS 설정 구성

XSCF의 DNS 설정을 구성하기 위한 검생 경로를 지정하는 경우 이름 서버도 함께 지정해야 합니다.

1. **shownameserver** 명령을 실행하여 이름 서버와 검색 경로를 표시합니다.
   2개 이상의 이름 서버와 2개 이상의 검색 경로가 등록된 경우 이는 줄 바꿈이 있는 라인으로 나열됩니다.

   다음에는 3개 이름 서버와 1개 검색 경로가 등록된 경우의 예가 나타나 있습니다.

```
XSCF> shownameserver
nameserver   10.0.0.2
namaserver   172.16.0.2
nameserver   192.168.0.2
search       company1.com
```

   다음에는 이름 서버와 검색 경로가 등록되지 않은 경우의 예가 나타나 있습니다.

```
XSCF> shownameserver
nameserver ---
search     ---
```

2. **setnameserver** 명령을 실행하여 이름 서버와 검색 경로를 지정합니다.
   다음에는 이름 서버로서 3개 IP 주소 10.0.0.2, 172.16.0.2 및 192.168.0.2의 추가 예가 나타나 있습니다.

```
XSCF> setnameserver 10.0.0.2 172.16.0.2 192.168.0.2
```

   다음에는 모든 구성된 이름 서버의 삭제 예가 나타나 있습니다.

```
XSCF> setnameserver -c del -a
```

   다음에는 등록된 1개 DNS 서버에 대한 3개 설정 가운데 2개 설정의 삭제 예가 나타나 있습니다.

```
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
```

   다음에는 검색 경로로서 1개 도메인 이름 company1.com의 추가 예가 나타나 있습니다.

```
XSCF> setnameserver -c addsearch company1.com
```

   다음에는 모든 구성된 검색 경로의 삭제 예가 나타나 있습니다.

```
XSCF> setnameserver -c delsearch -a
```

3. **applynetwork** 및 **rebootxscf** 명령을 실행하여 **setnameserver** 명령으로 구성한 이름 서버와 검색 경로 설정을 적용합니다.
   XSCF를 재설정하면 XSCF 세션이 분리됩니다. 다시 로그인합니다.
4. **showroute** 명령을 실행하여 설정을 표시합니다.

8.5.14 XSCF 네트워크에 IP 패킷 필터링 규칙 구성

XSCF IP 필터링 규칙은 입력 패킷에 구성할 수 있습니다. 필터링 규칙은 출력 패킷에는 구성할 수 없습니다.

1. **showpacketfilters** 명령을 실행하여 **XSCF-LAN**의 **IP** 패킷 필터링 규칙을 표시합니다.
   다음에는 XSCF 네트워크에 구성된 IP 패킷 필터링 규칙의 표시 예가 나타나 있습니다.

```
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
```

   다음에는 IP 패킷 필터링 규칙의 적용 방법을 표시하는 예가 나타나 있습니다.

```
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
```

   다음 예에서는 IP 패킷 필터링 규칙이 구성되지 않음을 나타냅니다.

```
XSCF> showpacketfilters -a
XSCF>
```

2. **setpacketfilters** 명령을 실행하여 **IP** 패킷 필터링 규칙을 구성합니다.
   IP 패킷 필터링 규칙은 구성되는 시간 순서 면에서 최고 우선순위를 갖습니다.
   다음에는 IP 주소 192.168.100.0/255.255.255.0의 통과 허용 예가 나타나 있습니다.

```
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
```

   다음에는 BB#00의 XSCF-LAN#0에서 IP 주소 192.168.100.0/255.255.255.0의 통과 허용 예가 나타나 있습니다.

```
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
```

다음에는 10.10.10.10에서 통신을 취소하기 위한 설정의 삭제 예가 나타나 있습니다.

```
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
```

다음에는 모든 구성된 IP 패킷 필터링 규칙의 삭제 예가 나타나 있습니다.

```
XSCF> setpacketfilters -c clear
(none)
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

8.5.15 XSCF 네트워크 설정 적용

setnetwork, setsscp, sethostname, setroute 및/또는 setnameserver 명령을 사용하여 설정을 완료한 후 네트워크 설정을 적용합니다.

1. **XSCF 쉘에서 applynetwork 명령을 실행합니다.**
   명령을 실행하면 네트워크 설정이 표시되어 설정을 확인할 수 있습니다.

```
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] :
```

2. **rebootxscf** 명령을 실행하여 **XSCF**를 재설정하고 설정을 완료합니다**.**

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

이때 세션이 분리됩니다. 새 인터페이스를 사용하여 세션을 재연결하고 다시 로그인합니다.

3. **shownetwork, showsscp, showhostname, showroute** 및**/**또는 **shownameserver** 명령을 실행하여 네트워크 설정을 표시하고 새로 구성한 네트워크 설정을 확인합니다**.**
4. **nslookup** 명령을 실행하여 호스트 이름의 정보를 확인합니다**.**
다음에는 호스트 이름 scf0-hostname의 정보 표시 예가 나타나 있습니다.

```
XSCF> nslookup scf0-hostname
Server: server.example.com
Address: 192.168.1.3

Name: scf0-hostname.company.com
Address: 192.168.10.10
```

8.5.16 XSCF 네트워크 연결의 상태 확인

1. **shownetwork** 명령을 실행하여 네트워크 연결의 상태를 표시합니다**.**

```
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. **ping** 명령을 실행하여 네트워크 장치에 대한 응답을 확인합니다.
   다음에는 호스트 이름 scf0-hostname으로 패킷을 3회 전송하는 예가 나타나 있습니다.

```
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. **traceroute** 명령을 실행하여 네트워크 장치로 가는 네트워크 경로를 확인합니다.
   다음에는 host server.example.com으로 가는 네트워크 경로의 표시 예가 나타나 있습니다.

```
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
```

8.6 XSCF에 로그인하기 위한 SSH/Telnet 서비스 구성

이 절에는 SSH 서비스 및 Telnet 서비스 설정의 구성 방법이 설명되어 있습니다. XSCF 쉘을 이용하는 터미널에서 지정된 물리 분할의 제어 도메인 콘솔을 사용하려면 SSH 또는 Telnet을 사용합니다. SSH 및 Telnet을 활성화/비활성화하는 설정을 구성하고 SSH 호스트 키 및 로그인 후 자동 시간 초과 설정을 구성합니다. 또한 SSH 사용자 공개 키를 XSCF에 등록합니다.

SSH와 Telnet은 동시 활성화가 가능합니다. 하지만 Telnet 연결은 보안 프로토콜을 기반으로 하지 않습니다. SSH를 활성화하는 경우 Telnet을 비활성화하는 것이 좋습니다.

SSH 클라이언트

시스템에서 SSH 기능을 다음 클라이언트 소프트웨어에 사용할 수 있습니다.

- Oracle Solaris 보안 쉘
- OpenSSH

- PuTTY
- TTSSH2의 UTF-8 TeraTerm Pro

소프트웨어 사용 조건은 소프트웨어 설명서를 참조하십시오.

포트 번호

SSH 포트 번호는 22가 되고 Telnet 포트 번호는 23이 되어야 합니다.

사용자 공개 키

XSCF-LAN 연결을 통해 SSH 사용자 키를 사용하는 경우 사용자 비밀 키와 사용자 공개 키를 클라이언트의 등록된 XSCF 사용자 계정에 생성하고 사용자 공개 키를 XSCF에 등록합니다.

사용자 이름을 지정하여 SSH 사용자 공개 키를 표시, 등록 또는 삭제하려면 useradm 사용자 권한이 필요합니다.

노트 - DSA 2048bit 사용자 공개 키는 TTSSH2 4.66 이상의 UTF-8 TeraTerm Pro에서 지원되지 않습니다.

콘솔

SPARC M10 시스템에서 물리 분할의 쓰기 가능(RW) 또는 참조 전용(RO) 제어 도메인 콘솔을 사용할 수 있습니다. 물리 분할당 1개 RW 콘솔을 사용할 수 있습니다. 제어 도메인 콘솔을 사용하려면 console 명령을 사용합니다. 콘솔의 자세한 내용은 "4장 로그인/로그아웃"을 참조하십시오.

8.6.1 SSH 및 Telnet과 관련된 설정 항목 및 명령의 확인

표 8-8에는 SSH 및 Telnet과 관련된 설정 항목 및 해당 XSCF 쉘 명령이 나타나 있습니다.

표 8-8 SSH 및 Telnet과 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
SSH의 활성화/비활성화	옵션	setssh(8), showssh(8)
호스트 키의 생성	옵션	setssh(8), showssh(8)
사용자 공개 키의 등록/삭제	옵션	setssh(8), showssh(8)
Telnet의 활성화/비활성화	옵션	settelnet(8), showtelnet(8)
시간 초과 시간	옵션	setautologout(8), showautologout(8)

8.6.2 SSH 및 Telnet 서비스의 활성화/비활성화

서비스의 활성화/비활성화 명령을 실행합니다. 설정이 즉시 적용됩니다.

1. **showssh** 명령을 실행하여 **SSH** 설정을 표시하거나 **showtelnet** 명령을 실행하여 **Telnet** 설정을 표시합니다.
   다음에는 SSH 서비스 설정의 표시 예가 나타나 있습니다.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
W9pqa/WxC21Ja4RQVN3009kmVwAAAIAON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzzFFj5XUzQBdabh5p5Rwz+1vriawFIZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

다음에는 Telnet 서비스 설정의 예가 나타나 있습니다.

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

2. **setssh** 명령을 실행하여 **SSH** 서비스 설정을 구성하거나 **settelnet** 명령을 실행하여 **Telnet** 설정을 구성합니다.
   다음에는 SSH 서비스의 활성화 예가 나타나 있습니다.

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

다음에는 Telnet 서비스의 비활성화 예가 나타나 있습니다.

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

8.6.3 SSH 서비스 호스트 키 구성

SSH 서비스를 처음 활성화할 때 호스트 키를 생성합니다.

XSCF-LAN 연결을 통해 SSH 서비스를 사용하는 경우 지문을 기록합니다. 호스트 공개 키의 텍스트 데이터를 클라이언트 디렉토리의 파일로 복사합니다.

1. **showssh** 명령을 실행하여 호스트 키와 지문을 표시합니다.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIBMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
W9pqa/WxC21Ja4RQVN3009kmVwAAAIAON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzzFFj5XUzQBdabh5p5Rwz+1vriawFIZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

2. **setssh** 명령을 실행하여 호스트 키를 생성합니다.
   다음에는 호스트 키의 생성 예가 나타나 있습니다.

```
XSCF> setssh -c genhostkey
Host key create. Continue? [y|n] : y
```

8.6.4 SSH 서비스를 위한 사용자 공개 키 등록/삭제

XSCF-LAN 연결을 통해 SSH 서비스를 위한 사용자 키를 사용하는 경우 사용자 비밀 키와 사용자 공개 키를 클라이언트의 등록된 XSCF 사용자 계정에 생성하고 사용자 공개 키를 XSCF에 등록합니다.

1. **showssh** 명령을 실행하여 사용자 공개 키를 표시합니다.
   다음에는 사용자 키의 미등록 예가 나타나 있습니다.

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

2. 사용자 비밀 키와 사용자 공개 키를 클라이언트의 등록된 **XSCF** 사용자 계정에 생성합니다.
   클라이언트에서 사용자 키를 생성하고 암호를 지정하는 방법은 사용하는 클라이언트 소프트웨어의 설명서를 참조하십시오. 암호를 설정하는 것이 좋습니다.

3. 사용자 공개 키 등록 옵션을 지정하고 **setssh** 명령을 실행한 후 **2**단계에서 생성한 사용자 공개 키를 복사하여 창의 필드에 붙여넣습니다.
   [Enter] 키를 눌러 등록하고 [Ctrl] 및 [D]를 눌러 절차를 완료합니다.

```
XSCF> setssh -c addpubkey -u efgh
Please input a public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
<Press [Ctrl] and [D]>
XSCF>
```

4. **showssh** 명령을 실행하여 사용자 공개 키와 사용자 공개 키 번호를 확인합니다.
   다음에는 번호 1로 사용자 키를 등록하는 예가 나타나 있습니다.

```
XSCF> showssh -c pubkey
Public key:
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

   다음 번 클라이언트에서 XSCF 쉘에 로그인할 때 XSCF 사용자 계정을 사용하여 SSH 연결을 합니다. 사용 키 인증을 통해 XSCF 쉘에 로그인할 수 있도록 합니다.

5. 사용자 공개 키를 삭제하려면 **setssh** 명령을 실행하고 사용자 공개 키 번호를 지정합니다.

```
XSCF> setssh -c delpubkey -s 1
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/
```

```
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

6. **showssh** 명령을 실행하여 사용자 공개 키가 삭제되었는지 확인합니다.

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

8.6.5 SSH/Telnet 서비스 시간 초과 시간의 구성

1. **showautologout** 명령을 실행하여 시간 초과 시간을 표시합니다.

```
XSCF> showautologout
30 min
```

2. **setautologout** 명령을 실행하여 시간 초과 시간을 구성합니다.
   다음에는 시간 초과 시간을 255분으로 구성하는 예가 나타나 있습니다.

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

구성된 시간 초과 시간은 다음 번 로그인 후에 적용됩니다.

8.7 XSCF에 로그인하기 위한 HTTPS 서비스 구성

이 절에는 HTTPS 서비스 설정의 구성 방법이 설명되어 있습니다.

HTTPS 서비스 설정은 XSCF-LAN에 연결하고 XSCF 웹을 사용하며 웹 브라우저 창을 사용하는 경우에 이용하도록 되어 있습니다. 이 절에는 HTTPS의 활성화/비활성화 방법과 HTTPS를 사용하기 위한 설정 구성 방법이 설명되어 있습니다. 시스템은 기본적으로 HTTPS를 비활성화합니다. 이 경우 보안 웹 콘솔을 사용할 수 있습니다.

인증 기관 선택

시스템과 웹 브라우저 환경을 고려하여 다음 인증 기관 가운데 하나를 선택합니다.

- 외부 인증 기관
- 인트라넷에서의 인증 기관
- 자치 인증 기관

환경에서 외부 인증 기관 또는 인트라넷에서의 인증 기관을 사용할 수 없는 경우 XSCF의 자치 인증 기관을 사용합니다. ("8.7.2 자치 인증 기관의 사용 흐름" 참조)

XSCF에서 구성된 자치 인증 기관은 다른 시스템에 외부 인증 기관으로서 사용할 수 없습니다.

자치 인증 인증서의 유효 기간

자치 인증 인증서의 유효 기간은 아래 나타난 바와 같이 고정됩니다.

- 서버 인증서: 10년

웹 서버 인증서의 유효 기간이 만료되거나 웹 서버 인증서가 변경된 경우 HTTPS 서비스 설정을 다시 구성합니다.

고유 이름(DN)

웹 서버 인증서 서명 요청(CSR)을 생성하려면 다음 고유 이름(DN)을 지정합니다.

- 2자 국가 코드(예: US 또는 JP)
- 지역
- 시
- 조직(회사) 이름, 부문/부서 이름
- 일반 이름(사용자 이름, 웹 서버 호스트 이름)
- 관리자 이메일 주소

국가 코드를 제외하고 최대 64자까지 허용됩니다. DN의 자세한 내용은 sethttps(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

8.7.1 외부 또는 인트라넷 인증 기관의 사용 흐름

이 절에는 외부 인증 기관 또는 인트라넷 인증 기관의 사용 흐름이 설명되어 있습니다.

1. **XSCF** 웹 서버 비밀 키를 생성합니다**.**
2. **XSCF**에서 웹 서버 인증서 서명 요청**(CSR)**을 생성합니다**.**
3. 인증서를 **XSCF** 웹 서버 인증서 서명 요청에 게시하도록 인증 기관에 요청합니다**.**
4. 인증 기관이 서명한 웹 서버 인증서를 **XSCF**로 가져옵니다**.**
5. **HTTPS**를 활성화합니다**.**

위 1 ~ 5단계에서 해당 옵션의 sethttps 명령을 실행합니다. XSCF 웹 설정을 구성하는 경우 필요한 설정 항목을 구성합니다.

XSCF가 2개 이상인 시스템의 경우 구성된 설정이 스탠바이 XSCF에 작동 적용됩니다.

8.7.2 자치 인증 기관의 사용 흐름

이 절에는 자치 인증 기관의 사용 흐름이 설명되어 있습니다.

웹 서버 비밀 키 또는 자치적으로 서명한 웹 서버 인증서도 없고 sethttps 명령에 대해 자치 인증을 위한 옵션 "enable"이 지정된 경우 1 ~ 4단계에서 구성한 모든 설정이 자동 구성됩니다.

웹 서버 비밀 키와 자치적으로 서명한 웹 서버 인증서가 있는 경우 아래 1 ~ 4단계를 수행합니다.

1. **XSCF** 자치 인증 기관을 구성합니다.
2. **XSCF** 웹 서버 비밀 키를 생성합니다.
3. **XSCF**에서 자치적으로 서명한 웹 서버 인증서를 생성합니다.
4. **HTTPS**를 활성화합니다.

XSCF가 2개 이상인 시스템의 경우 구성된 설정이 스탠바이 XSCF에 작동 적용됩니다.

8.7.3 HTTPS와 관련된 설정 항목 및 명령의 확인

표 8-9에는 HTTPS와 관련된 설정 항목 및 해당 XSCF 쉘 명령이 나타나 있습니다.

표 8-9 HTTPS와 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
HTTPS의 활성화/비활성화	옵션	sethttps(8), showhttps(8)
외부 인증서 • XSCF에서 웹 서버 비밀 키의 생성 • XSCF에서 웹 서버 CSR 및 기관으로의 인증서 발급 요청 생성 • XSCF로 웹 서버 인증서 가져오기	옵션	sethttps(8), showhttps(8)
자치 인증 • 자치 인증 기관의 구성 • 웹 서버 비밀 키의 생성 • 자치적으로 서명한 웹 서버 인증서의 생성	옵션	sethttps(8), showhttps(8)

8.7.4 HTTPS 서비스의 활성화/비활성화

1. **showhttps** 명령을 실행하여 **HTTPS** 서비스 설정을 표시합니다.
   다음에는 HTTPS 서비스 설정의 표시 예가 나타나 있습니다.

```
XSCF> showhttps
HTTPS status: enabled
Server key: installed in Apr 24 12:34:56 JST 2006
CA key: installed in Apr 24 12:00:34 JST 2006
CA cert: installed in Apr 24 12:00:34 JST 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIBwjCCASsCAQAwgYExCzAJBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTERMA8G
A1UEBxMIbG9jYWxpdHkxFTATBgNVBAoTDG9yZ2FuaXphdGlvbjEPMA0GA1UECxMG
b3JnYW5pMQ8wDQYDVQQDEwZjb21tb24xFjAUBgkqhkiG9w0BCQEWB2VlLm1haWww
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5D57X/k42LcipTWBWzv2GrxaVM
```

```
5GEyx3bdBW8/7WZhnd3uiZ9+ANlvRAuw/YYy7I/pAD+NQJesBcBjuyj9x+IiJl9F
MrI5fR8pOIywVOdbMPCar09rrU45bVeZhTyi+uQOdWLoX/Dhq0fm2BpYuh9WukT5
pTEg+2dABg8UdHmNAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAux1jH3dyB6Xho
PgBuVIakDzIKEPipK9qQfC57YI43uRBGRubu0AHEcLVue5yTu6G5SxHTCq07tV5g
38UHSg5Kqy9QuWHWMri/hxm0kQ4gBpApjNb6F/B+ngBE3j/thGbEuvJb+0wbycvu
5jrhB/ZV9k8X/MbDOxSx/U5nF+Zuyw==
-----END CERTIFICATE REQUEST-----
```

2. **sethttps** 명령을 실행하여 **HTTPS** 설정을 구성합니다.
   다음에는 HTTPS 서비스의 활성화 예가 나타나 있습니다.

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

웹 서버 비밀 키 또는 자치적으로 서명한 웹 서버 인증서도 없고 옵션 "enable"이 지정된 경우 자치 인증의 구성, 웹 서버 비밀 키의 생성, 웹 서버 인증서의 생성 및 활성화가 자동 완료됩니다.

다음에는 HTTPS 서비스의 비활성화 예가 나타나 있습니다.

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

8.7.5 외부 또는 인트라넷 인증 기관을 사용한 웹 서버 인증서 가져오기

1. **sethttps** 명령을 실행하여 웹 서버 비밀 키를 생성합니다.

```
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. **sethttps** 명령을 실행하고 **DN**을 지정하여 **CSR**을 생성합니다.
   다음에는 DN의 지정 예가 나타나 있습니다(JP, Kanagawa, Kawasaki, Example, development, scf-host,abc@example.com).

```
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example
development scfhost abc@example.com
```

3. **showhttps** 명령을 실행하여 **CSR**을 표시합니다. 표시된 **CSR(BEGIN**에서 **END)**을 복사하여 붙여넣은 후 텍스트 파일로 저장합니다.

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2006
CA key: installed in Jul 11 06:33:21 UTC 2006
CA cert: installed in Jul 11 06:33:21 UTC 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAOBgNVBAoTB0ZVSklUU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IImqKg==
-----END CERTIFICATE REQUEST-----
```

4. 복사한 **CSR**을 인증 기관으로 전송하여 웹 서버 인증서를 게시하도록 요청합니다.
5. **import** 옵션이 지정된 **sethttps** 명령을 실행하고 **4**단계에서 서명한 웹 서버 인증서를 복사하여 창의 필드에 붙여넣습니다.
   [Enter] 키를 누르고 [Ctrl] 및 [D]를 눌러 절차를 완료합니다.

```
XSCF> sethttps -c importca
Please import a certificate:
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgTELMAkGA1UEBhMCamox
:
R+OpXAVQvb2tjIn3kO99dq+begECo4mwknW1t7QI7A1BkcW2/MkOolIRa6iP1Zwg
JoPmwAbrGyAvGUtdzUoyIH0jl7dRQrVIRA==
-----END CERTIFICATE-----
<Press [Ctrl] and [D] >
```

6. **sethttps** 명령을 실행하여 **HTTPS**를 활성화합니다.

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

7. 클라이언트에서 **HTTPS**가 지정된 **XSCF** 웹에 액세스합니다. 창에 보안 경고가 표시되지 않고 인증서가 올바른지 확인합니다.

8.7.6 자치 인증 기관 구성 및 웹 서버 인증서 생성

웹 서버 비밀 키 또는 자치적으로 서명한 웹 서버 인증서도 없는 경우

1. **sethttps** 명령을 실행하고 **-c enable** 옵션을 지정합니다.

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

자치 인증의 구성, 웹 서버 비밀 키의 생성, 웹 서버 인증서의 생성 및 HTTPS의 활성화

가 자동 완료됩니다.

사용 가능한 웹 서버 비밀 키와 자치적으로 서명한 웹 서버 인증서가 있는 경우

기존 웹 서버 비밀 키와 인증서가 덮어쓰기가 됩니다.

1. **sethttps** 명령을 실행하고 **DN**을 지정하여 자치적으로 서명한 웹 서버 인증서를 생성합니다.
   다음에는 DN의 지정 예가 나타나 있습니다(JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com).

```
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. **showhttps** 명령을 실행하여 웹 서버 인증서가 생성되었는지 확인합니다.

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2012
CA key: installed in Jul 11 06:33:21 UTC 2012
CA cert: installed in Jul 11 06:33:21 UTC 2012
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAOBgNVBAoTB0ZVSklUU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IImqKg==
-----END CERTIFICATE REQUEST-----
```

3. **sethttps** 명령을 실행하여 **HTTPS**를 활성화합니다.

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

XSCF가 2개 이상인 시스템의 경우 구성된 설정이 스탠바이 XSCF에 작동 적용됩니다.

8.8 XSCF 보안 강화를 위한 감사 구성

이 절에는 XSCF 감사 설정의 구성 방법이 설명되어 있습니다.

감사 설정은 사용자에 의한 네트워크 작업을 감사하며 누가 XSCF에 로그인했고 언제

로그인했으며 어떤 작동을 수행했는지 자세한 액세스 레코드를 유지하는 데 사용됩니다. 시스템은 기본적으로 감사 설정을 활성화합니다. 감사 설정은 주로 감사의 활성화 또는 비활성화 여부와 감사 내역의 관리 방법을 구성합니다.

8.8.1 감사 용어 이해

표 8-10에는 XSCF 감사 설정의 용어와 설명이 나타나 있습니다.

표 8-10 감사 용어의 설명

용어	설명
감사	시스템 액세스를 감사하는 기능. 이는 감사 작업이라고도 합니다.
감사 이벤트	감사할 수 있는 보안 관련 시스템 작업. 숫자 값 또는 이름으로 2개 이상의 감사 이벤트를 지정할 수 있습니다. (예: AEV_LOGIN_SSH, LOGIN_SSH, 0 및 모두)
감사 클래스	관련 감사 이벤트의 그룹. (예: 로그인 감사 클래스의 감사 이벤트: SSH 로그인, Telnet 로그인, HTTPS 로그인 및 로그아웃) 2개 이상의 감사 클래스를 지정할 수 있습니다. (예: CS_AUDIT, AUDIT, 2 및 모두)
감사 레코드	1개 감사 레코드는 1개 감사 이벤트를 식별하는 정보입니다. 여기에는 이벤트 정보, 이벤트 시간 및 기타 관련 정보가 포함됩니다. 감사 레코드는 감사 파일에 저장됩니다.
감사 파일	감사 로그 파일이라고 함. 이는 감사 레코드를 저장합니다.
감사 내역	감사 파일의 컬렉션. 감사 내역은 감사할 항목을 참조 및 분석하는 데 사용할 수 있습니다.
감사 정책	감사 설정. 감사를 활성화/비활성화하고 감사 내역이 가득 찼을 때 관리 방법을 적용하는 데 사용됨.
감사 토큰	감사 레코드의 필드. 감사 토큰에는 사용자 및 권한과 같은 감사 이벤트 특성 정보가 있습니다.

8.8.2 감사 데이터 기록 이해

시스템은 XSCF 펌웨어 감사 모듈의 제어를 통해 사용자를 위한 감사 내역을 제공합니다. 가져온 관련 이벤트의 정보로부터 XSCF 펌웨어는 아래 설명된 바와 같이 감사 정보를 수집합니다.

1. 감사 이벤트의 데이터는 감사 레코드 형식으로 기록됩니다.
2. 감사 레코드는 시간 순서대로 **XSCF** 펌웨어 로컬 감사 파일에 저장됩니다.
3. 감사 파일의 그룹은 링크되어 감사 내역으로서 처리됩니다.

4. 감사 레코드는 감사 내역으로서 저장되며 사용자는 감사 내역을 참조할 수 있습니다**(viewaudit(8)** 참조**).**

8.8.3 감사 설정과 관련된 설정 항목 및 명령의 확인

표 8-11에는 감사와 관련된 설정 항목 및 해당 XSCF 쉘 명령이 나타나 있습니다.

표 8-11 감사와 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
감사의 활성화/비활성화	옵션	setaudit(8), showaudit(8)
로그 파일 전송, 데이터 삭제	옵션	setaudit(8), showaudit(8)
감사 정책 ■ 활성화/비활성화의 지정 또는 지정된 사용자에 전역 정책의 적용 ■ 감사 클래스의 활성화/비활성화 ■ 감사 이벤트스의 활성화/비활성화 ■ 모든 사용자에 대한 감사의 활성화/비활성화(전역 정책) ■ 임계값에 도달한 로컬 감사 파일의 알림이 게시되는 대상 이메일 주소 ■ 감사 내역이 가득 찼을 때 보류/카운팅 ■ 로컬 감사 파일 활용도(%)에 대한 경고 임계값	옵션	setaudit(8), showaudit(8)
감사 내역 표시	옵션	viewaudit(8)

8.8.4 감사의 활성화/비활성화

감사는 기본적으로 활성화됩니다. 감사 설정의 경우 auditadm 사용자 권한이 필요합니다.

감사를 비활성화하면 감사 내역에 쓰기가 중지됩니다. 감사를 활성화하면 쓰기가 재개됩니다. 시스템을 재부팅하면 감사가 비활성화된 후 활성화 시퀀스가 시작됩니다.

XSCF 로컬 감사 파일은 1차와 2차로 분류됩니다. 감사 파일 임계값을 초과하지 않는 한 아카이브로 데이터를 저장할 수 있습니다. 따라서 로컬 감사 파일 활용도는 절대 0이 될 수 없습니다.

1. **showaudit** 명령을 실행하여 감사 설정을 표시합니다**.**
   다음에는 모든 현재 시스템 감사 상태의 예가 나타나 있습니다.

```
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. **setaudit** 명령을 실행하여 설정을 활성화/비활성화합니다.
   다음에는 감사 데이터의 쓰기 비활성화와 로그 파일 전송 명령의 예가 나타나 있습니다.

```
XSCF> setaudit disable
```

다음에는 감사 데이터의 쓰기 활성화 예가 나타나 있습니다.

```
XSCF> setaudit enable
Turns on writing of the audit records for the audit trail.
```

8.8.5 감사 파일의 데이터 삭제

로컬 감사 파일이 가득 찬 경우 감사 내역 데이터를 삭제할 수 있습니다.

1. **showaudit** 명령을 실행하여 감사 설정을 표시합니다.
   다음에는 모든 현재 시스템 감사 상태의 예가 나타나 있습니다.

```
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. **setaudit** 명령을 실행하여 감사 내역 로깅 데이터를 삭제합니다.

```
XSCF> setaudit delete
```

8.8.6 감사 정책 구성

1. **showaudit** 명령을 실행하여 감사 정책 설정을 표시합니다.

```
XSCF> showaudit all
Auditing:              enabled
Audit space used:      13713 (bytes)
Audit space free:      4180591 (bytes)
Records dropped:       0
Policy on full trail: suspend
User global policy:    enabled
Mail:
Thresholds:            80% 100%
User policy:
Events:
        AEV_AUDIT_START enabled
        AEV_AUDIT_STOP enabled
```

2. **setaudit** 명령을 실행하여 감사 정책 설정을 구성합니다.
   다음에는 사용자 3명을 지정하고 감사 클래스를 AUDIT ~ LOGIN 그룹으로 활성화하며 감사 이벤트를 SSH 로그인으로 활성화하고 전역 정책을 사용자로 비활성화하는 설정의 구성 예가 나타나 있습니다.

```
XSCF> setaudit -a yyyyy,uuuuu,nnnnn=enabe -c
ACS_AUDIT,ACS_LOGIN=enable -e AEV_LOGIN_SSH=enable -g disable
```

   다음에는 경고 전송의 대상 이메일 주소 설정, 감사 내역이 가득 찼을 때 카운트 설정 및 파일 활용도에 대한 경고 임계값 설정의 예가 나타나 있습니다.

```
XSCF> setaudit -m yyyy@example.com -p count -t 50,75,90
```

3. **showaudit** 명령을 실행하여 설정을 확인합니다.

```
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
:
```

쓰기 보류를 지정하면 감사 내역이 가득 찼을 때 XSCF 쉘 및 XSCF 웹 작동이 잠기고 비활성화됩니다. 사용 가능한 공간을 사용할 수 있거나 감사 정책이 카운트로 변경될 때까지 후속 감사 내역이 쓰기가 되지 않습니다.

카운트가 지정되면 감사 내역이 가득 찼을 때 새 감사 내역 데이터가 취소(삭제)되고 레코드의 삭제 횟수가 카운트됩니다(삭제 카운트).

보류를 지정하려면 auditadm 사용자 권한이 있고 감사 정책이 비활성화된 사용자 계정을 사전에 생성해야 합니다.

보류가 지정되고 감사 내역이 가득 차면 XSCF가 잠깁니다. XSCF가 잠기면 감사 정책이 비활성화된 사전 구성의 사용자 계정으로 로그인하고 감사 내역을 삭제합니다. 그런 다음 XSCF 작동을 재개합니다.

감사 정책이 비활성화된 사용자 계정이 생성되고 보류가 지정되며 감사 내역이 가득 차면 감사 내역을 삭제할 수 없고 다른 기능을 실행할 수도 없습니다. 이 경우 기본 사용자 계정을 사용하여 로그인하고 감사 내역을 삭제합니다. 기본 계정으로 로그인은 『SPARC M10 시스템 설치 안내서』의 "6장 시스템의 초기 진단 구현"을 참조하십시오.

파일 활용도 경고는 콘솔 메시지 또는 보안 이메일로 표시됩니다.

다음에는 경고 메시지의 예가 나타나 있습니다.

예: WARNING: audit trail is 91% full

현재 감사 내역 파일의 공간은 삭제를 통해 사용할 수 있습니다.

8.8.7 감사 로그 보기

1. **viewaudit** 명령을 실행하여 감사 내역을 봅니다.

```
XSCF> viewaudit
file,1,2006-06-29 13:42:59.128 +09:00,20060629044259.0000000000.localhost
header,20,1,audit - start,localhost.localdomain,2006-06-29 13:42:59.131 +09:00
header,31,1,login - console,localhost.localdomain,2006-06-29 13:45:03.755
+09:00subject,1,default,normal,console
header,60,1,command - showpasswordpolicy,localhost.localdomain,2006-06-29
13:45:33.653 +09:00
subject,1,default,normal,console
command,showpasswordpolicy
```

```
platform access,granted
return,0
:
```

감사 레코드를 보는 방법은 "17장 로그 및 메시지 확인"을 참조하십시오.

9장

시스템 구성

이 장에는 전원 제어에 포커스를 맞춘 시스템 전체에 영향을 미치는 설정 항목이 설명되어 있습니다.

- 시스템 고도 설정/확인
- 시스템 활성화 제어
- 이중 전원 공급 활성화/비활성화
- 소비 전력 최소화
- DVD 드라이브 연결

9.1 시스템 고도 설정/확인

이 절에는 시스템 고도의 설정 및 확인 방법이 설명되어 있습니다.

SPARC M10 시스템은 시스템 설치 위치의 고도 및 온도에 따라 시스템 내부 냉각 팬의 회전을 제어합니다. 따라서 초기 시스템 시작 시에 고도 설정을 구성해야 합니다.

노트 - 설정은 현장 엔지니어가 구성해야 합니다.

다음 절차에서 실행하는 XSCF 명령의 자세한 내용은 설명서 페이지 및『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

9.1.1 시스템 고도 설정

시스템 고도를 설정하려면 XSCF 펌웨어 setaltitude 명령을 사용합니다.

```
XSCF> setaltitude -s altitude=value
```

값의 경우 서버 설치 위치의 고도를 미터 단위로 지정합니다. 이는 0부터 100 증분씩 지정할 수 있습니다.

노트 - 시스템 고도를 설정한 후 설정을 적용하려면 rebootxscf 명령을 실행하여 XSCF를 재설정해야 합니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **setaltitude** 명령을 실행하여 고도 설정을 구성합니다.
   다음에는 1,000m로 고도를 구성하는 예가 나타나 있습니다.

```
XSCF> setaltitude -s altitude=1000
1000m
```

3. 구성된 설정을 적용하려면 **rebootxscf** 명령을 실행하여 **XSCF**를 재설정합니다.

노트 - 다른 항목의 설정으로 진행하려면 모든 설정을 완료한 후에 작동을 시작하십시오.

```
XSCF> rebootxscf
```

9.1.2 시스템 고도 확인

시스템 고도를 확인하려면 XSCF 펌웨어 showaltitude 명령을 사용합니다.

```
XSCF> showaltitude
1000m
```

현재 구성된 시스템 고도 설정이 미터 단위로 표시됩니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **showaltitude** 명령을 실행하여 고도 설정을 표시합니다.
   다음에는 고도가 1,000m로 설정되었는지 확인하는 예가 나타나 있습니다.

```
XSCF> showaltitude
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.

9.2 시스템 활성화 제어

이 절에는 시스템 활성화 제어 설정이 설명되어 있습니다.

시스템 활성화 제어는 다음과 같이 사용됩니다.

- 응축 등에 의한 활성화 실패가 없도록 시스템이 웜업될 때까지 대기하는 데 사용됩니다(9.2.1 참조).
- 주변 장치에 전원이 공급될 때까지 시스템 활성화가 대기 상태에 있도록 하는 데 사용됩니다(9.2.1 참조).
- 소비 전력의 상한을 초과하지 않도록 물리 분할 활성화의 시간 차이를 설정하는 데 사용됩니다(9.2.1 참조).
- 데이터 센터의 에어 컨디셔닝된 온도가 해당 온도에 도달할 때까지 시스템 활성화가 대기 상태에 있도록 하는 데 사용됩니다(9.2.2 참조).

9.2.1 웜업 시간 설정/확인

웜업 시간은 SPARC M10 시스템 전원이 입력되어 전원 장치와 팬이 작동을 시작한 이후 도메인 활성화가 대기하는 시간입니다. 예를 들어 이는 응축으로 인한 시스템 활성화 실패를 방지하거나 SAN 부팅을 사용할 때 주변 장치에 전원이 공급될 때까지 대기 시간을 설정하는 데 사용됩니다.

setpowercapping 명령으로 구성하는 소비 전력의 상한과 관련하여 모든 물리 분할이 동시에 작동을 시작하고 소비 전력의 상한을 초과하는 경우가 있을 수도 있습니다. 이를 방지하도록 웜업 시간을 사용하여 물리 분할 활성화의 시간 차이를 설정할 수 있습니다.

웜업 시간이 설정되면 서버에 전원이 공급되고 전원 공급 시퀀스가 시작되며 지정된 웜업 시간이 경과될 때 OpenBoot PROM이 시작됩니다.

웜업 시간 설정

웜업 시간을 설정하려면 XSCF 펌웨어 powerupdelay 명령을 사용합니다.
이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

```
XSCF> setpowerupdelay -c warmup -s time
```

시간의 경우 웜업 시간을 분으로 지정합니다. 0 ~ 255의 정수를 지정할 수 있습니다.
기본 값은 0입니다.

노트 - 지정된 웜업 시간은 poweron 명령을 사용하여 시스템에 전원을 공급한 경우에만 사용할 수 있습니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **setpowerupdelay** 명령을 실행하여 웜업 시간 설정을 구성합니다.
   다음에는 웜업 시간을 5분으로 구성하는 예가 나타나 있습니다.

```
XSCF> setpowerupdelay -c warmup -s 5
```

   시스템이 실행되는 동안 웜업 시간이 구성되면 다음 번 시스템이 활성화될 때 구성된 시간이 적용됩니다.

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

웜업 시간 구성

웜업 시간을 확인하려면 XSCF 펌웨어 showpowerupdelay 명령을 사용합니다.
이 작동은 platadm, platop 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 물리 분할의 경우 pparadm, pparmgr 또는 pparop 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

```
XSCF> showpowerupdelay
```

- [warmup time]으로 구성된 웜업 시간이 분으로 표시됩니다.
- [wait time]은 "시작 대기 시간 확인"을 참조하십시오.

작동 절차

1. **platadm, platop, pparadm, pparmgr, pparop** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **showpowerupdelay** 명령을 실행하여 웜업 시간 설정을 표시합니다.
   다음에는 웜업 시간이 10분으로 설정되었는지 확인하는 예가 나타나 있습니다.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃

합니다.

9.2.2 시작 대기 시간 설정/확인

전원 공급 후 지정된 시간 동안 SPARC M10 시스템에서 시스템이 시작될 때까지 대기합니다. 이에 따라 예를 들어 에어 컨디셔닝된 온도가 데이터 센터의 해당 온도로 설정된 후 작동을 시작하도록 시스템을 제어할 수 있습니다.

시작 대기 시간이 구성되면 서버에 전원이 공급되고 지정된 시간이 경과된 후에 시스템이 시작됩니다.

시작 대기 시간 설정

시작 대기 시간을 설정하려면 XSCF 펌웨어 setpowerupdelay 명령을 사용합니다. 이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

```
XSCF> setpowerupdelay -c wait -s time
```

시간의 경우 시작 대기 시간을 분으로 지정합니다. 0 ~ 255의 정수를 지정할 수 있습니다.
기본 값은 0입니다.

노트 - 지정된 시작 대기 시간은 poweron 명령을 사용하여 시스템에 전원을 공급한 경우에만 사용할 수 있습니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **setpowerupdelay** 명령을 실행하여 시작 대기 시간 설정을 구성합니다.
   다음에는 시작 대기 시간을 5분으로 구성하는 예가 나타나 있습니다.

```
XSCF> setpowerupdelay -c wait -s 5
```

   시스템이 실행되는 동안 시작 대기 시간이 구성되면 다음 번 시스템이 활성화될 때 구성된 시간이 적용됩니다.

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

시작 대기 시간 구성

시작 대기 시간 설정을 확인하려면 XSCF 펌웨어 showpowerupdelay 명령을 사용합니다.

이 작동은 platadm, platop 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 물리 분할의 경우 pparadm, pparmgr 또는 pparop 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

```
XSCF> showpowerupdelay
```

- [wait time]으로 구성된 시작 대기 시간이 분으로 표시됩니다.
- [warmup time]은 "웜업 시간 확인"을 참조하십시오.

작동 절차

1. **platadm, platop, pparadm, pparmgr, pparop** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **showpowerupdelay** 명령을 실행하여 시작 대기 시간 설정을 표시합니다.
   다음에는 시작 대기 시간이 20분으로 설정되었는지 확인하는 예가 나타나 있습니다.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

9.3 이중 전원 공급 활성화/비활성화

SPARC M10 시스템이 이중 전원 공급으로 구성되는 경우 이중 전원 공급을 활성화 또는 비활성화해야 합니다.

이중 전원 공급 연결의 방법과 관련된 자세한 내용은『SPARC M10 시스템 설치 안내서』의 "2.6.2 이중 전원 공급"을 참조하십시오.

노트 - 이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

9.3.1 이중 전원 공급 활성화

이중 전원 공급을 활성화하려면 XSCF 펌웨어 setdualpowerfeed 명령을 사용합니다.

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s enable
```

시스템 내 모든 캐비닛으로의 이중 전원 공급을 활성화하려면 -a를 지정합니다.
시스템 내 원하는 캐비닛으로만의 이중 전원 공급을 활성화하려면 -b bb_id를 지정합니다. Bb_id의 경우 캐비닛의 BB-ID를 지정합니다. 시스템 구성에 따라 0 ~ 15 또는 80 ~ 83의 정수를 지정할 수 있습니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **setdualpowerfeed** 명령을 실행하여 이중 전원 공급을 활성화합니다.
   다음에는 BB-ID 1로의 이중 전원 공급을 활성화하는 예가 나타나 있습니다.

```
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.
```

9.3.2 이중 전원 공급 비활성화

이중 전원 공급을 비활성화하려면 XSCF 펌웨어 setdualpowerfeed 명령을 사용합니다.

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s disable
```

시스템 내 모든 캐비닛으로의 이중 전원 공급을 비활성화하려면 -a를 지정합니다.
시스템 내 원하는 캐비닛으로만의 이중 전원 공급을 비활성화하려면 -b bb_id를 지정합니다. Bb_id의 경우 캐비닛의 BB-ID를 지정합니다. 시스템 구성에 따라 0 ~ 15 또는 80 ~ 83의 정수를 지정할 수 있습니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **setdualpowerfeed** 명령을 실행하여 이중 전원 공급을 비활성화합니다.
   다음에는 모든 캐비닛의 처리 예가 나타나 있습니다.

```
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.
```

9.3.3 이중 전원 공급 설정 확인

이중 전원 공급 설정을 확인하려면 XSCF 펌웨어 showdualpowerfeed 명령을 사용합니다.

```
XSCF> showdualpowerfeed
```

상황에 따라 다음 가운데 하나가 출력됩니다.

- 이중 전원 공급이 활성화되는 경우

```
BB#00: Dual power feed is enabled.
```

- 이중 전원 공급이 비활성화되는 경우

```
BB#00: Dual power feed is disabled.
```

- 이중 전원 공급이 활성화 상태에서 비활성화 상태로 변경되는 경우

```
BB#00:enable -> disable
NOTE: Dual power feed will be change the next time the platform
is powered on.
```

- 이중 전원 공급이 비활성화 상태에서 활성화 상태로 변경되는 경우

```
BB#00:disable -> enable
NOTE: Dual power feed will be change the next time the platform
is powered on.
```

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **showdualpowerfeed** 명령을 실행하여 이중 전원 공급 설정을 확인합니다.
   다음에는 BB-ID 0과 1로 구성된 시스템이 비활성화에서 활성화로 변경되었는지 확인하는 예가 나타나 있습니다.

```
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.
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

9.4 소비 전력 최소화

이 절에는 SPARC M10 시스템의 소비 전력을 최소화하도록 준비된 다양한 기능이 설명되어 있습니다.

9.4.1 소비 전력의 상한 구성

SPARC M10 시스템에서 소비 전력의 상한과 상한 초과 시의 수행 작업을 구성할 수 있습니다.

소비 전력의 상한을 구성하려면 XSCF 펌웨어 setpowercapping 명령을 사용합니다. 설정은 명령 실행 직후 XSCF에 적용됩니다.

이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다.

```
XSCF> setpowercapping -s option=value [[-s option=value]...]
```

옵션 및 값의 경우 다음 설정을 구성할 수 있습니다.

- 소비 전력 한계 활성화/비활성화(activate_state)
  활성화 또는 비활성화를 지정합니다. (기본적으로 비활성화됨)
- 소비 전력의 상한 구성
  다음 가운데 하나를 지정합니다.
  - 와트(powerlimit_w) 0 ~ 999999의 값을 지정합니다.
  - 백분율(powerlimit_p) 0 ~ 100의 값을 지정합니다.
- 상한 초과 시의 허용 가능한 시간 연장(timelimit)
  10 ~ 99999의 값을 초로 지정할 수 있습니다. 다음 값 역시 지정할 수 있습니다.
  - 기본값 : 30초
  - 없음 : 허용 가능한 시간 연장 없음
- 위반 시의 작업(violation_actions)
  상한을 초과하는 동안 허용 가능한 시간 연장을 초과할 때 수행하는 작업을 지정합니다. 다음 설정 가운데 하나를 지정합니다. 기본 값은 없음입니다.

- 메시지를 출력합니다(없음).
- 메시지를 출력하고 소비 전력이 상한 미만이 될 때까지 물리 분할을 종료합니다(종료). PPAR-ID의 내림차순으로 물리 분할의 지정된 종료가 수행됩니다.
- 메시지를 출력하고 소비 전력이 상한 미만이 될 때까지 물리 분할의 전원을 강제 차단합니다(poff). PPAR-ID의 내림차순으로 물리 분할이 강제 종료됩니다.

노트 - 작동 중 평균 소비 전력에 따라 소비 전력의 상한이 구성되는 경우 SPARC M10 시스템에서 활성화 시퀀스의 자가 진단 또는 전원 공급 프로세스 시에 발생할 수 있는 돌입 전력이 문제를 일으킬 수 있습니다. 이 문제는 setpowerupdelay 명령을 사용하여 방지할 수 있으며 이 명령은 돌입 전력이 균등하도록 물리 분할의 전원 공급 간에 시간 지연을 설정하는 XSCF 명령입니다.

---

setpowercapping 명령의 자세한 내용은 setpowercapping(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **setpowercapping** 명령을 실행합니다.
   다음에는 소비 전력 한계의 활성화 예가 나타나 있습니다.

```
XSCF> setpowercapping -s activate_state=enabled
activate_state      :disabled -> enabled
powerlimit          :500w -> -
timelimit           :30 -> -
violation_actions   :none -> -
The specified options will be changed.
Continue? [y|n]     :y
configured.
activate_state      :enabled
powerlimit          :500w
timelimit           :30
violation_actions   :none
```

   다음에는 소비 전력의 상한을 1,000 W로 구성하고 상한 초과 시에 허용 가능한 시간 연장을 100초로 구성하는 예가 나타나 있습니다.

```
XSCF> setpowercapping -s powerlimit_w=1000 -s timelimit=100
activate_state : enabled -> -
powerlimit : 500w -> 1000w
timelimit : 30 -> 100
violation_actions :none -> -
The specified options will be changed.
Continue? [y|n]:y
configured.
activate_state :enabled
```

```
powerlimit :1000w
timelimit :100
violation_actions :none
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다**.**
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

9.4.2 비정상 온도/전압 해결

SPARC M10 시스템에는 하드웨어 고장으로 인한 비정상 온도 또는 전압과 같은 오류가 감지될 때 연속 작동을 위해 CPU 주파수를 감소시키는 기능이 있습니다. 이 기능은 SPARC M10 시스템 캐비닛을 기반으로 제어됩니다.
비정상을 감지하여 발생한 비정상 온도 또는 전압을 해결하거나 비정상을 일으킨 고장 부품을 교체하면 CPU 주파수가 정상으로 자동 복귀합니다.

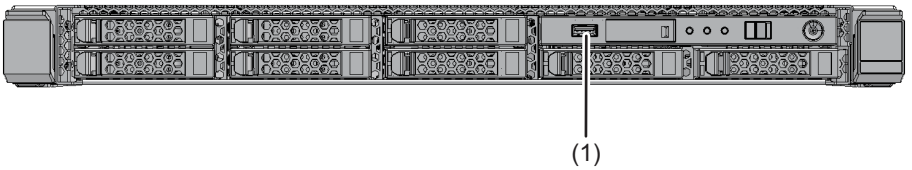
9.5 DVD 드라이브 연결

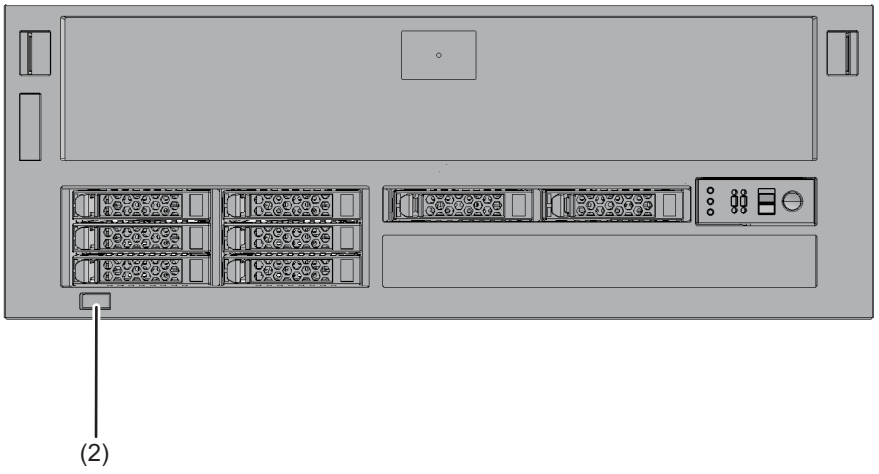
SPARC M10 시스템에는 내부 DVD 드라이브가 없습니다. Oracle Solaris 및/또는 비즈니스 응용 프로그램 소프트웨어를 설치하려면 USB를 통해 연결되는 외부 DVD 드라이브를 사용합니다.

9.5.1 USB를 통해 연결되는 외부 DVD 드라이브 사용

SPARC M10 시스템 캐비닛의 전면에는 1개 USB 포트가 있습니다. 외부 DVD 드라이브를 USB 포트에 연결하여 사용합니다.

그림 9-1 SPARC M10 시스템의 DVD 드라이브 연결용 USB 포트





번호	구성요소
1	DVD 드라이브 연결용 USB 포트(SPARC M10-1)
2	DVD 드라이브 연결용 USB 포트(SPARC M10-4/M10-4S1)

10장

물리 분할 제어

이 장에는 물리 분할을 제어하는 데 필요한 항목이 설명되어 있습니다.

- 물리 분할 구성
- 물리 분할 작동 모드 설정
- 물리 분할의 전원 공급
- 물리 분할의 전원 차단
- 물리 분할 재설정
- 물리 분할의 구성 변경

10.1 물리 분할 구성

이 절에는 물리 분할 구성의 요약이 설명되어 있습니다.

SPARC M10 시스템의 경우 SPARC M10 시스템 캐비닛은 1개 시스템 보드(PSB)로서 간주되며 1개 이상의 시스템 보드가 조합되어 분할을 구성합니다. 1개 이상의 시스템 보드로 구성된 분할을 물리 분할(PPAR)이라고 합니다.

각 시스템 보드마다 1개 물리 분할을 구성하는 경우 SPARC M10-4S에서 최대 16개의 물리 분할을 구성하거나 SPARC M10-1/M10-4에서 최대 1개의 물리 분할을 구성할 수 있습니다.

물리 분할은 XSCF 펌웨어 addboard 명령을 사용하여 구성합니다. 자세한 내용은 『SPARC M10 시스템 도메인 구성 안내서』의 "3장 물리 분할 구성"을 참조하십시오.

10.2 물리 분할 작동 모드 설정

이 절에는 물리 분할 작동 모드의 요약이 설명되어 있습니다.

각 물리 분할마다 다음 작동 모드를 설정할 수 있습니다.

- 자가 진단의 진단 레벨
- 자가 진단의 콘솔 메시지 상세 레벨
- 활성화 확인(XSCF와 하이퍼바이저 간의 모니터링)
- 호스트 와치독(하이퍼바이저와 제어 도메인 간의 모니터링) 시간 초과 시의 작동
- 브레이크 신호 억제
- 게스트 도메인의 자동 부팅
- 절전 작동
- I/O 버스 재구성

작동 모드를 설정하여 물리 분할을 작동 또는 유지 관리하는 동안 지정된 물리 분할이 불필요한 신호 및/또는 명령을 수신하지 않도록 할 수 있습니다.

물리 분할 작동 모드는 XSCF 펌웨어 setpparmode 명령을 사용하여 설정합니다. 자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』의 "3.6 PPAR 모드 설정/확인"을 참조하십시오.

10.3 물리 분할의 전원 공급

이 절에는 물리 분할의 전원 공급 방법이 설명되어 있습니다.

특정된 물리 분할에 전원을 공급하려면 XSCF 펌웨어 poweron 명령을 사용합니다. 자세한 내용은 "3.1.3 물리 분할의 개별 전원 공급"을 참조하십시오.

10.4 물리 분할의 전원 차단

이 절에는 물리 분할의 전원 차단 방법이 설명되어 있습니다.

특정된 물리 분할의 전원을 차단하려면 XSCF 펌웨어 poweroff 명령을 사용합니다. 자세한 내용은 "3.2.4 물리 분할의 개별 전원 차단"을 참조하십시오.

10.5 물리 분할 재설정

이 절에는 물리 분할 재설정의 요약이 설명되어 있습니다.

특정된 물리 분할을 재설정하려면 XSCF 펌웨어 reset 명령을 사용합니다. 자세한 내용은 "3.3.2 물리 분할 재설정"을 참조하십시오.

10.6 물리 분할의 구성 변경

이 절에는 물리 분할 구성 변경의 요약이 설명되어 있습니다.

SPARC M10 시스템에서 물리 분할을 구성한 후 시스템 보드를 추가 또는 제거하여 물리 분할의 구성을 변경할 수 있습니다.

물리 분할의 구성을 변경하려면 XSCF 펌웨어 addboard 또는 deleteboard 명령을 사용합니다. 자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』의 "6장 논리 도메인 구성요소 재구성"을 참조하십시오.

11장

논리 도메인 제어

이 장에는 논리 도메인의 제어와 논리 도메인의 제어 방법이 설명되어 있습니다.

- 논리 도메인 구성
- 제어 도메인용 OpenBoot PROM 환경 변수 설정
- 논리 도메인의 구성 변경
- 논리 도메인의 시간 구성
- 논리 도메인에서 패닉 발생

11.1 논리 도메인 구성

논리 도메인은 Oracle VM Server for SPARC가 제공하는 가상 하드웨어 환경입니다. 1개 플랫폼을 2개 이상의 가상 하드웨어 환경(논리 도메인)으로 나누고 Oracle Solaris를 각 논리 도메인에서 독립적으로 실행할 수 있습니다. 1개 SPARC M10 시스템에 논리 도메인이 2개 이상인 구성은 서버를 통합하고/하거나 시스템 작동 속도를 증가시킵니다. 또한 플랫폼에 장착된 CPU, 메모리 모듈, I/O 장치 및 기타 하드웨어 자원을 논리 도메인에 유연하게 할당하고 자원 활용률을 높일 수 있습니다.

SPARC M10 시스템의 경우 먼저 물리 분할(PPAR)을 구성한 후 물리 분할의 플랫폼에서 논리 도메인을 구성합니다.

논리 도메인의 구성 방법은 『SPARC M10 시스템 도메인 구성 안내서』의 "4장 빌딩 블록 연결 구성"을 참조하십시오.

11.2 제어 도메인용 OpenBoot PROM 환경 변수 설정

이 절에는 XSCF 펌웨어에 의해 설정되는 제어 도메인용 OpenBoot PROM 환경 변수가 설명되어 있습니다.

OpenBoot PROM 및 OpenBoot PROM 환경 변수의 자세한 내용은 Oracle Solaris 관련 설명서를 참조하십시오.

11.2.1 XSCF 펌웨어에 의해 설정되는 OpenBoot PROM 환경 변수

다음의 제어 도메인용 OpenBoot PROM 환경 변수는 XSCF 펌웨어에 의해 설정됩니다.

표 11-1 XSCF에 의해 설정되는 제어 도메인용 OpenBoot PROM 환경 변수

OpenBoot PROM 환경 변수	설명	설정 방법
auto-boot?	전원 공급 시에 제어 도메인을 자동으로 시작함 (기본값은 참임)	부팅 스크립트
input-device	제어 도메인 콘솔용 입력 장치를 구성함 (기본값은 가상 콘솔임)	부팅 스크립트
output-device	제어 도메인 콘솔용 출력 장치를 구성함 (기본값은 가상 콘솔임)	부팅 스크립트
use-nvramrc?	제어 도메인 시작 시 nvramrc의 내용 실행 여부 (기본값은 거짓임)	use-nvramrc 피연산자
security-mode	펌웨어 보안 모드를 설정함 (기본값은 없음임)	security-mode 피연산자

이 OpenBoot PROM 환경 변수를 설정하려면 XSCF 펌웨어 setpparparam 명령을 사용합니다.
다음 2개 설정 방법을 사용할 수 있습니다.

- 부팅 스크립트에서 환경 변수 설정
  부팅 스크립트는 OpenBoot PROM 환경 변수가 저장되는 스크립트입니다. Setpparparam -s boot-scipt를 사용하여 변수를 설정합니다. 부팅 스크립트는 환경 변수가 설정된 후 제어 도메인 시작 시에만 사용됩니다. 스크립트의 내용은 시작 후에 삭제됩니다. 2개 이상의 환경 변수를 설정하고 NULL 문자를 포함한 최대 255자를 저장할 수 있습니다.
- 피연산자를 사용한 환경 변수 설정
  특정 OpenBoot PROM 환경 변수는 setpparparam 명령의 피연산자로서 설정됩니다. 이 환경 변수를 설정하려면 관련 피연산자를 사용합니다.

11.2.2 제어 도메인용 OpenBoot 환경 변수 설정

XSCF 펌웨어 setpparparam 명령을 사용하여 제어 도메인용 OpenBoot PROM 환경 변수를 설정합니다.
Platadm 또는 fieldeng 권한이 있는 사용자 계정이 실행에 사용됩니다. 또는 대상 PPAR의 경우 pparadm 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

부팅 스크립트 구성

```
setpparparam -p ppar_id -s boot-script value
```

환경 변수가 부팅 스크립트에 저장되는 물리 분할(PPAR)을 ppar_id로 설정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.
부팅 스크립트에 저장될 OpenBoot PROM 환경 변수를 값으로 설정합니다. 값을 큰 따옴표("")를 붙여 지정합니다.

Use-nvramrc?를 거짓으로 설정

```
setpparparam -p ppar_id use-nvramrc
```

환경 변수가 저장되는 물리 분할(PPAR)을 ppar_id로 설정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.

Security-mode를 없음으로 설정

```
setpparparam -p ppar_id security-mode
```

환경 변수가 저장되는 물리 분할(PPAR)을 ppar_id로 설정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. 제어 도메인용 **OpenBoot PROM** 환경 변수를 설정합니다.
   다음 예에서는 PPAR-ID 00인 제어 도메인의 자동 부팅을 활성화합니다.

```
XSCF> setpparparam -p 0 -s boot-script "setenv auto-boot true"
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable bootscript will be changed.
Continue? [y|n]: y
```

11.2.3 제어 도메인용으로 설정된 OpenBoot PROM 환경 변수의 표시

setpparparam 명령을 통해 제어 도메인용으로 설정된 OpenBoot PROM 환경 변수를 표시하려면 XSCF 펌웨어 showpparparam 명령을 사용합니다.
Useradm, platadm, platop 또는 fieldeng 권한이 있는 사용자 계정이 실행에 사용됩니

다. 또는 대상 PPAR의 경우 pparadm, pparmgr 또는 pparop 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

```
showpparparam -p ppar_id
```

환경 변수가 표시되는 물리 분할(PPAR)을 -ppar_id로 설정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.

```
setpparparam -p ppar_id set-defaults
```

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. 제어 도메인용으로 설정된 **OpenBoot PROM** 환경 변수를 표시합니다.
   다음 예에서는 PPAR-ID 00인 제어 도메인의 환경 변수를 표시합니다.

```
XSCF> showpparparam -p 0
use-nvramrc         :false
security-mode       :none
bootscript          :
setenv auto-boot true
setenv input-device virtual-console
setenv input-device virtual-console
```

11.2.4 제어 도메인용으로 설정된 OpenBoot PROM 환경 변수의 삭제

제어 도메인용으로 설정된 OpenBoot PROM 환경 변수를 삭제하려면 XSCF 펌웨어 setpparparam 명령을 사용합니다.
Platadm 또는 fieldeng 권한이 있는 사용자 계정이 실행에 사용됩니다. 또는 대상 PPAR의 경우 pparadm 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

부팅 스크립트 삭제

```
setpparparam -p ppar_id -s boot-script -r
```

부팅 스크립트가 삭제되는 물리 분할(PPAR)을 ppar_id로 설정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.

모든 OpenBoot PROM 환경 변수의 초기화

```
setpparparam -p ppar_id set-defaults
```

환경 변수가 초기화되는 물리 분할(PPAR)을 ppar_id로 설정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. 제어 도메인용으로 설정된 **OpenBoot PROM** 환경 변수를 삭제합니다.
   다음 예에서는 PPAR-ID 00인 제어 도메인의 부팅 스크립트를 삭제합니다.

```
XSCF> setpparparam -p 0 -s boot-script -r
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable bootscript will be cleared.
Continue? [y|n]: y
```

11.3 논리 도메인의 구성 변경

논리 도메인을 구성하는 경우 CPU, 메모리 모듈 및 I/O 장치와 같은 물리 분할에서 구현되는 하드웨어 자원을 유연하게 할당할 수 있습니다. 작동 중 논리 도메인에서 CPU 및 메모리 모듈을 동적으로 재구성할 수도 있어 비즈니스 중단 없이도 갑작스러운 부하 변화와 같은 문제를 처리할 수 있습니다. 도메인의 실행 방식에 따라 자원을 추가 또는 제거할 수 있어 하드웨어 자원을 효과적으로 사용하고 서버에서의 활용률을 높일 수 있습니다.

논리 도메인 구성 변경과 필요 시 용량 제공(CoD)을 함께 사용하여 예약된 CoD 자원을 사용할 수 있습니다. 갑작스러운 자원 보강 요구에 대응하고자 예약된 CoD 자원을 할당하면 다른 도메인의 자원을 삭제하지 않고도 자원이 확장됩니다.

동적 CPU/메모리 재구성을 위해 Oracle VM Server for SPARC가 사용됩니다.

논리 도메인의 구성 변경 방법은『SPARC M10 시스템 도메인 구성 안내서』의 "6장 논리 도메인 구성요소 재구성"을 참조하십시오.

11.4 논리 도메인의 시간 구성

이 절에는 논리 도메인의 시간 구성에 필요한 지식과 설정 표준이 설명되어 있습니다.

SPARC M10 시스템은 다음 유형의 시간을 관리합니다.

- XSCF가 유지하는 시간
  XSCF가 관리하는 표준 시스템 시간. 이는 마스터 XSCF가 관리하며 모든 XSCF가 동일한 시간으로 구성됩니다. 시간은 전원 공급이 중단된 후라도 보장됩니다.
- 물리 분할이 유지하는 시간
  각 물리 분할마다 하이퍼바이저가 관리하는 시간.
- 논리 도메인이 유지하는 시간
  각 논리 도메인마다 관리되는 시간. 이는 각 논리 도메인마다 다르게 구성될 수 있습니다.

XSCF 시간과 논리 도메인 시간 간의 관계는 "8.4 XSCF 시간/날짜 설정"을 참조하십시오.

11.5 논리 도메인에서 패닉 발생

이 절에는 지정된 논리 도메인에서 패닉을 발생시키는 방법이 설명되어 있습니다.

논리 도메인에 비정상적인 부하 또는 끊김이 발생하는 경우 논리 도메인을 패닉 상태로 만들고 덤프 파일을 수집합니다.

11.5.1 게스트 도메인에서 패닉 발생

지정된 게스트 도메인에서 패닉을 발생시키려면 Oracle VM Server for SPARC ldm panic-domain 명령을 사용합니다. 제어 도메인에서 명령을 실행합니다.
ldm(1M) 명령의 자세한 내용은 사용 버전의 『Oracle VM Server for SPARC 참조 설명서』를 참조하십시오.

노트 - ldm panic-domain 명령은 지정된 게스트 도메인에서 패닉을 강제 발생시켜 디스크 또는 다른 구성요소에 고장을 일으킬 수도 있습니다. 비상 또는 유사 상황에서만 이 명령을 사용합니다.

```
primary# ldm panic-domain ldom
```

ldom에서 패닉을 발생시키는 게스트 도메인의 이름을 지정합니다.

노트 - XSCF 펌웨어 reset 명령을 사용하여 게스트 도메인에서 패닉을 발생시킬 수도 있습니다. 자세한 내용은 reset(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

11.5.2 제어 도메인에서 패닉 발생

지정된 제어 도메인에서 패닉을 발생시키려면 XSCF 펌웨어 reset 명령을 사용합니다. 이 작동은 platadm 또는 fieldeng 권한이 있는 사용자 계정으로 실행해야 합니다. 또는 대상 물리 분할의 경우 pparadm 또는 pparmgr 권한이 있는 사용자 계정을 사용하여 작동을 실행할 수 있습니다.

노트 - reset 명령은 지정된 제어 도메인에서 패닉을 강제 발생시켜 디스크 또는 다른 구성요소에 고장을 일으킬 수도 있습니다. 비상 또는 유사 상황에서만 이 명령을 사용합니다.

```
XSCF> reset -p ppar_id -g primary panic
```

Ppar_id의 경우 패닉을 발생시키는 제어 도메인이 속한 물리 분할의 ID를 지정합니다. 시스템 구성에 따라 0 ~ 15의 정수를 지정할 수 있습니다.

전원 공급이 분리되거나 제어 도메인이 종료되는 동안 reset 명령이 무시됩니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **reset** 명령을 실행하여 지정된 제어 도메인에서 패닉을 발생시킵니다.
   다음에는 물리 분할 ID 0의 제어 도메인에서 패닉을 발생시키는 예가 나타나 있습니다.

```
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>
```

3. **showdomainstatus** 명령을 실행하여 지정된 게스트 도메인에서 패닉을 발생시킵니다.

```
XSCF> showdomainstatus
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다**.**
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

12장

고 신뢰성 시스템 구성

이 장에는 고 신뢰성 시스템으로서 SPARC M10 시스템을 구성하는 방법이 설명되어 있습니다.

- 메모리 미러링 구성
- 하드웨어 RAID 구성
- SAN 부팅 사용
- iSCSI 사용
- SPARC M10 시스템과 I/O 장치의 전원 공급 연동
- 이중 전원 공급 사용
- 무정전 전원 공급 장치 사용

12.1 메모리 미러링 구성

이 절에는 SPARC M10 시스템이 지원하는 메모리 미러링의 설정 방법이 설명되어 있습니다.

12.1.1 메모리 미러링 개요

이 절에는 SPARC M10 시스템이 지원하는 메모리 미러링의 설정 방법이 설명되어 있습니다.

SPARC M10 시스템은 메모리 중복화로 데이터를 보호하도록 메모리 미러링을 지원합니다. 사용 가능한 메모리 용량이 절반으로 줄어듭니다. 하지만 데이터 신뢰성은 높아집니다.

메모리 액세스 컨트롤러는 메모리에 데이터 쓰기 및 메모리에서 데이터 읽기를 제어합니다. SPARC M10 시스템은 2개 메모리 액세스 컨트롤러가 제어하는 메모리를 그룹화하여 미러링을 구성합니다.

노트 - 미러링 그룹에 속하는 모든 메모리는 용량과 순위가 동일해야 합니다.

메모리의 물리 구성 규칙은『SPARC M10-1 Service Manual』또는『SPARC M10-4/M10-4S Service Manual』의 "8.2 메모리 구성 규칙"을 참조하십시오.

12.1.2 메모리 미러링 구성

SPARC M10 시스템에 장착된 메모리를 미러링으로서 구성하려면 XSCF 펌웨어의 setupfru 명령을 사용합니다.

노트 - 메모리를 미러링으로서 구성하려면 대상 시스템 보드(PSB)가 속하는 물리 분할(PPAR)의 전원을 차단해야 합니다.

```
XSCF> setupfru [-m {y|n}] device location
```

메모리 미러링을 구성하려면 -m y를 지정합니다.
Device는 미러링이 구성되는 장치를 지정합니다. 지정된 시스템 보드의 모든 CPU에 대해 메모리 미러링을 지정하려면 sb를 지정합니다. 지정된 CPU에 대해서만 메모리 미러링을 지정하려면 cpu를 지정합니다.

Location은 대상 장치의 위치를 지정합니다. Xx-0-z의 형식으로 위치를 지정합니다. Xx는 시스템 보드 번호를 지정하고 z는 CPU 칩 번호를 0 ~ 3으로 지정합니다.

작동 절차

1. **platadm** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4장 로그인/로그아웃"을 참조하십시오.

   위 사용자 계정 가운데 하나로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **setupfru** 명령을 실행하여 메모리 미러링을 구성합니다.
   다음 예에서는 시스템 보드 01-0에 장착된 모든 CPU가 메모리 미러 모드로 설정됨을 나타냅니다.

```
XSCF> setupfru -m y sb 01-0
```

   다음 예에서는 시스템 보드 02-0 내 CPU 칩 #1의 CPU가 메모리 미러 모드로 설정됨을 나타냅니다.

```
XSCF> setupfru -m y cpu 02-0-1
```

12.2 하드웨어 RAID 구성

이 절에는 SPARC M10 시스템이 지원하는 하드웨어 RAID 구성, 구성 방법 및 관리 방법이 설명되어 있습니다.

SPARC M10 시스템에서 하드웨어 RAID 볼륨을 생성 및 관리하는 데 다음 2개 환경을 사용할 수 있습니다.

- FCode 유틸리티
  이 유틸리티는 서버에서 대상을 표시하고 논리 볼륨을 관리하는 특수 명령 세트로 구성되어 있습니다. OpenBoot PROM 환경에서 이 명령을 사용합니다.

  FCode 유틸리티는 본 설명서의 예에 사용됩니다.

- LSI SAS2 통합 구성 유틸리티(SAS2IRCU)
  LSI SAS2IRCU(버전 14.00.00.00 이상)를 사용하여 서버에서 RAID 볼륨을 구성 및 관리할 수 있습니다.

  sas2ircu 명령 세트를 사용하려면 다음 URL에서 최신 버전의 SAS2IRCU를 다운로드하여 설치합니다.

  http://www.lsi.com/channel/support/pages/downloads.aspx?k=sas2ircu

  SAS2IRCU의 사용 방법은 다음 URL에 있는 상세 설명서를 참조하십시오.

  http://www.lsi.com/channel/support/pages/downloads.aspx?k=sas2ircu

12.2.1 하드웨어 RAID의 기본 정보

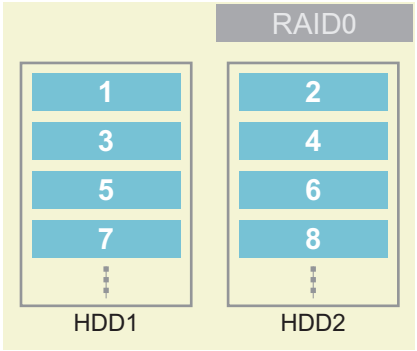
하드웨어 RAID는 데이터 액세스 속도를 가속시키고 데이터 보호의 신뢰성을 높이는 데 사용되는 기술입니다. 이는 2개 이상의 내부 디스크 드라이브를 전체적으로 관리하여 구현합니다.

SPARC M10 시스템은 온보드 SAS 컨트롤러의 통합 RAID 기능을 통해 하드웨어 RAID를 제공합니다. RAID0, RAID1 및 RAID1E의 하드웨어 RAID 기술이 지원됩니다.

- RAID0(스트립핑)
  데이터 쓰기 및 읽기가 2개 내부 디스크 드라이브로 분산되어 병렬로 수행됩니다. 이 기술은 데이터 액세스 속도를 증가시킵니다. 따라서 이는 디스크 가속을 필요로 하는 비즈니스에 사용됩니다.

  SPARC M10 시스템에서 2 ~ 8개 디스크 드라이브를 사용하여 RAID0 볼륨을 구성할 수 있습니다.

그림 12-1 RAID0의 메커니즘

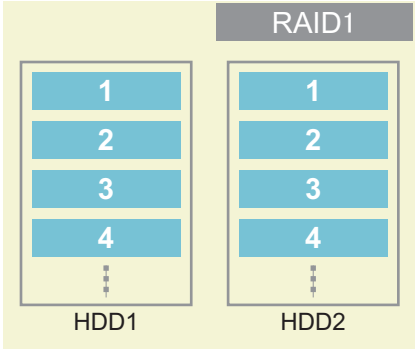


노트 - RAID0에는 데이터 허용 오차가 없습니다. 따라서 데이터 허용 오차 면에서 상위인 RAID1을 소프트웨어 RAID로 구성하여 RAID0에 사용하도록 조합하는 것이 좋습니다.

- RAID1(미러링)
  데이터 허용 오차를 증가시키도록 내부 디스크 드라이브가 중복되고 동일 데이터가 중복 구성으로 쓸 수 있습니다. 한 쪽 내부 디스크 드라이브가 고장이더라도 다른 쪽 드라이브를 사용하여 작동을 계속할 수 있습니다. 더욱이, 작동이 계속되는 동안에도 고장인 내부 디스크 드라이브를 교체할 수 있습니다. 반면, 데이터 저장을 위한 디스크 공간은 절반으로 감소합니다.

  SPARC M10 시스템에서 2개 디스크 드라이브를 사용하여 RAID1 볼륨을 구성할 수 있습니다.

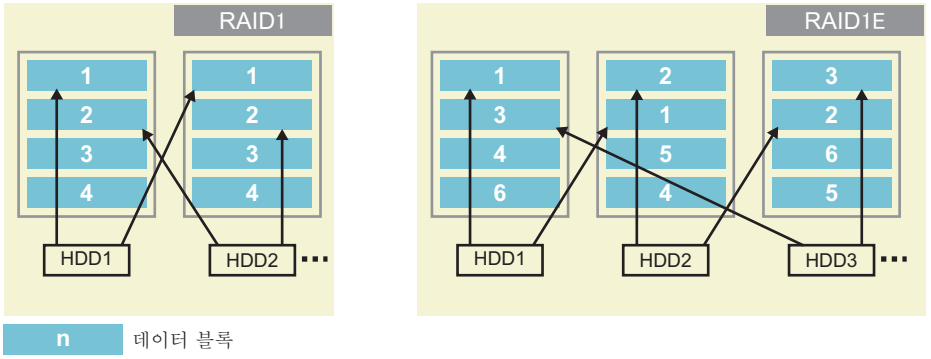
그림 12-2 RAID1의 메커니즘



- RAID1E(확장 미러링)
  데이터가 분할 및 중복됩니다. 그런 다음 여러 내부 디스크에 쓸 수 있습니다. 이 기술은 확장 유형의 RAID1이며 3개 이상의 내부 디스크 드라이브를 사용할 수 있습니다.

SPARC M10 시스템에서 3개, 5개 또는 7개 디스크 드라이브를 사용하여 RAID1E 볼륨을 구성할 수 있습니다.

그림 12-3 RAID1E의 메커니즘



SPARC M10 시스템에서 위의 RAID 유형을 조합하여 캐비닛당 최대 2개의 RAID 볼륨을 구성할 수 있습니다.

지원되는 디스크 드라이브

SPARC M10 시스템을 사용하여 하드웨어 RAID를 구성하려면 용량과 회전수가 동일한 디스크 드라이브를 사용합니다. 반도체 드라이브(SSD)는 지원되지 않습니다.

12.2.2 FCode 유틸리티 명령

하드웨어 RAID를 구성할 때 사용되는 FCode 유틸리티는 다음 명령을 제공합니다.

표 12-1 FCode 유틸리티 명령 목록

FCode 명령	설명
show-children	연결된 모든 논리 드라이브와 논리 볼륨을 나열합니다.
show-volumes	연결된 모든 논리 볼륨의 세부 사항을 나열합니다.
create-raid0-volume	RAID0 볼륨을 생성합니다. 적어도 2개 대상을 지정합니다.
create-raid1-volume	RAID1 볼륨을 생성합니다. 2개 대상을 지정합니다.
create-raid1e-volume	RAID1E 볼륨을 생성합니다. 적어도 3개 대상을 지정합니다.
delete-volume	RAID 볼륨을 삭제합니다.
activate-volume	디스크 교체 후 RAID 볼륨을 다시 활성화합니다.

12.2.3 하드웨어 RAID 작동 전 준비

FCode 유틸리티를 사용하여 하드웨어 RAID의 작동 준비를 합니다. 스크롤을 지원하는

xterm 또는 동급 터미널에서 이를 수행합니다.

작동 절차

1. 시스템 전원을 켭니다.
   전원이 이미 켜져 있으면 시스템을 재설정하고 OpenBoot PROM으로 자동 부팅을 비활성화합니다.
2. **ok** 프롬프트를 표시합니다.
3. **show-devs** 명령을 실행하여 서버에서 장치 경로를 나열합니다.

```
{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. **select** 명령을 실행하여 하드웨어 **RAID** 볼륨을 생성하는 컨트롤러를 선택합니다.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

5. **show-children** 명령을 실행하여 연결된 드라이브의 **SAS** 주소를 표시합니다.

```
{0} ok show-children

FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.57.00

Target a
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393c813ae74  SASAddress 50000393c813ae76  PhyNum 0
Target b
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81b24ec  SASAddress 50000393b81b24ee  PhyNum 1
Target c
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81af47c  SASAddress 50000393b81af47e  PhyNum 2
Target d
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81af3c0  SASAddress 50000393b81af3c2  PhyNum 3
Target e
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81b0f58  SASAddress 50000393b81b0f5a  PhyNum 4
Target f
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81b130c  SASAddress 50000393b81b130e  PhyNum 5
Target 10
```

```
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81b2420  SASAddress 50000393b81b2422  PhyNum 6
Target 11
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
  SASDeviceName 50000393b81acc84  SASAddress 50000393b81acc86  PhyNum 7
Target 12
  Unit 0   Encl Serv device   FUJITSU  NBBEXP           0d32
  SASAddress 500000e0e04d003d  PhyNum 14
{0} ok
```

12.2.4 하드웨어 RAID 볼륨 생성

하드웨어 RAID 볼륨을 생성하려면 생성하는 하드웨어 RAID 구성에 따라 다음 명령 가운데 하나를 사용합니다.

- RAID0 볼륨 생성

```
{0} ok target1 target2 create-raid0-volume
```

- RAID1 볼륨 생성

```
{0} ok target1 target2 create-raid1-volume
```

- RAID1E 볼륨 생성

```
{0} ok target1 target2 target3 create-raid1e-volume
```

이 명령 모두에 대해 다음 설정을 구성합니다.
대상 번호를 targetx로 지정합니다. show-children 명령으로 대상 번호를 확인할 수 있습니다.
이 명령은 대화형이며 실행 동안 볼륨 용량을 MB로, 볼륨 이름을 15자 이하로 지정합니다.

작동 절차

1. 하드웨어 **RAID** 볼륨의 생성 준비를 합니다.
   자세한 내용은 "12.2.3 하드웨어 RAID 작동 전 준비"를 참조하십시오.
2. 대상을 결정하여 **show-children** 명령의 실행 결과로부터 하드웨어 **RAID** 볼륨을 생성합니다.
3. **Create-raid0-volume, create-raid1-volume** 또는 **create-raid1e-volume**을 실행하여 물리 디스크로 하드웨어 **RAID** 볼륨을 생성합니다.
   다음 예에서는 a 및 b의 대상으로 RAID0 볼륨을 생성합니다.
   또한 1MB의 볼륨 용량과 볼륨 이름 raid0-volume이 실행 동안 지정됩니다.

```
{0} ok a b create-raid0-volume
Target a size is 583983104 Blocks, 298 GB
Target b size is 583983104 Blocks, 298 GB
The volume can be any size from 1 MB to 570296 MB
What size do you want?  [570296] 1
Volume size will be 2048 Blocks, 1048 KB
Enter a volume name:  [0 to 15 characters] raid0-volume
Volume has been created
{0} ok
```

다음 예에서는 a 및 b의 대상으로 RAID1 볼륨을 생성합니다.
또한 1MB의 볼륨 용량과 볼륨 이름 raid1-volume이 실행 동안 지정됩니다.

```
{0} ok a b create-raid1-volume
Target a size is 583983104 Blocks, 298 GB
Target b size is 583983104 Blocks, 298 GB
The volume can be any size from 1 MB to 285148 MB
What size do you want?  [285148] 1
Volume size will be 2048 Blocks, 1048 KB
Enter a volume name:  [0 to 15 characters] raid1-volume
Volume has been created
{0} ok
```

다음 예에서는 X, Y 및 Z의 대상으로 RAID1E 볼륨을 생성합니다.
또한 1MB의 볼륨 용량과 볼륨 이름 raid1e-volume이 실행 동안 지정됩니다.

```
{0} ok X Y Z create-raid1e-volume
Target a size is 583983104 Blocks, 298 GB
Target b size is 583983104 Blocks, 298 GB
Target c size is 583983104 Blocks, 298 GB
The volume can be any size from 1 MB to 427722 MB
What size do you want?  [427722] 1
Volume size will be 2048 Blocks, 1048 KB
Enter a volume name:  [0 to 15 characters] raid1e-volume
Volume has been created
{0} ok
```

4. **show-volumes** 명령을 실행하여 생성된 **RAID** 볼륨을 확인합니다.
   다음 예에서는 RAID 1 볼륨의 세부 사항을 확인합니다.

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                          2048 Blocks,
 1048 KB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2300RC        3706
  Disk 1
```

```
    Secondary  Optimal
    Target b      TOSHIBA  MBF2300RC        3706
{0} ok
```

5. **unselect-dev** 명령을 실행하여 컨트롤러를 선택 취소합니다.

```
{0} ok unselect-dev
{0} ok
```

12.2.5 하드웨어 RAID 볼륨 삭제

생성된 하드웨어 RAID 볼륨을 삭제하려면 FCode 유틸리티 delete-volume 명령을 사용합니다.

```
{0} ok volume_number delete-volume
```

volume_number는 show-volumes 명령에 의해 출력되는 볼륨 번호를 지정합니다. 명령이 실행되면 RAID 볼륨을 삭제할 것인지 묻는 확인 메시지가 나타납니다. "es" 또는 "no" 가운데 해당되는 것을 선택합니다.

작동 절차

1. **show-volumes** 명령을 실행하여 삭제할 **RAID** 볼륨을 확인합니다.
   다음 예에는 RAID1 볼륨이 볼륨 번호 0으로 생성되었음이 나타나 있습니다.

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                        2048 Blocks,
 1048 KB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2300RC        3706
  Disk 1
    Secondary  Optimal
    Target b      TOSHIBA  MBF2300RC        3706
{0} ok
```

2. **delete-volume** 명령을 실행하여 **RAID** 볼륨을 삭제합니다.
   다음 예에서는 볼륨 번호가 0인 RAID 볼륨을 삭제합니다.

```
{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
```

3. **show-volumes** 명령을 실행하여 **RAID** 볼륨이 삭제되었는지 확인합니다.

```
{0} ok show-volumes
No volumes to show
{0} ok
```

12.2.6 디스크 드라이브 상태 확인

이 절에는 하드웨어 RAID 볼륨을 구성하는 내부 디스크 드라이브의 상태 확인 방법이 설명되어 있습니다.

Fcode 유틸리티를 사용한 상태 표시

디스크 드라이브의 고장 여부를 확인하려면 시스템을 정지하고 FCode 유틸리티 show-volumes 명령을 사용합니다.

1. **ok** 프롬프트를 표시합니다.
2. **select** 명령을 실행하여 하드웨어 **RAID** 볼륨을 표시하는 컨트롤러를 선택합니다.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

3. **show-volumes** 명령을 실행하여 **RAID** 볼륨을 확인합니다.

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Degraded  Enabled
  2 Members                                          2048 Blocks,
 1048 KB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2300RC        3706
  Disk 1
    Secondary  Offline  Out Of Sync
    Target b      TOSHIBA  MBF2300RC        3706
{0} ok
```

4. **unselect-dev** 명령을 사용하여 컨트롤러를 선택 취소합니다.

```
{0} ok unselect-dev
{0} ok
```

LSI SAS2IRCU 유틸리티를 사용한 상태 표시

LSI SAS2IRCU 유틸리티를 사용하여 디스크 드라이브의 고장 여부를 확인할 수도 있습니다.

SAS2IRCU 유틸리티의 자세한 내용은 "12.2 하드웨어 RAID 구성"의 처음을 참조하십시오.

12.2.7 고장인 디스크 드라이브 확인

이 절에는 하드웨어 RAID 볼륨을 구성하는 내부 디스크 드라이브의 고장 확인 방법이 설명되어 있습니다.

디스크 드라이브 LED 확인

시스템의 디스크 드라이브에서 고장이 발생하면 드라이브 전면의 CHECK LED(황갈색)가 켜집니다. 이 CHECK LED로 시스템에서 고장이 발생한 디스크 드라이브를 식별할 수 있습니다. 이 LED의 위치와 자세한 설명은『SPARC M10-1 Service Manual』또는『SPARC M10-4/M10-4S Service Manual』의 "2장 시스템 구성요소 이해"를 참조하십시오.

오류 메시지 확인

디스크 드라이브에서 고장이 발생하면 콘솔 화면에 오류 메시지가 표시됩니다. 또한 /var/adm/messages 파일을 열어 메시지를 확인할 수도 있습니다.

Fcode 유틸리티를 사용한 상태 표시

디스크 드라이브의 고장 여부를 확인하려면 시스템을 정지하고 FCode 유틸리티 show-volumes 명령을 사용합니다.

자세한 내용은 "12.2.6 디스크 드라이브 상태 확인"를 참조하십시오.

LSI SAS2IRCU 유틸리티를 사용한 상태 표시

LSI SAS2IRCU 유틸리티를 사용하여 디스크 드라이브의 고장 여부를 확인할 수도 있습니다.
SAS2IRCU 유틸리티의 자세한 내용은 "12.2 하드웨어 RAID 구성"의 처음을 참조하십시오.

12.2.8 하드웨어 RAID 볼륨 재활성화

이 절에는 SPARC M10-4/M10-4S PCI 백플레인 또는 SPARC M10-1 마더보드 장치를 교체한 후 하드웨어 RAID 볼륨을 재활성화하는 방법이 설명되어 있습니다.
이는 하드웨어 RAID 볼륨을 부팅 장치로서 구성할 때 필요합니다.

작동 절차

1. **probe-scsi-all** 명령을 실행하여 **RAID** 볼륨이 목록에 없는지 확인합니다.

```
{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 13.00.57.00
```

```
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
```

2. 볼륨 정보를 표시하는 장치를 선택하고 활성화되지 않았는지 확인합니다.

```
{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                                        2048 Blocks, 1048 KB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2300RC        3706
  Disk 1
    Secondary  Optimal
    Target b      TOSHIBA  MBF2300RC        3706
{0} ok
```

3. **activate-volume** 명령을 실행하여 **RAID** 볼륨을 활성화합니다.

```
{0} ok 0 activate-volume
Volume 0 is now activated
{0} ok
```

4. **show-volumes** 명령을 실행하여 **RAID** 볼륨이 활성화되었는지 확인합니다.

```
{0} ok show-volumes
Volume 0 Target 11e  Type RAID1 (Mirroring)
  Name raid1-volume  WWID 0c233a838262c6c5
  Optimal  Enabled  Data Scrub In Progress
  2 Members                                          2048 Blocks, 1048 KB
  Disk 0
    Primary  Optimal
    Target a      TOSHIBA  MBF2300RC        3706
  Disk 1
    Secondary  Optimal
    Target b      TOSHIBA  MBF2300RC        3706
{0} ok
```

5. **unselect-dev** 명령을 실행하여 컨트롤러를 선택 취소합니다.

```
{0} ok unselect-dev
{0} ok
```

12.2.9 디스크 슬롯 번호

디스크의 활성 교체를 수행하려면 장착 또는 제거되는 드라이브의 물리 또는 논리 장치 이름을 알아야 합니다. 시스템에서 디스크 오류가 발생하는 경우 대개 시스템 콘솔을 사용하여 다음과 관련된 메시지를 확인할 수 있습니다. 고장 발생 가능성이 높은 디스크 또는 고장인 디스크. 이 정보는 /var/adm/messages 파일에 기록되기도 합니다.

이 오류 메시지는 대개 고장인 내부 디스크 드라이브와 그 물리 또는 논리 장치 이름을 표시합니다. 더욱이, 일부 응용 프로그램을 위해 디스크 슬롯 번호가 보고될 수도 있습니다.

장치 경로는 모델 또는 시스템 구성에 따라 달라집니다.

다음 표에는 SPARC M10 시스템의 장치 경로 예가 제공되어 있습니다. 이 표는 각 내부 디스크 드라이브의 논리 장치 이름 또는 물리 장치 이름과 내부 디스크 슬롯 번호를 대응시키는 데 사용할 수 있습니다.

표 12-2 디스크 슬롯 번호(SPARC M10-1/M10-4/M10-4S, 단일 장치 구성)

디스크 슬롯 번호	물리 장치 이름
슬롯 0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0
슬롯 1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1
슬롯 2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2
슬롯 3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3
슬롯 4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4
슬롯 5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5
슬롯 6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6

표 12-2 디스크 슬롯 번호(SPARC M10-1/M10-4/M10-4S, 단일 장치 구성) (계속)

디스크 슬롯 번호	물리 장치 이름
슬롯 7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7

표 12-3 디스크 슬롯 번호(SPARC M10-4S, 빌딩 블록 구성)

LSB 번호	디스크 슬롯 번호	물리 장치 이름
LSB#0	슬롯 0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0
	슬롯 1	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1
	슬롯 2	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2
	슬롯 3	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3
	슬롯 4	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4
	슬롯 5	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5
	슬롯 6	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6
	슬롯 7	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7
LSB#1	슬롯 0	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7
	슬롯 1	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p1
	슬롯 2	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p2
	슬롯 3	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p3
	슬롯 4	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p4
	슬롯 5	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p5
	슬롯 6	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p6
	슬롯 7	/pci@8800/pci@4/pci@0/pci@0/scsi@0/disk@p7
:		
LSB#15	슬롯 0	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p0
	슬롯 1	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p1
	슬롯 2	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p2
	슬롯 3	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p3
	슬롯 4	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p4
	슬롯 5	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p5
	슬롯 6	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p6
	슬롯 7	/pci@f800/pci@4/pci@0/pci@0/scsi@0/disk@p7

12.3 SAN 부팅 사용

SPARC M10 시스템은 SAN 부팅을 지원합니다.

SAN 부팅은 시작 디스크로서 서버의 내부 디스크 드라이브를 사용하지 않고 시작 디스크로서 외부 저장소가 구성되는 시스템입니다.

SPARC M10 시스템은 외부 저장 장치 간을 연결하는 데 파이버 채널 카드를 사용하고 OpenBoot PROM Fcode 기능의 SAN 부팅을 사용하는 시스템을 구성합니다.

SAN 부팅의 시스템 구성과 관련된 자세한 내용은 다음 Oracle 설명서를 참조하십시오.

- Oracle Solaris 관리:SAN 구성 및 다중 경로 제어
- Oracle Solaris 관리:SAN 구성 및 다중 경로 제어

12.4 iSCSI 사용

iSCSI는 IP 네트워크를 통해 SCSI 명령을 교환하는 데 사용되는 프로토콜입니다. 이 명령은 서버와 외부 저장소 간의 통신에 사용됩니다.

SPARC M10 시스템은 iSCSI를 사용하는 시스템을 구성할 수 있습니다. iSCSI를 사용하는 시스템이 구성되면 대용량 저장소를 TCP/IP 네트워크에 연결하고 여러 서버가 이를 공유하도록 할 수 있습니다.

12.5 SPARC M10 시스템과 I/O 장치의 전원 공급 연동

이 절에는 SPARC M10 시스템의 전원 공급 연동 기능과 그 설정에 대한 개요가 설명되어 있습니다.

12.5.1 SPARC M10 시스템 전원 공급 연동 기능의 기본 정보

전원 공급 연동 기능(Remote Cabinet Interface over LAN: RCIL)은 SPARC M10 시스템 간 또는 I/O 장치 간 전원 공급 연동을 제어하는 데 사용되는 인터페이스입니다. LAN 상의 IPMI에 기반한 독립 인터페이스가 사용됩니다. 일반 IPMI의 다음 기능이 지원되는 경우 제어되는 운영 체제와 하드웨어의 차이를 고려하지 않아도 됩니다. 이를 전원 공급 연동의 대상으로서 삽입할 수 있습니다.

- 전원 공급 및 전원 차단: 섀시 제어

- 전원 상태 가져오기: 섀시 상태 가져오기

표 12-4에는 SPARC M10 시스템 전원 공급 연동 기능의 용어와 그 정의가 나열되어 있습니다.

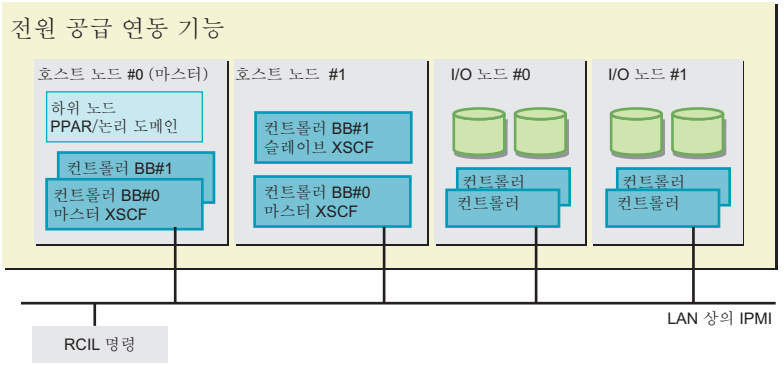
표 12-4 전원 공급 연동에 사용되는 용어 및 정의

용어	정의
호스트 노드	SPARC M10 시스템의 전원 공급 연동 기능을 지원하는 데 사용되는 SPARC M10 시스템과 같은 장치 전원 공급 연동 그룹을 설정할 때 마스터로서 설정되는 호스트 노드를 마스트 호스트 노드라고 합니다.
하위 노드	SPARC M10 시스템 캐비닛의 물리 분할
I/O 노드	SPARC M10 시스템의 전원 공급 연동 기능을 지원하는 I/O 장치 및 원격 배전 장치
전원 공급 연동 기능	호스트 노드, 하위 노드 및 I/O 노드와 같은 전원 공급 연동 대상의 그룹화로 얻는 그룹 고유 그룹 ID가 전원 공급 연동 그룹에 할당됩니다.

전원 공급 연동 기능을 사용하려면 연동되는 노드를 조합하여 전원 공급 연동 그룹을 생성합니다. 생성된 각 전원 공급 연동 그룹마다 전원 공급 연동을 제어할 수 있습니다.

노트 - 호스트 노드, 하위 노드 및 I/O 노드는 단일 전원 공급 연동 그룹에서만 설정할 수 있습니다.

그림 12-4 SPARC M10 시스템 전원 공급 연동 그룹의 이미지



12.5.2 전원 공급 연동의 연결 모드 이해

SPARC M10 시스템의 전원 공급 연동 기능을 지원하는 호스트 노드, 하위 노드 및 I/O 노드는 LAN을 통해 서로 연결됩니다.

다음에는 연결 사양이 설명되어 있습니다.

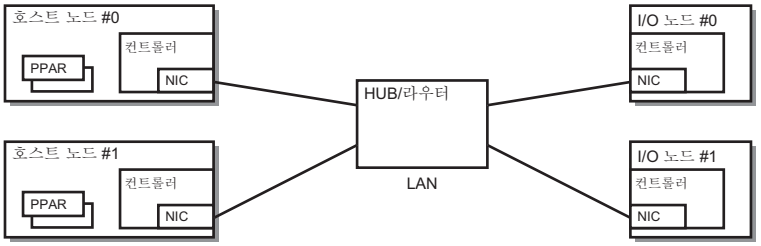
표 12-5 전원 제어 연결 사양

항목	설명
연결 모드	LAN 연결
전송 속도	100Mbps 이상
인터넷 프로토콜	IPv6(IPMI가 IPv6을 지원한 이후)
DHCP	지원되지 않음 SPARC M10 시스템의 전원 공급 연동 기능을 사용하려면 연결 대상의 고정 IP 주소를 설정해야 합니다.
연결 프로토콜	LAN 상의 IPMI (Intelligent Platform Management Interface)

표준 전원 공급 연동 연결

SPARC M10 시스템의 전원 공급 연동 기능과 연결된 컨트롤러가 장착되어 있는 호스트 노드, 하위 노드 및 I/O 노드는 동일한 LAN을 통해 서로 연결됩니다.

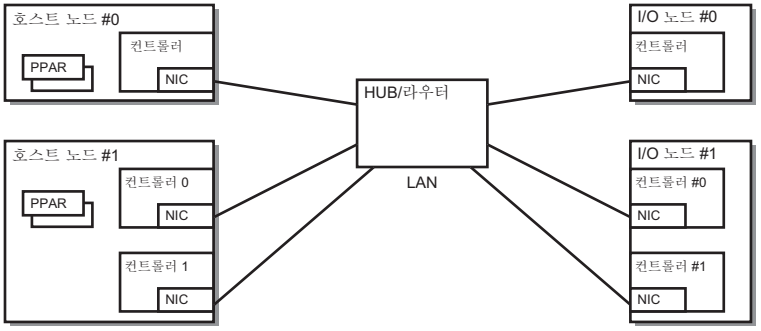
그림 12-5 전원 공급 연동 연결 모드



컨트롤러 중복 시의 연결

호스트 노드의 컨트롤러가 중복되면 각 컨트롤러를 동일한 LAN에 연결할 수 있습니다. 전원 공급 연동은 마스터 XSCF에서 작동합니다.

그림 12-6 컨트롤러가 중복된 전원 공급 연동 연결 모드



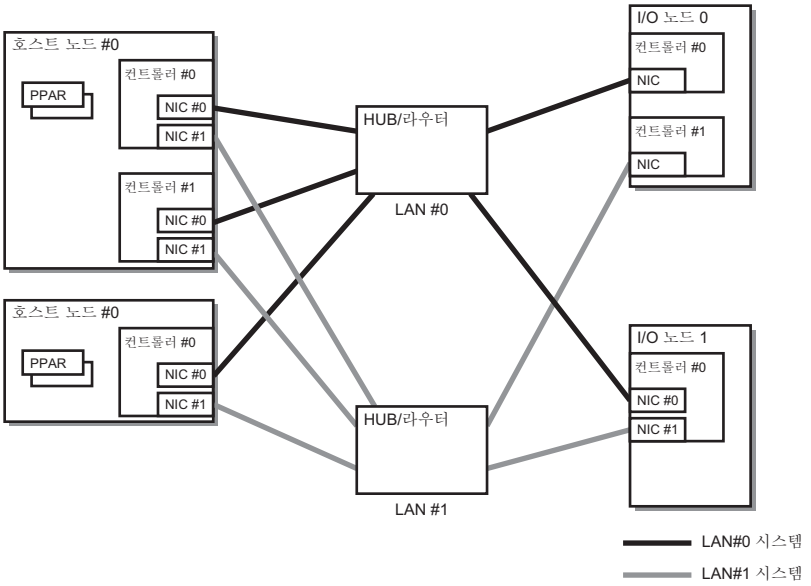
노트 - 컨트롤러가 중복되더라도 LAN 카드의 IP 주소가 가상 IP로서 컨트롤러 간에 공유되면 컨트롤러 가운데 하나가 연결됩니다.

경로 중복 시의 연결

다음 조건이 충족되면 전원 공급 연동 연결 경로가 중복될 수 있습니다.

- 2개 LAN 카드를 모든 노드의 컨트롤러에 장착할 수 있습니다.
- 2개 LAN 카드를 호스트 노드의 컨트롤러에 장착할 수 있으며 I/O 노드는 다음 구성 가운데 하나를 갖습니다.
- I/O 노드의 컨트롤러가 중복됩니다.
- 2개 LAN 카드를 I/O 노드의 컨트롤러에 장착할 수 있습니다.

그림 12-7 경로 중복 시의 전원 공급 연동 연결 모드



12.5.3 전원 공급 연동의 메커니즘

SPARC M10 시스템의 전원 공급 연동은 각 전원 공급 연동 그룹마다 제어됩니다.

그룹의 호스트 노드 가운데 전원 공급 연동 기능이 활성화되는 호스트 노드에 전원 공급 연동이 적용됩니다. 전원 공급 연동 그룹의 전원 상태는 그룹 내 호스트 노드 상태에 따라 결정됩니다.

- 온 상태
  전원 공급 연동 그룹의 호스트 노드 가운데 하나에 전원이 공급됩니다.
- 오프 상태
  전원 공급 연동 그룹의 모든 호스트 노드로 공급되는 전원이 차단됩니다.

이 절에는 설정이 다음과 같다는 가정 하에 전원 공급 및 전원 차단 시의 연동 메커니즘이 설명되어 있습니다.

표 12-6 전원 공급 연동의 메커니즘(예)

설정 항목	호스트 노드 #0	호스트 노드 #1	호스트 노드 #2	I/O 노드 #0	I/O 노드 #1
연동 설정	비활성화	활성화	활성화	설정 비활성화	설정 비활성화
마스터 노드	예	아니오	예	설정 비활성화	설정 비활성화

전원 공급 시의 연동 메커니즘

전원 공급 연동 그룹의 호스트 노드 가운데 하나라도 전원이 공급되고 이 그룹의 모든 호스트 노드, 하위 노드 및 I/O 노드에 전원이 공급됩니다. 전원은 호스트 노드 및 I/O 노드의 순서에 따라 공급됩니다.

노트 - 호스트 노드의 경우 I/O 노드 장치의 액세스가 가능해질 때까지 대기 시간을 설정할 수 있습니다. 시간을 설정하려면 XSCF 펌웨어 setpowerupdelay 명령을 사용합니다. 자세한 내용은 "9.2.2 시작 대기 시간 설정/확인"을 참조하십시오.

전원 차단 시의 연동 메커니즘

전원 공급 연동 그룹의 모든 호스트 노드로 공급되는 전원이 차단되면 그룹의 모든 I/O 노드로 공급되는 전원이 차단됩니다.

Wake-On-LAN을 통한 전원 공급 연동

SPARC M10 시스템의 전원 공급 연동 기능은 I/O 노드의 Wake-On-LAN 기능을 사용하여 시스템을 시작하는 기능을 지원합니다. Wake-On-LAN은 다음 조건을 충족하는 노드에 대해 설정할 수 있습니다. 일반적으로 전원 공급 연동 기능은 SPARC M10 시스템의 전원 공급 연동 기능을 지원하는 컨트롤러가 있는 호스트와 I/O 장치를 대상으로 합니다. 하지만 이 기능은 컨트롤러가 없는 장치에 대해 Wake-On-LAN을 설정하여 전원 공급을 연동할 수 있습니다.

- 전원 공급과 상태 획득이 Wake-On-LAN에서 가능합니다.
- 전원이 공급되면 IPMI 통신이 LAN을 통해 활성화됩니다.
- 전원 차단이 IPMI에서 가능합니다.

Wake-On-LAN은 호스트 노드와 I/O 노드 둘 모두에 대해 설정할 수 있습니다. Wake-On-LAN 설정 방법은 각 노드에 따라 달라집니다. 각 노드의 설명서를 참조하십시오.

노트 - Wake-On-LAN이 설정된 호스트 노드는 마스터 노드가 될 수 없습니다.

오류 복구 시의 연동

전원 공급 연동 그룹의 노드가 통신에 실패했다가 오류가 복구되면 다음 작동이 일어납니다.

- I/O 노드의 실패 시

전원 공급 연동 그룹으로 전원이 공급되면 마스터 호스트 노드는 전원 공급 명령을 내립니다.

- 호스트 노드의 실패 시
  전원 공급 연동 그룹으로 전원이 공급되더라도 마스터 호스트 노드는 전원 공급 명령을 내리지 않습니다.

12.5.4 전원 공급 연동의 설정 흐름

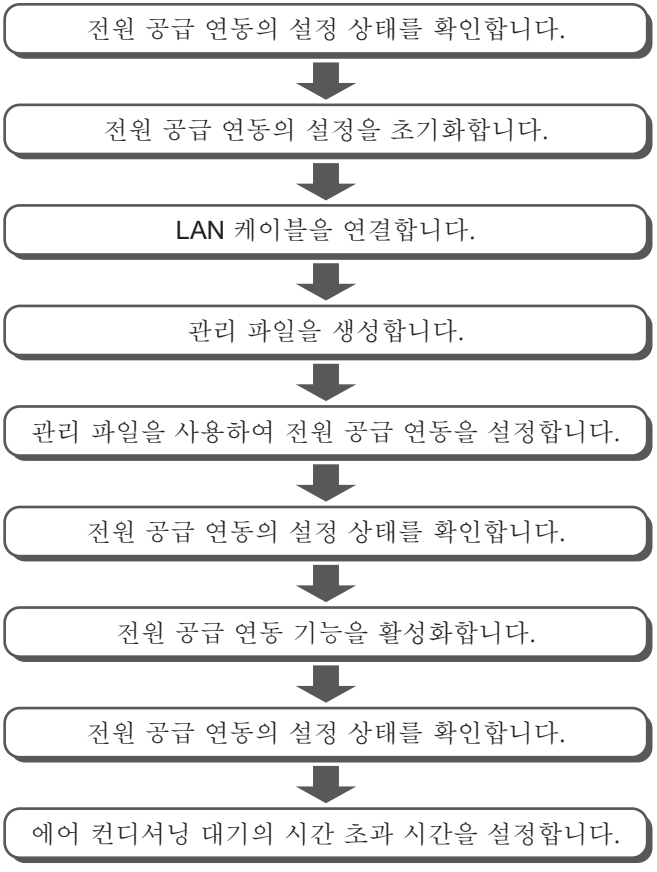
이 절에는 전원 공급 연동의 설정 방법이 다음 경우로 나뉘어 설명되어 있습니다.

- 전원 공급 연동 기능의 최초 설정
- 기존 전원 공급 연동 그룹에 노드 추가 또는 이 그룹에서 노드 삭제
- 또 다른 전원 공급 연동 그룹의 추가

전원 공급 연동 기능의 최초 설정

다음에는 전원 공급 연동의 최초 설정 흐름이 나타나 있습니다.

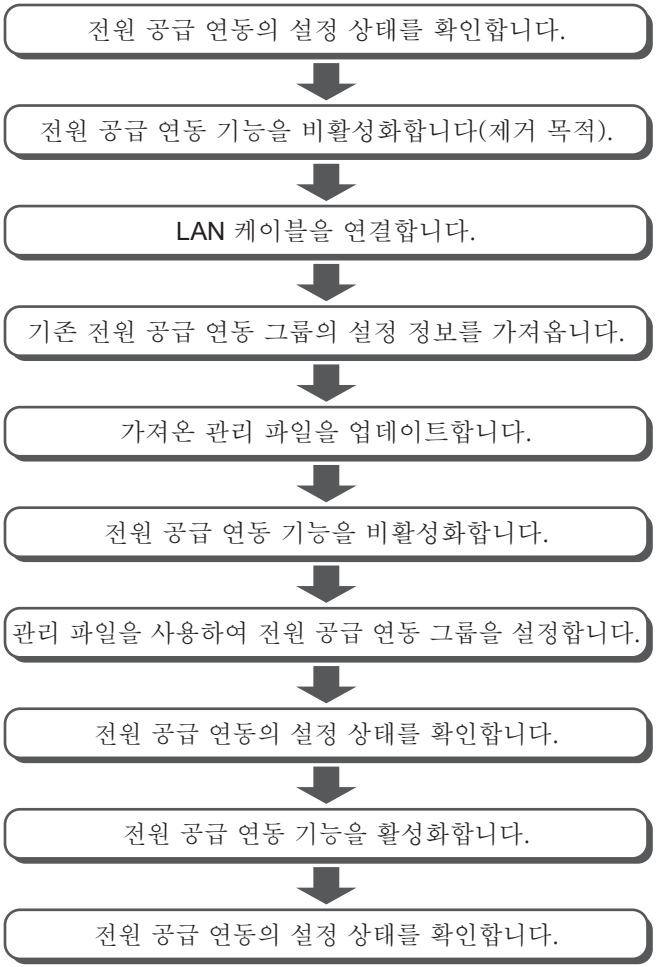
그림 12-8 전원 공급 연동의 최초 설정 흐름



기존 전원 공급 연동 그룹에 노드 추가 또는 이 그룹에서 노드 제거

다음에는 기존 전원 공급 연동 그룹에 노드를 추가하거나 이 그룹에서 노드를 삭제하는 흐름이 나타나 있습니다.

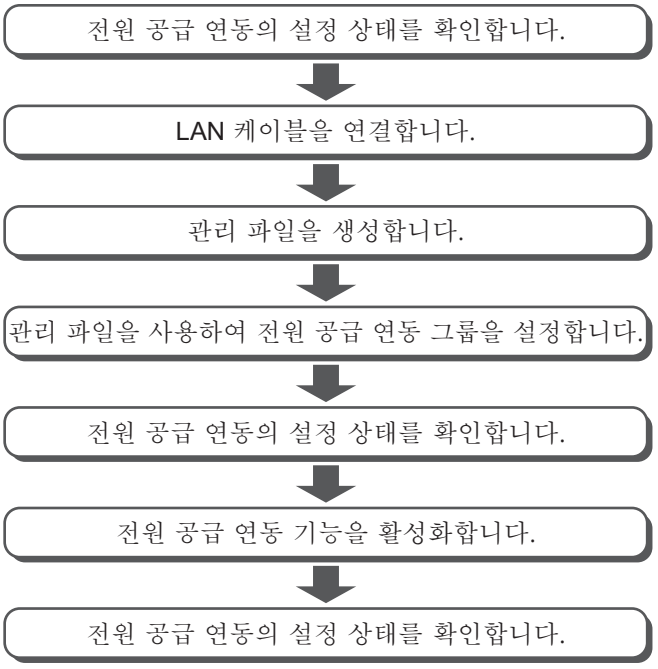
그림 12-9 기존 전원 공급 연동 그룹에 노드를 추가하거나 이 그룹에서 노드를 제거하는 흐름



또 다른 전원 공급 연동 그룹의 추가

다음에는 또 다른 전원 공급 연동 그룹의 추가 흐름이 나타나 있습니다.

그림 12-10 또 다른 전원 공급 연동 그룹의 추가 흐름



12.5.5 전원 공급 연동의 설정 상태 확인

전원 공급 연동의 설정 상태를 확인하려면 XSCF 펌웨어 showremotepwrmgmt 명령을 사용합니다.

```
XSCF> showremotepwrmgmt [-a|-G groupid [-N gnodeid]]
```

모든 전원 공급 연동 설정 상태를 확인하려면 "-a"를 지정합니다. 전원 공급 연동 그룹을 지정하려면 "-G groupid"를 지정합니다. 전원 공급 연동 그룹의 노드를 지정하려면 "-N gnodeid"를 지정합니다.

12.5.6 전원 공급 연동 설정 초기화

전원 공급 연동 설정 상태를 초기화하려면 XSCF 펌웨어 clearremotepwrmgmt 명령을 사용합니다.

```
XSCF> clearremotepwrmgmt
```

12.5.7 전원 공급 연동 기능 활성화/비활성화

전원 공급 연동 기능을 활성화/비활성화하려면 XSCF 펌웨어 setremotepwrmgmt 명령을 사용합니다.

```
XSCF> setremotepwrmgmt -c enable|disable
```

전원 공급 연동 기능을 활성화하려면 -c enable을 지정합니다. 비활성화하려면 -c disable을 지정합니다.

12.5.8 관리 파일 생성

전원 공급 연동 그룹의 설정용 관리 파일은 csv 파일 형식으로 생성됩니다. 관리 파일은 http, https, ftp 또는 파일로 액세스할 수 있는 URL 위치에서 생성할 수 있습니다.
관리 파일의 스크립팅 형식은 다음과 같습니다.

```
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,,,,,,,,, (Omission)
1,128,0x20,8a041209b35947899e7bfa5d578dbd42,0x03,0x00,default,,1
0.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,
```

다음 순서에 따라 각 라인마다 다음을 지정합니다. 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, 및 SubNode.

다음에는 설정 항목이 자세히 설명되어 있습니다.

표 12-7 전원 공급 연동 관리 파일의 설정 항목

항목	설명
GroupID	전원 공급 연동 그룹의 ID 이 값을 1 ~ 32의 정수(10진수)로서 지정합니다. 단일 관리 파일의 모든 그룹 ID는 동일해야 합니다.
NodeID	전원 공급 연동 장치의 노드 ID 이 값을 1 ~ 128의 정수(10진수)로서 지정합니다. 단일 관리 파일의 노드 ID는 고유해야 합니다.
NodeType	전원 공급 연동 장치의 노드 유형 다음 값 가운데 하나를 지정합니다. 0x00: 호스트 노드, 0x01: 마스터 호스트 노드, 0x10: I/O 노드, 0x20: 전원 공급 연동 박스

표 12-7 전원 공급 연동 관리 파일의 설정 항목 (계속)

항목	설명
NodeIdentName	전원 공급 연동 장치의 식별자 이 값을 시스템 GUID 또는 고유 문자열로서 지정합니다. 예에 나타난 바와 같이 시스템 GUID를 연속 32자리 문자열로서 지정합니다. 값은 16진수로서 처리됩니다. 대소문자를 구분하지 않습니다. 최대 32자리 16진수의 문자열을 지정합니다.
Linkage	전원 공급 연동을 나타내는 값(16진수) 다음 값 가운데 하나를 지정합니다. 0x00: 비활성화, 0x01: 활성화(온), 0x02: 활성화(오프), 0x03: 활성화(온+오프)
Operation	전원 공급 방법을 나타내는 값 다음 값 가운데 하나를 지정합니다. 0x00: IPMI, 0x01: WakeOnLAN
User	IPMI 사용자 이름 아무 것도 지정하지 않고 필드를 공백으로 둡니다. 공백이 아니면 작동을 보장할 수 없습니다.
Password	IPMI 암호 아무 것도 지정하지 않고 필드를 공백으로 둡니다.
IPAddress	컨트롤러 IPMI 포트의 IP 주소 IPv4 주소 값을 문자열로서 지정합니다.
SlaveAddress	컨트롤러의 IPMI 슬레이브 주소를 나타내는 값(16진수) 값에 접두사 "0x"를 붙입니다.
MAC Address	컨트롤러의 MAC 주소
SubNodeID	제어되는 하위 노드의 ID를 나타내는 문자열 이 값을 0 ~ 31로서 지정하거나 필드를 공백으로 둡니다. 대상 하위 노드 ID(10진수)를 쉼표(,)로 구분하고 값 전체에 큰 따옴표(")를 붙입니다. 공백 필드는 노드 전체에 대한 제어를 나타냅니다.

12.5.9 전원 공급 연동 그룹의 설정 정보 가져오기

전원 공급 연동 그룹의 설정 정보를 가져오려면 XSCF 펌웨어 getremotepwrmgmt 명령을 사용합니다.

```
XSCF> getremotepwrmgmt -G groupid configuration_file
```

-G groupid로 설정 정보를 가져오기 위한 전원 공급 연동 그룹의 ID를 지정합니다.
Configuration_file로 가져온 설정 정보가 저장되는 관리 파일의 이름을 지정합니다.

12.5.10 전원 공급 연동 그룹 설정

관리 파일을 사용하여 전원 공급 연동 그룹을 설정하려면 setremotepwrmgmt 명령을

사용합니다.

```
XSCF> getremotepwrmgmt -c config configuration_file
```

전원 공급 연동 그룹을 설정하려면 -c config를 지정합니다. Configuration_file로 설정에 사용되는 관리 파일을 지정합니다.

12.6 이중 전원 공급 사용

SPARC M10 시스템은 옵션으로서 이중 전원 공급을 지원합니다.

이중 전원 공급은 서버 전원이 서로 다른 2개 전원 공급 시스템으로부터 공급된다는 의미입니다. 전기 설비가 다른 시스템으로부터 전원을 공급할 수 있는 경우 서로 다른 2개 전원 공급 시스템으로부터 SPARC M10 시스템에 전원이 공급될 수 있습니다. 1개 전원 공급 시스템이 고장이거나 정전이 발생하는 경우 다른 전원 공급 시스템이 전원을 공급합니다. 따라서 SPARC M10 시스템은 작동을 계속할 수 있어 시스템 신뢰성이 높아집니다.

이중 전원 공급 연결의 방법과 관련된 자세한 내용은『SPARC M10 시스템 설치 안내서』의 "2.6.2 이중 전원 공급"을 참조하십시오.

더욱이, 연결 후의 설정 방법과 관련된 자세한 내용은 "9.3 이중 전원 공급 활성화/비활성화"를 참조하십시오.

12.7 무정전 전원 공급 장치 사용

SPARC M10 시스템은 옵션으로서 무정전 전원 공급 장치(UPS)의 연결을 지원합니다.

무정전 전원 공급 장치(UPS)를 사용하면 전원 오류 또는 광범위한 정전이 발생하더라도 시스템에 안정적으로 전원을 공급할 수 있습니다. APC 제조의 무정전 전원 공급 장치(UPS)가 지원되고 LAN이 도메인과 UPS 간의 인터페이스로서 사용됩니다.

무정전 전원 공급 장치의 연결 방법과 관련된 자세한 내용은 『SPARC M10 시스템 설치 안내서』의 "2.6.4 무정전 전원 공급 장치(UPS) 연결(옵션)"을 참조하십시오.

13장

시스템 구성 확장

이 장에는 시스템의 가상 CPU, 메모리와 같은 하드웨어 자원 및 I/O 장치의 구성을 변경하는 방법이 설명되어 있습니다.

- 가상 CPU의 구성 변경
- 메모리 구성 변경
- PCI 확장 장치 사용
- SPARC M10-4S 확장

13.1 가상 CPU의 구성 변경

이 절에는 Oracle VM Server for SPARC의 DR 기능을 사용한 가상 CPU의 구성 변경 방법이 설명되어 있습니다.

SPARC M10 시스템의 경우 다양한 비즈니스 프로세스가 논리 도메인 단위로 실행됩니다. 가상 CPU의 구성은 시스템 작동 상태에 따라 유연하게 변경할 수 있습니다.

노트 - 논리 도메인 자원을 동적으로 변경하려면 논리 도메인 동적 재구성(drd) 데몬이 대상 도메인에서 실행되어야 합니다.

SPARC M10 시스템의 경우 다양한 비즈니스 프로세스가 논리 도메인 단위로 실행됩니다. 일부 활성 프로세스에서 부하가 특정 논리 도메인에 집중되어 구성된 가상 CPU만을 사용할 때 성능 저하를 고려할 수 있습니다. 이러한 상황에서 동일한 물리 분할의 논리 도메인을 통해 시스템이 작동을 계속할 수 있습니다. 이는 비교적 부하가 적은 도메인의 가상 CPU를 동적으로 할당하여 수행합니다.

각 스레드마다 가상 CPU의 구성을 변경할 수 있습니다.

가상 CPU의 구성을 변경하려면 Oracle VM Server for SPARC의 ldm remove-vcpu 및 ldm add-vcpu 명령을 사용합니다. 이 명령은 root 권한으로 실행할 수 있습니다.

가상 CPU 삭제

```
primary# ldm remove-vcpu number ldom
```

Number에 삭제할 가상 CPU의 수를 지정합니다. 이는 스레드로 지정할 수 있습니다. ldom에 가상 CPU가 삭제되는 논리 도메인을 지정합니다.

가상 CPU 추가

```
primary# ldm add-vcpu number ldom
```

Number에 추가할 가상 CPU의 수를 지정합니다. 이는 스레드로 지정할 수 있습니다. ldom에 가상 CPU가 추가되는 논리 도메인을 지정합니다.

작동 절차

1. **XSCF** 콘솔을 대상 논리 도메인이 속한 제어 도메인 콘솔로 전환합니다.
   제어 도메인 콘솔로의 전환 방법과 관련된 자세한 내용은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

2. **ldm list-domain** 명령으로 각 도메인의 가상 **CPU** 수를 확인합니다.
   다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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. **ldm remove-vcpu** 명령으로 도메인의 가상 **CPU**를 삭제합니다.
   다음 예에서는 ldom3의 8개 가상 CPU를 삭제합니다.

```
primary# ldm remove-vcpu 8 ldom3
```

4. **ldm add-vcpu** 명령으로 도메인에 가상 **CPU**를 추가합니다.
   다음 예에서는 ldom1에 8개 가상 CPU를 추가합니다.

```
primary# ldm add-vcpu 8 ldom1
```

5. **ldm list-domain** 명령으로 각 도메인의 가상 **CPU** 수를 확인합니다.
   다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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
```

도메인 ldom3의 가상 CPU가 삭제되고 가상 CPU가 ldom1에 추가되었는지 확인할 수 있습니다.

6. 제어 도메인 콘솔에서 로그아웃하고 **XSCF** 콘솔로 돌아갑니다.
제어 도메인 콘솔에서 로그아웃하는 방법은 "4.4.2 제어 도메인 콘솔에서 로그아웃"을 참조하십시오.

   이후 다른 항목을 설정하려면 모든 설정을 완료한 후 제어 도메인 콘솔에서 로그아웃합니다.

13.2 메모리 구성 변경

이 절에는 Oracle VM Server for SPARC의 DR 기능을 사용한 메모리 구성의 변경 방법이 설명되어 있습니다.

SPARC M10 시스템의 경우 다양한 비즈니스 프로세스가 논리 도메인 단위로 실행됩니다. 메모리 구성은 시스템 작동 상태에 따라 유연하게 변경할 수 있습니다.

노트 - 논리 도메인 자원을 동적으로 변경하려면 논리 도메인 동적 재구성(drd) 데몬이 대상 도메인에서 실행되어야 합니다.

SPARC M10 시스템의 경우 다양한 비즈니스 프로세스가 논리 도메인 단위로 실행됩니다. 일부 활성 프로세스에서 부하가 특정 논리 도메인에 집중되어 구성된 메모리만을 사용할 때 성능 저하를 고려할 수 있습니다. 이러한 상황에서 동일한 물리 분할의 논리 도메인을 통해 시스템이 작동을 계속할 수 있습니다. 이는 비교적 부하가 적은 도메인의 메모리를 동적으로 할당하여 수행합니다.

메모리 구성은 256MB 단위로 변경할 수 있습니다.

메모리 구성을 변경하려면 Oracle VM Server for SPARC의 ldm remove-memory 및 ldm add-memory 명령을 사용합니다.

메모리 삭제

```
primary# ldm remove-memory size[unit] ldom
```

Size에 삭제할 메모리의 크기를 지정합니다. Unit에 메모리 단위를 지정합니다. ldom에 메모리가 삭제되는 논리 도메인을 지정합니다.

메모리 추가

```
primary# ldm add-memory size[unit] ldom
```

Size에 추가할 메모리의 크기를 지정합니다. Unit에 메모리 단위를 지정합니다. ldom에 메모리가 추가되는 논리 도메인을 지정합니다.

작동 절차

1. **XSCF** 콘솔을 대상 논리 도메인이 속한 제어 도메인 콘솔로 전환합니다.
   제어 도메인 콘솔로의 전환 방법과 관련된 자세한 내용은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

   대상 제어 도메인 콘솔로 이미 전환했으면 다음 단계로 이동합니다.

2. **ldm list-domain** 명령으로 각 도메인의 메모리 용량을 확인합니다.
   다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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. **ldm remove-memory** 명령으로 도메인의 메모리를 삭제합니다.
   다음 예에서는 ldom3의 1GB 메모리를 삭제합니다.

```
primary# ldm remove-memory 1G ldom3
```

4. **ldm add-memory** 명령으로 도메인에 메모리를 추가합니다.
   다음 예에서는 ldom1에 1GB 메모리를 추가합니다.

```
primary# ldm add-memory 1G ldom1
```

5. **ldm list-domain** 명령으로 각 도메인의 메모리 용량을 확인합니다.
   다음에는 primary와 ldom1, ldom2 및 ldom3 논리 도메인의 상태 확인 예가 나타나 있습니다.

```
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
```

도메인 ldom3의 메모리가 삭제되고 메모리가 ldom1에 추가되었는지 확인할 수 있습니다.

6. 제어 도메인 콘솔에서 로그아웃하고 **XSCF** 콘솔로 돌아갑니다.
제어 도메인 콘솔에서 XSCF 쉘로 돌아가는 방법과 관련된 자세한 내용은 "4.4 제어 도메인 콘솔에서 XSCF 쉘로 돌아가기"를 참조하십시오.

이후 다른 항목을 설정하려면 모든 설정을 완료한 후 제어 도메인 콘솔에서 로그아웃합니다.

13.3 PCI 확장 장치 사용

이 절에는 SPARC M10 시스템의 옵션으로서 제공되는 PCI 확장 장치의 개요가 설명되어 있습니다.

PCI 확장 장치는 최대 11개의 PCI-Express 슬롯을 확장할 수 있도록 하는 랙 장착식 장치입니다. 이는 SPARC M10 시스템에 장착된 동일 랙에 장착할 수 있습니다. SPARC M10 시스템에 내장된 PCI-Express 슬롯이 사용되지만 슬롯이 부족한 경우 PCI 확장 장치를 설치하여 시스템을 유연하게 확장할 수 있습니다.

더욱이, XSCF 펌웨어 ioxadm 명령을 사용하여 PCI 확장 장치 상태를 확인하고 전원을 공급/차단할 수도 있습니다.

PCI 확장 장치의 설치를 살펴볼 때 이와 관련하여 당사 판매 대리인에게 문의하십시오.

PCI 확장 장치의 설치와 관련된 자세한 내용은『SPARC M10 시스템 설치 안내서』의 "3.4.3 랙에 PCI 확장 장치 장착"을 참조하십시오.

13.3.1 PCI 확장 장치 확인

다음 항목을 확인할 수 있습니다. 시스템이 관리하는 PCI 확장 장치의 목록, 온도, 전압 전류, 팬 회전 속도 센서의 측정 값, 로케이터 LED 상태, 펌웨어 상태 등.

확인 방법은 "16.1.5 PCI 확장 장치 상태 표시"를 참조하십시오.

13.3.2 PCI 확장 장치의 전원 제어

이 절에는 PCI 확장 장치, I/O 보드, 전원 공급 장치 등을 제거하기 위한 전원 공급/차단 방법이 설명되어 있습니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
사용자 권한은 다음과 같습니다.
   - platop:

Env 및 list 피연산자의 실행을 활성화합니다.

- platadm:
  Env, list, locator, poweroff 및 poweron 피연산자의 실행을 활성화합니다.
- fieldeng:
  모든 피연산자의 실행을 활성화합니다.

XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **ioxadm** 명령으로 **PCI** 확장 장치의 전원 공급 장치로 가는 전원을 차단합니다.
   다음 예에서는 전원 공급 장치와 같은 지정된 부품을 제거할 수 있도록 이 부품으로 가는 전원을 차단합니다.

```
XSCF> ioxadm -f poweroff PCIBOX#12B4/PSU#1
```

노트 - 전원을 강제 차단하려면 -f 옵션을 지정하십시오. 유의할 점으로, -f 옵션을 사용하면 도메인이 손상될 수도 있습니다.

3. **ioxadm** 명령으로 **PCI** 확장 장치의 전원 공급 장치로 가는 전원을 복구합니다.
   다음 예에서는 전원이 차단된 부품에 전원을 다시 공급합니다.

```
XSCF> ioxadm poweron PCIBOX#12B4/PSU#1
```

노트 - 전원 공급 장치 또는 I/O 보드를 제거하려면 지정된 부품으로 가는 전원을 차단하십시오. 전원이 다시 공급되면 POWER 스위치가 on으로 설정될 때 ioxadm 명령을 실행하십시오.

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.

13.4 SPARC M10-4S 확장

SPARC M10-4S를 확장하여 시스템을 확장하는 작업 흐름, 준비 및 추가 절차의 자세한 내용은『SPARC M10 시스템 설치 안내서』의 "7장 빌딩 블록 구성에서 시스템 추가/제거하기 전"을 참조하십시오.

더욱이, 추가 SPARC M10-4S 캐비닛을 물리 분할에 추가하고 논리 도메인에 할당하는 방법은『SPARC M10 시스템 도메인 구성 안내서』의 "4장 논리 도메인 구성"을 참조하십시오.

14장

필요 시 용량 제공(CoD)

이 장에는 SPARC M10 시스템의 CPU를 사용하기 위한 라이센스 키(필요 시 용량 제공: CoD)의 개요와 그 설정 방법이 설명되어 있습니다.

- 필요 시 용량 제공(CoD)의 기본 정보
- CPU 코어 활성화의 기본 정보
- CPU 코어 활성화 키의 기본 정보
- CoD 자원 추가
- CoD 정보 표시
- CoD 오류에 대한 대응 조치
- CoD 사용 시 유의 사항

14.1 필요 시 용량 제공(CoD)의 기본 정보

필요 시 용량 제공(CoD)은 시스템에 설치된 CPU의 용량을 필요에 따라 유연하게 추가할 수 있도록 하는 기능입니다. 새 비즈니스의 운영, 시스템 보강 등을 위해 추가 CPU 용량이 필요한 경우 시스템 정지 없이도 CPU를 추가할 수 있습니다.

SPARC M10 시스템을 위해 제공되는 모든 CPU는 필요 시 용량 제공을 지원합니다. 서버에 설치된 CPU를 사용하려면 먼저 사용을 위한 라이센스 키를 구입해야 합니다. 이 라이센스 키를 CPU 코어 활성화라고 합니다. CPU 코어 활성화는 2개 코어 형태로 구입할 수 있습니다. 필요에 따라 비즈니스 운영에 필요한 CPU의 용량을 유연하게 결정할 수 있습니다.

14.2 CPU 코어 활성화의 기본 정보

지정된 용량의 CPU로 SPARC M10 시스템의 CPU를 사용하는 데 필요한 CPU 코어 활성화를 구입할 수 있습니다.
구입한 CPU 코어 활성화는 CPU의 영구 사용권을 보장합니다. CPU를 사용하기 전에

CPU 코어 활성화를 구입해야 합니다.
시스템 설치 시 확정 수량의 CPU 코어 활성화를 구입해야 합니다. 하지만 시스템을 도입한 후라도 시스템 작동 상태에 따라 다른 CPU 용도의 CPU 코어 활성화를 추가로 구입할 수 있습니다.

14.3 CPU 코어 활성화 키의 기본 정보

CPU 코어 활성화를 구입하면 구입한 CPU 코어 활성화를 위한 라이센스 키가 발급됩니다. 이 라이센스 키를 CPU 코어 활성화 키라고 합니다. CPU 코어 활성화 키에는 구입한 CPU의 용량 정보가 포함됩니다. CPU 코어 활성화 키가 나타내는 CPU를 CoD 자원이라고 합니다.

XSCF 펌웨어 명령을 사용하여 발급된 CPU 코어 활성화 키를 서버의 CoD 데이터베이스에 추가합니다. 이에 따라 구입한 CPU를 사용할 수 있습니다. CoD 데이터베이스는 각 서버마다 서비스 프로세서의 비휘발성 메모리에 저장됩니다.

CPU 코어 활성화 키는 각 서버마다 관리됩니다. CoD 데이터베이스에 추가되는 CPU 코어 활성화 키를 기반으로 각 물리 분할에 사용되는 CPU가 할당됩니다.

14.3.1 CPU 코어 활성화 키 및 사용 가능한 CPU

다음에는 예를 이용한 CPU 코어 활성화 키 및 사용 가능한 CPU가 설명되어 있습니다.

- CPU 코어 활성화 키(CPU: 2코어 라이센스의 예)

```
Product: SPARC M10-1
SequenceNumber: 1234567890123456
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA……..
```

여러 항목에 대한 정보가 CPU 코어 활성화 키의 각 라인에 "(항목 이름): (값)" 형식으로 설명되어 있습니다.

표 14-1 CPU 코어 활성화 키의 항목 및 값

항목	값
Product	SPARC M10-1, SPARC M10-4 또는 SPARC M10-4S 가운데 하나
SequenceNumber	1 ~ 16자리의 숫자 값
Cpu	CPU 용량(단위: 코어) noExpiration + 최대 4자리의 숫자 값
Text-Signature-xxxxxx-xxxxxx	서명

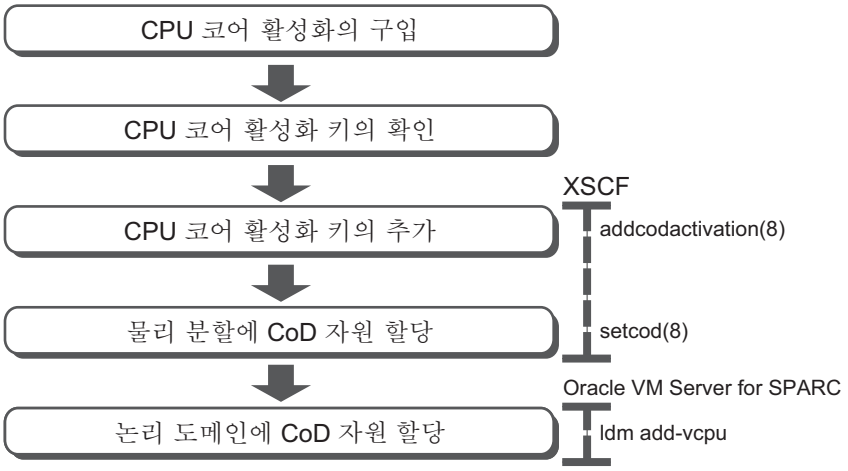
14.4 CoD 자원 추가

14.4.1 CoD 자원 추가까지 흐름

그림 14-1에는 CPU 코어 활성화 구입부터 CPU 사용까지 흐름이 나타나 있습니다.

흐름을 따라 설명이 제공되어 있습니다.

그림 14-1 CoD 자원 사용까지 흐름



14.4.2 CPU 코어 활성화의 구입

시스템에 설치되고 비즈니스에 사용되는 CPU의 수를 살펴 CoD 라이센스를 구입합니다.
CPU 코어 활성화의 구입 방법은 당사 판매 담당자에게 문의하십시오.

14.4.3 CPU 코어 활성화 키의 확인

CPU 코어 활성화 키는 전자 매체를 통해 제공됩니다. CPU 코어 활성화를 구입한 후에는 수령한 CPU 코어 활성화 키를 확인합니다. 내용이 구입 시 요청한 것과 다르지 않는지 확인합니다.

노트 - 구입 시 요청한 내용에 따라 여러 CPU 코어 활성화 키를 사용할 수 있습니다.

14.4.4 CPU 코어 활성화 키의 추가

CPU 코어 활성화 키를 시스템에 추가하려면 XSCF 펌웨어의 addcodactivation 명령을 사용합니다.
Platadm 권한이 있는 사용자 계정이 실행에 사용됩니다.

```
XSCF> addcodactivation key-signature
```

구입한 CPU 코어 활성화 키를 key-signature에 지정합니다. 지정하려면 수령한 CPU 코어 활성화 키의 내용을 복사하여 붙여넣습니다.

작동 절차

1. **platadm** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.

   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.

2. **addcodactivation** 명령을 실행하여 **CPU** 코어 활성화 키를 **CoD** 데이터베이스에 추가합니다.
   CPU 코어 활성화 키를 입력하려면 복사하여 붙여넣습니다. 확인 메시지에 "y"를 입력합니다.

   다음 예에서는 CPU 코어 활성화 키를 PARC M10-1에 추가합니다.

노트 - XSCF 웹을 통해 CPU 코어 활성화 키를 입력할 수도 있습니다.

```
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
```

3. **showcodactivation** 명령을 실행하여 **CPU** 코어 활성화 키가 **CoD** 데이터베이스에 추가되었는지 확인합니다.
   -r 옵션이 지정되면 키가 2단계에서 지정한 CPU 코어 활성화 키의 형식으로 출력됩니다.

   다음에는 SPARC M10-1에 등록된 CoD 데이터베이스의 예가 나타나 있습니다.

```
XSCF> showcodactivation -r
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA.....
```

4. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.

XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

노트 - CPU 코어 활성화 키는 다음 경우 가운데 하나에서 참조될 수 있습니다. XCP 버전이 업데이트되고 CoD 데이터베이스가 손실되며 CPU 코어 활성화 키가 특정 이벤트에 다시 추가되도록 요청을 받은 경우. CoD 라이센스 키를 안전한 곳에 보관하십시오.

노트 - 위의 문제 해결을 제외하고 동일한 CPU 코어 활성화 키를 2회 이상 추가하지 마십시오. 그렇지 않을 경우 계약 위반입니다.

14.4.5 물리 분할에 CoD 자원 할당

CoD 자원을 물리 분할에 할당하려면 XSCF 펌웨어의 setcod 명령을 사용합니다. Platadm 권한이 있는 사용자 계정이 실행에 사용됩니다.

```
XSCF> setcod -p ppar_id -s cpu permits
```

설정할 물리 분할 ID를 ppar_id에 지정합니다. 생략되어 있으면 대상 물리 분할에 대해 대화형으로 지정할 수 있습니다.

할당할 CoD 자원의 수를 permits에 지정합니다. 코어로 지정합니다. 사용권이 있는 자원의 수까지 자원을 지정할 수 있습니다. 또는 대화형으로 지정할 수 있습니다.

작동 절차

1. **platadm** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **setcod** 명령으로 **CoD** 자원을 물리 분할에 할당합니다.
   다음 예에서는 4개 CPU 코어를 SPARC M10-4S 물리 분할 1에 할당합니다.

```
XSCF> setcod -p 1 -s cpu 4
```

다음 예에서는 CPU를 대화형으로 할당합니다.

```
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]:
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

14.4.6 논리 도메인에 CoD 자원 할당

CoD 자원을 논리 도메인에 할당하려면 Oracle VM Server for SPARC의 ldm(1M) 명령을 사용합니다.

자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』의 "4장 논리 도메인 구성"을 참조하십시오.

14.4.7 CPU 코어 활성화 키의 삭제

CoD 데이터베이스에서 CPU 코어 활성화 키를 삭제하려면 XSCF 펌웨어의 deletecodactivation 명령을 사용합니다.
Platadm 권한이 있는 사용자 계정이 실행에 사용됩니다.

```
XSCF> deletecodactivation -i key-index
```

CPU 코어 활성화 키의 관리 번호를 key-index에 지정합니다. showcodactivation 명령으로 관리 번호를 확인할 수 있습니다.

CPU 코어 활성화가 삭제되면 CPU 코어 활성화의 수가 할당되는 CoD 자원의 수보다

적을 수 있습니다. 이 경우 CPU 코어 활성화 키가 CoD 데이터베이스에서 삭제되지 않습니다. 이 경우 CPU 코어 활성화 키를 삭제하려면 할당되는 CoD 자원의 수를 줄여야 합니다. setcod 명령으로 CPU 코어 활성화 할당을 변경합니다.

14.5 CoD 정보 표시

14.5.1 CoD 정보 표시

CoD 데이터베이스에 등록된 CoD 라이센스 키 정보를 표시하려면 XSCF 펌웨어의 showcod 명령을 사용합니다.
Platadm 또는 platop 권한이 있는 사용자 계정이 실행에 사용됩니다. 더욱이, 대상 물리 분할에 대해 pparadm, pparmgr 또는 pparop 권한이 있는 사용자 계정을 실행에 사용할 수도 있습니다.

```
XSCF> showcod [-p ppar_id]
```

표시할 물리 분할 ID를 -p ppar_id에 지정합니다. 생략되어 있으면 액세스 가능한 모든 물리 분할의 정보가 표시됩니다.

setcod 명령으로 다음 CoD 정보를 표시합니다.

- 설치된 CPU 코어 활성화의 수
- PPAR에 할당된 CPU 코어 활성화의 수

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **showcod** 명령을 실행하여 **CoD** 자원 정보를 표시합니다.
   다음 예에서는 물리 분할 1에 대해 액세스 권한이 있는 사용자 계정으로 CoD 자원 정보 모두를 표시합니다.

```
XSCF> showcod
PROC Permits assigned for PPAR 1 : 0
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

14.5.2 CoD 로그 확인

CPU 코어 활성화 키 추가 및 삭제와 같은 로그를 표시하려면 XSCF 펌웨어의 showcodactivationhistory 명령을 사용합니다.
Platadm, platop 또는 fieldeng 권한이 있는 사용자 계정이 실행에 사용됩니다.

```
XSCF> showcodactivationhistory [target_url]
```

결과를 파일로 출력하려면 파일 이름을 target_url에 지정합니다.

작동 절차

1. **Platadm, platop** 또는 **fieldeng** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **showcodactivationhistory** 명령을 실행하여 **CPU** 코어 활성화 키의 로그를 표시합니다.
   다음 예에서는 로그를 화면에 직접 출력합니다.

```
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 3 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 0 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 3 cores
11/07/2012 01:46:23PM PST: Capacity deleted: PROC 0 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 1 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 4 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 4 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 1 cores
11/30/2011 01:42:41PM PST: Summary: PROC 5 cores
Signature: 9138HVZQ0zFJh8EoRy7i1A
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.

   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

14.5.3 CPU 코어 활성화 키 정보 표시

CoD 데이터베이스에 등록된 CPU 코어 활성화 키 정보를 표시하려면 XSCF 펌웨어의 showcodactivation 명령을 사용합니다.
Platadm 또는 platop 권한이 있는 사용자 계정이 실행에 사용됩니다.

```
XSCF> showcodactivation [-r] [-i key-index] [-M]
```

CPU 코어 활성화 키의 관리 번호를 key-index에 지정합니다. 옵션 없이 showcodactivation 명령 실행으로 표시하여 관리 번호를 확인합니다. 생략되어 있으면 등록된 모든 CPU 코어 활성화 키의 정보가 표시됩니다.

CoD 데이터베이스에 등록된 데이터 형식으로 값을 표시하려면 -r 옵션을 지정합니다. 이 옵션이 생략되어 있으면 값이 표 형식으로 표시됩니다.

출력 결과를 화면별로 표시하려면 -M 옵션을 지정합니다.

작동 절차

1. **Platadm** 또는 **platop** 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **showcodactivation** 명령을 실행하여 **CoD** 데이터베이스의 **CoD** 라이센스 키 정보를 표시합니다.
   다음 예에서는 추가 시 사용하는 형식으로 관리 번호 2의 CoD 라이센스 키 정보를 표시합니다.

```
XSCF> showcodactivation -r -i 2
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA……..
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   XSCF에서 작업을 계속하려면 수행이 필요한 작업을 마친 후 XSCF에서 로그아웃합니다.

14.5.4 CoD 자원 사용 상태 표시

CoD 자원 사용 상태에는 다음 정보 항목이 포함됩니다.

- 사용 중인 CoD 자원
- 설치된 CPU
- 등록된 CPU 코어 활성화 키
- 활성화 위반 여부

CoD 자원 라이센스 키 사용 정보를 표시하려면 XSCF 펌웨어의 showcodusage 명령을 사용합니다.
Platadm, platop 또는 fleldeng 권한이 있는 사용자 계정이 실행에 사용됩니다. 더욱이, 대상 물리 분할에 대해 pparadm, pparmgr 또는 pparop 권한이 있는 사용자 계정을 실행에 사용할 수도 있습니다.

```
XSCF> showcodusage [-v] [-M] [-p {resource|ppar|all}]
```

출력 결과를 화면별로 표시하려면 -M 옵션을 지정합니다.

-p all을 지정하여 CoD 자원 활성화 사용 정보 모두를 출력합니다.

-p ppar을 지정하여 각 물리 분할의 CoD 자원 라이센스 키 사용 정보를 출력합니다.

-p resource를 지정하여 각 CoD 자원의 활성화 사용 정보를 출력합니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오.
   위 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **showcodusage** 명령을 실행하여 **CoD** 자원 라이센스 키 정보를 표시합니다.
   다음 예에서는 추가 시 사용하는 형식으로 관리 번호 2의 CoD 라이센스 키 정보를 표시합니다.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-------- ------ --------- ------------- ------
PROC          4         4 16 OK: 12 cores available
```

3. **XSCF**에서 로그아웃하려면 **exit** 명령을 실행합니다.
   이후 XSCF 작동을 계속하려면 모든 작동을 완료한 후 XSCF에서 로그아웃합니다.

14.6 CoD 오류에 대한 대응 조치

14.6.1 사용되는 CPU의 수가 CPU 코어 활성화에서 허용되는 수를 초과하는 경우

사용되는 CPU의 수가 CPU 코어 활성화에서 허용되는 수를 초과하는 경우 문제로서 간주됩니다.

이러한 문제가 발생하는 경우 메시지가 XSCF 콘솔 및 제어 도메인 콘솔로 출력됩니다. 더욱이, XSCF 이메일 알림 기능과 SNMP 기능으로 알림이 수신될 수 있습니다.

이메일 알림 기능은 "15.2 고장 발생 시 이메일을 통한 알림 수신"을 참조하십시오.
SNMP 기능은 "15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리"를 참조하십시오.

메시지가 출력되거나 알림이 발행된 경우 CoD 자원의 사용 정지와 같은 조치가 취해집니다.
문제가 해결되지 않으면 시스템은 도메인에서 CPU 코어 활성화 수를 초과하는 CPU를 삭제합니다. 모든 도메인에서 CPU 삭제가 시도됩니다. 삭제되지 않으면 도메인이 정지됩니다. 조치 방법은『SPARC M10-1 Service Manual』또는『SPARC M10-4/M10-4S Service Manual』의 "3장 고장 진단"을 참조하십시오.

14.6.2 고장으로 인해 CoD 자원 수가 CPU 코어 활성화 수 미만인 경우

고장으로 인해 사용 가능한 CoD 자원 수가 CPU 코어 활성화 수 미만인 것으로 가정합니다. 이 경우 물리 분할에 과잉 CPU 자원이 포함되면 과잉 CPU를 등록된 CPU 코어 활성화 키에 사용할 수 있습니다. 고장인 CPU 자원의 CoD 자원은 해제되어 과잉 자원에 할당됩니다.

14.7 CoD 사용 시 유의 사항

다음 항목은 CoD 사용 시 유의 사항으로서 설명되어 있습니다.

- 라이브 마이그레이션 시의 제어
- CoD 정보 저장/복원
- SPARC M10-4S 확장/성능 저하

라이브 마이그레이션 시의 제어

전송 소스와 대상 둘 모두에 충분한 CPU 코어 활성화가 없는 경우 전송 대상 서버를 위한 CPU 코어 활성화를 구입해야 합니다. 동일 서버 내 마이그레이션의 경우 대상 서버를 위한 새 CPU 코어 활성화를 구입해야 합니다.

라이브 마이그레이션의 자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』의 "7장 게이스 도메인 마이그레이션"을 참조하십시오.

CoD 정보 저장/복원

CoD 정보의 CPU 코어 활성화 키는 XSCF 구성의 정보에 저장됩니다. 저장된 CPU 코어 활성화 키는 키가 저장된 서버에서만 복원할 수 있습니다.

CoD 정보의 자세한 내용은 "14.5.1 CoD 정보 표시"를 참조하십시오. XSCF 구성 정보의 자세한 내용은 "15.7 XSCF 설정 정보 저장/복원"을 참조하십시오.

SPARC M10-4S 확장/성능 저하

SPARC M10-4S를 확장하려면 새 SPARC M10-4S를 사용하거나 또 다른 시스템에서 성능 저하가 있는 SPARC M10-4S를 사용합니다. 추가된 SPARC M10-4S에서 CPU를 사용하려면 새 CPU 코어 활성화 키를 구입하거나 부품이 제거된 시스템에서 일부 CPU용 CPU 코어 활성화 키를 전송하여 CoD 자원을 추가합니다.

SPARC M10-4S의 부품을 제거할 때 CoD 정보에 저장되어서 CPU 코어 활성화 키를 삭제하지 않아도 됩니다.

15장

고장 대응

이 장에는 SPARC M10 시스템 고장에 대응하는 과정에서 사전에 설정하는 기능이 설명되어 있습니다. 이 시스템은 고장 발생에 대응하는 과정에서 다양한 기능을 제공합니다. 조기에 고장을 찾아 처리하려면 사용자는 시스템 모니터링 설정 지정, 하드웨어 중복화 및 데이터 저장과 같은 일부 조치로 대응해야 합니다.

이 장에는 이 관리 방법이 설명되어 있습니다.

- 고장 대응 조치 및 기능 이해
- 고장 발생 시 이메일을 통한 알림 수신
- SNMP 에이전트를 사용한 시스템 상태 모니터링/관리
- 시스템 모니터링
- 고장 성능 저하 메커니즘 이해
- 중복 구성요소 구성
- XSCF 설정 정보 저장/복원
- 논리 도메인 구성 정보 저장/복원
- 하드 디스크 내용 저장/복원
- 하이퍼바이저의 덤프 파일 수집
- 공장 기본 상태로 서버 복귀

15.1 고장 대응 조치 및 기능 이해

표 15-1에는 고장 발생 시의 대응 조치와 기능이 나열되어 있습니다. 각 항목의 자세한 내용은 다음 절을 참조하십시오.

표 15-1 고장 대응 조치 및 기능

조치	기능	관련된 명령
조기에 고장 정보를 사용자에 전송합니다.	이메일 알림	setsmtp(8), showsmtp(8), setemailreport(8), showemailreport(8)

표 15-1 고장 대응 조치 및 기능 (계속)

조치	기능	관련된 명령
고장과 이벤트를 모니터링/관리합니다.	SNMP 에이전트 기능을 사용한 시스템 모니터링	setsnmp(8), showsnmp(8), setsnmpusm(8), showsnmpusm(8), setsnmpvacm(8), showsnmpvacm(8)
조기에 고장을 찾고 서버 작동을 파악합니다.	■ 시스템 모니터링, 하트비트, 활성 모니터링 ■ 서버 작동 제어	setpparmode(8), showpparmode(8), setpparparam(8), showpparparam(8)
고장이 다른 섹션에 영향을 미치는 일이 없도록 하거나 중복 구성으로 조치를 취합니다.	■ 고장 성능 저하 ■ 중복 구성요소 구성	showstatus(8), showhardconf(8)
현재 설정 데이터를 보호하고 원래 상태로 되돌립니다.	■ XSCF 설정 정보 저장/복원 ■ 논리 도메인 정보 저장/복원 ■ 하드 디스크 저장/복원	dumpconfig(8), restoreconfig(8), Oracle VM Server for SPARC 명령

15.2 고장 발생 시 이메일을 통한 알림 수신

이 시스템의 고장 또는 이벤트 발생에 대응하는 과정에서 고장 또는 이벤트 상태를 이메일로 사용자에게 알리도록 XSCF를 설정할 수 있습니다.

이메일 알림을 구성하는 것이 좋습니다. XSCF의 이메일 알림이 설정되면 특정 사용자는 서버 또는 물리 분할의 고장 알림을 바로 수신할 수 있습니다. 특정 사용자에는 platadm 사용자 권한이 있는 시스템 관리자가 포함됩니다.

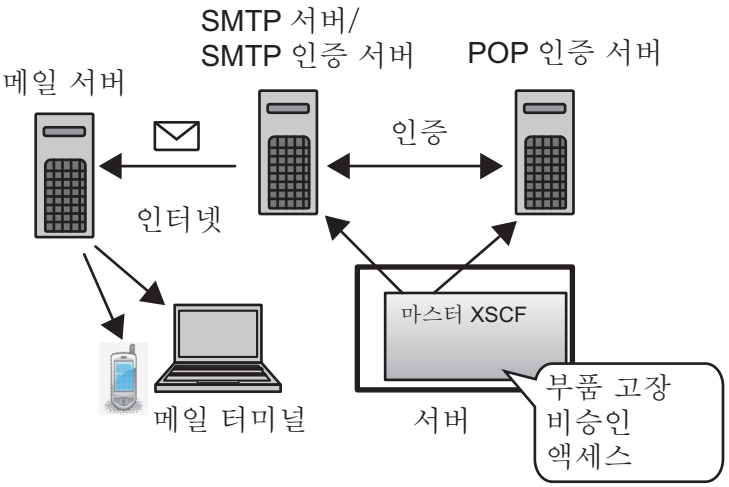
15.2.1 이메일 알림 기능의 특징

이메일 알림 기능의 특징은 다음과 같습니다.

- 시스템에서 XSCF가 모니터링하는 부품의 고장을 이메일을 사용하여 보고함
  시스템이 다운되거나 재부팅이 불가능한 심각한 오류가 발생하더라도 확실하게 이메일을 전송할 수 있습니다.
- 이메일 전송 시에 POP 인증 기능과 SMTP 인증 기능을 활성화함
  불법 이메일 전송을 방지하도록 SMTP 서버에서 이메일 전송을 수락하기 전에 POP 인증(SMTP 이전에 POP) 또는 SMTP 인증(SMTP-AUTH)을 수행할 수 있습니다.

그림 15-1에는 XSCF가 각 서버를 통해 이메일을 전송하는 개요가 제공되어 있습니다.

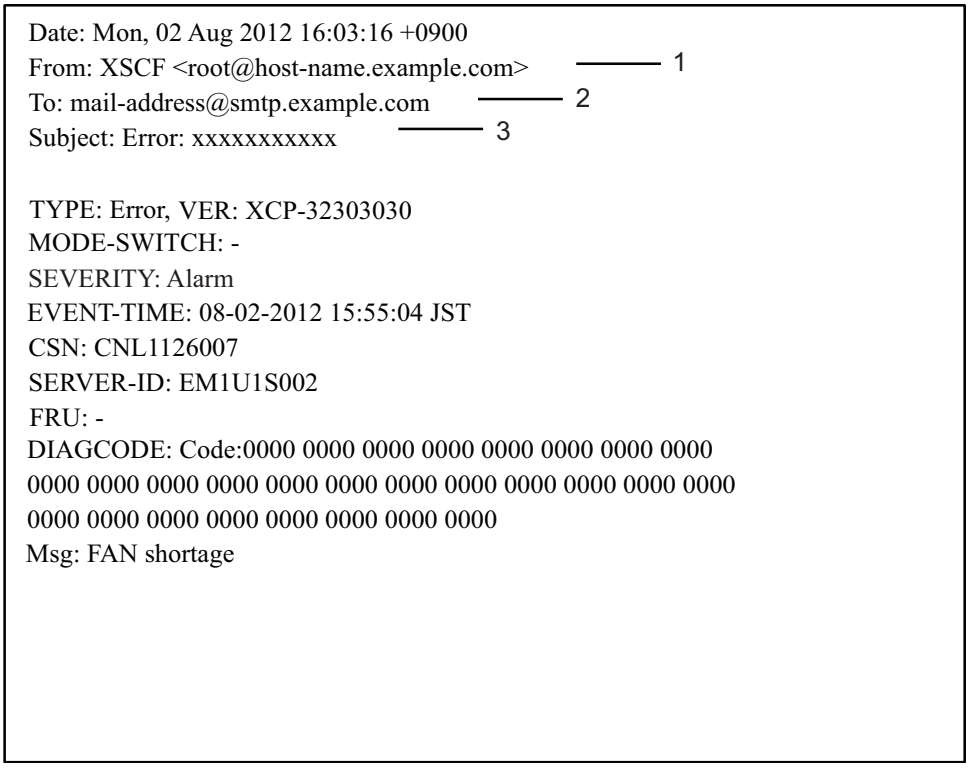
그림 15-1 XSCF 이메일 기능 개요



15.2.2 고장 알림 세부 사항

그림 15-2에는 알림 이메일의 예가 제공되어 있습니다.

그림 15-2 부품 고장 시의 이메일 예



1	이메일 설정으로 지정하는 "회신 대상 이메일 주소"
2	이메일 설정으로 지정하는 "대상 이메일 주소"
3	이메일 제목

이메일 예에서는 다음 항목을 나타냅니다.

- TYPE: 알림 유형
- VER: 버전
- MODE: 모드 스위치 상태
- SEVERITY: 오류 레벨
- EVENT-TIME: 고장 발생 시간(현지 시간 표시)
- CSN: 새시 일련 번호, 캐비닛 일련 번호
- SERVER-ID: 이 시스템의 ID
- FRU: 고장일 가능성이 높은 구성요소
- DIAGCODE:
  현장 엔지니어와 당사 서비스 엔지니어가 문제를 분석하는 데 사용. 사용자는 이 코드를 현장 엔지니어 또는 당사 서비스 엔지니어로 보고합니다. 이는 문제를 조기 해결하는 데 유용합니다.

- Msg: 문제 개요를 나타내는 메시지

15.2.3 이메일 알림과 관련된 설정 항목 및 명령의 확인

표 15-2에는 XSCF 이메일 알림과 관련된 설정 항목 및 연관된 XSCF 쉘 명령이 나열되어 있습니다.

표 15-2 이메일 알림과 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
SMTP 서버 ■ 호스트 이름 ■ 포트 번호 ■ 회신 대상 이메일 주소	옵션	setsmtp(8), showsmtp(8)
이메일 알림 기능의 활성화/비활성화 여부	옵션	setemailreport(8), showemailreport (8)
대상 이메일 주소	옵션	setemailreport(8), showemailreport (8)
인증 서버 ■ POP 인증/SMTP 인증 ■ 호스트 이름 ■ 사용자 ID/암호	옵션	setsmtp(8), showsmtp(8)

1개 SMTP 서버만 지정됩니다. 호스트 이름으로 SMTP 서버를 지정하려면 DNS 서버로 서버 이름을 확인할 수 있어야 합니다.

SMTP 서버의 기본 포트 번호는 25입니다.

회신 대상 이메일 주소는 대상 이메일 주소로 계속되는 경로에서 문제가 발생할 때 이 경로에서 이메일 서버가 사용하는 이메일 주소입니다. 이 이메일 서버는 오류 이메일을 전송합니다.

15.2.4 이메일 알림 설정의 흐름

다음에는 XSCF 이메일 알림 설정의 흐름이 설명되어 있습니다.

1. **XSCF**에 로그인합니다**.**
2. **SMTP** 서버의 호스트 이름 또는 **IP** 주소를 지정합니다**(setsmtp(8)** 참조**).**
3. **POP** 또는 **SMTP** 인증을 선택합니다**(setsmtp(8)** 참조**).**
4. 회신 대상 이메일 주소를 지정합니다**(**사양에서**)(setsmtp(8)** 참조**).**
5. 시스템 관리자를 위한 대상 이메일 주소를 지정합니다**(setemailreport(8)** 참조**).**
6. **XSCF** 이메일 알림을 활성화합니다**(setemailreport(8)** 참조**).**

7. 테스트 이메일을 발행합니다.
이메일 설정이 완료되면 테스트 이메일이 자동 발행됩니다. 테스트 이메일이 발행되어 시스템 관리자에게 도착하면 설정이 완료된 것입니다. 테스트 이메일이 도착하지 않으면 문제는 다음 가운데 하나가 됩니다. 오류 이메일이 회신 대상 주소로 전송되고(지정된 주소에서) 오류 로그가 기록됩니다. 원인을 찾아 문제를 해결합니다. 그런 다음 1단계에서 시작하여 절차를 다시 수행합니다. 테스트가 정상적으로 완료되면 이메일 알림 기능이 활성화됩니다.

15.2.5 호스트 이름, 포트 번호, 회신 대상 이메일 주소 및 SMTP 서버의 인증 방법 설정

1. **showsmtp** 명령을 실행하여 **SMTP** 서버 설정 정보를 표시합니다.

```
XSCF> showsmtp
Mail Server:
Port : 25
Authentication Mechanism: none
Reply address:
```

2. **setsmtp** 명령을 실행하여 **SMTP** 서버 정보를 설정합니다.
다음 예에서는 호스트 이름, 포트 번호, 회신 대상 이메일 주소 및 SMTP 인증을 지정합니다.

```
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
```

다음 예에서는 대화형 모드에서 호스트 이름, 포트 번호, 회신 대상 이메일 주소 및 POP 인증을 지정합니다.

```
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. **showsmtp** 명령을 실행하여 **SMTP** 서버 설정 정보를 확인합니다.

```
XSCF> showsmtp
Mail Server: 192.1.4.5
Port: 25
Authentication Mechanism : pop
User Name: usr001
```

```
Password: ********
Reply Address: yyyy@example.com
```

15.2.6 대상 이메일 주소 및 이메일 알림 기능의 활성화/비활성화 여부 설정

"15.2.5 호스트 이름, 포트 번호, 회신 대상 이메일 주소 및 SMTP 서버의 인증 방법 설정"에 나타난 바와 같이 SMTP 서버를 사전에 설정합니다.

XSCF 이메일 기능을 설정한 후 설정 확인을 위해 테스트 이메일을 발행할 수 있습니다. 다음이 표시됩니다. 테스트 이메일의 발행 시간(현지 시간 표시) 및 이메일 전송 소스 정보. 더욱이, 테스트 이메일 제목에 문자 "Test Mail:"이 포함됩니다.

1. **showemailreport** 명령을 실행하여 이메일 알림 설정 정보를 표시합니다.

```
XSCF> showemailreport
E-Mail Reporting: disabled
```

2. **setemailreport** 명령을 실행하여 이메일 알림 정보를 설정합니다.
   다음 예에서는 대화형 모드에서 이메일 알림의 활성화를 지정하고 대상 이메일 주소를 지정합니다.

```
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. **showemailreport** 명령을 실행하여 이메일 알림 설정 정보를 확인합니다.

```
XSCF> showemailreport
E-Mail Reporting: enabled
E-Mail Recipient Address: xxxxx@example.com'
```

4. 제목이 **"Test Mail"**인 테스트 이메일을 수신할 수 있는지 확인합니다.

15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리

이 절에는 시스템 고장 및 이벤트의 모니터링 방법이 설명되어 있습니다.

XSCF로 SNMP 에이전트가 설정되면 서버 관리자는 고장 및 이벤트를 모니터링/관리할 수 있습니다.

15.3.1 SNMP의 기본 정보

SNMP(Simple Network Management Protocol)는 네트워크 관리 프로토콜입니다.

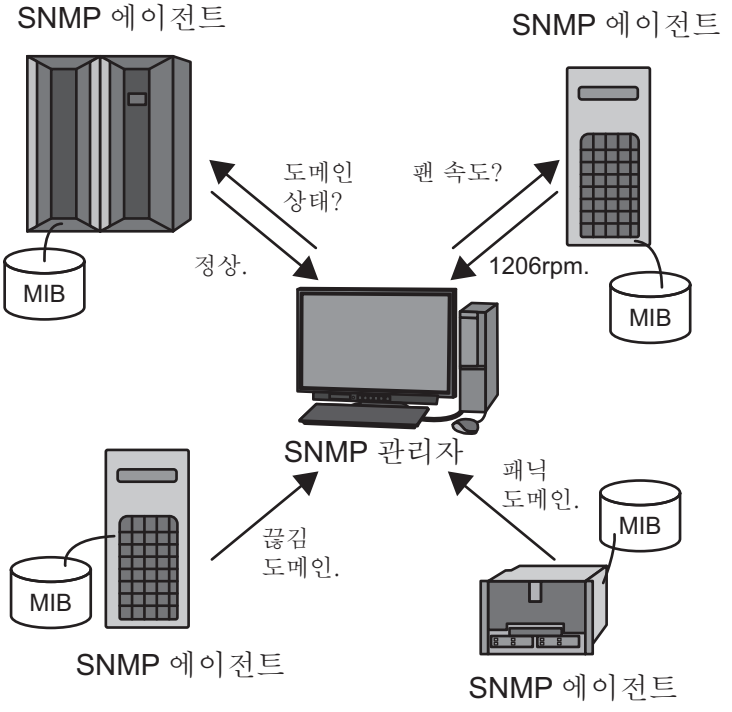
SNMP는 네트워크에 연결된 브리지, 라우터 및 스위치를 테스트 또는 변경하는 데 사용되는 쿼리, 명령 또는 응답 프로토콜입니다. 이는 기타 장치에 연결된 LAN 및 WAN의 구성 파라미터를 테스트 또는 변경하기도 합니다.

현재 SNMPv1, SNMPv2c 및 SNMPv3이 제공됩니다. SNMPv1 및 SNMPv2c와 달리 SNMPv3에는 추가된 암호화 및 인증 기능이 있습니다.

SNMP 관리자는 네트워크 터미널의 작동 및 문제 상태를 중앙 관리합니다. SNMP 에이전트는 관리자 요청에 응답하는 과정에서 MIB(Management Information Base)라고 하는 관리 정보를 반환합니다. 더욱이, 에이전트는 특정 정보에 대해서 트랩이라고 하는 기능을 사용하여 관리자를 위한 비동기 알림을 수행할 수도 있습니다.

그림 15-3에는 SNMP에 의한 네트워크 관리 환경의 예가 나타나 있습니다.

그림 15-3 네트워크 관리 환경의 예



SNMP가 사용하는 기본 포트 번호

SNMP는 다음의 기본 포트 번호를 사용합니다.

- SNMP 에이전트: 포트 161
- 트랩: 포트 162

15.3.2 SNMP 용어

표 15-3에는 SNMP 용어가 나열되어 있습니다.

표 15-3 SNMP 용어

용어	설명
USM	User-based Security Model(사용자 기반 보안 모델)의 약어. SNMPv3이 정의한 사용자 기반 보안 모델
VACM	View-based Access Control Model(보기 기반 액세스 제어 모델)의 약어. SNMPv3이 정의한 보기 기반 액세스 제어 모델
그룹	VACM 모델에 속하는 사용자의 집합체. 그룹은 그룹에 속하는 모든 사용자의 액세스 권한으로 정의됩니다.
OID	Object Identifier(개체 식별자)의 약어. 개체 식별 번호. MIB 정의 파일의 개체에 대해서 정수와 점의 연결로 표시하는 MIB의 숫자형 주소.
보기 (MIB 보기)	MIB 정의 파일을 참조하는 방법. 보기는 OID 또는 OID 마스크로 정의된 MIB의 하위 트리입니다. MIB 액세스 제어 보기를 그룹에 할당할 수 있습니다.

15.3.3 MIB 정의 파일의 기본 정보

SNMP 에이전트 기능에는 MIB라고 하는 관리 정보가 있습니다. 이 MIB 정보는 관리자 요청에 응답하는 과정에서 반환됩니다.

표준 MIB

XSCF는 인터넷 표준으로서 정의되는 MIB-II(SNMPv2 및 v3을 지원) 및 MIB-I (SNMPv1을 지원)을 지원합니다. 이는 주로 다음 정보를 관리합니다.

- XSCF-LAN과 관련된 기본 정보(관리자 이름 등)
- XSCF-LAN 통신 처리와 관련된 정보
- XSCF SNMP 에이전트 작동과 관련된 정보

XSCF가 지원하는 표준 MIB의 자세한 내용은 "부록 C XSCF MIB 정보"를 참조하십시오.

확장 MIB

표준 MIB 외에 이 시스템은 다음의 확장 MIB도 지원합니다.

- XSCF 확장 MIB: XSCF SNMP 에이전트용 확장 MIB

이 MIB는 주로 다음 정보를 관리합니다.

- 시스템과 관련된 기본 정보(일련 번호 등)
- 시스템과 관련된 다양한 상태 정보(예: 상위 Oracle Solaris의 작동 상태)

- 시스템의 물리 분할 정보
- 시스템의 부품 고장 정보
- 시스템의 전원 값/설정과 관련된 정보

다음 예에는 XSCF 확장 MIB의 관리 정보 데이터가 나타나 있습니다.

```
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 }
```

XSCF가 지원하는 XSCF 확장 MIB의 자세한 내용은 "부록 C XSCF MIB 정보"를 참조하십시오.

확장 MIB 정의 파일 설치

MIB 정의 파일은 ASN1 표준의 표기법에 따라 정의됩니다.
XSCF 확장 MIB 정의 파일은 이 시스템을 모니터링하도록 SNMP 관리자가 사용하는 관리 정보를 정의합니다. 서버를 모니터링하려면 XSCF 확장 SNMP 정의 파일을 SNMP 관리자에 설치합니다.

설치 방법은 사용하는 SNMP 관리자의 설명서를 참조하십시오. 확장 MIB 정의 파일을 가져오기 위한 위치는『SPARC M10 시스템 제품 노트』또는 펌웨어 다운로드 사이트의 MIB 정의 파일 정보를 참조하십시오.

15.3.4 확장 MIB의 전원 정보 참조/전원 정보 설정

논리 도메인에서 XSCF 확장 MIB의 전원 정보를 참조할 수 있습니다. 논리 도메인에서 XSCF 확장 MIB의 전원 정보를 참조하는 방법과 관련된 자세한 내용은 사용 버전의『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

더욱이, SNMP 관리자는 이 시스템의 소비 전력을 제어할 수도 있습니다. XSCF 확장 MIB의 전원 값 설정과 관련된 자세한 내용은 사용하는 SNMP 관리자의 설명서를 참조하십시오.

15.3.5 트랩의 기본 정보

SNMP 에이전트 기능은 이벤트가 발생할 때 SNMP 관리자를 위해 트랩이라고 하는 알림을 수행합니다. XSCF 트랩은 다음 이벤트를 다룹니다.

- XSCF 장애 조치가 발생했습니다.
- 시스템 보드 및 구성요소의 확장, 제거, 교체와 같이 구성이 변경되었습니다.
- 고장이 시스템 부품에서 발생하거나 시스템의 고장 부품을 교체하여 고장을 수정합니다.
- 시작, 패닉 및 전원 분리와 같이 물리 분할 상태가 변경되었습니다.
- 시스템 보드(PSB)가 물리 분할에 삽입되거나 PSB가 분리되었습니다.
- 하이퍼바이저가 중단되었습니다.
- PCI 확장 장치 부품의 추가 및 삭제와 같이 구성이 변경되었습니다.
- PCI 확장 장치 부품의 LED 상태가 변경되었습니다.
- PCI 확장 장치에서 온도 이상이 발생합니다.
- 모드 스위치가 변경되었습니다.
- 패닉과 같이 논리 도메인 상태가 변경되었습니다.
- 최대 소비 전력 값(W)과 같은 전원 정보.
- XSCF SNMP 에이전트 기능이 시작되었습니다(표준 트랩).
- XSCF SNMP 에이전트에 불법으로 액세스했습니다(표준 트랩).
- SNMP 에이전트 시작 시 관리 개체 구성이 변경될 때 생성되는 콜드 스타트 트랩이 발행되었습니다(표준 트랩).

트랩 대상 부품은 시스템에서 XSCF가 모니터링하는 부품 가운데 고장 위치와 부품 번호를 지정할 수 있는 부품입니다. 더욱이, 부품을 지정할 수 없더라도 XSCF 이벤트 알림을 발행하면 트랩이 발생합니다.

다음 예에는 시스템에서 부품 고장이 발생할 때 생성되는 SNMP 트랩이 나타나 있습니다.

```
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 paplcommunity    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)
```

이 예에는 다음 정보가 포함됩니다.

- 트랩을 발행한 XSCF의 IP 주소(예: 10.26.147.50)
- SNMPv1의 커뮤니티 문자열(예: paplcommunity)
- 트랩 유형(예: EnterpriseSpecific, device-specific Trap)
- 트랩 발행 시간(예: Uptime: 6:27:33:28)
- 추가 트랩 정보

가능성이 높은 고장 부품, 이벤트 유형 또는 오류 레벨이 포함될 수 있습니다.

15.3.6 SNMP 에이전트와 관련된 설정 항목 및 명령의 확인

표 15-4에는 XSCF SNMP 에이전트와 관련된 설정 항목 및 연관된 XSCF 쉘 명령이 나열되어 있습니다.

표 15-4 SNMP 에이전트와 관련된 설정 항목

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
시스템 관리 정보 ■ 에이전트 시스템 설정 위치 ■ 관리자 이메일 주소 ■ 에이전트 시스템 설명 ■ 에이전트 포트 번호(수신 포트 번호)	옵션	setsnmp(8), showsnmp(8)
에이전트의 활성화/비활성화 여부	옵션 기본값 비활성화	setsnmp(8), showsnmp(8)
SNMPv3 트랩 ■ 사용자 이름 ■ 인증 암호 ■ 암호화 암호 ■ 로컬 에이전트 엔진 ID 또는 수신 호스트에 긍정 확인 요청 ■ 인증 알고리즘 ■ 트랩 대상 포트 번호 ■ 트랩 대상 호스트 이름	옵션	setsnmp(8), showsnmp(8)
SNMPv3 트랩 비활성화	옵션	setsnmp(8), showsnmp(8)
SNMPv1 및 SNMPv2c 통신의 활성화/비활성화 여부	옵션	setsnmp(8), showsnmp(8)
SNMPv1/SNMPv2c 트랩 ■ 트랩 유형 사양 ■ 커뮤니티 문자열 ■ 트랩 대상 포트 번호 ■ 트랩 대상 호스트 이름	옵션	setsnmp(8), showsnmp(8)
SNMPv1/SNMPv2c 트랩 비활성화	옵션	setsnmp(8), showsnmp(8)
SNMP 설정 초기화	옵션	setsnmp(8), showsnmp(8)
USM 관리 정보 (SNMPv3용 설정) ■ 사용자 인증/암호화 암호 등록 ■ 사용자 인증/암호화 암호 변경 ■ 사용자 복사 ■ 사용자 삭제	옵션	setsnmpusm(8), showsnmpusm(8)

표 15-4 SNMP 에이전트와 관련된 설정 항목 (계속)

설정 항목	설정이 필수 설정 또는 옵션 설정인지 여부	관련된 명령
VACM 관리 정보 (SNMPv3용 설정) ■ 사용자 액세스 제어 그룹의 등록 ■ 사용자 액세스 제어 그룹의 삭제 ■ MIB 액세스 제어 보기의 생성 ■ MIB 액세스 제어 보기의 삭제 ■ 그룹에 MIB 액세스 제어 보기의 할당 ■ MIB 액세스 제어 보기에서 그룹 삭제	옵션	setsnmpvacm(8), showsnmpvacm(8)

15.3.7 SNMP 에이전트 설정의 흐름

다음에는 XSCF SNMP 에이전트 설정의 흐름이 설명되어 있습니다.

각 항목의 자세한 내용은 다음 항목을 참조하십시오.

SNMPv1 및 SNMPv2c의 경우 통신 데이터 암호화가 제공되지 않아 통신이 안전하지 못할 수 있습니다. SNMPv3의 경우 에이전트와 관리자측 둘 모두에서 인증/암호화를 설정하여 보다 안전하게 전송 및 수신할 수 있습니다. 이 시스템은 기본 SNMP 에이전트로서 SNMPv3을 제공합니다.

전송 및 수신 시작

1. **XSCF**에 로그인합니다**.**
2. **SNMPv1, SNMPv2c** 및 **SNMPv3** 에이전트 프로토콜에 공통인 다음 관리 정보를 설정합니다**(setsnmp(8)** 참조**).**
   - 에이전트 시스템 설정 위치
   - 관리자 이메일 주소
   - 에이전트 시스템 설명
   - 에이전트 포트 번호(수신 포트 번호)
3. **SNMPv3** 또는 **SNMPv1** 및 **SNMPv2c**용 다음 관리 정보를 설정합니다**. (setsnmp (8)** 참조**)**

- SNMPv3 관리 정보 설정
  - 사용자 이름
  - 인증 암호
  - 암호화 암호
  - 인증 알고리즘
  - 트랩 대상 포트 번호
  - 트랩 대상 호스트 이름
- SNMPv1 및 SNMPv2c 관리 정보 설정

- 트랩 유형 사양(v1, v2c 선택 또는 <v2c 및 사용 가능한 응답> 알림)
- 커뮤니티 이름
- 트랩 대상 포트 번호
- 트랩 대상 호스트 이름

4. **XSCF SNMP** 에이전트 기능을 활성화합니다**.** 사용자 환경에 따라 다음 둘 가운데 하나 또는 둘 모두를 활성화합니다**. (setsnmp(8)** 참조**)**
   - SNMPv1 및 SNMPv2c 활성화
   - SNMPv3 활성화

노트 **-** XSCF SNMP 에이전트가 활성화된 경우 3단계의 설정 항목 이외 MIB 정보 모두가 초기화됩니다.

전송 및 수신 정지 또는 비활성화

- XSCF SNMP 에이전트 기능 비활성화

사용자 환경에 따라 다음 둘 가운데 하나 또는 둘 모두를 비활성화합니다.

- SNMPv1 및 SNMPv2c 비활성화
- SNMPv3 비활성화

- SNMPv3의 대상 트랩 대상 호스트로 전송 비활성화

다음을 지정하여 전송을 비활성화합니다.

- 사용자 이름
- 트랩 대상 호스트

- SNMPv1 및 SNMPv2c의 대상 트랩 대상 호스트로 전송 비활성화

다음을 지정하여 전송을 비활성화합니다.

- 프로토콜 유형(v1/v2c) 사양
- 트랩 대상 호스트

사용자 관리(USM 관리) 및 MIB 정의 파일의 액세스 제어 보기 관리(VACM 관리) 수행

SNMPv3에 대해 USM 및 VACM 관리가 수행됩니다.

1. **XSCF**에 로그인합니다**.**
2. 다음 사용자 관리 정보를 등록**,** 변경 또는 삭제합니다**. (setsnmpusm(8), setsnmpvacm(8)** 참조**)**
   - 사용자 인증 알고리즘 사양
   - 사용자 인증/암호화 암호 등록
   - 사용자 인증/암호화 암호 변경
   - 사용자 복사
   - 사용자 삭제
3. 다음 사용자에 대해 액세스 제어 그룹 및 액세스 제어 보기**(MIB** 보기**)**를 등록**,** 할당 또는 삭제합니다**.**
   - 사용자 액세스 제어 그룹의 등록

- 사용자 액세스 제어 그룹의 삭제
- MIB 액세스 제어 보기의 생성
- MIB 액세스 제어 보기의 삭제
- 그룹에 MIB 액세스 제어 보기의 할당
- MIB 액세스 제어 보기에서 그룹 삭제

15.3.8 SNMP 에이전트의 시스템 관리 정보 설정 및 SNMP 에이전트의 활성화/비활성화 여부 지정

SNMP 에이전트는 기본값으로서 비활성화됩니다. 에이전트의 기본 포트 번호는 161입니다. 이메일 주소를 최대 128자까지 지정합니다. 수신측 이메일 주소가 제한되면 설정을 확인합니다.

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.
   다음 예에는 관리 정보가 설정되지 않은 상태가 나타나 있습니다.

```
XSCF> showsnmp
Agent Status:       Disabled
Agent port:         161
System Location:    Unknown
System Contact:     Unknown
System Description: Unknown
:
```

2. **setsnmp** 명령을 실행하여 **SNMP** 설정을 수행합니다.
   다음 예에서는 시스템 위치, 설명 및 관리자 이메일 주소를 지정합니다.

```
XSCF> setsnmp -l MainTower21F -c foo@example.com -d DataBaseServer
```

3. **setsnmp** 명령을 실행하여 **SNMP** 에이전트를 활성화합니다.
   다음 예에서는 에이전트를 활성화합니다.

```
XSCF> setsnmp enable
```

   다음 예에서는 에이전트를 비활성화합니다.

```
XSCF> setsnmp disable
```

4. **showsnmp** 명령을 실행하여 **SNMP** 설정을 확인합니다.

```
XSCF> showsnmp
Agent Status:       Enabled
Agent port:         161
System Location:    MainTower21F
```

```
System Contact:     foo@example.com
System Description: DataBaseServer
:
```

15.3.9 SNMPv3 트랩 설정

전송과 수신측에 공통인 SNMPv3 사용자 이름과 인증/암호화 암호를 지정합니다. 엔진 ID는 "0x"로 시작하는 16진수의 짝수가 되어야 합니다.

인증 알고리즘은 보안 해시 알고리즘 256(SHA256)입니다.

트랩 대상 호스트의 기본값은 설정되지 않습니다. 트랩 대상의 기본 포트 번호는 162입니다.

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.
   다음 예에는 SNMPv1 및 SNMPv2c가 설정된 상태가 나타나 있습니다.

```
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 Protocol
-------- ---- ---- ---------------- -------- --------------
host1      62  v1  public              n/a   n/a
host2    1162  v2  public              n/a   n/a
SNMP V1/V2c:
Status:             Enabled
Community String:   public
```

2. **setsnmp** 명령을 실행하여 **SNMPv3** 트랩 설정을 수행합니다.
   다음 예에서는 사용자 이름, 엔진 ID, 인증 알고리즘, 인증 암호, 암호화 암호 및 트랩 대상 호스트 이름 또는 IP 주소를 지정합니다.

```
XSCF> setsnmp addv3traphost -u yyyyy -n 0x### -r SHA host3
Authentication Password: xxxxxxxx
Encryption Password: xxxxxxxx
```

3. **showsnmp** 명령을 실행하여 **SNMPv3** 트랩 설정을 확인합니다.

```
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 Protocol
-------- ---- ---- ---------------- -------- --------------
host3    162   v3     n/a              yyyyy n/a
host1     62   v1     public           n/a   n/a
host2   1162   v2     public           n/a   n/a
SNMP V1/V2c:
Status:            Enabled
Community String:  public

Enabled MIB Modules:
SP MIB
```

15.3.10 SNMPv3의 대상 호스트로 트랩 비활성화

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.

```
XSCF> showsnmp
```

2. **setsnmp** 명령을 실행하여 **SNMPv3**의 대상 트랩 대상 호스트를 비활성화합니다.

```
XSCF> setsnmp remv3traphost -u yyyyy host3
```

3. **showsnmp** 명령을 실행하여 대상 트랩 대상 호스트의 비활성화 여부를 확인합니다.

```
XSCF> showsnmp
```

15.3.11 SNMPv1 및 SNMPv2c 통신 활성화/비활성화

SNMPv1 및 SNMPv2c를 활성화하는 데 사용되는 커뮤니티 문자열은 읽기 전용입니다.

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.

```
XSCF> showsnmp
```

2. **setsnmp** 명령을 실행하여 **SNMPv1** 및 **SNMPv2c** 통신을 활성화합니다.
   다음 예에서는 SNMPv1 및 SNMPv2c를 활성화합니다.

```
XSCF> setsnmp enablev1v2c public
```

다음 예에서는 SNMPv1 및 SNMPv2c를 비활성화합니다.

```
XSCF> setsnmp disablev1v2c
```

3. **setsnmp** 명령을 실행하여 **SNMP** 에이전트를 활성화합니다.

```
XSCF> setsnmp enable
```

4. **showsnmp** 명령을 실행하여 에이전트의 활성화/비활성화 여부를 확인합니다.

```
XSCF> showsnmp
```

15.3.12 SNMPv1 및 SNMPv2c 트랩 설정

다음 3개에서 트랩 유형을 선택합니다.

- v1
- v2
- 알림

알림이 지정되면 SNMPv2c 에이전트를 사용하여 InformRequest를 전송합니다.

트랩 대상의 기본 포트 번호는 162입니다.

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.

```
XSCF> showsnmp
```

2. **setsnmp** 명령을 실행하여 **SNMPv1** 또는 **SNMPv2c** 트랩을 설정합니다.
   다음 예에서는 SNMPv2c 유형을 지정합니다.

```
XSCF> setsnmp addtraphost -t v2 -s public host2
```

   다음 예에서는 SNMPv1 유형을 지정합니다.

```
XSCF> setsnmp addtraphost -t v1 -s public host1
```

3. **showsnmp** 명령을 실행하여 **SNMPv1** 및 **SNMPv2c** 트랩 설정을 확인합니다.

```
XSCF> showsnmp
```

15.3.13 SNMPv1 및 SNMPv2c의 대상 호스트로 트랩 비활성화

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.

```
XSCF> showsnmp
```

2. **setsnmp** 명령을 실행하여 **SNMPv1** 또는 **SNMPv2c**의 대상 트랩 대상 호스트를 비활성화합니다.
   다음 예에서는 SNMPv2c 유형을 비활성화합니다.

```
XSCF> setsnmp remtraphost -t v2 host2
```

3. **showsnmp** 명령을 실행하여 트랩 대상 호스트의 비활성화 여부를 확인합니다.

```
XSCF> showsnmp
```

15.3.14 기본값으로 SNMP 설정 복귀

SNMP 에이전트를 비활성화하여 구성된 데이터를 기본 값으로 복귀시킬 수 있습니다.

1. **showsnmp** 명령을 실행하여 **SNMP** 설정을 표시합니다.

```
XSCF> showsnmp
```

2. **setsnmp** 명령을 실행하여 **SNMP**를 기본 설정으로 복귀시킵니다.
   이 경우 SNMP 에이전트가 비활성화됩니다.

```
XSCF> setsnmp default
```

3. **showsnmp** 명령을 실행하여 **SNMP**가 기본 설정으로 복귀되었는지 확인합니다.

```
XSCF> showsnmp
```

4. **setsnmp** 명령을 실행하고 **SNMP**를 다시 설정한 후 **SNMP** 에이전트를 활성화합니다.

```
XSCF> setsnmp enable
```

5. **showsnmp** 명령을 실행하여 **SNMP** 설정을 확인합니다.

```
XSCF> showsnmp
```

15.3.15 USM 관리 정보 설정

USM 관리 정보는 SNMPv3용 설정입니다. 다음을 구성합니다.

- 사용자 인증 알고리즘
- 인증/암호화 암호
- 사용자 복사/삭제

1. **showsnmpusm** 명령을 실행하여 **USM** 관리 정보를 표시합니다.

```
XSCF> showsnmpusm

Username  Auth Protocol
--------  ------------------
yyyyy     SHA
user2     SHA
```

2. **setsnmpusm** 명령을 실행하여 **USM** 관리 정보를 설정합니다.
   다음 예에서는 새 사용자의 인증 알고리즘, 인증 암호 및 암호화 암호를 등록합니다. 8자 이상의 문자열로서 암호를 지정합니다.

```
XSCF> setsnmpusm create -a SHA yyyyy
Authentication Password: xxxxxxxx
Encryption Password: xxxxxxxx
```

   다음 예에서는 인증 암호만 변경합니다.
   (암호를 입력하지 않으면 시스템을 입력을 요청합니다.)

```
XSCF> setsnmpusm passwd -c auth -o xxxxxxxx -n xxxxxxxx yyyyy
```

   다음 예에서는 기존 사용자를 복사 및 추가합니다.

```
XSCF> setsnmpusm clone -u yyyyy newuser
```

   다음 예에서는 사용자를 삭제합니다.

```
XSCF> setsnmpusm delete yyyyy
```

3. **showsnmpusm** 명령을 실행하여 **USM** 관리 정보를 표시합니다.

```
XSCF> showsnmpusm

Username  Auth Protocol
--------  ------------------
yyyyy     SHA
user2     SHA
```

15.3.16 VACM 관리 정보 설정

VACM 관리 정보는 SNMPv3용 설정입니다. 다음을 구성합니다.

- 액세스 제어 그룹을 위한 사용자 등록/삭제
- MIB 액세스 제어 보기의 생성/삭제
- 그룹에 MIB 액세스 제어 보기의 할당
- MIB 액세스 제어 보기에서 그룹 삭제

액세스 제어 보기가 그룹에 할당되면 읽기 전용 보기가 할당됩니다.

1. **showsnmpvacm** 명령을 실행하여 **VACM** 관리 정보를 표시합니다.

```
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. **setsnmpvacm** 명령을 실행하여 **VACM** 관리 정보를 설정합니다.
   다음 예에서는 액세스 제어 그룹 xxxxx를 사용자에 추가합니다.

```
XSCF> setsnmpvacm creategroup -u yyyyy xxxxx
```

다음 예에서는 액세스 제어 그룹 xxxxx에서 사용자를 삭제합니다.

```
XSCF> setsnmpvacm deletegroup -u yyyyy xxxxx
```

다음 예에서는 MIB 액세스 제어 보기를 무조건 생성합니다.

```
XSCF> setsnmpvacm createview -s .1 all_view
```

다음 예에서는 OID 마스크를 사용하여 MIB 액세스 제어 보기를 생성합니다.

```
XSCF> setsnmpvacm createview -s .1.3.6.1.2.1 -m fe excl_view
```

다음 예에서는 MIB 액세스 제어 보기를 삭제합니다.

```
XSCF> setsnmpvacm deleteview -s .1.3.6.1.2.1 excl_view
```

다음 예에서는 MIB 액세스 제어 보기를 그룹 xxxxx에 할당합니다.

```
XSCF> setsnmpvacm createaccess -r all_view xxxxx
```

다음 예에서는 모든 MIB 액세스 제어 보기에서 그룹을 삭제합니다.

```
XSCF> setsnmpvacm deleteaccess group1
```

3. **showsnmpvacm** 명령을 실행하여 구성된 **VACM** 관리 정보를 확인합니다**.**

```
XSCF> showsnmpvacm
```

15.4 시스템 모니터링

이 절에는 Oracle Solaris와 이 시스템의 각 펌웨어에 대한 모니터링이 설명되어 있습니다.

15.4.1 하트비트 기능/활성 모니터링의 메커니즘 이해

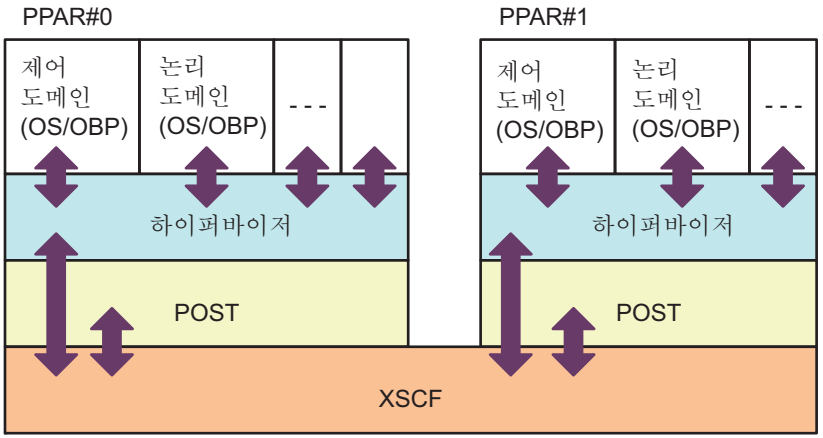
Oracle Solaris, OpenBoot PROM, 하이퍼바이저, POST 및 XSCF는 통신을 구축하고 활성화 상태를 서로 모니터링합니다. 이상이 감지되면 고장에 따른 영향이 확산되지 않도록 패닉이 생성되거나 각기 정지됩니다.

이 시스템에서 논리 도메인/OpenBoot PROM은 하이퍼바이저로 모니터링합니다. 하이퍼바이저와 POST는 XSCF로 모니터링합니다.

하이퍼바이저와 논리 도메인 간 및 하이퍼바이저와 OpenBoot PROM 간 모니터링 메커니즘을 하트비트 기능(호스트 와치독)이라고 합니다. 또한 XSCF와 하이퍼바이저 간 및 XSCF와 POST 간 모니터링 메커니즘을 활성 모니터링 기능이라고 합니다.

그림 15-4에는 각 자원 간의 상호 모니터링이 나타나 있습니다.

그림 15-4 시스템 모니터링 특징



노트 - 그림에서 OBP는 OpenBoot PROM을 나타냅니다.

XSCF는 물리 분할이 실행되는 동안 하이퍼바이저를 통해 하이퍼바이저와 OpenBoot PROM을 모니터링합니다. 지정된 시간 동안 응답이 정지하면 XSCF는 이상이 발생한 것으로 결정하여 물리 분할로 공급되는 전원을 차단하거나 물리 분할을 재설정합니다.

하이퍼바이저는 주기적으로 Oracle Solaris의 작동 상태를 모니터링하여 Oracle Solaris 끊김을 감지합니다. Oracle Solaris 끊김을 감지하면 하이퍼바이저는 관련 도메인에서 Oracle Solaris 패닉을 생성합니다.

노트-XSCF와 하이퍼바이저 간의 활성 모니터링 기능은 setpparmode 명령으로 활성화/비활성화할 수 있습니다. XSCF와 하이퍼바이저 간 활성 모니터링 기능의 지원 정보는 최신 『SPARC M10 시스템 제품 노트』를 참조하십시오.

15.4.2 모니터링 및 서버 작동 제어

시스템을 실행하거나 유지 관리하는 동안 각 물리 분할 또는 논리 도메인의 일부 기능을 억제하고자 할 수도 있습니다. 예를 들어 시스템 유지 관리 시 시스템의 자동 부팅을 원하지 않고(자동 부팅 억제 활성화) 콘솔로부터의 브레이크 신호 수신을 원하지 않습니다(브레이크 신호 억제 활성화).

이 시스템은 모니터링 방법 및 진단 레벨과 같은 각 물리 분할의 작동 모드를 지정합니다. 그런 다음 이는 논리 도메인과 물리 분할의 작동을 제어합니다.

setpparmode 명령을 사용하여 지정된 각 물리 분할마다 다음을 설정할 수 있습니다. 하드웨어의 초기 진단 레벨, 메시지 레벨, 활성 모니터링 기능, 호스트 와치독 시간 초과 시의 반응, 브레이크 신호 전송 억제의 활성화/비활성화, 게스트 도메인의 자동 부팅 활성화/비활성화, 절전 기능의 활성화/비활성화 및 IO 버스 재구성 기능의 활성화/비활성화.

또한 setpparparam 명령을 사용하여 지정된 각 물리 분할마다 제어 도메인의 자동 부팅 활성화/비활성화를 설정할 수 있습니다.

Oracle Solari와 하이퍼바이저 간의 하트비트 기능(호스트 와치독)을 활성화 또는 비활성화하려면 관련 도메인의 Oracle Solaris에 설치된 scfd 드라이버의 구성 파일(scfd.conf)을 설정합니다. 호스트 와치독의 활성화로 논리 도메인을 모니터링합니다.

setpparmode 명령에 의한 서버 작동 제어의 자세한 내용은 『SPARC M10 시스템 도메인 구성 안내서』의 "3장 물리 분할 구성"을 참조하십시오.

노트 - setpparmode 명령 기능의 지원 정보는 최신 『SPARC M10 시스템 제품 노트』를 참조하십시오.

15.5 고장 성능 저하 메커니즘 이해

하드웨어가 소위 성능 저하에 실패하면 시스템에서 구성요소를 분리합니다. 성능 저하는 구성요소 액세스를 분리하여 시스템 문제가 확산되지 않도록 합니다.

성능 저하의 경우는 다음과 같습니다.

- 예약 성능 저하
  재부팅 또는 치명적인 오류 발생 시에 성능 저하가 바로 불가능하면 다시 시작할 때 성능 저하가 되도록 시스템에서 성능 저하를 예약합니다. 이 기능은 성능 저하 위치를 기억하고 있는 XSCF에 의해 구현될 수 있습니다.
- Oracle Solaris 작동 중의 성능 저하
  CPU, 메모리 등은 Oracle Solaris 작동 중에도 분리가 가능하도록 성능 저하됩니다. 대상 구성요소는 Oracle Solaris 작동 중에도 분리가 가능하도록 하는 구성요소입니다.
- POST 작동 중의 성능 저하
  물리 분할은 물리 분할의 재설정 없이 성능 저하됩니다.
- OpenBoot PROM 작동 중의 예약 성능 저하
  이 성능 저하는 OpenBoot PROM 작동 중에 예약하며 재설정 후에 수행합니다. PCI 어댑터 오류, 메모리 오류 등이 처리됩니다.
- FTL 전송 경로의 동적 레인 성능 저하
  레인은 FTL 전송 경로의 재설정 없이 동적으로 성능 저하됩니다.

showstatus 명령을 사용하여 구성요소의 성능 저하 정보를 표시합니다. 고장 성능 저하 정보의 자세한 내용은 "16.1.4 고장/성능 저하된 구성요소의 확인"을 참조하십시오.

15.6 중복 구성요소 구성

구성요소가 고장이더라도 구성요소에 중복 구성이 있으면 시스템은 남은 구성요소로

작동을 계속할 수 있습니다.

구성요소 중복 구성의 자세한 내용은 사용 서버의 『서비스 설명서』를 참조하십시오.

또한 showhardconf 명령을 사용하여 구성요소 구성을 표시합니다. 구성요소 확인의 자세한 내용은 "16.1.2 시스템에 장착된 구성요소의 확인"을 참조하십시오.

15.7 XSCF 설정 정보 저장/복원

XSCF 설정 정보를 저장/복원하려면 XSCF 쉘에서 dumpconfig 및 restoreconfig 명령을 실행합니다. 옵션이 지정된 명령을 실행하여 XSCF의 설정 정보 모두를 지정된 위치에 저장하거나 지정된 위치로부터 복원합니다.

15.7.1 XSCF 설정 정보의 저장/복원 방법 이해

다음 2개 방법을 사용하여 XSCF 설정 정보를 저장/복원할 수 있습니다.

- 설정 정보는 USB 장치를 마스터 XSCF의 XSCF 장치 패널(후면 패널)에 장착된 USB 커넥터에 연결하여 로컬로 저장/복원합니다.
- 데이터는 네트워크를 통해 네트워크 호스트로 전송됩니다. 암호화 프로토콜이 데이터 전송에 사용됩니다.

저장 목적

dumpconfig 명령을 사용한 XSCF 설정 정보의 저장 목적은 다음과 같습니다.

- 설정 정보를 백업하면 갑작스러운 고장 시에 데이터를 복귀시킬 수 있습니다.
- 마스터 XSCF의 설정 정보를 복사하면 또 다른 서버의 XSCF가 동일한 설정 정보를 사용할 수 있습니다.

저장 및 복원 주의 사항

- USB 장치를 FAT32 파일 시스템으로 포맷해야 합니다. 설정 정보를 로컬로 저장/복원하는 데 사용되는 USB 장치의 용량과 처리 주의 사항은 당사 서비스 엔지니어에게 문의하십시오.
- 설정 정보는 설정 정보가 저장된 동일 모델의 시스템으로 복원할 수 있습니다. 예를 들어 SPARC M10-1 시스템에 저장된 설정 정보는 SPARC M10-1 시스템으로만 복원할 수 있습니다. 데이터가 복원되면 현재 시스템의 구성 파일과 복원되는 구성 파일 간의 일관성이 확인됩니다. 구성 파일은 구성 파일 버전, 시스템 이름 및 기타 정보의 일관성이 확인되는 경우에만 복원됩니다. 하지만 구성 파일 버전은 XCP 버전에 따라 달라지지 않습니다. 저장/복원 시에 XCP 버전이 동일하더라도 각 구성 파일의 버전이 서로 다를 수 있습니다.
- XSCF가 2개 이상인 시스템은 마스터 XSCF측에서 저장/복원을 수행합니다.
- 데이터 저장은 옵션이 지정된 dumpconfig 명령으로 암호화합니다. 암호화된 데이터는 restoreconfig 명령을 실행할 때 저장 시 지정한 키를 입력하여 안전하게 복원할 수 있습니다.

- 저장된 구성 파일의 헤드에는 다음 식별 정보가 포함됩니다. 식별 정보는 텍스트로 참조할 수 있습니다.
  - 사용자 설명
  - 데이터 버전
  - 암호화의 활성화 또는 비활성화 여부
  - 저장 시간
  - 시스템 이름
  - 일련 번호
  - XCP 버전
- XSCF 네트워크를 설정할 때 복원 옵션을 지정합니다
- 설정 정보를 복원하려면 모든 물리 분할로 공급되는 전원을 차단합니다. 또한 복원 명령이 실행된 후에는 물리 분할의 재시작 여부를 시스템이 묻습니다. 재시작 후에는 설정이 반영됩니다.

15.7.2 XSCF 설정 정보 저장

다음에는 XSCF 구성 파일의 저장 절차가 설명되어 있습니다.

데이터 암호화를 활성화하려면 dumpconfig(8) 명령의 자세한 내용에 대해 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

마스터 XSCF의 USB에 설정 정보 저장

1. **USB** 장치를 마스터 **XSCF**의 **XSCF** 장치 패널**(**후면 패널**)**에 있는 **USB** 커넥터에 연결합니다**.**
2. **XSCF**의 로컬 **USB** 장치를 출력 파일로서 지정하고 **dumpconfig(8)** 명령을 실행합니다**.**

```
XSCF> dumpconfig file:///media/usb_msd/backup-file.txt
```

3. 데이터 전송이 완료되면 **USB** 커넥터에서 **USB** 장치를 제거합니다**.**
4. 저장된 구성 파일의 헤드에서 식별 정보를 확인합니다**.**

네트워크를 통한 대상 디렉토리 지정 및 설정 정보 저장

1. 대상 디렉토리를 지정하고 **dumpconfig** 명령을 실행합니다**.**

```
XSCF> dumpconfig ftp://server/backup/backup-sca-ff2-16.txt
:
```

2. 데이터 전송이 완료되면 저장된 구성 파일의 헤드에서 식별 정보를 확인합니다**.**

구성 파일의 형식

저장된 구성 파일의 형식은 다음과 같습니다.

- 파일 이름: 사용자 지정 이름
- 파일 형식: base64 인코딩 텍스트

15.7.3 XSCF 설정 정보 복원

다음에는 구성 파일의 복원 절차가 설명되어 있습니다.

암호화된 데이터의 자세한 내용은 restoreconfig(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

마스터 XSCF의 USB에서 설정 정보 복원

1. 모든 물리 분할로 공급되는 전원을 차단합니다.
2. 구성 파일이 들어 있는 **USB** 장치를 마스터 **XSCF**의 **XSCF** 장치 패널**(**후면 패널**)**에 있는 **USB** 커넥터에 연결합니다.
3. **XSCF** 장치의 로컬 **USB** 장치를 입력 파일로서 지정하고 **restoreconfig** 명령을 실행합니다.

```
XSCF> restoreconfig file:///media/usb_msd/backup-file.txt
```

메시지로 복원될 구성 파일의 식별 정보를 표시합니다.

4. 내용이 올바르면 복원을 위해 **"y"**를 입력합니다.
XSCF가 재설정됩니다.
5. 세션이 일단 분리됩니다. 다시 연결합니다.
6. 복원이 완료되면 **USB** 커넥터에서 **USB** 장치를 제거합니다.

네트워크를 통한 대상 디렉토리 지정 및 설정 정보 복원

1. 모든 도메인으로 공급되는 전원을 차단합니다.
2. 대상 디렉토리를 지정하고 **restoreconfig** 명령을 실행합니다.

```
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]:
```

메시지로 복원될 구성 파일의 식별 정보를 표시합니다.

3. 내용이 올바르면 복원을 위해 **"y"**를 입력합니다.

XSCF가 재설정됩니다.

4. 세션이 일단 분리됩니다. 다시 연결합니다.

15.8 논리 도메인 구성 정보 저장/복원

이 절에는 논리 도메인 구성 정보의 저장 방법과 저장된 구성 정보의 복원 방법이 설명되어 있습니다.

15.8.1 논리 도메인 구성 정보 저장/표시

논리 도메인 구성 정보는 물리 분할(PPAR)에 기반하여 저장할 수 있습니다. 구성 정보를 저장하려면 대상 물리 분할의 제어 도메인에 로그인합니다. 저장된 구성 정보는 물리 분할 내의 서비스 프로세서에 저장됩니다.

각 물리 분할마다 최대 8개 세트의 논리 도메인 구성 정보를 저장할 수 있습니다. 이 세트 가운데 하나는 공장 기본 상태를 포함하며 그 이름이 공장 기본값입니다. 공장 기본값이 이미 설정되어 있기 때문에 남은 구성 파일 세트를 최대 7개까지 저장할 수 있습니다. 다양한 구성 패턴을 사전에 저장하여 물리 분할을 다시 시작할 때 비즈니스에 적합한 논리 도메인 구성을 지정할 수 있습니다. 논리 도메인 구성 정보의 자세한 내용은 사용 버전의『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

논리 도메인 구성 정보 저장

논리 도메인 구성 정보를 저장하려면 하위 명령 add-spconfig가 지정된 Oracle VM Server for SPARC의 ldm(1M) 명령을 실행합니다.

```
primary# ldm add-spconfig config_name
```

Config_name의 경우 논리 도메인 구성 정보를 XSCF에 저장하는 데 사용되는 파일 이름을 지정합니다.

논리 도메인 구성 정보 표시

논리 도메인 구성 정보는 물리 분할의 제어 도메인 또는 마스터 XSCF에서 표시할 수 있습니다.

- 물리 분할의 제어 도메인에서 정보 표시
  제어 도메인에서 저장된 논리 도메인 구성 정보를 표시하려면 하위 명령 list-spconfig가 지정된 Oracle VM Server for SPARC의 ldm 명령을 실행합니다.

```
primary# ldm list-spconfig
```

- XSCF 쉘에서 정보 표시
  XSCF 쉘에서 저장된 논리 도메인 구성 정보를 표시하려면 XSCF 펌웨어의 showdomainconfig 명령을 사용합니다.

```
XSCF> showdomainconfig -p ppar_id
```

표시할 물리 분할을 -p ppar_id에 지정합니다. Ppar_id의 경우 표시되는 물리 분할의 PPAR-ID를 0 ~ 15의 값으로 지정할 수 있습니다.

작동 절차

1. **XSCF** 쉘을 대상 물리 분할의 제어 도메인 콘솔로 전환합니다.
   제어 도메인 콘솔로의 전환 방법과 관련된 자세한 내용은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오. 대상 제어 도메인 콘솔로 이미 전환했으면 다음 단계로 이동합니다.
2. **ldm list-spconfig** 명령을 실행하여 현재 저장된 논리 도메인 구성 정보를 표시합니다.

```
primary# ldm list-spconfig
```

3. **ldm add-spconfig** 명령을 실행하여 논리 도메인 상태를 구성 정보로서 저장합니다.
   다음에는 구성 정보를 이름이 ldm_set1인 파일에 저장하는 예가 나타나 있습니다.

```
primary# ldm add-spconfig ldm_set1
```

4. **ldm list-spconfig** 명령을 실행하여 구성 정보가 올바로 저장되었는지 확인합니다.

```
primary# ldm list-spconfig
```

15.8.2 논리 도메인 구성 정보 복원

물리 분할을 다시 시작할 때 물리 분할에 저장된 특정 논리 도메인 구성 정보를 지정할 수 있습니다. 이 기능은 현재 구성과 다른 논리 도메인 구성으로 다시 시작하고자 할 때 사용할 수 있습니다.

노트 - 논리 도메인 구성 정보를 복원하려면 논리 도메인 구성 정보를 사전에 저장해야 합니다. 자세한 내용은 "15.8.1 논리 도메인 구성 정보 저장/표시"를 참조하십시오.

저장된 논리 도메인 구성 정보 복원

제어 도메인에서 저장된 논리 도메인 구성 정보를 복원하려면 아래 나타난 바와 같이 XSCF 펌웨어의 setdomainconfig 명령을 실행합니다.

```
XSCF> setdomainconfig -p ppar_id [-i index]
```

대상 물리 분할을 -p ppar_id에 지정합니다. Ppar_id의 경우 물리 분할의 PPAR-ID를 0

~ 15의 값으로 지정할 수 있습니다. 구성 정보의 색인 번호를 -i index에 지정합니다. 생략되어 있으면 저장된 구성 정보의 목록을 확인하는 동안 색인 번호를 대화형으로 지정할 수 있습니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오. 해당 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **setdomainconfig** 명령을 실행하여 논리 도메인을 다시 시작하는 데 사용되는 구성 정보를 지정합니다.
   다음에는 저장된 구성 정보의 목록을 확인하는 동안 PPAR-ID 0의 논리 도메인 구성을 대화형으로 지정하는 예가 나타나 있습니다.

```
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:'8/9/2012 12:43:56 PM'
------------------------------------------------------------------------------
Select Index of Using config_name:3
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "ldm-set1".
Continue? [y|n] :y
XSCF>
```

다음에는 PPAR-ID 0에 대해 색인 번호 1을 지정하여 구성 정보를 지정하는 예가 나타나 있습니다.

```
XSCF> setdomainconfig -p 0 -i 1
Index       :1
config_name :ldm-set2
domains     :8
date_created:'2012-08-08 11:34:56'
------------------------------------------------------------------------------
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "ldm-set2".
```

```
Continue? [y|n] : y
XSCF>
```

공장 기본값으로 논리 도메인 복원

제어 도메인에서 저장된 논리 도메인 구성 정보를 복원하려면 아래 나타난 바와 같이 XSCF 펌웨어의 setdomainconfig 명령을 실행합니다.

```
XSCF> setdomainconfig -p ppar_id -c default
```

대상 물리 분할을 -p ppar_id에 지정합니다. Ppar_id의 경우 물리 분할의 PPAR-ID를 0 ~ 15의 값으로 지정할 수 있습니다. 논리 도메인 구성을 공장 기본 상태로 복원하려면 -c default를 지정합니다.

작동 절차

1. 해당 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다.
   XSCF에 로그인 방법은 "4.1 XSCF 쉘에 로그인"을 참조하십시오. 해당 사용자 계정으로 XSCF에 이미 로그인했으면 다음 단계로 이동합니다.
2. **setdomainconfig** 명령을 실행하여 논리 도메인을 다시 시작하는 데 사용되는 구성 정보를 지정합니다.
   다음에는 PPAR-ID 0의 논리 도메인 구성을 공장 기본값으로 복원하는 예가 나타나 있습니다.

```
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>
```

15.9 하드 디스크 내용 저장/복원

하드 디스크 고장 등으로 인한 중요 데이터의 손실이 없도록 정기적으로 하드 디스크의 내용을 백업해야 합니다.

SPARC M10 시스템은 RAID 기능을 사용하는 디스크 중복 구성을 지원합니다. 디스크 중복 구성은 시스템 작동의 신뢰성을 높여줍니다.

다발성 디스크 고장으로 인한 데이터 손실의 대응 차원에서 주기적으로 하드 디스크의 내용을 백업해야 합니다.

작동 중인 시스템에 적합한 백업 방법을 찾아 구현해야 합니다. 더욱이, 하드 디스크 내용의 저장 및 백업 방법은 구현하는 백업 방법에 따라 달라집니다. 구현하는 백업 방법

에 따라 적합한 방법을 적용합니다.

15.10 하이퍼바이저의 덤프 파일 수집

이 절에는 하이퍼바이저의 덤프 파일을 수집하기 위한 설정 방법이 설명되어 있습니다.

15.10.1 하이퍼바이저 덤프의 기본 정보

하이퍼바이저는 하드웨어 고장 또는 소프트웨어 오류로 인해 중단될 수 있습니다. 하이퍼바이저가 중단되면 하이퍼바이저 정보는 덤프 파일로서 저장됩니다.
이를 하이퍼바이저 덤프 기능이라고 합니다.
수집된 덤프 파일은 문제를 진단하는 데 소중한 정보가 될 수 있습니다.

덤프 파일 수집 시 시스템은 공장 기본 구성으로 일시적으로 다시 시작됩니다. 덤프 파일이 정상적으로 수집되면 시스템은 수집 전에 사용된 구성으로 다시 시작됩니다.

덤프 파일은 제어 도메인에서 수집되며 다음의 파일 이름이 할당됩니다. 최대 8개 파일이 수집될 수 있습니다.

- 저장 디렉토리:
  /var/opt/SUNWldm
- 파일 이름:
  hvdump.x.gz
  x: 0 ~ 7의 정수가 자동 할당됩니다.

다음 하위 절에는 하이퍼바이저 덤프 기능에 사용되는 명령이 설명되어 있습니다.

15.10.2 하이퍼바이저 덤프 기능에 사용되는 명령

하이퍼바이저 덤프 활성화/비활성화

Oracle VM Server for SPARC의 ldm set-hvdump 명령을 사용하여 하이퍼바이저 덤프를 설정합니다.

```
#primary ldm set-hvdump [hvdump=on|off] [hvdump-reboot=on|off]
```

Hvdump는 하이퍼바이저 덤프 기능의 활성화 여부를 지정합니다. On을 지정하여 기능을 활성화하고 off를 지정하여 비활성화합니다. 이 기능은 기본적으로 활성화됩니다(on).

Hvdump-reboot는 덤프 파일 수집 후 시스템을 수집 이전에 사용된 구성으로 다시 시작할 것인지 그 여부를 지정합니다. On을 지정하여 다시 시작하고 off를 지정하여 다시 시작하지 않습니다. 시스템은 기본적으로 다시 시작되지 않습니다(off). Off로 설정되면 시스템은 덤프 파일 수집 후 공장 기본 구성으로 정지합니다.

노트 - 하이퍼바이저 덤프 기능이 꺼져 있는 동안에는 Oracle Solaris가 이전 도메인 구성으로 시작될 수 없습니다. 이전 도메인 구성으로 시작하려면 먼저 PPAR의 전원을 꺼야 합니다. XSCF 펌웨어에서 poweroff 명령을 실행하거나 Oracle Solaris에서 "shutdown -i5"를 실행한 후 XSCF에서 poweron 명령을 실행하여 PPAR을 부팅하십시오.

하이퍼바이저 덤프 설정 표시

ldm list-hvdump 명령을 사용하여 하이퍼바이저 덤프 설정을 표시합니다.

```
primary# ldm list-hvdump
```

다음 정보가 표시됩니다.

[hvdump]: 하이퍼바이저 덤프 기능의 활성화 여부. 활성화되면 on이 표시됩니다. 비활성화되면 off가 표시됩니다.

[hvdump-reboot]: 덤프 파일 생성 후 시스템의 다시 시작 여부. 다시 시작되면 on이 표시됩니다. 다시 시작되지 않으면 off가 표시됩니다.

노트 - 덤프 파일 수집이 정상적으로 종료되지 않은 경우 "Pending hvdump exists" 또한 표시됩니다.

작동 절차

1. **XSCF** 콘솔에서 대상 제어 도메인 콘솔로 전환합니다.
   제어 도메인 콘솔로의 전환 방법과 관련된 자세한 내용은 "4.3 XSCF 쉘에서 제어 도메인 콘솔로 전환"을 참조하십시오.

   대상 제어 도메인 콘솔로 이미 전환했으면 다음 단계로 이동합니다.

2. 하이퍼바이저 덤프 기능을 설정합니다.
   다음 예에서는 하이퍼바이저 덤프 기능을 활성화하고 덤프 파일 수집 후 제어 도메인이 다시 시작되어야 하는지 지정합니다.

```
primary# ldm set-hvdump hvdump=on hvdump-reboot=on
```

3. 하이퍼바이저 덤프 기능 설정을 표시합니다.
   다음 예에는 하이퍼바이저 덤프 기능이 활성화되고 덤프 파일 수집 후의 다시 시작이 활성화됨이 나타나 있습니다.

```
#primary ldm list-hvdump
hvdump=on
hvdump-reboot=on
```

15.10.3 하이퍼바이저 덤프 사용 시 주의 사항

하이퍼바이저 덤프 기능을 사용할 때 다음에 유의합니다.

- 덤프 파일의 수집을 위한 디렉토리가 다음 상태 가운데 하나에 있으면 하이퍼바이저에 오류가 발생하더라도 덤프 파일이 수집되지 않습니다.
  - 8개 덤프 파일이 이미 있습니다.
  - /var/opt/SUNWldm 디렉토리의 실행 공간이 부족합니다.

  덤프 파일의 수집 요구 사항을 충족하도록 덤프 파일 수와 디스크 용량에 대해서 덤프 파일 수집 디렉토리를 평소 확인합니다.
- 위와 같은 이유로 덤프 파일이 수집되지 않으면 덤프 처리가 정지됩니다. 문제 해결 후 처리를 다시 시작하려면 ldm start-hvdump 명령을 실행합니다. ldm start-hvdump 명령을 실행하지 않고 제어 도메인을 다시 시작하면 덤프 파일이 수집되지 않고 로깅된 하이퍼바이저 정보가 삭제됩니다.
- ldm hvdump-reboot가 on으로 설정되더라도 OpenBoot PROM 환경 변수 자동 부팅이 off이면 시스템이 ok 프롬프트에서 다시 시작되지 않고 정지됩니다.
- 제어 도메인이 의도와 달리 공장 기본 상태(공장 기본값)로 시작되면 하이퍼바이저 덤프 처리가 완료되지 않을 수도 있습니다. ldm list-hvdump 명령을 실행하여 덤프 파일이 수집되었는지 확인합니다.

  다음 예에는 덤프 파일의 수집 실패가 나타나 있습니다.

```
primary# ldm list-hvdump
hvdump=on
hvdump-reboot=on
Pending hvdump exists
```

15.11 공장 기본 상태로 서버 복귀

이 절에는 SPARC M10 시스템을 공장 기본 상태로 복귀시키는 방법이 설명되어 있습니다.
SPARC M10 시스템 캐비닛의 XSCF 설정 정보에 대한 백업 데이터 또는 XSCF 장치의 XSCF 설정 정보를 공장 기본 설정으로 복원하려면 XSCF 쉘에서 initbb 또는 restoredefaults 명령을 실행합니다.

주의 - 명령을 실행하면 사용자 정의 XSCF 장치 설정 정보와 오류 정보 또는 각 캐비닛의 XSCF 백업 정보가 삭제됩니다.

15.11.1 초기화 명령 이해

initbb 및 restoredefaults 명령 각각의 역할은 다음과 같습니다.

- **restoredefaults** 명령
  이 명령은 마스터 캐비닛을 초기화합니다. 이 명령은 XSCF 장치 설정 정보와 백업 정보 둘 모두를 초기화하거나 XSCF 장치 설정 정보만 초기화합니다.
- **initbb** 명령
  이 명령은 마스터 XSCF에서 마스터 캐비닛 이외의 다른 캐비닛과 관련된 정보를 초기화합니다. 이 명령은 XSCF가 1개인 시스템에는 사용할 수 없습니다.

노트 - XSCF 장치 또는 다른 시스템 용도의 XSCF 장치가 포함된 FRU를 사용할 때는 restoredefaults 명령으로 XSCF 장치 설정 정보만 초기화합니다. 이 경우 초기화된 FRU의 교체 없이 입력 전원을 차단/공급할 때 마스터 캐비닛에 남아 있는 백업 정보를 사용하여 XSCF 장치 설정 정보를 복원합니다.

15.11.2 서버 초기화

XSCF가 1개인 시스템

restoredefaults 명령을 사용하여 서버를 초기화합니다.

작동 절차

1. **XSCF**를 직렬로 연결합니다**.**
2. **XSCF**에 로그인합니다**.**
3. **poweroff -a** 명령을 실행하여 시스템 전체의 전원을 공급합니다**.**
4. **restoredefaults** 명령을 실행하여 캐비닛**(XSCF** 장치 설정 정보와 백업 정보**)**을 초기화하거나 **XSCF** 장치 설정 정보를 초기화합니다**.**

노트 - restoredefaults(8) 명령의 옵션 지정 방법과 주의 사항은『SPARC M10 Systems XSCF Reference Manual』및 설명서 페이지를 참조하십시오.

XSCF가 여러 개인 시스템

초기화 전제 조건은 다음과 같습니다.

- 캐비닛은 XSCF 네트워크를 통해 연결됩니다.
- 초기화할 캐비닛의 BB-ID와 동일한 PPAR-ID를 갖는 물리 분할이 실행되는 경우 이 물리 분할의 전원을 차단합니다.
- 초기화할 캐비닛의 PSB는 시스템 보드 풀 상태에 있어야 합니다.
- 초기화할 캐비닛의 PSB는 어떠한 PPAR에도 속해서는 안 됩니다.
- 마스터 이외의 크로스바 박스를 초기화하려면 poweroff -a 명령을 실행하여 시스템

전체의 전원을 차단합니다.

작동 절차

1. **XSCF**를 직렬로 연결합니다**.**
2. 마스터 **XSCF**에 로그인합니다**.**
3. **BB-ID**를 지정하고 **initbb** 명령을 실행하여 대상 캐비닛을 초기화합니다**.**
   마스터 이외의 대상 캐비닛에 대해 이 단계를 수행합니다.

   다음 번 마스터 캐비닛을 초기화하는 경우 다음 절차를 수행합니다.
4. 모든 캐비닛에서 **XSCF DUAL** 제어 케이블 및 **XSCF BB** 제어 케이블을 제거하여 다른 캐비닛에서 마스터 캐비닛을 분리합니다**.**
5. **poweroff -a** 명령을 실행하여 시스템 전체의 전원을 공급합니다**.**
6. **restoredefaults** 명령을 실행하여 캐비닛**(XSCF** 장치 설정 정보와 백업 정보**)**을 초기화하거나 **XSCF** 장치 설정 정보를 초기화합니다**.**

노트 - initbb(8) 및 restoredefaults(8) 명령의 옵션 지정 방법과 주의 사항은『SPARC M10 Systems XSCF Reference Manual』및 설명서 페이지를 참조하십시오.

노트 - 케이블 연결 방법은『SPARC M10 시스템 설치 안내서』의 "4장 빌딩 블록 연결 구성"을 참조하십시오.

노트 - 이 명령의 지원 정보는『SPARC M10 시스템 제품 노트』를 참조하십시오.

16장

시스템 상태의 확인

이 장에는 시스템을 구성 또는 작동할 때 시스템 하드웨어 구성/상태와 물리 분할 구성/상태를 확인하는 방법이 설명되어 있습니다.

- 시스템 구성/상태의 확인
- 물리 분할 확인

16.1 시스템 구성/상태의 확인

16.1.1 시스템 구성/상태와 관련된 항목 및 명령의 확인

표 16-1에는 시스템 구성/상태를 확인하기 위한 항목과 XSCF 쉘 명령이 나열되어 있습니다.

각 항목의 자세한 내용은 다음 절을 참조하십시오.

표 16-1 구성 및 상태의 확인 명령

확인 항목	관련된 명령
장착된 구성요소의 확인 ■ 시스템에 장착된 모든 부품 ■ 모드 스위치 상태	showhardconf(8)
고장/성능 저하된 구성요소의 확인	showstatus(8)
시스템 환경 정보의 확인 ■ 주변 온도 ■ 전압 ■ 팬 속도 레벨 ■ 소비 전력 ■ 공기 배출량	showenvironment(8)
PCI 확장 장치 설정 정보의 확인	ioxadm(8)

16.1.2 시스템에 장착된 구성요소의 확인

showhardconf 명령을 사용하여 시스템에 장착된 모든 구성요소와 그 상태를 확인할 수 있습니다. 또한 문제 부품이 별표(*)로 표시됩니다. 시스템 관리자는 구성요소의 구성, 장착된 장치 수, 모드 스위치 상태 및 현장 대체 가능 장치(FRU)를 파악할 수 있습니다.

작동 절차

1. **showhardconf** 명령을 실행하여 구성요소의 구성과 모드 스위치 상태를 확인합니다.
   다음에는 SPARC M10-1 시스템의 예가 나타나 있습니다.

```
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. **showhardconf** 명령을 실행하여 장착된 **FRU**의 수를 확인합니다.
   다음에는 SPARC M10-1 시스템의 예가 나타나 있습니다.

```
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     |
+-----------------------------------+------------+
```

구성요소 정보

표 16-2에는 개별 구성요소에 대해 표시되는 정보 항목이 나열되어 있습니다. 구성요소의 계층 구조와 관련된 자세한 내용은 showhardconf로 확인할 수 있습니다.

표 16-2 구성요소 정보

구성요소	설명
SPARC M10-4/M10-4S 정보	장치 번호, 상태, 역할, 버전, 일련 번호, FRU 번호 역할은 마스터, 스탠바이 또는 슬레이브로서 표시됩니다.
CPU 메모리 장치(하위) 정보 (SPARC M10-4/M10-4S)	상태, 버전, 일련 번호, FRU 번호, 메모리 용량
CPU 메모리 장치(상위) 정보 (SPARC M10-4/M10-4S)	상태, 버전, 일련 번호, FRU 번호, 메모리 용량
마더보드 장치 정보 (SPARC M10-1)	상태, 버전, 일련 번호, FRU 번호, 메모리 용량
CPU 정보	장치 번호, 상태, 버전, 일련 번호, CPU 작동 주파수, CPU 유형, CPU 코어 수, CPU 스트랜드 수
메모리 정보	장치 번호, 상태, 코드, 유형(고유 ID), 용량
PCI 정보	장치 번호, 상태, 이름 속성, 벤더 ID, 장치 ID, 하위 시스템 벤더 ID, 하위 시스템 ID, VPD 번호, 연결, PCI 확장 장치 정보
PCI 확장 장치 정보	장치 번호, 상태, 버전, 일련 번호, FRU 번호, IO 보트 정보: 상태, 일련 번호, 유형, FRU 번호 링크 보드 정보: 상태, 버전, 일련 번호, FRU 번호 PCI 정보: 장치 번호, 상태, 이름 속성, 벤더 ID, 장치 ID, 하위 시스템 벤더 ID, 하위 시스템 ID, VPD 번호 팬 백플레인(FANBP) 정보: 장치 번호, 상태, 일련 번호, FRU 번호 전원 공급 장치 백플레인(PSUBP) 정보: 장치 번호, 상태, 일련 번호, FRU 번호 전원 공급 장치(PSU) 정보: 장치 번호, 상태, 일련 번호, FRU 번호 팬 장치 정보; 장치 번호, 상태, FRU 번호
크로스바 장치(XBU) 정보 (SPARC M10-4/M10-4S)	장치 번호, 상태, 버전, 일련 번호, FRU 번호,
스루 보드 장치(THU) 정보 (SPARC M10-4/M10-4S)	상태, 버전, 일련 번호, FRU 번호
운영 패널 정보	상태, 버전, 일련 번호, FRU 번호
XSCF 장치 정보	상태, 버전, 일련 번호, FRU 번호
전원 공급 장치 백플레인 (PSUBP) 정보	상태, 버전, 일련 번호, FRU 번호
전원 공급 장치(PSU) 정보	장치 번호, 상태, 일련 번호, FRU 번호, 전원 상태, 전원 공급 유형, 전압 전원 공급 유형은 AC(교류) 또는 DC(직류)로서 표시됩니다.
팬 장치(FANU) 정보	장치 번호, 상태
크로스바 박스(XBBOX) 정보 (SPARC M10-4S)	장치 번호, 상태, 역할, 버전, 일련 번호, FRU 번호

표 16-2 구성요소 정보 (계속)

구성요소	설명
크로스바 백플레인 장치 (XBBPU) 정보 (SPARC M10-4S)	상태, 일련 번호, FRU 번호
XSCF 인터페이스 장치 (XSCFIFU) 정보 (SPARC M10-4S)	상태, 버전, 일련 번호, FRU 번호, 유형

16.1.3 시스템 환경의 확인

showenvironment 명령으로 시스템 내 모든 센서의 값을 표시합니다. 시스템 흡기 온도, 전압 및 팬 속도를 파악하여 시스템 관리자는 시스템 환경에 잘못된 것이 있는지 확인할 수 있습니다. 또한 시스템의 소비 전력과 공기 배출량을 파악하여 설비 관리자는 에너지 절감에 적용할 수 있는 시스템 설치 현장의 부품을 식별할 수 있습니다.

작동 절차

1. **showenvironment** 명령을 실행하여 시스템의 주변 온도와 전압을 확인합니다**.**
   다음에는 흡기 온도의 표시 예가 나타나 있습니다.

```
XSCF> showenvironment
BB#00
    Temperature:30.71C
BB#01
    Temperature:29.97C
```

   다음에는 구성요소 온도의 표시 예가 나타나 있습니다.

```
XSCF> showenvironment temp
BB#00
    Temperature:30.71C
    CMUU:30.71C
       CPU#0:30.71C
       CPU#1:30.71C
    CMUL:30.71C
       CPU#0:30.71C
       CPU#1:30.71C
```

   다음에는 구성요소 전압의 표시 예가 나타나 있습니다.

```
XSCF> showenvironment volt
MBU
    1.0V Power Supply Group:1.010V
    1.8V Power Supply Group:1.700V
    CPU#0
```

```
        1.0V Power Supply Group:1.000V
    CPUM#1-CHIP#0
        1.0V Power Supply Group:1.000V
MEMB#0
    1.2V Power Supply Group:1.200V
    1.8V Power Supply Group:1.700V
    2.5V Power Supply Group:2.500V
:
```

주변 온도 및 팬 속도 레벨

팬 속도 레벨은 고도 설정과 더불어 주변 온도에 따라 달라집니다. 팬 속도 레벨의 경우 레벨 번호가 클수록 팬 속도가 빠릅니다.

표 16-3에는 showenvironment 명령에 의해 표시되는 구성된 고도와 주변 온도에 해당되는 팬 속도 레벨이 나열되어 있습니다.

표 16-3 고도와 주변 온도에 해당되는 팬 속도 레벨

팬 속도 레벨	고도별 주변 온도			
	500m 이하	501 ~ 1,000m	1,001 ~ 1,500m	1,501 ~ 3,000m
고속 (레벨-3 ->레벨-4)	31℃ 이상	29℃ 이상	27℃ 이상	25℃ 이상
고속 (레벨-4 ->레벨-3)	29℃ 이하	27℃ 이하	25℃ 이하	23℃ 이하
중속 (레벨-2 ->레벨-3)	26℃ 이상	24℃ 이상	22℃ 이상	20℃ 이상
중속 (레벨-3 ->레벨-2)	24℃ 이하	22℃ 이하	20℃ 이하	18℃ 이하
저속 (레벨-1 ->레벨-2)	22℃ 이상	20℃ 이상	18℃ 이상	16℃ 이상
저속 (레벨-2 ->레벨-1)	20℃ 이하	18℃ 이하	16℃ 이하	14℃ 이하

작동 절차

1. **showenvironment 명령을 실행하여 팬 속도 레벨을 확인합니다.**
   다음에는 전원 공급 장치 및 팬 장치의 팬 속도 레벨에 대한 표시 예가 나타나 있습니다.

```
XSCF> showenvironment Fan
BB#00
    FANU#0:Low speed
        FAN#0: 4101rpm
    PSU#0
        PSU#0:Low speed
           PSU#0: 3879rpm
```

```
            PSU#0: 3835rpm
    PSU#1
        PSU#1:Low speed
            PSU#1: 3924rpm
            PSU#1: 3970rpm
```

소비 전력 및 공기 배출량

시스템의 소비 전력과 공기 배출량을 표시하려면 전력 모니터 기능 및 공기량 표시기를 사용합니다. 전력 모니터 기능 및 공기량 표시기를 사용하여 작동 중인 시스템이 실제로 소비하는 전력량과 공기 배출량을 평소 확인할 수 있습니다.

소비 전력을 표시하려면 `showenvironment power` 명령을 사용합니다. 결과로서 시스템의 소비 전력 값, 캐비닛 등의 최대 소비 전력 값(허용 AC 소비 전력) 및 실제 소비 전력 값(실제 AC 소비 전력)이 표시됩니다. 전원 공급 유형이 DC이면 "...DC power..."가 대신 표시됩니다.

공기 배출량을 표시하려면 `showenvironment air` 명령을 사용합니다. 또한 SNMP 에이전트 기능을 사용하여 소비 전력 및 공기 배출량 관련 정보를 가져올 수도 있습니다.

SNMP 에이전트 기능을 통해 소비 전력 및 공기 배출량 정보를 가져오려면 최신 XSCF 확장 MIB 정의 파일을 SNMP 관리자에 설치합니다.

XSCF 확장 MIB 정의 파일을 가져오기 위한 위치는『SPARC M10 시스템 제품 노트』또는 펌웨어 다운로드 사이트의 MIB 정의 파일 정보를 참조하십시오.

노트 - 다음의 경우 소비 전력 및 공기 배출량 값이 MIB 정보, `showenvironment power` 명령, `showenvironment air` 명령 및 XSCF 웹을 통해 올바로 표시되지 않을 수도 있습니다. 1분 후 값을 다시 확인합니다.

- 시스템의 전원 공급/차단 동안 또는 전원 공급/차단이 완료된 후 잠시 동안
- 전원 공급 장치의 활성 교체 동안 또는 활성 교체가 완료된 후 잠시 동안

노트 - 소비 전력 및 공기 배출량에는 PCI 확장 장치와 주변 I/O 장치의 정보가 포함되지 않습니다.

작동 절차

1. **showenvironment** 명령을 실행하여 시스템의 공기 배출량을 확인합니다.
   다음에는 SPARC M10-1 시스템의 공기 배출량 예가 나타나 있습니다.

```
XSCF> showenvironment air
BB#00
    Air Flow:53CMH
```

2. **showenvironment(8)** 명령을 실행하여 시스템의 소비 전력을 확인합니다.
   다음 예에는 시스템의 최대 공급 전력 값, 최소 소비 전력 값 및 최대 소비 전력 값

과 캐비닛의 최대 소비 전력 값 및 실제 소비 전력 값이 순서대로 나타나 있습니다.

```
XSCF> showenvironment power
Power Supply Maximum      :1000W
Installed Hardware Minimum:718W
Peak Permitted            :3725W
BB#00
    Permitted AC power consumption:1000W
    Actual AC power consumption   :38W
```

노트 - 전력 모니터 및 공기량 표시기가 측정하는 값은 기준 값입니다. 이 값은 시스템 부하에 따라 달라집니다.

16.1.4 고장/성능 저하된 구성요소의 확인

showstatus 명령을 사용하여 시스템을 구성하는 FRU 가운데 고장이나 성능 저하된 장치 또는 구성요소의 일부를 확인할 수 있습니다. 상태가 비정상인 장치 또는 구성요소의 일부는 별표(*)로 표시됩니다.

표 16-4에 나타난 바와 같이 5개 종류의 상태가 있습니다.

표 16-4 구성요소 상태

구성요소	의미
고장	문제가 되는 부품이 고장이어서 장치가 작동하지 않습니다.
성능 저하	장치가 작동합니다. 장치의 일부 구성요소가 고장 또는 성능 저하되거나 이 구성요소에서 일부 오류가 감지되어 장치가 고장 상태를 보이더라도 정상적으로 작동합니다.
구성 취소	장치가 정상이지만 구성 오류나 환경 오류 또는 다른 장치의 성능 저하로 인해 성능 저하됩니다.
유지 관리	장치가 서비스 모드에 있습니다. deletefru, replacefru 또는 addfru 명령이 실행 중입니다.
정상	정상.

작동 절차

1. **showstatus 명령을 실행하여 구성요소 상태를 확인합니다.**
   상태가 비정상인 장치는 별표(*)로 표시됩니다.

   다음 예에는 고장으로 인해 BB#00 CPU 메모리 장치(하위)의 메모리와 CPU는 물론 XBBOX#80의 PSU도 성능 저하됨이 나타나 있습니다.

```
XSCF> showstatus
   BB#00;
      CMUL Status:Normal;
*        CPU#0 Status:Faulted;
*        MEM#00A Status:Faulted;
   XBBOX#80;
*     PSU#0 Status:Faulted;
```

다음 예에는 고장으로 인해 마더보드 장치의 메모리가 성능 저하됨이 나타나 있습니다.

```
XSCF> showstatus
   MBU Status:Normal;
*      MEM#0A Status:Faulted;
```

다음 예에는 크로스바 장치의 성능 저하로 인해 CPU 메모리 장치가 성능 저하됨이 나타나 있습니다.

```
XSCF> showstatus
   BB#00
       CMUU Status:Normal;
*         CPU#1 Status:Deconfigured;
*      XBU#0 Status:Degraded;
```

다음 예에는 장치가 성능 저하되지 않음이 나타나 있습니다.

```
XSCF> showstatus
No failures found in System Initialization.
```

노트 - 고장/성능 저하된 구성요소의 고장 및 성능 저하 정보는 문제가 되는 부품을 교체하여 삭제할 수 있습니다.
부품 교체 작업은 현장 엔지니어에게 문의하십시오.

16.1.5 PCI 확장 장치 상태 표시

이 절에는 시스템에 연결된 PCI 확장 장치, PCI 확장 장치의 부품, 시스템 내장 PCI 슬롯에 장착된 다운링크 카드 및 PCI 확장 장치의 상태를 확인하는 방법이 설명되어 있습니다.

ioxadm 명령을 사용하여 PCI 확장 장치의 상태와 설정을 확인할 수 있습니다.

노트 - PCI 확장 장치 하드웨어 구성은『PCI Expansion Unit for SPARC M10 Systems Service Manual』의 "2장 PCI 확장 장치의 구성요소 이해"를 참조하십시오. ioxadm(8) 명령의 자세한 내용 또는 사용 예는 명령 설명서 페이지 및『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

표 16-5에는 PCI 확장 장치와 관련된 용어가 설명되어 있습니다.

표 16-5 PCI 확장 장치와 관련된 용어

용어	설명
호스트 경로	장치 경로. 장치 번호가 뒤에 오는 장치 이름은 1개 부품 단위로서 사용되며 호스트 경로는 부품의 계층적 위치를 나타냅니다. (예: BB#00-PCI#0)
다운링크 카드 경로	다운링크 카드는 캐비닛 내장 PCI 슬롯에 장착되고 PCI 확장 장치에 연결됩니다. PCI 확장 장치는 1개 또는 2개 다운링크 카드에 연결됩니다. 어떤 다운링크 카드가 PCI 확장 장치에 연결되는지는 부품의 계층적 위치를 사용하여 다운링크 카드 경로로 나타냅니다. (예: BB#00-PCI#0)

표시 정보

표 16-6에는 ioxadm 명령을 실행하여 표시하는 정보의 개요가 설명되어 있습니다.

표 16-6 PCI 확장 장치의 표시 정보

표시 항목	표시 정보
목록 표시 (list)	■ PCI 확장 장치와 캐비닛 내장 슬롯에 장착된 다운링크 카드 사이 경로 목록 ■ PCI 슬롯에 장착된 카드의 자세한 정보 ■ PCI 확장 장치의 자세한 정보 ■ PCI 확장 장치 내 FRU(I/O 보트, 전원 공급 장치)의 자세한 정보 표시 정보에는 전원 공급 장치의 유형, 펌웨어 버전, 일련 번호, 부품 번호 및 상태가 포함됩니다.
환경 표시 (env)	■ 지정된 PCI 확장 장치 또는 다운링크 카드의 센서 측정 값으로 표시되는 환경 조건 ■ PCI 확장 장치 내 FRU 또는 PCI 슬롯에 장착된 카드의 환경 정보 표시 정보에는 다음이 포함됩니다. ■ 전류(A) ■ 전압(V) ■ 팬 속도(RPM) ■ 온도(C) ■ LED 상태 ■ 스위치
로케이터 LED 표시 (locator)	■ 지정된 PCI 확장 장치 및 PCI 확장 장치 내 각 부품의 로케이터 LED 상태 로케이터 LED 상태는 다음 가운데 하나가 됩니다. ■ 점멸 ■ 켜짐 ■ 꺼짐

작동 절차

다음에는 PCI 확장 장치, I/O 보트, 링크 카드 또는 전원 공급 장치 관련 정보 목록의 표시 방법이 설명되어 있습니다.

1. **ioxadm** 명령을 실행하여 **PCI** 확장 장치 및 카드를 확인합니다**.**

다음에는 PCI 확장 장치 및 다운링크 카드의 목록 표시 예가 나타나 있습니다.

```
XSCF> ioxadm list
PCIBOX      Link
PCIBOX#0033 BB#00-PCI#1
PCIBOX#12B4 BB#01-PCI#0
```

다음에는 PCI 확장 장치의 표시 예가 나타나 있습니다.

```
XSCF> ioxadm list PCIBOX#12B4
PCIBOX      Link
PCIBOX#12B4 BB#01-PCI#0
```

다음에는 명령으로 호스트 경로와 세부 출력 모드를 지정하고 헤더를 숨기는 카드의 표시 예가 나타나 있습니다.

```
XSCF> ioxadm -A -v list BB#00-PCI#1
BB#00-PCI#1 F20 - 000004 5111500-01 On
```

작동 절차

다음에는 센서 측정 값으로 환경을 표시하는 방법이 설명되어 있습니다.

1. **ioxadm** 명령을 실행하여 환경 정보를 확인합니다.
   다음에는 온도, 전압, 전류 , 팬 속도 등에 대한 센서 측정 값의 표시 예가 나타나 있습니다.

```
XSCF> ioxadm env -te PCIBOX#A3B5
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
```

다음에는 1개 링크와 관련된 모든 센서 측정 값의 표시 예가 나타나 있습니다.

```
XSCF> ioxadm -A env BB#00-PCI#1
BB#00-PCI#1 LINK On - LED
BB#00-PCI#1 MGMT On - LED
```

작동 절차

다음에는 PCI 확장 장치 및 지정된 부품의 로케이터 LED 상태를 표시하는 방법이 설명되어 있습니다.

1. **ioxadm** 명령을 실행하여 **PCI** 확장 장치의 상태를 확인합니다**.**
   다음에는 PCI 확장 장치의 로케이터 LED 상태에 대한 표시 예가 나타나 있습니다.

```
XSCF> ioxadm locator PCIBOX#12B4
Location            Sensor     Value Resolution Units
PCIBOX#12B4         LOCATE     Blink -          LED
```

16.2 물리 분할 확인

16.2.1 물리 분할 및 논리 도메인 구성/상태와 관련된 항목 및 명령의 확인

표 16-7에는 물리 분할 구성/상태, 빌딩 블록 상태 및 논리 도메인 상태를 확인하기 위한 항목과 XSCF 쉘 명령이 나열되어 있습니다. 각 항목의 자세한 내용은 다음 절을 참조하십시오.

표 16-7 구성 및 상태의 확인 명령

확인 항목	관련된 명령
물리 분할 구성 목록(PCL)의 확인 ■ PPAR-ID ■ LSB 번호 ■ PSB 번호 ■ 구성 정책 ■ I/O의 사용 가능 여부 ■ 메모리의 사용 가능 여부	showpcl(8)
물리 분할 작동 상태의 확인	showpparstatus(8), showpcl(8)
시스템 보드 설정의 확인 ■ 위치(시스템 보드, CPU) ■ 메모리 미러 모드	showfru(8)
시스템 보드 상태의 확인	showboards(8)

표 16-7 구성 및 상태의 확인 명령 (계속)

확인 항목	관련된 명령
논리 도메인 상태의 확인	showdomainstatus(8) Oracle VM Server for SPARC 명령

노트 - 물리 분할 설정/구성/상태와 물리 분할에서 논리 도메인을 구성하는 방법과 관련된 자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』를 참조하십시오.

16.2.2 물리 분할 구성의 확인

showpcl 및 setpcl 명령은 각 물리 분할 또는 물리 분할을 구성하는 각 LSB마다 설정되는 물리 분할 구성 목록(PCL)을 각각 표시 및 구성합니다. 시스템 관리자는 LSB를 물리 분할에 통합할 때 PCL을 확인하고 설정을 할 수 있습니다.

showpcl 명령을 사용하여 지정된 물리 분할의 PCL을 확인할 수 있습니다.

표 16-8에는 물리 분할과 관련된 용어가 설명되어 있습니다.

표 16-8 물리 분할과 관련된 용어

용어	설명
PSB	PSB는 Physical System Board(물리적 시스템 보드)를 나타냅니다. PSB는 1개 SPARC M10 시스템 캐비닛에 장착된 물리 구성요소(CPU, 메모리 및 I/O)로 구성되어 있습니다. SPARC M10-1의 경우 물리적 시스템 보드는 마더보드 장치를 나타냅니다. SPARC M10-4/M10-4S의 경우 물리적 시스템 보드는 CPU 메모리 장치를 나타냅니다. 하드웨어의 확장/제거/교체를 위한 유지 관리 시 물리적 시스템 보드를 캐비닛을 나타내는 장치로서 사용할 수 있습니다.
LSB	LSB는 Logical System Board(논리적 시스템 보드)를 나타냅니다. PSB에 할당되는 논리 장치 이름. 각 물리 분할마다 논리적 시스템 보드 세트가 할당되어 있습니다. PSB 번호를 물리 분할의 논리적 시스템 보드에 할당하면 시스템 전체가 이 보드를 시스템 보드로서 인식할 수 있습니다. LSB 번호는 물리 분할에 메모리와 같은 자원 할당을 제어하는 데 사용됩니다.
물리 분할 구성	시스템 하드웨어 자원을 소프트웨어 작동을 위한 독립 장치로 분할하는 것을 말합니다. 물리 분할은 군집 형태의 PSB로 되어 있으며 시스템은 하나 또는 여러 물리 분할로 구성됩니다. 다음과 같이 XSCF를 사용하여 물리 분할을 구성합니다. 1. LSB 번호를 PSB에 할당합니다. 2. PSB를 물리 분할(PPAR)에 할당합니다. 3. 물리 분할은 LSB 자원과 LSB 번호로 작동합니다.
물리 분할 구성 목록 (PCL)	각 물리 분할 또는 물리 분할을 구성하는 각 LSB마다 구성된 하드웨어 자원 정보를 말합니다. PCL은 setpcl 및 showpcl 명령을 사용하여 구성 및 표시할 수 있습니다.

표 16-8 물리 분할과 관련된 용어 (계속)

용어	설명
구성 정책	하드웨어 초기 진단에서 오류를 감지할 때 성능 저하시키는 논리 자원 장치를 각 물리 분할마다 지정할 수 있습니다. 구성 정책에서는 시스템 보드 또는 개별 자원을 성능 저하 장치로서 지정합니다.
I/O 비활성화(no-io)	특정 물리 분할에 대해 시스템 보드에서 I/O 장치의 논리적 사용을 비활성화하는 시스템 보드 구성을 말합니다. 이는 더 적은 하드웨어 자원으로 DR 기능을 활성화합니다.
메모리 비활성화 (no-mem)	특정 물리 분할에 대해 시스템 보드에서 메모리의 논리적 사용을 비활성화하는 시스템 보드(PSB) 구성을 말합니다.
PSB 상태	각 PSB의 상태를 나타냅니다. 시스템 보드 전원 상태(전원), 진단 상태(테스트), 할당된 상태(할당), 연결 상태(연결), 작동 상태(구성) 및 성능 저하 상태(고장). 물리 분할을 다시 구성할 때 진행률을 확인할 수 있습니다. PSB 상태 정보는 showpcl 및 showboards 명령을 사용하여 참조할 수 있습니다.
시스템 보드 풀(SP)	어떠한 물리 분할에도 속하지 않는 시스템 보드의 상태를 말합니다. CPU 또는 메모리 부하가 많은 물리 분할의 경우 시스템 보드 풀 상태의 시스템 보드를 가져와 이 물리 분할에 추가할 수 있습니다. 이러한 시스템 보드는 불필요할 때 시스템 보드 풀 상태로 되돌릴 수 있습니다.

PCL은 단일 LSB의 정의 목록입니다. 최대 16개 LSB의 LSB 정보(PCL)를 1개 물리 분할에 대해 구성할 수 있습니다.

표 16-9에는 물리 분할 구성 목록(PCL)의 세부 사항이 설명되어 있습니다.

표 16-9 PCL

용어	설명
PPAR-ID	PPAR의 ID
LSB 번호	LSB 번호
PSB 번호	LSB에 할당된 PSB 번호 동일한 PSB 번호를 동일 물리 분할 내의 다른 LSB에 할당할 수 없습니다.
no-mem (메모리 비활성화 옵션)	참: 메모리가 비활성화됨 거짓: 메모리가 활성화됨(기본값)
no-io (I/O 비활성화 옵션)	참: I/O가 통합되지 않음 거짓: I/O가 통합됨(기본값)
구성 정책	FRU: 성능 저하가 현장 대체 가능 장치(FRU) 단위로 수행됨(기본값) PSB: 성능 저하가 PSB 단위로 수행됨 시스템: 물리 분할 단위. 성능 저하 없이 물리 분할의 전원이 차단됩니다. SPARC M10-1/M10-4 시스템에 대해 구성 정책만 설정할 수 있습니다.
물리 분할 상태	전원의 분리 여부 또는 POST 초기화의 완료 여부와 같은 물리 분할의 작동 상태를 나타냅니다. 정의의 자세한 내용은 showpcl(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

다음에는 물리 분할 구성의 확인 방법이 설명되어 있습니다. 각 실행 예의 의미는 표 16-9를 참조하십시오.

1. **showpcl** 명령을 실행하여 **PCL** 정보를 확인합니다.
   다음에는 PPAR-ID 00에 맞게 구성된 PCL 정보의 표시 예가 나타나 있습니다.

```
XSCF> showpcl -p 0
PPAR-ID    LSB    PSB   Status
00                      Hypervisor Started
           00     00-0
           04     01-0
           08     02-0
           12     03-0
```

   다음에는 PPAR-ID 00에 맞게 구성된 PCL 세부 정보의 표시 예가 나타나 있습니다.

```
XSCF> showpcl -v -p 0
PPAR-ID    LSB    PSB   Status  No-Mem   No-IO   Cfg-policy
00                     Hypervisor Started
                                                 System
           00     -
           01     -
           02     -
           03     -
           04     01-0          False    False
           05     -
           06     -
           07     -
           08     02-0          True     False
           09     -
           10     -
           11     -
           12     03-0          False    True
           13     -
           14     -
           15     -
```

노트 - 물리 분할 구성의 자세한 내용은『SPARC M10 시스템 도메인 구성 안내서』의 "3장 물리 분할 구성"을 참조하십시오.

16.2.3 물리 분할 작동 상태의 확인

showpparstatus 명령을 사용하여 전원 분리 상태 또는 초기화 상태와 같은 물리 분할의 작동 상태를 확인할 수 있습니다.

노트 - 물리 분할 작동 상태의 자세한 정의는 showpparstatus(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

노트 - 물리 분할의 논리 도메인 상태는 showdomainstatus 명령으로 확인할 수 있습니다. 자세한 내용은 "16.2.6 논리 도메인 상태의 확인"를 참조하십시오.

노트 - 물리 분할 상태의 자세한 내용은 『SPARC M10 시스템 도메인 구성 안내서』의 "3장 물리 분할 구성"을 참조하십시오.

작동 절차

다음에는 물리 분할 작동 상태의 확인 방법이 설명되어 있습니다. 상태 옵션을 지정한 showpcl 명령으로 동일한 정보를 가져올 수 있습니다.

1. **showpparstatus 명령을 실행하여 물리 분할 상태를 확인합니다.**
   다음에는 모든 물리 분할의 상태에 대한 표시 예가 나타나 있습니다.

```
XSCF> showpparstatus -a
PPAR-ID PPAR Status
00            Powered Off
01            Initialization Phase
02            Initialization Phase
03            Running
```

16.2.4 시스템 보드 설정의 확인

showfru 명령을 사용하여 시스템 보드(PSB)의 설치 위치와 메모리 미러링 설정을 확인합니다.

PSB로 물리 분할을 구성할 때 다음을 확인할 수 있습니다.

- 시스템 보드 위치
  시스템 보드(PSB)가 장착된 빌딩 블록(BB-ID)의 ID를 확인할 수 있습니다. 위치는 "BB-ID-PSB 번호" 형태로 표시됩니다.

  예 00-0: 빌딩 블록-ID 0의 PSB

- CPU 위치
  CPU가 장착된 시스템 보드 번호와 BB-ID를 확인할 수 있습니다. 위치는 "BB-ID-PSB 번호-CPU 번호" 형태로 표시됩니다. 예 01-0-2: 빌딩 블록-ID 1의 PSB 상 CPU 2

- 메모리 미러 모드
  시스템 보드의 각 CPU 세트에 대한 메모리 미러 모드의 설정 여부를 확인할 수 있습니다.

  예: 메모리 미러 모드가 설정됨

  아니오: 메모리 미러 모드가 설정되지 않음

노트 - 메모리 미러링의 설정/자세한 내용은 "12장 고 신뢰성 시스템 구성"을 참조하십시오.

작동 절차

1. **showfru** 명령을 실행하여 정보 정보를 확인합니다.
   다음에는 모든 장치에 맞게 설정된 정보의 표시 예가 나타나 있습니다.

```
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
:
```

   다음에는 지정된 PSB에 맞게 구성된 정보의 표시 예가 나타나 있습니다.

```
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
```

   다음에는 지정된 CPU에 맞게 구성된 정보의 표시 예가 나타나 있습니다.

```
XSCF> showfru sb 01-0-3
Device   Location    Memory Mirror Mode
sb       01-0
    cpu  01-0-3      yes
```

16.2.5 시스템 보드 상태의 확인

시스템 보드(PSB)는 1개 캐비닛을 구성하는 물리 구성요소(CPU, 메모리 및 I/O)로 이루어져 있습니다. 캐비닛 상태는 시스템 보드 상태와 같습니다.

showboards 명령으로 시스템 보드 상태를 표시합니다. addboard 또는 deleteboard 명령을 실행하여 시스템 보드를 물리 분할에 연결하거나 물리 분할에서 시스템 보드를 분리한 경우 showboards 명령을 사용하여 물리 분할에 시스템 보드 연결/물리 분할에서 시스템 보드 분리 또는 작동 성공/실패와 같은 진행 상태를 확인할 수 있습니다.

showboards 명령을 사용하여 시스템 보드 전원 상태(전원), 진단 상태(테스트), 할당된 상태(할당), 연결 상태(연결), 작동 상태(구성) 및 성능 저하 상태(고장)를 확인할 수 있습니다.

노트 - 시스템 보드 상태의 자세한 정의는『SPARC M10 시스템 도메인 구성 안내서』, showboards(8) 명령 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

작동 절차

다음에는 시스템 보드 상태의 확인 방법이 설명되어 있습니다.

1. **showboards 명령을 실행하여 시스템 보드 상태를 확인합니다.**
   다음에는 모든 시스템 보드의 상태에 대한 표시 예가 나타나 있습니다.

```
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
```

   다음에는 PSB 00-0 세부 정보의 표시 예가 나타나 있습니다.

```
XSCF> showboards 00-0
PSB  PPAR-ID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- ------------ ----------- ---- ---- ---- ------- --------
00-0 00(00)       Assigned    y    y    y    Passed  Normal
```

   다음에는 시스템 보드 풀 상태에 있고 PPAR-ID 00에 대해 정의된 PSB의 표시 예가 나타나 있습니다.

```
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
```

16.2.6 논리 도메인 상태의 확인

showdomainstatus 명령을 사용하여 물리 분할의 제어 도메인에서 Oracle Solaris의 작동 상태, 제어 도메인에서 OpenBoot PROM의 상태 등을 확인할 수 있습니다.

노트 - 논리 도메인 작동 상태의 자세한 정의는 showdomainstatus(8) 명령 설명서 페이지 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오. 또한 Oracle VM Server for SPARC 명령을 사용하여 논리 도메인 상태를 확인할 수도 있습니다. 자세한 내용은 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

작동 절차

다음에는 논리 도메인 작동 상태의 확인 방법이 설명되어 있습니다.

1. **showdomainstatus** 명령을 실행하여 지정된 **PPAR**에 속한 논리 도메인의 작동 상태를 확인합니다.
   다음에는 PPAR-ID 0의 모든 논리 도메인에 대한 작동 상태의 표시 예가 나타나 있습니다.

```
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
```

   다음에는 PPAR-ID 0의 논리 도메인 "guest01"에 대한 작동 상태의 표시 예가 나타나 있습니다.

```
XSCF> showdomainstatus -p 0 -g guest01
Logical Domain Name   Status
guest01               Solaris powering down
```

17장

로그 및 메시지 확인

이 장에는 SPARC M10 시스템에 표시 및 저장되는 로그 및 메시지 유형과 참조 명령이 설명되어 있습니다.

- XSCF로 저장된 로그 확인
- 경고 및 알림 메시지의 확인

17.1 XSCF로 저장된 로그 확인

이 절에는 XSCF 로그 정보의 확인 방법이 설명되어 있습니다.

XSCF 로그 정보는 시스템 문제를 조사하는 데 사용됩니다. 로그 정보는 시스템 관리자, 도메인 관리자 및 현장 엔지니어가 참조할 수 있습니다. 서버 작동 상태, 서버 사용 또는 시스템에 고장이 발생할 경우 로그 정보를 확인하여 무슨 일이 발생했는지 찾아낼 수 있습니다.

17.1.1 로그 유형 및 참조 명령의 확인

시스템에 의해 수집/관리되는 로그에는 고장 정보와 관련된 로그, 이벤트 기록용 로그, 보안과 관련된 로그 및 서버 환경과 관련된 로그가 포함됩니다.

이 로그에는 다음 유형이 포함됩니다.

로그 유형

다음 로그 유형은 시스템에 의해 수집되며 시스템 관리자가 참조할 수 있습니다.

- 고장 정보와 관련된 로그
  - 고장 관리 로그(FM 로그)(*)
  - 오류 로그
  - Syslog(*)
  - 모니터 메시지 로그

  * 이 로그는 Oracle Solaris에서만 참조됩니다. 자세한 내용은 Oracle Solaris 관련

설명서를 참조하십시오.

- 이벤트 기록용 로그
  - 전원 로그
  - 이벤트 로그
  - 콘솔 로그
  - 패닉 로그
  - IPL 로그
- 보안 및 인증과 관련된 로그
  - 감사 로그
  - CoD 로그
- 서버 환경과 관련된 로그
  - 온도 이력 로그

로그 개요 및 참조 방법

표 17-1에는 고장 정보와 관련된 로그의 유형, 개요 및 참조 방법이 나열되어 있습니다. 각 로그의 유형, 개요 및 참조 방법이 아래 제공되어 있습니다. 명령의 자세한 내용은 설명서 페이지 및『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오. 각 로그 유형의 자세한 내용은 다음 절을 참조하십시오.

표 17-1 고장 정보와 관련된 로그

로그 유형	설명	크기(엔트리 크기)/ <표준 저장 기간> 아카이브	출력 표시 대상/ 참조 방법
고장 관리 로그(FM 로그)	시스템에 발생한 오류 이벤트, 알림 및 고장용 로그. 로그의 표시 형태가 Oracle Solaris와 호환됩니다.		도메인/ fmdump(1M)
오류 로그	시스템에 발생한 오류 이벤트, 알림 및 고장용 로그. 로그의 표시 형태가 플랫폼에 한정됩니다.	약 1,024개 생성 (변수-길이) <약 1개월> 아카이브됨	XSCF/ showlogs (8) XSCF 웹
Syslog (SYSLOG)	출력 Oracle Solaris 메시지 기록용 로그. 고장이 발생하면 고장의 개요가 출력됩니다.		도메인/ Oracle Solaris 명령을 사용하여 로그를 참조합니다.
모니터 메시지 로그 (모니터 메시지 로그)	XSCF의 메시지 기록, 이상 보고용 로그.	512KB, 약 10,000개 라인	XSCF/ showlogs (8) XSCF 웹

노트 - Oracle Solaris 명령에 의해 표시되는 로그는 아카이브되지 않습니다.

표 17-2에는 이벤트 기록용 로그의 유형, 개요 및 참조 방법이 나열되어 있습니다.

표 17-2 이벤트 기록용 로그

로그 유형	설명	크기(엔트리 크기)/ <표준 저장 기간> 아카이브	참조 방법
전원 로그 (전원 로그)	서버의 전원 이벤트 기록용 로그.	1,920개 생성 (x 16B) <약 1개월> 아카이브됨	showlogs (8) XSCF 웹
이벤트 로그 (XSCF 이벤트 로그)	시스템 작동, 운영 패널 작동 및 Oracle Solaris로 보고된 이벤트 기록용 로그.	4,096개 생성 (x 48 B) <약 1개월> 아카이브됨	showlogs (8) XSCF 웹
콘솔 로그 (콘솔 로그)	제어 도메인 콘솔 메시지 기록용 로그. 입력 전원이 차단되면 로그가 삭제됩니다.	512KB/PPAR, 약 10,000개 라인/PPAR <약 1주> 아카이브됨	showlogs (8) XSCF 웹
패닉 로그 (패닉 로그)	패닉 발생용 콘솔 로그.	1개 생성 64KB/PPAR (약 1,200개 라인) <1회> 아카이브됨	showlogs (8) XSCF 웹
IPL 로그 (IPL 로그)	전원 공급부터 Oracle Solaris 시작 완료까지 기간용 로그.	1개 생성 32KB/PPAR, 약 600개 라인 /PPAR <1회> 아카이브됨	showlogs (8) XSCF 웹

표 17-3에는 보안과 관련된 로그의 유형, 개요 및 참조 방법이 나열되어 있습니다.

표 17-3 보안과 관련된 로그

로그 유형	설명	크기(엔트리 크기)/ <표준 저장 기간> 아카이브	참조 방법
감사 로그 (감사 로그)	XSCF 감사용 로그	4MB <약 1개월> 아카이브됨	viewaudit (8) XSCF 웹
CoD 로그 (CoD 활성화 로그)	CPU 코어 활성화의 추가 및 삭제용 로그	1,024개 생성 (x 32KB) 코어당 라이센스 아카이브됨	showcodactivationhistory (8) XSCF 웹

표 17-4에는 서버 환경과 관련된 로그의 유형, 개요 및 참조 방법이 나열되어 있습니다.

표 17-4 서버 환경과 관련된 로그

로그 유형	설명	크기(엔트리 크기)/ <표준 저장 기간> 아카이브	참조 방법
온도 이력 로그 (온도 및 습도 이력)	서버 환경의 온도 이력이 포함된 로그	16,384개 생성 (x 16B) (10분마다) <약 1년> 아카이브됨	showlogs (8) XSCF 웹

노트 - 로그가 가득 차면 가장 오래된 로그에서 시작하여 로그 데이터가 덮어쓰기가 됩니다.

17.1.2 로그 참조

이 절에는 각 XSCF 로그 정보 유형의 참조 방법이 설명되어 있습니다.

XSCF 쉘 또는 XSCF 웹에서 로그 확인

다음은 로그 정보의 참조를 위한 공통 절차입니다.

1. 보려는 로그를 참조하는 데 필요한 사용자 권한을 확인합니다.
   각 로그의 사용자 권한은 다음과 같습니다.
   - 오류 로그, 모니터 메시지 로그, 이벤트 로그, 온도 이력 로그
     platadm, platop, fieldeng
   - 전원 logplatadm, platop, pparadm, pparmgr, fieldeng
   - 콘솔 로그, 패닉 로그, IPL 로그
     platadm, platop, pparadm, pparmgr, pparop, fieldeng
   - 감사 로그
     auditadm, auditop
   - CoD 로그
     platadm, platop, fieldeng
2. **XSCF** 쉘 터미널 또는 **XSCF** 웹에 연결하기 위한 호스트 이름 또는 **IP** 주소를 지정합니다.
3. 필요한 사용자 권한이 있는 **XSCF** 사용자 계정과 암호로 **XSCF**에 로그인합니다.
4. 원하는 로그의 참조 명령을 실행하거나 관련 메뉴 항목을 선택합니다.
5. 로그를 참조합니다.

노트 - XSCF 웹 메뉴의 자세한 내용은 "부록 B XSCF 웹 페이지 목록"을 참조하십시오.

17.1.3 오류 로그 확인

오류 로그에는 고장 정보가 포함됩니다. 시스템에 발생한 고장 또는 알림과 관련된 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, error 옵션

사용 시기

다음의 경우 XSCF에서 오류 로그를 참조합니다.

- 메시지가 도메인 콘솔, XSCF 쉘 터미널 또는 XSCF 웹으로 출력될 때 고장 발생 여부를 확인하는 경우.
- 이전에 등록된 이메일 주소로 보고되었을 때 정보가 고장 정보인지 여부를 확인하는 경우.
- SNMP 관리자에서 트랩이 발생했을 때 정보가 고장 정보인지 여부를 확인하는 경우.

작동 절차

1. **XSCF 쉘에서 error 옵션이 지정된 showlogs 명령을 실행합니다.**

```
XSCF> showlogs error
Date: Oct 20 17:45:31 JST 2012
      Code: 00112233-444555666777-888999aaabbbcccdddeeefff
      Status: Warning Occurred: Oct 20 오후 5:45:31.000 JST 2012
      FRU: /PSU#1,/PSU#2
      Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Date: Oct 20 17:45:31 JST 2012
      Code: 00112233-444555666777-888999aaabbbcccdddeee000
      Status: Alarm Occurred: Oct 20 오후 5:45:31.000 JST 2012
      FRU: /PSU#1,/PSU#2,/PSU#3,*
      Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
```

노트 - 명령 예의 레이아웃은 기능 개선을 위해 사전 통지 없이 변경될 수 있습니다.

위 예에서 다음 항목이 표시됩니다.

- 각 문제가 로깅된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- 현장 엔지니어 또는 서비스 엔지니어가 문제 해결에 사용하는 DIAGCODE(코드)

노트 - 사용자는 현장 엔지니어와 서비스 엔지니어에게 이 코드를 알려주어야 합니다. 이는 문제를 조기 해결하는 데 유용합니다.

- 구성요소의 고장 레벨(상태)
  다음 항목 가운데 하나가 표시됩니다.
  알람: 관련 구성요소의 고장 또는 비정상

경고: 관련 구성요소 내 일부 하위 구성요소의 성능 저하 또는 알람

정보: 알림

통지: 시스템 상태 알림

- 각 문제가 발생한 시간(발생)
  이 날짜는 현지 시간으로 표시됩니다.

- 고장 가능성이 높은 교체 구성요소(FRU)
  첫 번째, 두 번째 및 세 번째 의심 구성요소가 있는 경우 이는 구분자로서 쉼표(,)로 나열됩니다. 추가 의심 구성요소의 경우 "*"(별표)가 마지막 쉼표(,) 뒤에 표시됩니다. 각 구성요소는 구성요소 장착 경로 형식에 따라 계층적으로 표시됩니다. 두 번째 이후 의심 구성요소의 표시 여부는 고장이 감지된 위치에 따라 달라집니다.

  다음에는 "FRU:"의 표시 경우가 설명되어 있습니다.

a. "/PSU#1,/PSU#2"가 표시됨
위는 다음을 나타냅니다. PSU#1 및 PSU#2가 각각 첫 번째 및 두 번째 의심 구성요소로서 감지되었습니다. 필요하다면 각 구성요소를 교체해야 할 수도 있습니다.

b. "/PSU#1,/PSU#2,/PSU#3,*"가 표시됨
위는 다음을 나타냅니다. PSU#1, PSU#2 및 PSU#3이 첫 번째, 두 번째 및 세 번째 의심 구성요소로서 감지되고 다른 구성요소도 감지되었습니다. 필요하다면 각 구성요소를 교체해야 할 수도 있습니다.

c. "/BB#0/PCI#3"이 표시됨
위는 다음을 나타냅니다. BB#0/PCI#3이 의심 구성요소로서 감지되었고 빌딩 블록 번호 0의 PCI 슬롯 번호 3이 문제입니다. 필요하다면 PCI 슬롯 번호 3에 연결된 장치를 교체해야 할 수도 있습니다.

d. "/MBU/MEM#02A"가 표시됨
위는 다음을 나타냅니다. /MBU/MEM#02A가 의심 구성요소로서 감지되었고 마더보드 장치의 메모리 슬롯 번호 02A가 문제입니다. 필요하다면 메모리 슬롯 번호 02A를 교체해야 할 수도 있습니다.

e. "/BB#0/CMUL/MEM#02A"가 표시됨
위는 다음을 나타냅니다. /BB#0/CMUL/MEM#02A가 의심 구성요소로서 감지되었고 빌딩 블록 ID 0 CPU 메모리 장치(하위)의 메모리 슬롯 번호 02A가 문제입니다. 필요하다면 메모리 슬롯 번호 02A를 교체해야 할 수도 있습니다.

f. "/BB#0/CMUL/MEM#02A-03A"가 표시됨
위는 다음을 나타냅니다. /BB#0/CMUL/MEM#02A-03A가 의심 구성요소로서 감지되었고 빌딩 블록 ID 0 CPU 메모리 장치(하위)의 메모리 슬롯 번호 02A 및 02B가 문제입니다. 필요하다면 메모리 슬롯 번호 02A 및 02B의 메모리를 쌍으로 교체해야 할 수도 있습니다.

- 문제의 개요를 나타내는 1개 행의 메시지(Msg)

노트 - showlogs(8) 명령의 자세한 내용은 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

17.1.4 모니터 메시지 로그의 확인

시스템에 발생한 이벤트는 XSCF에 로그인한 사용자를 위해 모니터링 메시지로서 실시간 표시됩니다. XSCF 펌웨어는 모니터 메시지 로그로 이 메시지를 수집합니다. 모니터 메시지 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, monitor 옵션

작동 절차

1. **XSCF** 쉘에서 **monitor** 옵션이 지정된 **showlogs** 명령을 실행합니다**.**

```
XSCF> showlogs monitor
Oct 20 17:45:31 monitor message: xxxxxxx
Oct 20 5:55:31 PM monitor message: xxxxxxx
```

다음 항목이 표시됩니다.

- 각 모니터 메시지 로그가 수집된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- 모니터링 메시지(메시지)

17.1.5 전원 로그 확인

전원 작동 또는 재설정이 시스템에서 수행되면 전원 로그가 수집됩니다. 전원 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, power 옵션

작동 절차

1. **XSCF** 쉘에서 **power** 옵션이 지정된 **showlogs** 명령을 실행합니다**.**
   다음에는 전원 로그의 표시 예가 나타나 있습니다.

```
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 Reuest 00
Locked
Oct 20 17:50:31 JST 2012 Cabinet Power Off Self Reset       00
Service
```

다음 예에서는 시작 시간과 종료 시간을 지정하고 최근 순서대로 전원 로그를 나열합니다.

```
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 Reuest 00
Locked
Oct 20 17:35:31 JST 2012 PPAR Power On     Operator        00
Locked
```

노트 - 명령 예의 레이아웃은 기능 개선을 위해 사전 통지 없이 변경될 수 있습니다.

위 예에서 다음 항목이 표시됩니다.

- 각 전원 로그가 수집된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- 발생한 전원 이벤트의 유형(이벤트)
  다음에는 전원 이벤트(이벤트)와 그 의미가 나열되어 있습니다.

이벤트	의미
SCF 재설정:	XIR이 재설정됨
PPAR 전원 공급:	물리 분할 전원이 공급됨
PPAR 전원 차단:	물리 분할 전원이 차단됨
PPAR 재설정:	물리 분할이 재설정됨
캐비닛 전원 공급:	서버 전원이 공급됨
캐비닛 전원 차단:	서버 전원이 차단됨
XIR:	XIR이 재설정됨

- 전원 이벤트 명령의 발생 요인(원인)
  다음에는 원인(원인)과 그 의미가 나열되어 있습니다.

원인	의미
자체 재설정:	XSCF의 자체 재설정으로 XSCF가 재설정됨
전원 공급:	입력 전원 공급으로 XSCF가 재설정됨
시스템 재설정:	오류 감지로 XSCF가 재설정됨
패널:	운영 패널의 스위치 작동으로 전원 이벤트가 발생됨
예약:	TOD 타이머의 설정으로 전원 이벤트가 발생됨
IPMI:	RCIL에 연결된 I/O 장치로 전원 이벤트가 발생됨
전원 복구:	전원 복구로 전원이 공급됨.
운영자:	운영자 명령으로 전원 이벤트가 발생됨
정전:	정전으로 전원이 차단됨.

소프트웨어 요청:	Oracle Solaris 명령으로 전원 이벤트가 발생됨
알람:	서버 환경 또는 하드웨어 고장으로 전원 이벤트가 발생됨
치명적:	치명적으로 전원 이벤트가 발생됨

- 전원 이벤트의 PPAR-ID 또는 BB-ID(ID)
  BB-ID는 이벤트가 시스템 전원 공급 또는 시스템 전원 차단일 때 표시됩니다.

  PPAR-ID는 이벤트가 PPAR 전원 공급, PPAR 전원 차단 또는 PPAR 재설정일 때 표시됩니다.

  "--"은 이벤트가 모든 BB 또는 모든 PPAR에 대한 이벤트일 때 표시됩니다.
- 운영 패널의 모드 스위치 상태(스위치)
  다음에는 스위치와 그 의미가 나열되어 있습니다.

스위치 상태	의미
잠김:	모드 스위치가 잠김임
서비스:	모드 스위치가 서비스임

17.1.6 이벤트 로그 확인

시스템 상태 변경, 구성 변경, 운영 패널 작동 또는 물리 분할이나 시스템의 Oracle Solaris로 이벤트 전송과 같이 시스템에서 이벤트가 발생하면 이벤트 로그가 수집됩니다. 이벤트 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, event 옵션

작동 절차

1. **XSCF** 쉘에서 **event** 옵션이 지정된 **showlogs** 명령을 실행합니다**.**

```
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
```

다음 항목이 표시됩니다.

- 각 이벤트 로그가 수집된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- 이벤트 메시지(메시지)

17.1.7 콘솔 로그 확인

XSCF를 통해 출력되는 제어 도메인 콘솔 메시지는 콘솔 로그로서 수집됩니다. 콘솔 로

그는 각 줄 바꿈 코드마다 1개 항목으로서 수집됩니다. 일부의 경우 콘솔 로그는 콘솔 메시지 로그로 불릴 수도 있습니다. 콘솔 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, console 옵션

작동 절차

1. **XSCF** 쉘에서 **console** 옵션이 지정된 **showlogs** 명령을 실행합니다.

```
XSCF> showlogs console -p 0
PPAR-ID: 00
Oct 20 5:45:31 PM JST 2012   console message: xxxxxxx
Oct 20 5:55:31 PM JST 2012   console message: xxxxxxx
```

다음 항목이 표시됩니다.

- 물리 분할 ID(PPAR ID)
- 각 콘솔 로그가 수집된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- 콘솔 메시지(메시지)

17.1.8 패닉 로그 확인

패닉의 경우 콘솔 메시지가 도메인 콘솔로 출력됩니다. 이 콘솔 메시지는 패닉 로그로 수집됩니다. 일부의 경우 패닉 로그는 패닉 메시지 로그로 불릴 수도 있습니다. 패닉 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, panic 옵션

작동 절차

1. **XSCF** 쉘에서 **panic** 옵션이 지정된 **showlogs** 명령을 실행합니다.

```
XSCF> showlogs panic -p 0
<<panic>>
Date: Oct 20 18:45:31 JST 2012     PPAR-ID: 00
Oct 20 17:45:31 JST 2012    panic message: xxxxxxx
Oct 20 5:55:31 PM JST 2012    panic message: xxxxxxx
```

다음 항목이 표시됩니다.

- 물리 분할 ID(PPAR-ID)
- 각 패닉 로그가 수집된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- 패닉 메시지(메시지)

17.1.9 IPL 로그 확인

물리 분할의 전원이 공급되면 실행 상태가 설정될 때까지 콘솔 메시지가 제어 도메인 콘솔로 출력됩니다. 이 콘솔 메시지는 IPL 로그로 수집됩니다. 일부의 경우 IPL 로그는 IPL 메시지 로그로 불릴 수도 있습니다. IPL 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, ipl 옵션

작동 절차

1. **XSCF** 쉘에서 **ipl** 옵션이 지정된 **showlogs** 명령을 실행합니다.

```
XSCF> showlogs ipl -p 0
<<ipl>>
Date: Oct 20 18:45:31 JST 2012     PPAR-ID: 00
Oct 20 17:45:31 JST 2012    ipl message: xxxxxxx
Oct 20 5:55:31 PM JST 2012    ipl message: xxxxxxx
```

다음 항목이 표시됩니다.

- 물리 분할 ID(PPAR-ID)
- 각 IPL 로그가 수집된 시간(날짜)
  이 날짜는 현지 시간으로 표시됩니다.
- IPL 메시지(메시지)

17.1.10 감사 로그 확인

시스템이 감사 기능을 사용하면 감사 로그가 수집됩니다. 감사 로그를 참조하려면 다음 명령을 사용합니다.

- viewaudit 명령

작동 절차

1. **XSCF** 쉘에서 **viewaudit** 명령을 실행합니다.
   다음에는 모든 감사 레코드의 표시 예가 나타나 있습니다.

```
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
```

위 예에 나타난 바와 같이 기본적으로 레코드는 텍스트 형식으로 표시됩니다. 라인당 1개 토큰이 표시되며 이때 쉼표가 필드 구분자로서 사용됩니다.

다음에는 토큰 유형과 필드가 나열되어 있습니다(표시 순서를 따름).

- 파일 토큰
  라벨, 버전, 시간, 파일 이름
- 헤더 토큰
  라벨, 레코드 바이트 카운트, 버전, 이벤트 유형, 기계 주소, 시간

  (이벤트 기록됨)
- 주제 토큰
  라벨, 감사 세션 ID, UID, 작동 모드, 터미널 유형, 원격 IP 주소, 원격 포트
- Upriv 토큰
  라벨, 성공/실패
- Udpriv 토큰
  라벨, 성공/실패, 사용자 권한, 도메인 ID 1, ..., 도메인 ID N
- 명령 토큰
  라벨, 명령 이름, 피연산자 1, ..., 피연산자 N
- 인증 토큰
  라벨, 인증 결과, 사용자 이름, 메시지, 터미널 유형, 원격 IP 주소, 원격 포트
- 반환 토큰
  라벨, 반환 값
- 텍스트 토큰
  라벨, 텍스트 문자열

노트 - 일부 필드는 환경에 따라 출력되지 않을 수도 있습니다.

다음에는 주 감사 이벤트와 토큰이 나열되어 있습니다.

- 로그인 Telnet
  헤더

  주제

  텍스트

  반환
- 로그인 SSH
  로그인 Telnet과 동일
- 로그인 BUI
  로그인 Telnet과 동일

- 로그아웃
  헤더

  주제
- 감사 시작
  헤더
- 감사 정지
  헤더
- 쉘 명령
  헤더

  주제

  명령

  텍스트

  Upriv | Updpriv

  반환

노트 - 일부 토큰은 환경에 따라 출력되지 않을 수도 있습니다. 또한 정보는 기능 개선을 위해 사전 통지 없이 변경될 수 있습니다.
노트 - viewaudit(8) 명령의 각 로그 옵션, 감사 클래스 및 감사 이벤트와 관련된 자세한 내용은 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

17.1.11 CoD 로그 확인

CoD 로그는 CPU 코어 활성화의 추가 또는 삭제 시에 수집됩니다. 일부의 경우 CoD 로그는 CoD 활성화 로그로 불릴 수도 있습니다. CoD 로그를 참조하려면 다음 명령을 사용합니다.

- showcodactivationhistory 명령

작동 절차

1. **XSCF** 쉘에서 **showcodactivationhistory** 명령을 실행합니다**.**
   다음 예에는 CoD 로그가 나타나 있습니다.

```
XSCF> showcodactivationhistory
08/24/2012 11:06:03AM UTC: Report Generated 4Socket SN: 2081208016
08/15/2012 02:37:05AM UTC: Activation history initialized: PROC 0 cores
08/16/2012 4:47:10 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:17 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:22 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:28 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:37 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:44 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:49 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 4:47:54 AM:00AM UTC: Capacity added: PROC 1 cores
08/16/2012 04:48:00AM UTC: Capacity added: PROC 1 cores
```

```
08/16/2012 4:48:06 AM:00AM UTC: Capacity added: PROC 1 cores
08/21/2012 10:25:58AM UTC: Configuration backup created: PROC 10 cores
08/21/2012 11:04:31AM UTC: Configuration restored: PROC 10 cores
08/23/2012 03:07:20AM UTC: Activation history initialized: PROC 0 cores
08/24/2012 05:39:14AM UTC: Configuration backup created: PROC 0 cores
08/24/2012 11:06:03AM UTC: Summary: PROC 0 cores
Signature: GLROg9xhegN0dA2QilJ0lbozonV/ufWEgY994fwuXPA
```

노트 - showcodactivationhistory(8) 명령의 자세한 내용은 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

17.1.12 온도 이력 로그 확인

온도 이력 로그에는 서버의 흡기 온도 이력이 포함됩니다. 온도 이력 로그는 10분 간격으로 기록됩니다. 온도 이력 로그를 참조하려면 다음 명령과 옵션을 사용합니다.

- showlogs 명령, env 옵션

작동 절차

1. **XSCF** 쉘에서 **env** 옵션이 지정된 **showlogs** 명령을 실행합니다.

```
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
:
```

다음 항목이 표시됩니다.

- 각 온도 이력 로그가 수집된 시간(날짜).
  이 날짜는 현지 시간으로 표시됩니다.
- 온도(온도)
- 캐비닛 전원 공급 상태(공급 또는 차단)(전원)

17.1.13 스냅샷으로 파일에 로그 저장

이 절에는 XSCF 로그 정보를 파일로 저장하는 방법이 설명되어 있습니다.

로그 정보를 저장하려면 XSCF 쉘에서 snapshot 명령을 실행합니다. 또는 XSCF 웹에서 스냅샷 메뉴를 선택합니다. 모든 XSCF 로그 정보가 지정된 위치에 저장됩니다.

현장 엔지니어 또는 서비스 엔지니어가 로그 정보를 저장합니다. 또한 시스템 관리자도 요청 시에 이 작동을 수행할 수 있습니다.

로그 저장 방법

다음에는 로그 저장 방법이 설명되어 있습니다. 방법의 자세한 내용은 다음 절을 참조하십시오.

- USB 장치를 마스터 캐비닛 후면 패널에 장착된 XSCF 장치의 USB 커넥터에 연결하여 로컬로 로그 정보를 저장합니다.

노트 - USB 장치를 FAT32 파일 시스템으로 포맷해야 합니다. 로컬로 로그를 저장하는 데 사용되는 USB 장치의 용량과 처리는 서비스 엔지니어에게 문의하십시오.

노트 - 저장된 로그 데이터는 지정된 암호화 옵션으로 암호화됩니다. 시스템 관리자가 로그를 저장하는 경우 로그 파일 및 암호화 정보의 처리와 로그 파일의 전송 방법은 서비스 엔지니어에게 문의하십시오.

노트 - 시스템에 여러 XSCF 장치가 있는 경우 스탠바이 XSCF 경우와 같이 다른 캐비닛의 로그 데이터가 마스터 XSCF로부터 수집될 수 있습니다.

로그 파일 출력 형식

로그 파일의 저장을 위한 출력 형식은 다음과 같습니다.

- 파일 이름: 파일은 XSCF 호스트 이름, IP 주소 및 로그 저장 시간으로 구성된 이름으로 자동 생성됩니다.
  로그 파일은 사용자 지정 파일 이름으로 생성되지 않습니다.
- 파일 형식: zip

시스템에 여러 XSCF 장치가 있는 경우 생성되는 1개 zip 파일에는 1개 빌딩 블록과 각 크로스바 박스로 구성된 각 SPARC M10-4S 캐비닛의 정보가 포함됩니다. 단일 캐비닛 번호가 지정되는 경우 시스템에 공통된 로그 외에 지정된 캐비닛에 특정된 로그 정보도 저장됩니다. 모든 캐비닛이 지정되는 경우 시스템에 공통된 로그 외에 모든 캐비닛의 로그 정보도 저장됩니다.

17.1.14 로컬 USB 장치로 로그 저장

다음에는 XSCF 웹 또는 XSCF 쉘을 사용하여 로그 정보를 USB 장치에 저장하는 방법이 설명되어 있습니다.

웹 브라우저 작동 절차

1. **USB** 장치를 서버 후면 패널에 있는 **XSCF** 장치의 **USB** 커넥터에 연결합니다.
2. 스냅샷 메뉴를 선택하고 저장 작동 페이지를 표시합니다.
3. 웹 브라우저 창에서 로그 정보의 저장 위치로서 **USB** 장치를 선택합니다.
4. 출력 로그 파일의 암호화 암호를 지정합니다.
   데이터 전송이 수행됩니다.
5. 로그 저장이 완료되었는지 확인합니다.
   로그 저장이 완료되면 서비스 엔지니어에게 연락합니다.

명령 작동 절차

1. **USB** 장치를 서버 후면 패널에 있는 **XSCF** 장치의 **USB** 커넥터에 연결합니다.
2. **XSCF** 쉘에서 출력 파일용 **USB** 장치를 지정한 채 **snapshot** 명령을 실행합니다.

```
XSCF> snapshot -d usb0 -a
```

데이터 전송이 수행됩니다.

3. 로그 저장이 완료되었는지 확인합니다.
로그 저장이 완료되면 서비스 엔지니어에게 연락합니다.

노트 - 데이터 암호화를 활성화하기 위한 snapshot(8) 명령의 암호화 옵션 사용과 관련된 자세한 내용은 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

17.2 경고 및 알림 메시지의 확인

이 절에는 주로 제어 도메인 콘솔로 출력되고 이메일 및 SNMP 에이전트 기능을 통해 보고되는 고장 및 알림 메시지의 확인 방법이 설명되어 있습니다.

17.2.1 메시지 유형 및 참조 방법의 확인

메시지 유형

다음 메시지 유형은 서버 오류 또는 상태의 알림 시에 사용자가 가장 흔히 보게 되는 유형입니다.

- syslog 메시지(*)
- FMA 메시지(*)
- IPL 메시지
- 패닉 메시지
- 콘솔 메시지
- 모니터링 메시지
- 기타 알림 메시지

*: 이 메시지는 Oracle Solaris에서만 참조됩니다. 자세한 내용은 Oracle Solaris 관련 설명서를 참조하십시오.

메시지 개요 및 참조 방법

표 17-5에는 메시지 유형, 개요 및 참조 방법이 나열되어 있습니다.

표 17-5 각 메시지의 개요

메시지 유형	설명	출력 표시 대상/ 참조 방법
syslog 메시지	이 메시지는 Oracle Solaris에 의해 보고됩니다.	도메인/ 제어 도메인 콘솔에서 확인할 수 있음
FMA 메시지	이 메시지에는 하드웨어 또는 소프트웨어 고장 시 Oracle Solaris의 FMA(Fault Management Architecture)에 의해 자동 생성되는 진단 결과가 설명되어 있습니다. 이 메시지 출력으로 사용자는 시스템의 통지된 고장에 해당되는 부분을 식별할 수 있습니다. FMA 메시지는 로그 정보로서 저장됩니다(고장 로그 또는 오류 로그). Oracle Solaris의 fmdump(1M) 명령 또는 XSCF 쉘의 showlogs 명령을 사용하여 보다 자세히 조사하도록 메시지 내용을 표시할 수 있습니다. 사용자는 제어 도메인 콘솔에 표시된 MSG-ID 기반의 지정된 URL을 사용하여 내용을 확인할 수도 있습니다.	도메인/ 제어 도메인 콘솔에서 확인할 수 있음
IPL 메시지	이 메시지는 제어 도메인 OS의 시작 동안 출력됩니다. IPL 메시지는 제어 도메인 콘솔로 출력되고 로그 정보(IPL 로그)로서 XSCF에 저장됩니다. IPL 로그는 각 제어 도메인마다 마지막 단일 시스템 시작에 해당되는 정보를 보존합니다. XSCF 쉘의 showlogs 명령을 사용하여 IPL 로그를 표시할 수 있습니다.	도메인/ 제어 도메인 콘솔에서 확인할 수 있음
패닉 메시지	이 메시지는 패닉 시에 출력됩니다. 패닉 메시지는 도메인 콘솔로 출력되고 로그 정보(패닉 로그)로서 XSCF에 저장됩니다. 패닉 로그는 각 제어 도메인마다 마지막 단일 패닉 이벤트에 해당되는 정보를 보존합니다. XSCF 쉘의 showlogs 명령을 사용하여 패닉 로그를 표시할 수 있습니다.	도메인/ 제어 도메인 콘솔에서 확인할 수 있음
콘솔 메시지	콘솔 메시지는 syslog 메시지, FMA 메시지, 패닉 메시지, IPL 메시지와 POST, OpenBoot PROM 및 Oracle Solaris에 의해 출력되는 기타 메시지를 설명하는 데 사용되는 일반 용어입니다. 콘솔 메시지는 각 제어 도메인의 도메인 콘솔로 출력될 때 로그 정보(콘솔 로그)로서 XSCF에 저장됩니다. XSCF 쉘의 showlogs 명령을 사용하여 콘솔 로그를 표시할 수 있습니다. 유의할 점으로, 게스트 도메인의 콘솔 메시지는 논리 도메인 관리자가 관리합니다. 자세한 내용은 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오. 콘솔 메시지는 가장 오래된 메시지에서 시작하여 덮어쓰기가 됩니다. 콘솔 메시지가 덮어쓰기가 되더라도 시스템 시작 메시지는 IPL 로그에 보존되며 패닉의 경우에는 로그가 패닉 로그에 보존됩니다. 시스템에 여러 XSCF 장치가 있는 경우 마스터 XSCF에 저장된 콘솔 메시지는 스탠바이 XSCF로 복사되지 않습니다. 이에 따라 XSCF 장치의 전환 후에는 이전 마스터측 콘솔 메시지가 참조될 수 없습니다.	도메인/ 제어 도메인 콘솔에서 확인할 수 있음

표 17-5 각 메시지의 개요 (계속)

메시지 유형	설명	출력 표시 대상/ 참조 방법
모니터링 메시지	XSCF는 이 메시지를 출력하여 시스템 고장 또는 알림을 보고합니다. 모니터링 메시지는 showmonitorlog 명령을 사용하여 출력하며 로그 정보(모니터 메시지 로그 또는 오류 로그)로서 XSCF에 저장됩니다. XSCF 쉘의 showlogs 명령을 사용하여 보다 자세히 조사하도록 모니터 메시지 로그 및 오류 로그를 표시할 수 있습니다. 또한 자세한 정보를 얻도록 서비스 엔지니어가 메시지의 DIAGCODE 출력을 사용합니다. 모니터링 메시지는 가장 오래된 메시지에서 시작하여 덮어쓰기가 됩니다. 시스템에 여러 XSCF 장치가 있는 경우 마스터 XSCF에 의해 출력되는 모니터링 메시지는 스탠바이 XSCF에서도 관리됩니다. XSCF 장치의 전환 후라도 이전 마스터측 모니터링 메시지가 참조될 수 있습니다.	도메인, XSCF/ 제어 도메인 콘솔에서 확인할 수 있음 showmonitor -log 명령으로 확인할 수 있음
기타 알림 메시지	위 메시지 외에 정상적인 전원 차단 시, 재설정 처리의 수행 시 또는 이벤트 발생 시 도메인 콘솔에 표시되는 알림 메시지도 있습니다.	도메인/ 제어 도메인 콘솔에서 확인할 수 있음

17.2.2 보고된 메시지 처리

이 절에는 Oracle Solaris 메시지 또는 각 XSCF 기능으로부터 보고된 메시지의 인식 후 조치와 메시지가 설명되어 있습니다.

제어 도메인 콘솔에서 메시지의 알림 또는 고장 인식/처리

1. 사용자는 **syslog** 메시지 또는 제어 도메인 콘솔로 출력되는 **FMA** 메시지과 같이 콘솔 메시지의 알림 또는 고장을 인식합니다.
   다음에는 제어 도메인 콘솔에서 FMA 메시지의 표시 예가 나타나 있습니다.

```
SUNW-MSG-ID: SUNOS-8000-J0, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Thu Apr 19 10:48:39 JST 2012
PLATFORM: ORCL,SPARC64-X, CSN: PP115300MX, HOSTNAME: 4S-LGA12-D0
SOURCE: eft, REV: 1.16
EVENT-ID: fcbb42a5-47c3-c9c5-f0b0-f782d69afb01
DESC: The diagnosis engine encountered telemetry from the listed devices for
which it was unable to perform a diagnosis - ereport.io.pciex.rc.epkt@
chassis0/cpuboard0/chip0/hostbridge0/pciexrc0 class and path are incompatible.
AUTO-RESPONSE: Error reports have been logged for examination.
IMPACT: Automated diagnosis and response for these events will not occur.
REC-ACTION: Use 'fmadm faulty' to provide a more detailed view of this event.
Use 'fmdump -eV' to view the unexpected telemetry. Please refer to the
associated reference document at http://support.oracle.com/msg/SUNOS-8000-J0
```

```
for the latest service procedures and policies regarding this diagnosis.
```

노트 - 메시지 예는 사전 통지 없이 변경될 수 있습니다.

2. **FMA** 메시지의 고장 정보가 로그에 저장되므로 제어 도메인 콘솔에서 로그 파일을 참조합니다. 이를 위해 제어 도메인 콘솔에서 **syslog** 참조 명령 또는 **fmdump(1M)** 명령과 같은 **Oracle Solaris** 명령을 실행합니다.
   이 명령을 사용하여 고장 정보를 식별하는 방법은 Oracle Solaris 관련 설명서를 참조하십시오.
3. 제어 도메인 콘솔에 표시된 메시지 **ID(SUNW-MSG-ID)**에 따라 지정된 **URL**에 액세스하여 알림 또는 고장의 내용을 확인합니다.
   메시지 ID(MSG-ID)를 찾을 수 없으면 syslog 정보에서 자세한 정보를 얻습니다.
4. 보다 자세한 정보를 얻으려면 **XSCF**에 로그인하고 **showlogs** 명령을 실행하여 고장 정보를 식별합니다.
5. 지정 **URL**에 제공된 정보에서 권장하는 처리에 따라 고장을 해결합니다.

노트 - 최신 URL 정보는 『SPARC M10 시스템 제품 노트』에 나열된 메시지 관련 웹 사이트를 참조하십시오.

Syslog 메시지 및 FMA 메시지 외에 사용자는 콘솔 메시지, 패닉 메시지, IPL 메시지 또는 XSCF 로그에 저장된 모니터링 메시지를 참조하여 고장을 인식할 수도 있습니다. 각 log 옵션이 지정된 XSCF 쉘의 showlogs 명령을 사용하여 이 로그 정보를 참조할 수 있습니다.

showlogs 명령의 자세한 내용은 "17.1 XSCF로 저장된 로그 확인"을 참조하십시오.

이메일에 의해 보고된 고장의 인식/처리

1. 사용자는 **XSCF**에 의해 보고된 이메일의 주제 또는 메시지의 텍스트로서 알림 또는 고장을 인식합니다.
   고장 시의 이메일 메시지 예는 "15.2 고장 발생 시 이메일을 통한 알림 수신"을 참조하십시오.
2. 보다 자세한 정보를 얻으려면 **XSCF**에 로그인하고 **showlogs** 명령을 실행하여 고장 정보를 식별합니다.
3. 로그 정보를 확인하고 필요한 경우 이메일 메시지 또는 로그의 **DIAGCODE** 출력을 서비스 엔지니어에게 알려줍니다.
   서비스 엔지니어는 DIAGCODE를 사용하여 자세한 정보를 얻을 수 있습니다.

SNMP 트랩 메시지의 알림 또는 고장 인식/처리

1. 사용자는 **XSCF**로부터 **SNMP** 관리자가 발행한 트랩 정보의 알림 또는 고장을 인식합니다.
   트랩 예는 "15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리"를 참조하십시오.
2. 보다 자세한 정보를 얻으려면 **XSCF**에 로그인하고 **showlogs** 명령을 실행하여 고장 정보를 식별합니다.

3. 로그 정보를 확인하고 필요한 경우 로그의 **DIAGCODE** 출력을 서비스 엔지니어에게 알려줍니다.

XSCF 쉘에서 모니터링 메시지의 알림 또는 고장 인식/처리

1. 사용자는 **showmonitorlog** 명령을 실행하여 **XSCF** 모니터링 메시지 출력의 알림 또는 고장을 인식합니다.
   다음에는 모니터링 메시지의 예가 나타나 있습니다.

```
XSCF> showmonitorlog
PAPL2-5-0:Alarm:/BB#0/CPU#0:XSCF:Uncorrectable
error ( 80006000-20010000-0108000112345678):
```

노트 - 명령 예는 기능 개선을 위해 사전 통지 없이 변경될 수 있습니다.

2. 보다 자세한 정보를 얻으려면 **XSCF**에 로그인하고 **showlogs** 명령을 실행하여 고장 정보를 식별합니다.
3. 로그 정보를 확인하고 필요한 경우 로그의 **DIAGCODE** 출력을 서비스 엔지니어에게 알려줍니다.

18장

펌웨어/소프트웨어 업데이트

이 장에는 SPARC M10 시스템의 펌웨어/소프트웨어 업데이트 방법이 설명되어 있습니다.

- XCP 펌웨어 업데이트
- Oracle Solaris 및 Oracle VM Server for SPARC 업데이트

18.1 XCP 펌웨어 업데이트

이 절에는 SPARC M10 시스템 펌웨어의 관리 프로그램(XCP)을 다운로드하여 기존 펌웨어를 최신 펌웨어로 업데이트하는 방법이 설명되어 있습니다.

시스템 관리자와 현장 엔지니어가 펌웨어를 업데이트합니다.

18.1.1 펌웨어 업데이트의 기본 정보

업데이트하는 펌웨어의 유형

이 시스템은 하드웨어/소프트웨어를 제어하는 여러 펌웨어를 제공합니다. 이 펌웨어를 패키지화하여 얻는 프로그램 모듈을 XCP(XSCF 제어 패키지)라고 합니다.

사용자는 사이트에서 XCP 펌웨어를 다운로드 및 업데이트하여 새 펌웨어의 기능을 사용할 수 있습니다.

다음 유형의 XSCF 펌웨어가 있습니다.

- POST 펌웨어, OpenBoot PROM 펌웨어 및 하이퍼바이저 펌웨어
  (이후 CMU 펌웨어라고 함)

  3개 유형의 펌웨어는 CPU 메모리 장치에서 업데이트되는 펌웨어 하나로 정리되며 버전이 관리됩니다. 본 설명서에서 이 3개 유형의 펌웨어는 통칭하여 CMU 펌웨어로 불릴 수도 있습니다.
- XSCF 펌웨어

이 펌웨어는 XSCF 장치에서 업데이트됩니다. 사용자는 전체 펌웨어(이후 XCP 펌웨어라고 함) 업데이트 또는 XSCF 펌웨어만 업데이트를 선택할 수 있습니다.

펌웨어 업데이트의 특징

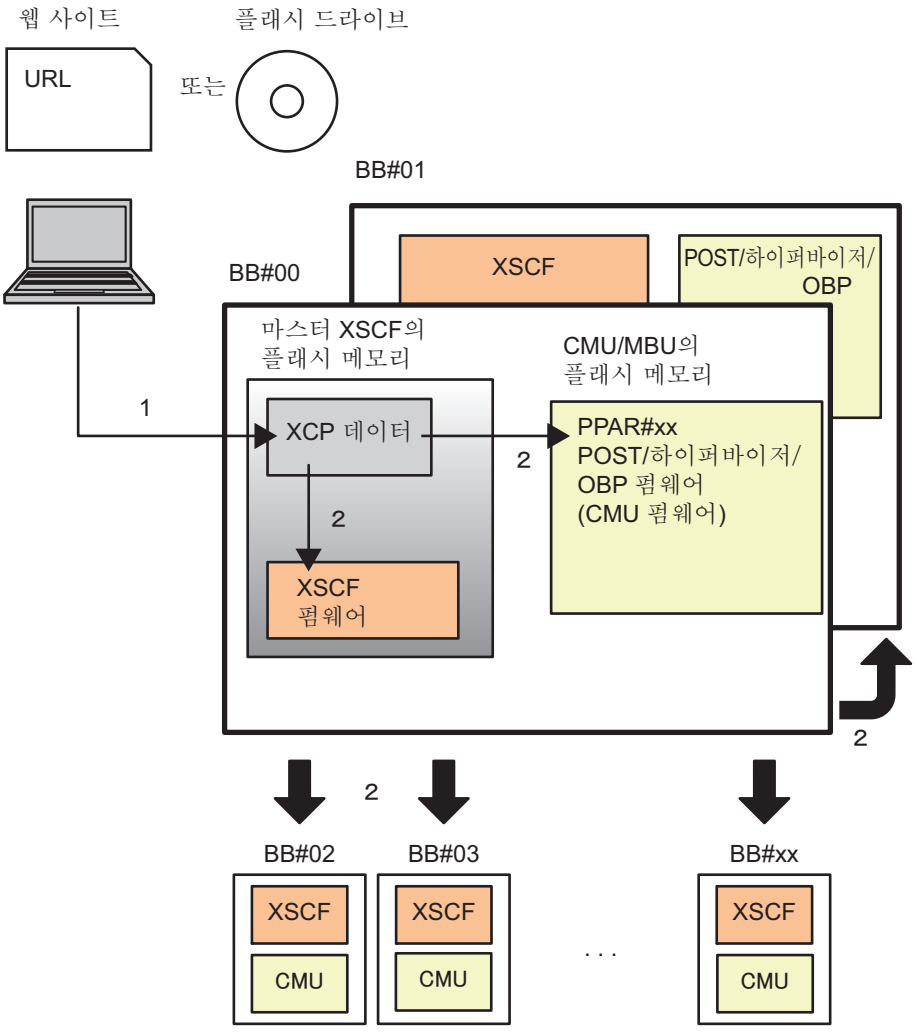
XSCF가 관리하는 펌웨어 업데이트의 특징은 다음과 같습니다.

- 새 펌웨어는 물리 분할의 전원 차단 없이도 업데이트할 수 있습니다. 하지만 CMU 펌웨어 업데이트는 대상 물리 분할에 적용되므로 재부팅이 필요합니다.
- 부품을 교체한 경우 교체한 부품은 작동 중인 펌웨어 버전에 자동 적용됩니다. 하지만 입력 전원을 차단한 채 교체하면(콜드 교체) 부품이 펌웨어 버전에 작동 적용되지 않습니다.
- 시스템이 여러 물리 분할로 구성되더라도 다른 물리 분할에 아무런 영향 없이 최신 펌웨어로 업데이트할 수 있습니다.

펌웨어 업데이트의 메커니즘

그림 18-1은 펌웨어 업데이트의 메커니즘을 나타내는 개념적 그림입니다.

그림 18-1 펌웨어 업데이트의 개념



1 XCP 가져오기

2 업데이트(XSCF 펌웨어에 "적용"이 포함됨)

이 시스템의 펌웨어 업데이트에는 다음 3개 작동(XCP 가져오기, 업데이트 및 적용)이 있습니다.

1. **XCP** 가져오기**(**다운로드**)**
   웹 사이트 등에서 가져온 XCP의 이미지 파일을 이 시스템에 저장하는 것을 "XCP 가져오기"라고 합니다. XCP를 가져온 경우 작동 중인 펌웨어는 아직 업데이트되지 않은 상태입니다. 또한 1개 생성에 버전 수만큼의 XCP를 가져오기도 합니다.

2. 업데이트
   가져온 XCP의 이미지 파일을 이 시스템의 플래시 메모리에 쓰기를 하는 것을 "업데이트"라고 합니다. 업데이트되면 XSCF 펌웨어만 적용됩니다. 이제 XSCF 펌웨어

업데이트가 완료되었습니다.

3. 적용
   실제 사용할 이 시스템의 플래시 메모리에 쓰기가 된 펌웨어를 활성화하는 것을 "적용"이라고 합니다. XSCF 펌웨어의 적용은 위 2의 업데이트로 완료됩니다. 하지만 CMU 펌웨어는 대상 물리 분할 또는 제어 도메인의 재부팅으로 적용됩니다.

각 물리 분할마다 이 시스템이 구분되는 것으로 가정합니다. 이 경우 업데이트되면 CMU 펌웨어는 모든 물리 분할의 제어 도메인 플래시 메모리에 새로 쓰기가 됩니다. 하지만 업데이트만 된 경우 작동 중인 CMU 펌웨어는 아직 업데이트되지 않은 상태입니다. 도메인의 CMU 펌웨어 업데이트를 완료하려면 대상 물리 분할(제어 도메인)을 재부팅해야 합니다.

펌웨어 쓰기가 되는 플래시 메모리에는 2개 영역이 있습니다. 현재 뱅크 및 예약 뱅크. 펌웨어 업데이트는 이 2개 뱅크를 사용하여 제어합니다. 현재 뱅크는 시스템에 현재 사용 중인 펌웨어를 포함하며 예약 뱅크는 펌웨어를 안전하게 업데이트하는 데 사용됩니다.

풀링된 시스템 보드의 업데이트는 다음 경우에 완료됩니다.

- 풀링된 시스템 보드가 물리 분할에 할당되는 것으로 가정합니다. 이 경우 보드를 대상 물리 분할에서 재부팅하고 Oracle Solaris에 삽입하면 최신 펌웨어로 업데이트됩니다.

버전 일치

다음의 경우 이 시스템은 펌웨어 버전을 자동 일치시킵니다.

- 물리 분할 내 여러 시스템 보드의 펌웨어 버전이 서로 다르다고 가정합니다. 이 경우 물리 분할 전원을 공급하거나 입력 전원을 공급하면 펌웨어 버전이 자동 일치됩니다.
- 유지 관리 부품을 교체 또는 추가한 경우 이 부품은 작동 중인 펌웨어 버전에 자동 적용됩니다.

여러 XSCF 사용 시의 업데이트

시스템에 여러 XSCF가 있는 경우 마스터 XSCF가 펌웨어 업데이트를 수행합니다. 펌웨어 업데이트는 스탠바이 XSCF가 먼저이고 마스터 XSCF가 그 다음인 순서대로 자동 수행됩니다. 이 경우 XSCF는 자신을 재설정하거나 마스터 및 스탠바이 XSCF 네트워크를 전환합니다. 따라서 네트워크가 한 번 분리됩니다. 이에 따라 다시 로그인해야 합니다.

업데이트의 자세한 내용은 "18.1.3 펌웨어 업데이트"를 참조하십시오.

18.1.2 펌웨어 업데이트 전

업데이트 주의 사항

- XCP의 출시와 더불어 버전의 제품 노트도 일반에게 공개됩니다. 제품 노트에는 다음이 설명되어 있습니다. 추가된 기능, 소프트웨어 패치 정보, 새 하드웨어와 펌웨어 간의 대응, 버그 정보, 설명서 수정 등. 더욱이, 최신 제품 노트에는 과거 제품 노트의 수정도 포함됩니다. 적용하는 펌웨어 버전의 제품 노트와 최신 버전의 제품 노트 모두를 읽어보시기 바랍니다.
- 작동 중인 시스템에서 이전 버전의 XCP 데이터로 펌웨어를 업데이트하면 시스템

작동을 예상할 수 없습니다.

- 고장인 FRU가 있으면 펌웨어 업데이트가 불가능합니다. 업데이트 전에 고장인 FRU가 있는지 확인합니다. 고장이 발생하면 고장을 수정한 후 펌웨어를 업데이트합니다. FRU 상태를 확인하려면 showhardconf 명령을 사용합니다. FRU에 마크(*)가 있는지 확인합니다.
- XCP 전체의 펌웨어와 XSCF 펌웨어가 업데이트되는 동안 XSCF가 재설정되므로 XSCF 통신이 한 번 분리됩니다. 이 경우 XSCF에 다시 연결하여 로그인합니다.
- 1개 이상의 물리 분할을 업데이트 및 적용할 수 있습니다. CMU 펌웨어를 적용하려면 대상 물리 분할을 적용하도록 재부팅합니다.

업데이트될 파일의 제공 방법 및 파일 형식

XCP 펌웨어의 이미지 파일은 다음 위치와 형식으로 제공됩니다.

- 제공 방법: 웹 사이트
  웹 사이트의 자세한 내용은『SPARC M10 시스템 제품 노트』의 펌웨어 다운로드와 관련된 설명을 참조하십시오. 현장 엔지니어는 CD-ROM, DVD-ROM 또는 플래시 드라이브를 사용할 수 있습니다.
- 형식: 압축 tar 파일(tar.gz) 또는 Windows 실행 파일(exe)
  예: BBXCP2020.tar.gz

펌웨어 버전의 확인 방법

이 시스템의 펌웨어 버전을 "XCP 버전"이라고 합니다. 버전 번호가 클수록 최근 펌웨어입니다. 펌웨어를 업데이트하기 전에 현재 시스템의 XCP 버전을 확인합니다.

다음 예에는 XCP 버전이 나타나 있습니다.

```
XSCF> version -c xcp
BB#00-XSCF#0 (Master)
XCP0 (Current): 2020
XCP1 (Reserve): 2020
BB#01-XSCF#0 (Standby)
XCP0 (Current): 2020
XCP1 (Reserve): 2020
BB#02-XSCF#0
XCP0 (Current): 2020
XCP1 (Reserve): 2020
```

version 명령을 사용하여 XCP의 각 펌웨어 버전을 확인할 수도 있습니다.

XCP 버전은 "xyyz"와 같이 4자리로 표시됩니다. 각 번호의 의미는 다음과 같습니다.

- x: 메이저 릴리스 번호
- yy: 마이너 릴리스 번호
- z: 마이크로 릴리스 번호

마이크로 릴리스 수정 횟수가 설명서 수정 횟수를 넘어설 수도 있습니다. 이러한 이유로 마이크로 릴리스 번호는 설명서에 변수로서 표시될 수도 있습니다.

- 예: XCP201x

업데이트 방법 및 작업 시간

표 18-1에는 업데이터 방법과 대략적인 작업 시간이 나열되어 있습니다.

표 18-1 업데이트 방법 및 작업 시간

업데이트 방법	시스템 상태	시간
XSCF가 1개인 시스템의 경우 XCP가 업데이트됩니다.	물리 분할 전원이 차단 또는 공급됩니다.	약 45분
XSCF가 1개인 시스템의 경우 XSCF 펌웨어만 업데이트됩니다.	물리 분할 전원이 차단 또는 공급됩니다.	약 20분
XSCF가 여러 개인 시스템의 경우 XCP가 업데이트됩니다. 다음이 업데이트됩니다. 모든 물리 분할의 CMU 펌웨어 및 모든 XSCF 장치의 XSCF 펌웨어. 마스터 XSCF 펌웨어만 업데이트될 수 있습니다.	물리 분할 전원이 차단 또는 공급됩니다.	약 120분
XSCF가 여러 개인 시스템의 경우 XSCF 펌웨어만 업데이트됩니다. 각 XSCF 장치의 XSCF 펌웨어가 동시에 업데이트됩니다. 또한 마스터 XSCF의 XSCF 펌웨어만 업데이트될 수 있습니다.	물리 분할 전원이 차단 또는 공급됩니다.	약 40분
부품 교체를 통해 펌웨어 버전이 일치되도록 자동 업데이트가 수행됩니다. 교체 후 각 부품의 펌웨어 버전은 교체 전 펌웨어 버전과 자동 일치됩니다. 다음 부품을 교체합니다. ■ 버전이 일치되도록 CPU 메모리 장치(하위)를 추가/교체합니다. ■ 버전이 일치되도록 크로스바 박스 또는 SPARC M10-4S의 XSCF 장치를 교체/추가합니다.	물리 분할 전원이 차단 또는 공급됩니다. 입력 전원을 차단한 채 교체하면(콜드 교체) 자동 업데이트가 수행되지 않습니다.	약 5분

노트 - SPARC M10-1의 마더보드 장치 또는 SPARC M10-4 및 SPARC M10-4S의 모든 XSCF를 교체하는 경우 버전이 교체 전 XSCF 펌웨어 버전과 자동 일치되지 않습니다. 운영자가 XCP 버전 일치 또는 업데이트를 수행하십시오.

노트 - 마더보드 장치 또는 모든 XSCF를 교체하는 경우 입력 전원의 차단 직후에는 부품을 교체하지 마십시오. 그렇지 않을 경우 모든 데이터가 손실됩니다. 입력 전원을 차단하기 전에 dumpconfig 명령으로 데이터를 백업하고 replacefru 명령으로 부품을 제거한 후 addfru 명령으로 부품을 추가하십시오.

업데이트 흐름

펌웨어 업데이트는 다음 순서에 따라 XSCF 쉘 또는 XSCF 웹에서 수행합니다. 1. XCP 가져오기, 2. XCP 업데이트 및 3. 적용.

다음은 기본 펌웨어 업데이트 절차입니다.

1. 사이트에서 **XCP** 펌웨어의 이미지 파일을 가져옵니다**.**
2. **Platadm** 또는 **fieldeng** 사용자 권한이 있는 사용자 계정으로 **XSCF**에 로그인합니다**.**
3. **USB** 또는 네트워크 디렉토리의 **XCP** 펌웨어 이미지 파일을 시스템으로 가져옵니

다**(getflashimage(8)** 참조**).**
XCP는 Oracle Solaris가 활성 또는 정지 상태인 동안에도 시스템으로 가져올 수 있습니다.

4. **XCP** 또는 **XSCF** 펌웨어를 업데이트합니다**(flashupdate(8)** 참조**).**
여기서 XSCF 펌웨어가 적용됩니다.
5. 물리 분할을 재부팅하여 **CMU** 펌웨어를 적용합니다**(poweron(8)** 및 **reset(8)** 참조**).**
6. 펌웨어 버전을 확인합니다**(version(8)** 참조**).**

이 4개 명령의 자세한 내용은 관련 설명서 페이지 또는『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오. 또한 연관된 XSCF 웹 메뉴는 "부록 B XSCF 웹 페이지 목록"을 참조하십시오.

18.1.3 펌웨어 업데이트

이 절에는 XSCF 쉘을 사용하여 펌웨어를 업데이트하는 방법이 설명되어 있습니다. 업데이트 절차는 XSCF 웹의 경우와 동일합니다. XSCF 웹 페이지는 "부록 B XSCF 웹 페이지 목록"을 참조하십시오.

각 업데이트의 설명에 앞서 다음 항목 "XCP 이미지 파일 준비" 및 "시스템으로 XCP 가져오기"를 수행합니다.

XCP 이미지 파일 준비

1. 웹 사이트에서 **PC** 또는 이 시스템과 연결된 워크스테이션의 아무 폴더에나 **XCP** 이미지 파일을 다운로드합니다**.**
2. **XCP** 버전을 확인합니다**.**
XCP 버전으로서 펌웨어 프로그램의 파일 이름에서 4자리 번호를 확인합니다 (tar.gz 형식).

   예: BBXCP2020.tar.gz의 경우 XCP 버전은 2020입니다.

시스템으로 XCP 가져오기

1. **XSCF** 쉘에 로그인합니다**.**
2. **getflashimage** 명령을 실행하여 현재 시스템에 있는 펌웨어 제품 목록을 확인합니다**.**

```
XSCF> getflashimage -l
Existing versions:
        Version                 Size Date
        BBXCP2010.tar.gz 51298982 Thu Jan 15 20:09:09 JST 2012
```

3. 가져온 **XCP** 이미지 파일**(tar.gz)**을 지정하고 **getflashimage** 명령을 실행하여 **XCP**를 시스템으로 가져옵니다**.**

   다음 예에서는 원격 ftp 서버에 로그인하기 위한 사용자 이름과 호스트 이름(필요

한 인증 암호)을 지정하고 새 버전 2020의 펌웨어 프로그램(tar.gz)을 가져옵니다.

```
XSCF> getflashimage -u yyyyy ftp://imgserver/img/BBXCP2020.tar.gz
Existing versions:
        Version              Size Date
        BBXCP2010.tar.gz 51298982 Thu Jan 15 20:09:09 JST 2012
Warning: About to delete old versions.
Continue? [y|n]: y
Removing BBXCP2010.tar.gz.
Password: [not echoed]
  0MB received
  1MB received
  2MB received
...
  40MB received
Download successful: 41470 Kbytes in 46 secs (940.250 Kbytes/
sec)
MD5: 683fb5240e4937948dd6ad83b4a99669
```

4. 정상 종료 메시지 **"Download successful: ..." and "MD5: ..."**가 나타나면 **XCP** 가져오기가 완료된 것입니다**. getflashimage -l** 명령을 사용하여 가져온 버전을 확인합니다**.**

노트 **-** XCP 가져오기 후에 메시지 "Error: File is invalid or corrupt"가 나타나면 가져온 XCP 이미지 파일이 해당 파일이 아닌 것입니다. 불법 XCP 이미지 파일을 가져왔거나 고객이 파일을 다운로드한 후 불법 액세스하여 XCP 이미지 파일을 변경한 것이 그 원인일 수 있습니다. 이 경우 올바른 XCP 이미지 파일을 가져와 XCP를 다시 가져오십시오.

XSCF가 1개인 시스템의 XCP 업데이트

다음 작동을 수행합니다. XSCF 펌웨어 다운로드 및 적용과 CMU 펌웨어 다운로드.

1. **"**시스템으로 **XCP** 가져오기**"**를 수행합니다**.**
2. **version** 명령을 실행하여 작동 중인 펌웨어의 버전을 확인합니다**.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current) : 2010
CMU            : 02.00.0010
     POST          : 1.20.0
     OpenBoot PROM : 4.34.0+1.1.0
     Hypervisor    : 0.22.0
XSCF           : 02.00.0010
XCP1 (Reserve) : 2010
CMU            : 02.00.0010
     POST          : 1.20.0
     OpenBoot PROM : 4.34.0+1.1.0
     Hypervisor    : 0.22.0
XSCF           : 02.00.0010
```

3. **flashupdate** 명령을 실행하여 펌웨어를 새 버전으로 업데이트할 수 있는지 확인합

니다.

```
XSCF> flashupdate -c check -m xcp -s 2020
```

메시지 출력 없이 "XSCF>" 프롬프트가 나타나면 펌웨어 업데이트가 활성화됩니다.

메시지 "An internal error has occurred."가 나타나면 이전 XCP 펌웨어가 아직 적용되지 않은 것입니다. 따라서 펌웨어 업데이트가 비활성화됩니다. 이전 업데이트가 완료된 후 펌웨어 업데이트를 다시 수행합니다.

4. **flashupdate** 명령을 실행하여 펌웨어 업데이트를 수행합니다.
   다음 예에서는 XCP를 버전 2010에서 2020으로 업데이트합니다.

```
XSCF> flashupdate -c update -m xcp -s 2020
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [2400sec]   0..... 30..... 60.....
90..... 120..... 150..... 180..... 210..... 240.....-
270..... 300..... 330..... 360..... 390..... 420..... 450.....
480..... 510.....|
540.....570.....600
```

여기서 XSCF가 재설정되어 XSCF 세션이 분리됩니다. XSCF에 다시 연결합니다. 이제 XSCF 펌웨어만의 적용이 완료되었습니다.

5. **monitor** 옵션이 지정된 **showlogs** 명령을 실행하여 **XSCF** 펌웨어 업데이트의 완료를 확인합니다.

```
XSCF> showlogs monitor
:
Jun 20 07:25:48 PAPL1-1-0 Event: SCF:XCP update has been
completed (XCP version=2020:last version=2010)
```

업데이트 동안 오류가 발견되지 않았는지 확인합니다. 메시지 "XCP update has been completed"가 나타나면 업데이트가 완료된 것입니다.

6. 물리 분할을 다시 시작하여 **CMU** 펌웨어 업데이트를 완료합니다. 물리 분할의 논리 도메인 또한 재설정됩니다.
7. **XSCF** 쉘 명령줄에서 **version** 명령을 실행하여 펌웨어 버전이 시스템 작동 동안 펌웨어가 적용된 버전인지 확인합니다.
8. 물리 분할을 지정하고 **console** 명령을 실행하여 제어 도메인 콘솔로 전환합니다.
9. **Oracle Solaris**에서 **prtdiag(1M)** 명령을 실행하여 펌웨어가 제어 및 논리 도메인의 펌웨어가 적용된 펌웨어인지 확인합니다.

XSCF가 1개인 시스템의 XSCF 펌웨어만 업데이트

다음 작동을 수행합니다. XSCF 펌웨어 다운로드 및 적용.

1. **"**시스템으로 **XCP** 가져오기**"**를 수행합니다**.**
2. **version** 명령을 실행하여 작동 중인 펌웨어의 버전을 확인합니다**.**

```
XSCF> version -c xcp -v
```

3. **flashupdate** 명령을 실행하여 **XSCF** 펌웨어를 새 버전으로 업데이트할 수 있는지 확인합니다**.**

```
XSCF> flashupdate -c check -m xscf -s 2020
```

메시지 출력 없이 "XSCF>" 프롬프트가 나타나면 펌웨어 업데이트가 활성화됩니다.

메시지 "An internal error has occurred."가 나타나면 이전 XCP 펌웨어가 아직 적용되지 않은 것입니다. 따라서 펌웨어 업데이트가 비활성화됩니다. 이전 업데이트가 완료된 후 펌웨어 업데이트를 다시 수행합니다.

4. **flashupdate** 명령을 실행하여 펌웨어 업데이트를 수행합니다**.**
다음 예에서는 XSCF 펌웨어를 버전 2010에서 2020으로 업데이트합니다.

```
XSCF> flashupdate -c update -m xscf -s 2020
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [2400sec]
  0..... 30..... 60..... 90..... 120..... 150..... 180.....
210...... 240......-
270..... 300..... 330..... 360..... 390..... 420..... 450.....
480......510.....|
540.....570.....600
```

여기서 XSCF가 재설정되어 XSCF 세션이 분리됩니다. XSCF에 다시 연결합니다. 이제 XSCF 펌웨어의 업데이트/적용이 완료되었습니다.

5. **monitor** 옵션이 지정된 **showlogs** 명령을 실행하여 **XSCF** 펌웨어 업데이트의 완료를 확인합니다**.**

```
XSCF> showlogs monitor
:
Jun 20 07:25:48 PAPL1-1-0 Event: SCF:XCP update has been
completed (XCP version=2020:last version=2010)
```

업데이트 동안 오류가 발견되지 않았는지 확인합니다. 메시지 "XCP update has been completed"가 나타나면 업데이트가 완료된 것입니다.

6. **XSCF** 쉘 명령줄에서 **version** 명령을 실행하여 펌웨어 버전이 시스템 작동 동안 펌웨어가 적용된 버전인지 확인합니다**.**

XSCF가 여러 개인 시스템의 XCP 업데이트

다음 작동을 수행합니다. XSCF 펌웨어 다운로드 및 적용과 CMU 펌웨어 다운로드.

모든 XSCF 장치의 XSCF 펌웨어가 동시에 업데이트됩니다. 마스터 XSCF 펌웨어만 업데이트될 수 있습니다.

1. **showhardconf** 명령을 실행하여 마스터 **XSCF** 및 스탠바이 **XSCF**의 상태가 정상인지 확인합니다.
2. 마스터 **XSCF**에 로그인합니다.
3. **"**시스템으로 **XCP** 가져오기**"**를 수행합니다.
4. **version** 명령을 실행하여 작동 중인 펌웨어의 버전을 확인합니다.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current) : 2010
CMU            : 02.01.0000
     POST          : 1.20.0
     OpenBoot PROM : 4.34.0+1.1.0
     Hypervisor    : 0.22.0
XSCF           : 02.00.0010
XCP1 (Reserve) : 2010
CMU            : 02.01.0000
     POST          : 1.20.0
     OpenBoot PROM : 4.34.0+1.1.0
     Hypervisor    : 0.22.0
XSCF           : 02.00.0010
BB#01-XSCF#0 (Standby)
XCP0 (Current) : 2010
CMU            : 02.01.0000
     POST          : 1.20.0
     OpenBoot PROM : 4.34.0+1.1.0
     Hypervisor    : 0.22.0
XSCF           : 02.00.0010
XCP1 (Reserve) : 2010
CMU            : 02.01.0000
     POST          : 1.20.0
     OpenBoot PROM : 4.34.0+1.1.0
     Hypervisor    : 0.22.0
XSCF           : 02.00.0010
```

5. **flashupdate** 명령을 실행하여 펌웨어를 새 버전으로 업데이트할 수 있는지 확인합니다.

```
XSCF> flashupdate -c check -m xcp -s 2020
```

메시지 출력 없이 "XSCF>" 프롬프트가 나타나면 펌웨어 업데이트가 활성화됩니다.

메시지 "An internal error has occurred."가 나타나면 이전 XCP 펌웨어가 아직 적용되지 않은 것입니다. 따라서 펌웨어 업데이트가 비활성화됩니다. 이전 업데이트

가 완료된 후 펌웨어 업데이트를 다시 수행합니다.

6. **flashupdate** 명령을 실행하여 펌웨어 업데이트를 수행합니다.
   다음 예에서는 XCP를 버전 2010에서 2020으로 업데이트합니다.

```
XSCF> flashupdate -c update -m xcp -s 2020
The XSCF will be reset. Continue? [y|n] :y XCP update is
started. [2400sec]   0..... 30..... 60..... 90..... 120.....
150..... 180..... 210..... 240.....-
270..... 300..... 330..... 360..... 390..... 420..... 450.....
480.....510.....|
540.....570.....600
```

   펌웨어 업데이트는 스탠바이 XSCF에 이은 마스터 XSCF 순서대로 자동 수행됩니다. 스탠바이측 업데이트가 완료되면 마스터 및 스탠바이 XSCF가 전환됩니다. 여기서 XSCF가 재설정되어 XSCF 세션이 분리됩니다. 이제 XSCF 펌웨어만의 적용이 완료되었습니다.

7. **XSCF**에 다시 연결합니다.
   펌웨어 업데이트가 완료되면 마스터 및 스탠바이 XSCF의 상태가 원래 상태와 반대가 됩니다. 예를 들어 빌딩 블록 ID 0(BB-ID 0)의 마스터 XSCF에 대해 펌웨어 업데이트가 수행되면 업데이트 완료 시에 빌딩 블록 ID 1(BB-ID 1)이 마스터측이 됩니다.
8. **showhardconf** 명령을 실행하여 마스터 **XSCF** 및 스탠바이 **XSCF**의 상태가 원래 상태와 반대가 되는지 확인합니다.
9. **XSCF**를 전환하려면 **switchscf** 명령을 실행합니다.

```
XSCF> switchscf -t Standby
The XSCF unit switch between the Active and Standby states.
Continue? [y|n] :y
```

10. **monitor** 옵션이 지정된 **showlogs** 명령을 실행하여 **XSCF** 펌웨어 업데이트의 완료를 확인합니다.

```
XSCF> showlogs monitor
:
Jun 20 07:25:48 PAPL1-1-0 Event: SCF:XCP update has been
completed (XCP version=2020:last version=2010)
```

    업데이트 동안 오류가 발견되지 않았는지 확인합니다. 메시지 "XCP update has been completed"가 나타나면 업데이트가 완료된 것입니다.

11. 물리 분할을 다시 시작하여 **CMU** 펌웨어 업데이트를 완료합니다. 물리 분할의 논리 도메인 또한 재설정됩니다.
12. **XSCF** 쉘 명령줄에서 **version** 명령을 실행하여 펌웨어 버전이 시스템 작동 동안 펌웨어가 적용된 버전인지 확인합니다.
13. 물리 분할을 지정하고 **console** 명령을 실행하여 도메인 콘솔로 전환합니다.

14. **Oracle Solaris**에서 **prtdiag(1M)** 명령을 실행하여 펌웨어가 제어 및 논리 도메인의 펌웨어가 적용된 펌웨어인지 확인합니다.

XSCF가 여러 개인 시스템의 XSCF 펌웨어만 업데이트

다음 작동을 수행합니다. XSCF 펌웨어 다운로드 및 적용.

모든 XSCF 장치의 XSCF 펌웨어가 동시에 업데이트됩니다. 또한 마스터 XSCF의 XSCF 펌웨어만 업데이트될 수 있습니다.

1. **"XSCF**가 여러 개인 시스템의 **XCP** 업데이트**"**의 **1 ~ 4**단계를 실행합니다.
2. **flashupdate** 명령을 실행하여 **XSCF** 펌웨어를 새 버전으로 업데이트할 수 있는지 확인합니다.

```
XSCF> flashupdate -c check -m xscf -s 2020
```

   메시지 출력 없이 "XSCF>" 프롬프트가 나타나면 펌웨어 업데이트가 활성화됩니다.

   메시지 "An internal error has occurred."가 나타나면 이전 XCP 펌웨어가 아직 적용되지 않은 것입니다. 따라서 펌웨어 업데이트가 비활성화됩니다. 이전 업데이트가 완료된 후 펌웨어 업데이트를 다시 수행합니다.

3. **flashupdate** 명령을 실행하여 펌웨어 업데이트를 수행합니다.
   다음 예에서는 XSCF 펌웨어를 버전 2010에서 2020으로 업데이트합니다.

```
XSCF> flashupdate -c update -m xscf -s 2020
The XSCF will be reset. Continue? [y|n] :y XCP update is
started. [2400sec]   0..... 30..... 60..... 90..... 120.....
150..... 180..... 210..... 240.....- 270..... 300.....
 330..... 360..... 390..... 420..... 450..... 480.....510.....|
540.....570.....600
```

   펌웨어 업데이트는 스탠바이 XSCF에 이은 마스터 XSCF 순서대로 자동 수행됩니다. 스탠바이측 업데이트가 완료되면 마스터 및 스탠바이 XSCF가 전환됩니다. 여기서 XSCF가 재설정되어 XSCF 세션이 분리됩니다. 이제 XSCF 펌웨어만의 적용이 완료되었습니다.

4. **"XSCF**가 여러 개인 시스템의 **XCP** 업데이트**"**의 **7 ~ 10**단계와 동일한 작동을 실행합니다.
5. **XSCF** 쉘 명령줄에서 **version** 명령을 실행하여 펌웨어 버전이 시스템 작동 동안 펌웨어가 적용된 버전인지 확인합니다.

부품 교체에 의한 펌웨어 버전 일치

다음의 경우 부품을 교체하고 펌웨어 버전을 일치시킵니다.

- CMU 펌웨어 버전이 일치되도록 CPU 메모리 장치(하위)를 추가/교체합니다.
- XSCF 펌웨어 버전이 일치되도록 크로스바 박스 또는 SPARC M10-4S의 XSCF 장치를 추가/교체합니다.

노트 - SPARC M10-1의 마더보드 장치 또는 모든 XSCF를 교체하는 경우 버전이 교체 전 XSCF 펌웨어 버전과 자동 일치되지 않습니다. 운영자가 XCP 펌웨어 업데이트를 수행하여 버전을 확인하십시오.

노트 - 마더보드 장치 또는 모든 XSCF를 교체하는 경우 입력 전원의 차단 직후에는 부품을 교체하지 마십시오. 그렇지 않을 경우 모든 데이터가 손실됩니다. 입력 전원을 차단하기 전에 dumpconfig 명령으로 데이터를 백업하고 replacefru 명령으로 부품을 제거한 후 addfru 명령으로 부품을 추가하십시오.

CPU 메모리 장치 추가/교체 시의 버전 일치

1. **CPU** 메모리 장치**(**하위**)**의 추가**/**교체 및 물리 분할에 할당을 완료한 후 물리 분할의 전원을 공급합니다**.**
   이 경우 CMU 펌웨어가 자동 업데이트됩니다. (자동 버전 일치)
2. **version** 명령을 실행하여 대상 물리 분할의 **CMU** 펌웨어 버전을 확인합니다**.**

```
XSCF> version -c cmu -v
PPAR-ID 0: 02.01.0000
   POST            : 1.20.0
   OpenBoot PROM   : 4.34.0+1.1.0
   Hypervisor      : 0.22.0
PSB#00: 02.01.0000(Current)
   POST            : 1.20.0
   OpenBoot PROM   : 4.34.0+1.1.0
   Hypervisor      : 0.22.0
PSB#00: 02.01.0000(Reserve)
   POST            : 1.20.0
   OpenBoot PROM   : 4.34.0+1.1.0
   Hypervisor      : 0.22.0

:
```

크로스바 박스 또는 SPARC M10-4S의 XSCF 장치 추가/교체 시 버전 일치

- 입력 전원 공급 중의 작동

1. 현장 엔지니어가 유지 관리 지침에 따라 교체를 수행하는 경우 **XSCF** 펌웨어 버전 일치가 자동으로 수행됩니다**.**
2. 교체한 부품의 **XSCF** 펌웨어 버전을 확인합니다**.**

- 입력 전원 차단 중의 작동

1. **version** 명령을 실행하여 원래 펌웨어 버전을 확인합니다**.**
2. 입력 전원을 차단하여 부품을 교체합니다**.**
3. 입력 전원을 공급합니다**.**
4. 마스터 **XSCF**에 로그인합니다**.**
5. **version** 명령을 실행합니다**.**
   펌웨어 버전이 동일한 버전이면 작동이 종료됩니다.

펌웨어 버전이 다르면 메시지가 출력됩니다.

이 경우 다음을 수행합니다.

- 스탠바이 또는 슬레이브 XSCF의 버전이 다른 경우(스탠바이 또는 슬레이브 XSCF가 교체됨):

a. sync 옵션이 지정된 **flashupdate** 명령을 실행합니다.

```
XSCF> flashupdate -c sync
```

version 명령을 실행하여 펌웨어 버전을 확인합니다.

- 마스터 XSCF의 버전이 다른 경우(원래 상태로 복귀):

a. switch 명령을 실행하여 **XSCF**를 마스터에서 스탠바이 **XSCF**로 전환합니다.

```
XSCF> switchscf -t Standby
```

b. 새 마스터 **XSCF**에 로그인합니다.

c. sync 옵션이 지정된 **flashupdate** 명령을 실행합니다.

d. version 명령을 실행하여 펌웨어 버전을 확인합니다.

노트 - 마더보드 장치 또는 모든 XSCF를 교체하는 경우 입력 전원의 차단 직후에는 부품을 교체하지 마십시오. 그렇지 않을 경우 모든 데이터가 손실됩니다. 입력 전원을 차단하기 전에 dumpconfig 명령으로 데이터를 백업하고 replacefru 명령으로 부품을 제거한 후 addfru 명령으로 부품을 추가하십시오.

18.1.4 펌웨어 업데이트 중 문제

펌웨어 업데이트 동안 시스템 끊김이 발생하거나 아래 나열된 오류 메시지가 출력되는 경우 비정상 XSCF 장치는 사용이 불가능하며 고장 부품으로서 처리됩니다.

- XSCF가 1개인 시스템
  쓰기 오류 또는 재설정 실패 오류
- XSCF가 여러 개인 시스템
  스탠바이나 마스터측에 쓰기 오류 또는 재설정 실패 오류

하지만 펌웨어 업데이트 동안 이상이 발생하면 펌웨어 업데이트를 다시 시도합니다. 펌웨어 업데이트가 정상적으로 종료될 수 있습니다.

18.1.5 펌웨어 업데이트와 관련된 FAQ

Q: CMU 펌웨어를 적용할 때 **2**회 재부팅해도 괜찮습니까**?**

A: 아무런 문제가 없습니다.

Q: XSCF가 여러 개인 시스템의 경우 마스터 **XSCF**와 스탠바이 **XSCF**가 중간에 전환되는 이유는 무엇입니까**?**

A: 이유는 다음과 같습니다. 마스터 XSCF는 스탠바이 XSCF에서 펌웨어가 업데이트되도록 제어합니다. 스탠바이측 펌웨어 업데이트가 완료되면 스탠바이측 또는 새 펌웨어가 마스터측으로 전환됩니다. 그런 다음 스탠바이측(이전 마스터측) XSCF에서 펌웨어가 다시 업데이트됩니다.

Q: CMU 펌웨어의 펌웨어 업데이트를 모든 물리 분할에 동시 적용할 수 있습니까?

A: 예. poweron 명령으로 모든 물리 분할을 지정하여 새 펌웨어를 적용할 수 있습니다.

18.2 Oracle Solaris 및 Oracle VM Server for SPARC 업데이트

이 절에는 논리 도메인에 설치된 Oracle Solaris의 업데이트 방법이 설명되어 있습니다.

물리 분할에 맞게 구성된 논리 도메인 각각에는 Oracle Solaris가 이미 설치되어 있습니다. 각 논리 도메인마다 Oracle Solaris를 개별적으로 업데이트할 수 있습니다.

업데이트 전

제어 도메인에서 Oracle Solaris를 업데이트하기 전에 아래 나타난 데이터를 사전에 저장하고 업데이트 후에는 데이터를 복원합니다.

- 자동 저장 구성 디렉토리
  /var/opt/SUNWldm/autosave-*
- 논리 도메인 제약 조건 데이터베이스 파일
  이는 /var/opt/SUNWldm/ldom-db.xml에서 찾을 수 있는 논리 도메인 제약 조건 데이터베이스 파일입니다.

자세한 내용은 사용 버전의『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

업데이트

Oracle Solaris를 업데이트하려면 SPARC M10 시스템 지원 버전의 Oracle Solaris를 설치하고 SRU(Support Repository Update)를 적용합니다.
Oracle Solaris의 지원 버전과 픽스 관련 최신 정보는『SPARC M10 시스템 제품 노트』를 참조하십시오.

Oracle Solaris 및 Oracle VM Server for SPARC의 업데이트 방법은 사용 버전의『Oracle VM Server for SPARC 관리 안내서』 및 Oracle Solaris 관련 설명서를 참조하십시오.

19장

XSCF/시스템 문제 해결

이 장에는 XSCF 사용 중과 시스템 실행 중에 발생할 수 있는 문제가 설명되고 문제에 대한 솔루션이 제공되어 있습니다.

- XSCF 문제 해결
- 질문과 대답/FAQ
- XSCF가 있는 시스템 문제 해결

19.1 XSCF 문제 해결

이 절에는 XSCF 사용 중에 발생할 수 있는 문제가 설명되고 문제에 대한 솔루션이 제공되어 있습니다.

XSCF에 로그인할 수 없음

- 로그인에 올바른 사용자 이름을 입력했는지 확인합니다.
- 올바른 암호를 입력했는지 확인합니다.
- XSCF 사용자 수를 확인합니다. 사용자 수와 관련된 정보는 "4.7 연결 가능한 사용자 수"를 참조하십시오.

XSCF의 로그인 암호를 잊어버림

- password 명령을 사용하여 암호를 재설정하도록 platadm 또는 useradm 사용자 권한이 있는 시스템 관리자에게 요청합니다.
- 시스템 관리자가 로그인 암호를 잊어버린 경우 "기본" 계정을 사용하여 로그인한 후 password 명령을 사용하여 다시 등록합니다. "기본" 계정을 사용한 로그인 인증과 관련된 자세한 내용은 『SPARC M10 시스템 설치 안내서』의 "6장 시스템의 초기 진단 구현"을 참조하십시오.

직렬 포트를 통해 XSCF에 연결할 수 없음

- 터미널 소프트웨어가 직렬 포트에 연결되었는지 확인합니다.
- 터미널 소프트웨어의 설정을 확인합니다. (9600 bps의 전송 속도 설정, 0의 지연 설

정 등). 설정과 관련된 자세한 내용은 "4.1.2 직렬 연결로 XSCF 쉘에 로그인하는 방법"을 참조하십시오.

XSCF-LAN을 통해 Telnet을 사용하여 XSCF에 연결할 수 없음

- LAN 케이블이 XSCF 터미널과 서버 사이에 올바로 연결되었는지 확인합니다.
- 터미널 소프트웨어가 Telnet 포트에 연결되었는지 확인합니다.
- shownetwork 명령을 사용하여 XSCF-LAN 설정의 활성화 여부를 확인합니다.
- showtelnet 명령을 사용하여 Telnet 서비스의 활성화 여부를 확인합니다.
- 입력한 IP 주소 및 포트 번호가 설정과 일치하는지 확인합니다.
- Telnet/SSH를 사용한 연결 수가 최대 수를 초과하지 않는지 확인합니다. 최대 수와 관련된 정보는 "4.7 연결 가능한 사용자 수"를 참조하십시오.
- 필요한 경우 직렬 포트를 통해 XSCF에 직접 연결된 PC의 콘솔을 사용하여 XSCF 쉘에 로그인하고 shownetwork 명령을 사용하여 XSCF-LAN 설정을 확인합니다.

XSCF-LAN을 통해 SSH를 사용하여 XSCF에 연결할 수 없음

- LAN 케이블이 XSCF 터미널과 서버 사이에 올바로 연결되었는지 확인합니다.
- shownetwork 명령을 사용하여 XSCF-LAN 설정의 활성화 여부를 확인합니다.
- showssh 명령을 사용하여 SSH 서비스의 활성화 여부를 확인합니다.
- 입력한 IP 주소 및 포트 번호가 설정과 일치하는지 확인합니다.
- Telnet/SSH를 사용한 연결 수가 최대 수를 초과하지 않는지 확인합니다. 최대 수와 관련된 정보는 "4.7 연결 가능한 사용자 수"를 참조하십시오.
- 필요한 경우 직렬 포트를 통해 XSCF에 직접 연결된 PC의 콘솔을 사용하여 XSCF 쉘에 로그인하고 shownetwork 명령을 사용하여 XSCF-LAN 설정을 확인합니다.
- 호스트 키의 설정이 올바른지 확인합니다. XSCF 장치를 교체하면 호스트 키 설정이 XSCF의 사전 설정된 키 설정으로 복원됩니다.
- 클라이언트 소프트웨어의 설정이 올바른지 확인합니다.

XSCF의 IP 주소를 모름

- shownetwork 명령을 사용하여 현재 네트워크 구성을 확인합니다. 아직 설정되지 않은 경우 설정을 확인하도록 시스템 관리자에게 요청합니다.
- 필요한 경우 직렬 포트를 통해 XSCF에 직접 연결된 PC의 콘솔을 사용하여 XSCF 쉘에 로그인하고 shownetwork 명령을 사용하여 XSCF-LAN 설정을 확인합니다.

XSCF 쉘 터미널 또는 도메인 콘솔이 갑자기 분리됨

- 누군가 setnetwork, setroute, sethostname, setnameserver 및 setsscp 명령이 사용된 후 applynetwork 및 rebootxscf 명령을 실행했거나 flashupdate 명령이 실행된 것일 수 있습니다. XSCF를 사용하려면 재연결하고 시스템에 다시 로그인합니다.
- 누군가 setdate 또는 switchscf 명령을 실행한 것일 수 있습니다. XSCF를 사용하려면 재연결하고 시스템에 다시 로그인합니다.
- 로그인 후 지정된 시간 동안 XSCF 쉘을 사용하지 않으면 자동 종료됩니다. 시간 모니터링 기능이 활성화되고 XSCF 설정에서 이 기능에 대해 시간이 지정된 경우에만

지정된 시간 경과 시 이처럼 강제 종료됩니다.

- 클라이언트가 이스케이프 문자(예: "#")를 설정하고 "." (마침표) 키를 입력한 경우 Oracle Solaris 보안 쉘 또는 OpenSSH SSH 클라이언트가 분리됩니다. Oracle Solaris 보안 쉘 또는 OpenSSH SSH 클라이언트의 이스케이프 문자 설정과 console 명령을 사용하여 설정한 이스케이프 문자 설정이 동일하면 터미널이 분리됩니다. 따라서 설정 하나의 값을 변경합니다. 자세한 정보는 SSH 클라이언트 설명서를 참조하십시오.

서버 전원을 공급/차단할 수 없음

- platadm 또는 fieldeng 권한 이외의 사용자 권한으로 작동하는 동안 시스템 전체의 전원 공급/차단 작동이 불가능합니다. 사용자 권한과 관련된 정보는 "8.3.3 사용자 권한 유형"을 참조하십시오.

XSCF 사용자를 추가할 수 없음

- XSCF 등록 사용자 수를 확인합니다. 등록 사용자 수와 관련된 정보는 "4.7 연결 가능한 사용자 수"를 참조하십시오. 그렇지 않으면 시스템 관리자에게 문의하십시오.

이메일 보고서가 XSCF에서 수신되지 않음

- XSCF가 모든 이벤트를 반드시 보고하는 것은 아닙니다. 이는 각 부품 고장 또는 인증 오류 이벤트에 대해 이메일 메시지를 전송합니다. 오류 로그의 관련 이벤트 여부를 확인하고 이 이벤트가 보고될 이벤트 로그의 이벤트인지 확인하려면 "17.1 XSCF로 저장된 로그 확인"을 참조하십시오.
- showemailreport 명령을 사용하여 설정의 활성화 여부를 확인합니다. 이 이벤트에 대해 이메일 메시지가 수신되지 않은 경우 오류 이메일 메시지가 오류 이메일 수신자에게 전송되었는지 확인하거나 기록된 오류의 로그를 확인합니다.
- 이메일 메시지 수신에 휴대폰을 사용하는 경우 수신 메시지의 설정된 제한 사항에 대해서 폰 설정을 확인합니다.

XSCF 웹의 맨 위 페이지에 액세스할 수 없음

- showhttps 명령을 사용하여 XSCF 웹 설정의 활성화 여부를 확인합니다.
- 입력한 URL이 올바른지 확인합니다. (예: "https"의 "s" 누락 여부)
- 설정된 IP 주소를 통한 액세스가 허용되는지 확인하도록 시스템 관리자에게 요청합니다.
- 웹 브라우저의 SSL/TLS 기능 설정이 활성화되었는지 확인합니다.

XSCF 웹 창을 표시할 수 없음

- XSCF 웹의 맨 위 페이지에서 시스템에 로그인한 후라도 XSCF 웹 창이 표시되지 않으면 JavaScript가 웹 브라우저 설정에서 비활성화된 것일 수 있습니다. 브라우저 설정에서 JavaScript를 활성화하고 로그인을 다시 시도합니다.
- 웹 브라우저 설정에서 팝업 창 표시가 비활성화되어 있으면 XSCF 웹 창이 표시되지 않습니다. 브라우저 설정을 확인합니다.

XSCF 웹 암호를 잊어버림

- XSCF 웹 인증은 XSCF 쉘 인증과 동일합니다. 위 "XSCF의 로그인 암호를 잊어버림"을 참조하십시오.

로그인 후 첫 번째 XSCF 웹 액세스 시도에 실패함

- 웹 브라우저 설정에서 쿠키가 허용되어 있는지 확인합니다.

XSCF 웹의 웹 페이지가 브라우저에서 올바로 표시되지 않음

- 일부 버전의 웹 브라우저는 창을 올바로 표시하지 않습니다. 지원되는 브라우저는 "4.5 XSCF 웹에 로그인"을 참조하고 브라우저를 최신 버전으로 업데이트합니다.

경고 메시지가 XSCF 웹에 표시됨

- 보안 경고 메시지의 내용을 확인하고 XSCF 웹 사용을 중단합니다. 확인된 경고 내용에 대한 대응 조치를 수행합니다. 만료 날짜가 지나면 XSCF의 HTTPS 서비스 설정을 재설정합니다. HTTPS 서비스 설정과 관련된 자세한 내용은 "8.7 XSCF에 로그인하기 위한 HTTPS 서비스 구성"을 참조하십시오.

기타 문제

- 시스템 관리자에게 문의하십시오. XSCF 로그 데이터를 수집/저장해야 하는 경우 XSCF 쉘 명령을 사용하여 저장합니다. 로그 저장 방법은 "17.1.13 스냅샷으로 파일에 로그 저장"을 참조하십시오.

19.2 질문과 대답/FAQ

이 절에는 XSCF 사용과 관련된 질문과 대답이 포함되어 있습니다.

Q: IP 주소가 XSCF-LAN용 LAN 포트에 기본적으로 할당됩니까?

A: IP 주소는 XSCF-LAN에 기본적으로 할당되지 않습니다. XSCF-LAN IP 주소와 관련된 자세한 내용은 "8.5.2 XSCF 네트워크 인터페이스 이해"를 참조하십시오.

Q: IP 주소가 SSCP에 기본적으로 할당됩니까?

A: IP 주소는 기본적으로 할당됩니다. SSCP의 기본 IP 주소는 "8.5.4 SSCP에서 IP 주소 설정 이해"를 참조하십시오. 기본 IP 주소가 사용자 LAN의 환경에 영향을 미칠 수도 있는 경우 변경합니다.

Q: 서버 전원 공급 후 Oracle Solaris가 시작되는 동안 Oracle Solaris 끊김 이벤트가 발생하는 경우 XSCF에서 서버 전원을 차단할 수 있습니까?

A: 게스트 도메인의 끊김 시 ldm panic-domain 명령을 사용하여 Oracle Solaris 덤프를 수집합니다. lmd 명령의 자세한 내용은 사용 버전의 『Oracle VM Server for SPARC 참조 설명서』를 참조하십시오.
제어 도메인의 끊김 시 다음을 수행합니다.

a. XSCF 쉘에서 panic 옵션의 reset 명령을 실행하여 Oracle Solaris 덤프를 수행

합니다.

b. a.를 수행한 후 **Oracle Solaris** 덤프에 실패하면 **XSCF**에서 **sendbreak**를 실행하고 **sync**를 선택합니다.

c. b.를 수행한 후 재설정 작동에 실패하면 **XSCF** 쉘에서 **por** 옵션의 **reset** 명령을 실행하거나 다음 방법 가운데 하나를 사용하여 전원을 강제 차단합니다.

방법 1: 서버 운영 패널의 전원 버튼을 4초 동안 누르고 있습니다.
방법 2: XSCF 쉘에서 poweroff 명령을 실행합니다.

Q: 서버 입력 전원의 공급 시점부터 **Oracle Solaris** 시작 시까지 **XSCF**에 의해 어떤 종류의 처리가 실행됩니까**?**

A: 시스템 시작 전의 처리 흐름은 다음과 같습니다. 자세한 내용은 "3장 시스템 시작/정지"을 참조하십시오.

a. 운영자가 입력 전원을 공급합니다.

b. XSCF가 시작됩니다.

c. 운영자가 서버 전원을 공급합니다.

d. XSCF가 하드웨어를 초기화합니다.

e. POST가 시작되어 하드웨어의 초기 진단을 수행합니다.

f. OpenBoot PROM이 시작됩니다.

g. OpenBoot PROM이 부팅 프로세스를 시작합니다.

h. Oracle Solaris가 시작됩니다.

Q: 정상적으로 **XSCF**에 로그인 또는 로그아웃하는 동안 어떤 종류의 메시지가 터미널에 표시됩니까**?**

A: 다음에는 XSCF에 로그인 성공/실패가 나타나 있습니다. 다음 예에는 로그인 성공이 나타나 있습니다.

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

다음 예에는 로그인 실패가 나타나 있습니다.

```
login: jsmith
Password: xxxxxxxx
Login incorrect
```

A: 다음에는 XSCF에서 로그아웃 성공/실패가 나타나 있습니다. 다음 예에는 로그아웃 성공이 나타나 있습니다.

```
XSCF> exit
Logout
```

다음 예에는 로그아웃 실패가 나타나 있습니다.

```
XSCF> exit
Not supported in this system.
```

노트 - 위 예는 터미널의 클라이언트 소프트웨어에 따라 달라집니다.

Q: MIB 정의 파일의 오류 정보와 **XSCF** 오류 로그 간의 관계는 무엇입니까**?**

A: MIB 정의 파일에 나타난 오류 정보는 XSCF의 최신 오류 로그입니다.

19.3 XSCF가 있는 시스템 문제 해결

이 절에는 서버가 응답하지 않는 경우(시스템에 문제 또는 패닉이 발생했다는 의미) XSCF를 효과적으로 사용하는 방법이 설명되어 있습니다.

서비스 엔지니어에게 문의 전

서비스 엔지니어에게 문의하기 전에 먼저 아래 절차를 따릅니다. 이 절차는 문제를 해결하고 불필요한 문의를 사전에 없애는 데 도움이 될 수 있습니다.

1. 서버가 응답하지 않는 경우 운영 패널의 모드 스위치를 서비스 모드로 설정합니다.
2. 다음 방법 가운데 하나를 사용하여 시스템 상태를 확인합니다.

- SSH/Telnet을 통해 XSCF 쉘을 사용할 수 없는 경우

  a. 터미널을 **XSCF**의 직렬 포트에 연결합니다.

  b. 사용자 계정과 암호를 입력하여 **XSCF** 쉘에 로그인합니다.

  c. XSCF 쉘을 사용하여 오류 로그와 기타 정보를 확인합니다.

- SSH/Telnet 또는 직렬 포트를 통해 XSCF 쉘을 사용할 수 있는 경우

  a. XSCF 사용자 계정을 사용하여 **XSCF**에 로그인합니다.

  b. XSCF-LAN 포트를 통해 연결하고 **XSCF** 쉘을 사용하여 오류 로그와 기타 정보를 확인합니다. 오류 로그와 관련된 자세한 내용은 "17.1 XSCF로 저장된 로그 확인"을 참조하고 정정 작업을 확인합니다.

  c. 그렇지 않을 경우 직렬 포트를 통해 **XSCF** 쉘을 사용하여 **XSCF** 이벤트 로그와 서버 상태를 확인합니다. 다음 명령을 사용하여 문제 발생 시점에 일어난 이벤트를 확인합니다.

  showlogs error

  showlogs event

  showlogs power

  showlogs monitor

  showlogs console

  오류가 발견되면 "17.1 XSCF로 저장된 로그 확인"을 참조하십시오.

  d. 최신 메시지에 대해 **XSCF** 콘솔 로그 또는 패닉 로그를 확인합니다. 문제 감지 후 메시지가 **Oracle Solaris**에 의해 출력된 것일 수 있습니다. 패닉과 관련된 경우

panic 옵션의 **showlogs** 명령을 사용하여 패닉 발생 시점에 일어난 이벤트를 확인합니다.

3. 위 사항의 확인 후에도 문제를 발견할 수 없으면 시스템을 다시 시작합니다.
4. 문제가 발견되면 **"17.1 XSCF**로 저장된 로그 확인**"**을 참조하고 관련 구성요소의 교체를 위한 **XSCF** 쉘 명령의 유지 관리 지침 사용과 같은 설명된 정정 작업에 기반한 조치를 취합니다.

부록 A

WWN을 지원하는 SAS2 장치의 식별

이 부록에는 WWN 값에 기반한 SAS2 장치의 식별 방법이 설명되어 있습니다.

A.1 WWN(World Wide Name) 구문

현재 Oracle Solaris는 논리 장치 이름에 WWN(World Wide Name) 구문을 사용하고 있습니다. 이 절에는 WWN 기반 장치 이름을 특정 SCSI 장치에 매핑하는 방법이 설명되어 있습니다.

부팅 장치를 예로 들어 이전(tn; 대상 ID) 장치 이름과 WWN 기반 장치 이름 간의 표기법 차이를 나타냅니다.

표 A-1 장치 이름 간의 표기법 차이

WWN 값을 사용하는 부팅 장치 이름	이전 부팅 장치 이름(대상 **ID**를 사용)
c#t*WWN*d# WWN은 전세계적으로 이 장치에 사용되는 고유한 16진수입니다. 제조업체는 이 수를 장치에 할당합니다.	c0t0d0

WWN 값은 이전 논리 장치 이름 구조에는 부합되지 않습니다. 따라서 c#tWWNd# 값에서 바로 대상 장치를 식별할 수 없습니다.

WWN 기반 장치 이름을 특정 물리 장치에 매핑하려면 OpenBoot PROM의 probe-scsi-all 명령을 사용합니다. 자세한 내용은 "A.3 probe-scsi-all 명령을 사용한 디스크 슬롯의 식별"를 참조하십시오.

A.2 probe-scsi-all 명령 출력 요약

OpenBoot PROM의 probe-scsi-all 명령 출력에는 시스템 내 모든 SCSI 장치의 목록과 각 장치의 기본 정보가 포함됩니다. 표시 항목이 아래 나열되어 있습니다.

표 A-2 probe-scsi-all 명령 구성

엔터티 이름	설명
Target	각 SAS 장치에 할당되는 고유한 대상 ID
SASDeviceName	제조업체가 SAS 장치에 할당하는 WWN 값 이는 Oracle Solaris가 인식합니다.
SASAddress	OpenBoot PROM 펌웨어가 인식하고 SCSI 장치에 할당되는 WWN 값
PhyNum	대상 드라이브에 연결되는 컨트롤러 포트의 16진수 ID
VolumeDeviceName (RAID 볼륨을 구성하는 경우)	Oracle Solaris가 인식하고 RAID 볼륨에 할당되는 WWN 값 RAID 볼륨에 포함되는 각 SCSI 장치의 SASDeviceName을 대체함.
VolumeWWID (RAID 볼륨을 구성하는 경우)	OpenBoot PROM 펌웨어가 인식하고 RAID 볼륨에 할당되는 WWN 기반 값 RAID 볼륨에 포함되는 각 SCSI 장치의 SASAddress를 대체함.

A.3 probe-scsi-all 명령을 사용한 디스크 슬롯의 식별

이 절에는 OpenBoot PROM의 probe-scsi-all 명령을 사용하여 디스크 슬롯을 식별하는 방법이 설명되어 있습니다.
이는 디스크 슬롯을 해당 WWN 값과 연관시킬 수 있습니다.

A.4 probe-scsi-all 명령을 사용한 디스크 슬롯의 식별 예(SPARC M10-1/M10-4/M10-4S)

이 절에는 온보드 SAS 컨트롤러에 연결된 PhyNum과 디스크 슬롯 간의 대응이 설명되어 있습니다.

SPARC M10-1/M10-4/M10-4S의 경우 SAS 컨트롤러는 HDD 백플레인에 연결됩니다.
다음 표에는 HDD 백플레인의 PhyNum과 디스크 슬롯의 매핑이 나열되어 있습니다.

표 A-3 PhyNum과 디스크 슬롯의 매핑

PhyNum	디스크 슬롯
0	0
1	1

표 A-3 PhyNum과 디스크 슬롯의 매핑 (계속)

PhyNum	디스크 슬롯
2	2
3	3
4	4
5	5
6	6
7	7

노트 - SPARC M10-1/M10-4/M10-4S에서 디스크 슬롯의 물리적 위치는『SPARC M10-1 Service Manual』및『SPARC M10-4/M10-4S Service Manual』의 "내부 디스크 유지 관리" 절을 참조하십시오.

probe-scsi-all 명령 출력의 예

다음에는 8개 내부 디스크 드라이브가 SPARC M10-1에 장착되어 있을 때 디스크 슬롯을 식별하는 방법이 설명되어 있습니다.

1. **probe-scsi-all** 명령을 실행합니다.
   디스크 슬롯 0에 장착된 내부 디스크 드라이브의 PhyNum은 0입니다. 내부 디스크 드라이브는 Target a에 할당되며 SASDeviceName 값은 50000393c813ae74입니다.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0  <---- SAS controller

FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.57.00

Target a
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393c813ae74  SASAddress 50000393c813ae76  PhyNum 0
Target b
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b24ec  SASAddress 50000393b81b24ee  PhyNum 1
Target c
   Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81af47c  SASAddress 50000393b81af47e  PhyNum 2
Target d
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81af3c0  SASAddress 50000393b81af3c2  PhyNum 3
Target e
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b0f58  SASAddress 50000393b81b0f5a  PhyNum 4
Target f
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b130c  SASAddress 50000393b81b130e  PhyNum 5
Target 10
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
```

```
    SASDeviceName 50000393b81b2420  SASAddress 50000393b81b2422  PhyNum 6
Target 11
  Unit 0   Disk   TOSHIBA  MBF2300RC        3706    585937500 Blocks, 300 GB
    SASDeviceName 50000393b81acc84  SASAddress 50000393b81acc86  PhyNum 7
Target 12
  Unit 0   Encl Serv device   FUJITSU  NBBEXP           0d32
    SASAddress 500000e0e04d003d  PhyNum 14
{0} ok
```

노트 - 위 방법은 SPARC M10-4/M10-4S의 디스크 슬롯을 식별하는 데도 사용할 수 있습니다.

부록 B

XSCF 웹 페이지 목록

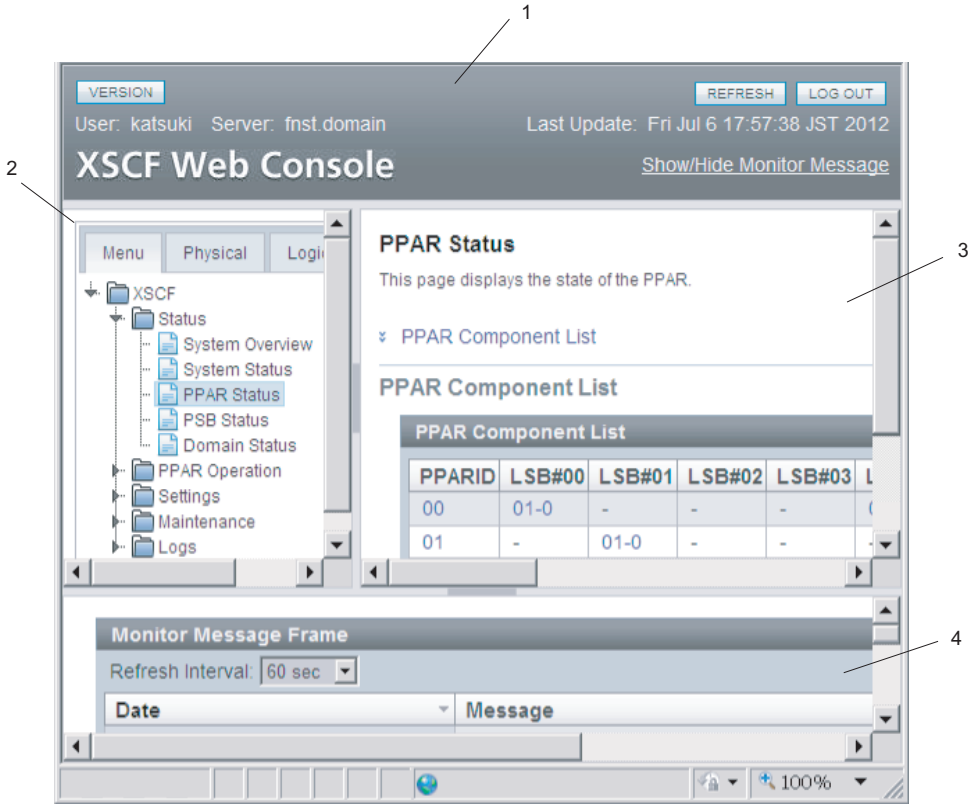
이 장에는 XSCF 웹 페이지의 요약이 설명되어 있습니다.
XSCF 웹에 로그인 또는 로그아웃 방법은 "4장 로그인/로그아웃"을 참조하십시오.

- 페이지 요약
- 메뉴 구성 이해
- 사용 가능한 페이지

B.1 페이지 요약

그림 B-1에는 로그인 후 표시되는 XSCF 웹 콘솔 창이 나타나 있습니다.

그림 B-1 XSCF 웹 콘솔 창



1	마스트 헤드 프레임
2	메뉴 프레임(트리 프레임)
3	메인 프레임
4	이벤트 프레임

로그인 후 표시되는 XSCF 웹 콘솔은 4개 프레임으로 구성되어 있습니다. 좌측 프레임의 메뉴 항목을 선택하면 정보가 우측 프레임에 표시되며 이를 통해 사용자는 서버를 작동 및/또는 관리할 수 있습니다.

표 B-1에는 XSCF 웹 콘솔 프레임의 유형과 요약이 제공되어 있습니다.

표 B-1 프레임 요약

프레임 유형	요약
마스트 헤드 프레임	이는 창 맨 위에 위치합니다(그림 B-1의 1). 이는 로그인하기 위해 지정하는 사용자 계정 이름, 연결된 호스트 이름 및 기타 정보를 표시합니다. 프레임에서 로그아웃하면 로그인 페이지로 돌아갑니다.

표 B-1 프레임 요약 (계속)

프레임 유형	요약
메뉴 프레임 (트리 프레임)	창 좌측에 위치합니다(그림 B-1의 2). 메뉴 항목을 선택하면 정보가 우측 메인 프레임에 표시됩니다. 3개 메뉴 모음이 있습니다. 메뉴는 트리 형식으로 표시됩니다. ■ 메뉴: 설정, 작동 및 상태 보기 메뉴를 표시합니다. ■ 물리: 시스템의 물리 구성요소 구성을 표시합니다. ■ 논리: 물리 분할별로 논리 구성요소 구성을 표시합니다.
메인 프레임	창 우측에 위치합니다(그림 B-1의 3). 트리 프레임에서 메뉴 항목을 선택하면 해당 페이지가 표시됩니다.
이벤트 프레임 (모니터 메시지 프레임)	창 맨 아래에 위치합니다(그림 B-1의 4). 시스템 전체의 이벤트가 모니터 메시지 형태로 표시됩니다. 프레임은 주기적으로 새로고침이 됩니다. 간격은 프레임에서 변경할 수 있습니다. 새로고침 간격은 60초로 디폴트됩니다.

표 B-2에는 XSCF 웹 콘솔에 표시되는 주요 페이지의 기능과 요약이 나타나 있습니다.

표 B-2 주요 페이지 요약

페이지의 기능	요약
로그인 페이지	이는 XSCF 웹 콘솔 로그인 페이지입니다. 로그인 페이지에서 XSCF 사용자 계정을 사용하여 로그인합니다.
서버 상태 표시	시스템 전체, 물리 분할(PPAR) 및 논리 도메인의 상태가 표시됩니다. PCI 확장 장치의 상태도 표시됩니다. [Menu] 모음에서 [Status]를 선택합니다.
물리 분할 작동	물리 분할 및 논리 도메인을 작동할 수 있습니다. 물리 분할 전원, 시스템 보드 구성 관리 등을 처리할 수 있습니다. [Menu] 모음에서 [PPAR Operation]을 선택합니다.
서버 구성	시스템 전체 및 XSCF를 사용하기 위한 설정을 구성할 수 있습니다. [Menu] 모음에서 [Settings]을 선택합니다.
서버 유지 관리	데이터를 저장/복원하고 펌웨어를 업데이트하며 XSCF를 재설정하고 XSCF를 전환하며 원격 유지 관리 서비스의 처리, 로그 저장 등을 수행할 수 있습니다. [Menu] 모음에서 [Maintenance]를 선택합니다.
로그 보기	오류 로그, 전원 로그, 이벤트 로그 및 콘솔 로그를 볼 수 있습니다. [Menu] 모음에서 [Logs]를 선택합니다.
스탠바이측 페이지	이 페이지는 스탠바이 XSCF에 로그인하면 표시됩니다. XSCF 전환, 로그 저장 등을 수행할 수 있습니다.

B.2 메뉴 구성 이해

이 절에는 메뉴 구성이 설명되어 있습니다.

메뉴 프레임에서 [Menu] 모음을 선택하면 다음 항목이 표시됩니다.

```
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
  + Settings
    + Network
      - Current
      - Reserve
    + Service
      - Service State
      - HTTPS
      - SSH
      - Telnet
      - NTP
      - SMTP
      - SNMP
      - SNMP Security
    + User Manager
      - Account
    - Autologout
    - CoD Reservation
    - CoD Activation
    - Audit
    - Email Reporting
    - Time
    - Power Capping
    - Power Schedule
    - Add-In Card Manager
  + Maintenance
    - Configuration Management
    - Firmware Update
    - Reboot XSCF
    - Switch Over
    - Snapshot
  + Logs
    - Error Log
```

```
    - Power Log
    - Event Log
    - Console Log
    - Panic Log
    - Environment Log
    - IPL Message Log
    - Monitor Message Log
    - Audit Log
```

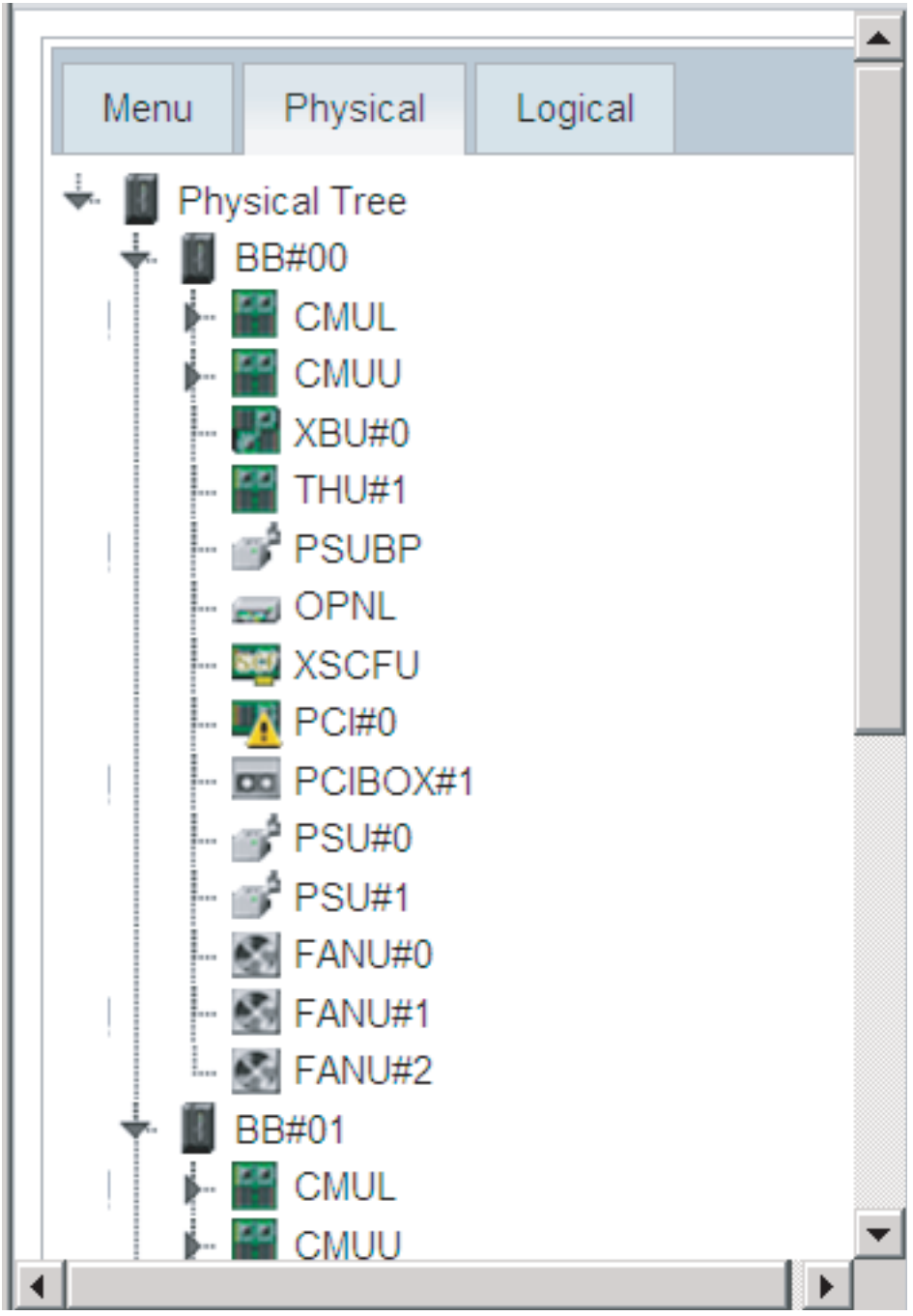
노트 - 메뉴 항목은 기능 개선 또는 일부 이유로 인해 변경될 수 있습니다. 메뉴 항목은 모델 또는 상황에 따라 다를 수 있습니다.

메뉴 항목을 선택하면 해당 페이지가 메인 프레임에 표시됩니다.

XSCF가 2개 이상인 시스템의 경우 [Switch Over]을 사용하여 전환할 수 있습니다. 메뉴 항목에 해당되는 페이지의 요약은 "B.3 사용 가능한 페이지"를 참조하십시오.

그림 B-2에는 [Physical] 모음이 메뉴 프레임에 표시될 때 표시되는 창의 예가 나타나 있습니다.

그림 B-2 물리 구성요소 트리



노트 - 본 설명서에 나타난 표시 레이아웃과 표시 내용은 단지 샘플에 불과하며 기능 개선 또는 일부 이유로 인해 변경될 수 있습니다.

[Physical] 모음을 선택하면 시스템의 구성요소가 트리 구성으로 표시됩니다. 트리 프레임의 구성요소를 선택하면 구성요소의 정보와 상태가 메인 프레임에 표시됩니다.

[Logical] 모음을 선택하면 물리 분할에 속하는 논리 구성요소가 트리 스타일로 표시됩니다. 트리 프레임의 구성요소를 선택하면 물리 분할에 속하는 논리 구성요소의 정보와 상태가 메인 프레임에 표시됩니다.

B.3 사용 가능한 페이지

이 절에는 메인 프레임에서 사용 가능한 페이지의 요약이 설명되어 있습니다. 페이지의 기능은 XSCF 쉘 명령의 기능과 동일합니다. 기능의 자세한 정보는 "8장 XSCF 펌웨어 구성," 명령을 설명하는 장 또는 『SPARC M10 Systems XSCF Reference Manual』을 참조하십시오.

B.3.1 시스템, 물리 분할 및 논리 도메인의 상태를 표시하는 페이지

표 B-3에 나열된 기능은 시스템 정보를 표시하도록 제공됩니다. [Menu] -> [Status] -> [System Overview]를 선택합니다.

표 B-3 시스템 정보

항목	요약	명령
제품 이름	서버 제품의 이름을 표시합니다.	showhardconf(8)
일련 번호	시스템 일련 번호가 표시됩니다.	
시스템 모드 스위치 상태	운영 패널의 모드 스위치 상태가 표시됩니다.	
전원 공급 유형	전원 입력 공급 유형이 표시됩니다.	
전원 상태	전원 입력 공급/차단이 표시됩니다.	
전원 위상	시스템 전원 입력 위상이 표시됩니다.	
XSCF 버전	XSCF 펌웨어 버전이 표시됩니다.	version(8)
캐비닛 상태	캐비닛이 마스터 또는 스탠바이인지 그 여부가 표시됩니다.	showbbstatus(8)
시스템 시간	시스템 시간이 표시됩니다.	showdate(8)
고장인 구성요소	작동 불능의 고장인 구성요소가 표시됩니다.	showstatus(8)
온도	캐비닛으로의 흡기 온도가 표시됩니다.	showenvironment(8)
공기 배출량	캐비닛의 공기 배출량이 표시됩니다.	showenvironment(8)
전원 캡핑 상태	시스템 소비 전력을 줄이는 전원 캡핑 기능의 활성화 또는 비활성화 여부가 표시됩니다.	showpowercapping (8)

표 B-4에 나열된 기능은 시스템 구성요소의 상태를 표시하도록 제공됩니다. [Menu] -> [Status] -> [System Status]를 선택합니다.

표 B-4 구성요소 상태

항목	요약	명령
소비 전력 온도 전압 팬 정보	구성요소의 소비 전력, 배기 온도, 전압 및 팬 회전이 표시됩니다.	showenvironment(8)

표 B-5에 나열된 기능은 물리 분할(PPAR)의 상태를 표시하도록 제공됩니다. [Menu] -> [Status] -> [PPAR Status]를 선택합니다.

표 B-5 물리 분할 상태

항목	요약	명령
PPAR 구성 정보 표시	PPAR의 LSB 번호에 해당되는 PSB 번호가 표형태로 표시됩니다.	showpcl(8)
PPAR 상태	PPAR의 작동 상태와 구성 정책이 표시됩니다.	showpcl(8)
PSB 정보	PSB의 정보가 표시됩니다.	showboards(8)

표 B-6에 나열된 기능은 PSB의 상태를 표시하도록 제공됩니다. [Menu] -> [Status] -> [PSB Status]를 선택합니다.

표 B-6 PSB 상태

항목	요약	명령
PSB 상태	PSB에 포함된 PPAR ID와 기타 세부 상태가 나열됩니다.	showboards(8)

표 B-7에 나열된 기능은 논리 도메인의 상태를 표시하도록 제공됩니다. [Menu] -> [Status] -> [Domain Status]를 선택합니다.

표 B-7 논리 도메인 상태

항목	요약	명령
논리 도메인 상태	지정된 PPAR에 속하는 논리 도메인의 작동 상태가 표시됩니다.	showdomainstatus(8), showpparstatus(8)

B.3.2 물리 분할을 작동하는 페이지

표 B-8에 나열된 기능은 물리 분할의 전원을 작동하도록 제공됩니다. [Menu] -> [PPAR Operation] -> [PPAR Power]을 선택합니다.

표 B-8 물리 분할 전원 작동

항목	요약	명령
시스템 전원 공급/차단	이는 시스템 전원을 공급/차단하는 데 사용됩니다(모든 물리 분할).	showpparstatus(8), poweron(8), poweroff(8)
전원 공급/차단 /PPAR 재설정	이를 통해 지정된 PPAR에 다음 작동을 수행할 수 있습니다. ■ 전원 공급/차단 ■ 강제 전원 차단 ■ por: PPAR 재설정 ■ panic: 논리 도메인에 패닉 명령 내림 ■ sir: 논리 도메인 재설정 ■ xir: CPU 재설정 ■ 브레이크 신호 전송	showpparstatus(8), poweron(8), poweroff(8), reset(8), sendbreak(8)

표 B-9에 나열된 기능은 물리 분할의 작동 모드를 구성하도록 제공됩니다. [Menu] -> [PPAR Operation] -> [PPAR Mode Configuration]을 선택합니다.

표 B-9 물리 분할 작동 모드

항목	요약	명령
PPAR 모드 표시/구성	이를 통해 지정된 PPAR에 다음 모드를 표시 또는 구성할 수 있습니다. ■ 호스트 ID ■ 하드웨어 진단 레벨 ■ 진단 메시지 레벨 ■ 활성 모니터링 기능 활성화/비활성화 ■ 호스트 와치독 시간 초과 시의 작동 ■ 브레이크 신호 전송 억제 ■ 논리 도메인 자동 부팅 기능 활성화/비활성화 ■ 저전력 작동 활성화/비활성화 ■ I/O 경로 재구성 ■ PPAR 이더넷 주소(mac 주소)	showpparmode(8), setpparmode(8)

노트 - XSCF와 하이퍼바이저 간 활성 모니터링 기능의 지원 정보는 최신『SPARC M10 시스템 제품 노트』를 참조하십시오.

표 B-10에 나열된 기능은 물리 분할을 구성하도록 제공됩니다. [Menu] -> [PPAR Operation] -> [PPAR Configuration]을 선택합니다.

표 B-10 물리 분할 구성

항목	요약	명령
PPAR 구성 정보 (PCL) 표시	지정된 PPAR 시스템 보드의 PCL이 표시됩니다. PPAR의 구성 정책 또한 표시되어 구성할 수 있습니다. SPARC M10-1/SPARC M10-4와 관련하여 PPAR-ID 00의 정보가 표시되고 구성 정책만 구성할 수 있습니다.	showpcl(8), setpcl(8)
PCL 구성	이를 통해 PCL을 구성할 수 있습니다. PPAR LSB를 PSB와 연관시키거나 LSB로 구성 정보를 구성할 수 있습니다. SPARC M10-1/SPARC M10-4는 이 기능을 지원하지 않습니다.	showpcl(8), setpcl(8)
PSB 추가/삭제/구성	이를 통해 PPAR에 대한 PSB 구성의 다음 변경 명령을 제공할 수 있습니다. ■ PPAR에 시스템 보드 예약 또는 포함 ■ PPAR에서 시스템 보드 분리 ■ 한 PPAR에서 다른 PPAR로 시스템 보드 마이그레이션 『SPARC M10 시스템 도메인 구성 안내서』에 설명된 절차에 따라 위 작동을 수행합니다. SPARC M10-1/SPARC M10-4는 이 기능을 지원하지 않습니다.	addboard (8), deleteboard (8)

표 B-11에 나열된 기능은 메모리 미러 모드에서 시스템 보드를 구성하도록 제공됩니다. [Menu] -> [PPAR Operation] -> [PSB Configuration]을 선택합니다.

표 B-11 시스템 보드 설정

항목	요약	명령
메모리 미러 정보 표시/구성	이를 통해 시스템 보드에서 CPU의 메모리 미러 모드 정보를 표시 또는 구성할 수 있습니다.	showfru(8), setupfru(8)

표 B-12에 나열된 기능은 논리 도메인을 구성하도록 제공됩니다. [Menu] -> [PPAR Operation] -> [Domain Configuration]을 선택합니다.

표 B-12 논리 도메인 구성

항목	요약	명령
논리 도메인 구성 정보 표시	이를 통해 지정된 PPAR의 논리 도메인 구성 정보를 표시할 수 있습니다. 구성 정보의 요소는 다음과 같습니다. ■ 구성 이름 ■ 구성 논리 도메인의 수 ■ 구성 날짜 PPAR에 대해 현재 실행 중인 논리 도메인 구성의 이름과 다음 번 실행되도록 예약된 논리 도메인 구성의 이름도 표시됩니다.	showdomainconfig (8)

표 B-12 논리 도메인 구성 (계속)

항목	요약	명령
논리 도메인 구성 설정	이를 통해 논리 도메인 구성을 설정할 수 있습니다. 지정된 PPAR에 대해 다음 번 실행되도록 예약된 논리 도메인의 구성을 설정할 수 있습니다.	setdomainconfig(8)

B.3.3 서버를 구성하는 페이지

XSCF 네트워크 설정

표 B-13에 나열된 기능은 XSCF 네트워크 설정을 구성하도록 제공됩니다. [Menu] -> [Setting] -> [Network] -> [Current]를 선택하거나 [Menu] -> [Setting] -> [Network] -> [Reserve]을 선택합니다. [Current] 또는 [Reserve] 메뉴를 사용하여 네트워크 설정을 구성할 수 있습니다. [Current] 메뉴는 현재 실행 중인 XSCF 네트워크의 정보를 표시합니다. [Reserve] 메뉴를 통해 구성된 정보를 확인할 수 있습니다.

[Current] 메뉴로 네트워크 설정을 구성한 후에는 [Reserve] 메뉴로 자동 안내됩니다. 네트워크 설정을 구성한 후 [Apply]에 이어 [Reserve] 메뉴의 [Reboot] 메뉴를 클릭하여 설정을 적용합니다.

표 B-13 XSCF 네트워크 설정

메뉴	항목	요약	명령
[Current]	XSCF 네트워크 정보/상태 표시, XSCF 네트워크 구성	현재 실행 중인 XSCF 네트워크의 정보와 상태가 표시됩니다. XSCF 네트워크 인터페이스의 호스트 이름, 도메인 이름, IP 주소 및 네트워크 마스크와 그 활성화/비활성화 설정을 구성할 수 있습니다. [Edit] 버튼을 클릭하여 [Reserve] 메뉴로 이동한 후 네트워크 설정을 구성합니다. 구성된 정보는 [Reserve] 메뉴에서 확인할 수 있습니다.	shownetwork(8) showhostname(8)
	경로 표시/구성	이를 통해 현재 경로를 표시할 수 있습니다. 또한 경로를 구성할 수도 있습니다. [Edit] 버튼을 클릭하여 [Reserve] 메뉴로 이동한 후 경로 설정을 구성할 수 있습니다. 구성된 정보는 [Reserve] 메뉴에서 확인할 수 있습니다.	shownameserver(8) setnameserver(8)
	DNS 표시/구성	이를 통해 현재 이름 서버와 검색 경로를 표시할 수 있습니다. 또한 이름 서버와 검색 경로를 구성할 수도 있습니다. [Edit] 버튼을 클릭하여 [Reserve] 메뉴로 이동한 후 DNS 설정을 구성할 수 있습니다. 구성된 정보는 [Reserve] 메뉴에서 확인할 수 있습니다.	shownameserver(8) setnameserver(8)

표 B-13 XSCF 네트워크 설정 (계속)

메뉴	항목	요약	명령
[Reserve]	XSCF 네트워크 설정 정보 표시 XSCF 네트워크 구성	XSCF 네트워크 설정 정보가 표시됩니다. XSCF 네트워크 인터페이스의 호스트 이름, 도메인 이름, IP 주소 및 네트워크 마스크와 그 활성화/비활성화 설정을 구성할 수 있습니다. [Current Status] 버튼을 클릭하면 [Current] 메뉴가 표시되고 현재 작동과 관련된 정보도 표시됩니다.	applynetwork(8) setnetwork(8) sethostname(8)
	경로 설정 정보 표시 /경로 구성	경로 설정 정보가 표시됩니다. 또한 경로를 구성할 수도 있습니다. [Current Status] 버튼을 클릭하면 [Current] 메뉴가 표시되고 현재 작동과 관련된 정보도 표시됩니다.	applynetwork(8) setroute(8)
	DNS 설정 정보 표시 /DNS 구성	이를 통해 이름 서버와 검색 경로의 설정 정보를 표시할 수 있습니다. 또한 이름 서버와 검색 경로를 구성할 수도 있습니다. [Current Status] 버튼을 클릭하면 [Current] 메뉴가 표시되고 현재 작동과 관련된 정보도 표시됩니다.	applynetwork(8) setnameserver(8)
	네트워크 설정 적용	이를 통해 구성된 네트워크 설정을 표시/적용할 수 있습니다. 설정을 저장한 후 XSCF를 재설정하하여 절차를 완료합니다.	applynetwork(8) rebootxscf(8)

노트 - SSCP 링크 주소는 XSCF 웹을 사용하여 구성/표시할 수 없습니다. setsscp 및 showsscp 명령을 사용하여 주소를 구성/표시하십시오.

노트 - IP 패킷 필터링 규칙은 XSCF 웹을 사용하여 구성/표시할 수 없습니다. setpacketfilters 및 showpacketfilters 명령을 사용하여 필터링 규칙을 구성/표시하십시오.

서비스 기능 설정

표 B-14에 나열된 기능은 서비스 기능을 활성화/비활성화하도록 제공됩니다. [Settings] -> [Service] -> [Service State]를 선택합니다.

표 B-14 서비스 기능을 활성화/비활성화하는 설정

항목	요약	명령
서비스 기능 상태 표시 서비스 기능 활성화/비활성화	다음 서비스 기능의 상태는 목록 형태로 표시됩니다. 서비스 기능을 활성화/비활성화할 수 있습니다. ■ HTTPS 서비스 ■ SNMPv3 서비스 ■ SSH 서비스 ■ Telnet 서비스 ■ NTP 서버 서비스 SNMPv3 서비스의 활성화/비활성화를 시도하면 SNMP 에이전트 설정을 구성할 수 있는 SNMP의 구성 메뉴가 표시됩니다. NTP 서버 서비스를 선택하면 XSCF가 NTP 서버로서 기능하도록 설정을 활성화/비활성화할 수 있습니다.	showhttps(8) sethttps(8) showsnmp(8) setsnmp(8) showssh(8) setssh(8) showtelnet(8) settelnet(8) shownntp(8) setntp(8)

표 B-15에 나열된 기능은 HTTP 서비스 기능을 활성화/비활성화하도록 제공됩니다. [Settings] -> [Service] -> [HTTPS]를 선택합니다.

표 B-15 HTTP 서비스 기능을 활성화/비활성화하는 설정

항목	요약	명령
HTTP 서비스 활성화/비활성화/설정 표시	이를 통해 HTTPS 서비스를 활성화/비활성화하거나 설정을 표시할 수 있습니다.	showhttps(8) sethttps(8)

노트 - HTTPS 서비스를 비활성화하면 XSCF 웹을 사용할 수 없습니다. HTTPS 서비스를 활성화하려면 sethttps 명령을 사용하십시오.

표 B-16에 나열된 기능은 SSH 서비스 기능을 활성화/비활성화하도록 제공됩니다. [Settings] -> [Service] -> [SSH]를 선택합니다.

표 B-16 SSH 서비스 기능을 활성화/비활성화하는 설정

항목	요약	명령
SSH 서비스 활성화/비활성화/설정 표시	이를 통해 SSH 서비스를 활성화/비활성화하거나 설정을 표시할 수 있습니다.	showssh(8) setssh(8)

노트 - 호스트 키 생성, 사용자 공개 키 등록/삭제 및 XSCF 쉘 시간 초과 설정은 XSCF 웹에서 지원되지 않습니다. showssh 및 setssh 명령을 사용하여 기능을 처리하십시오.

표 B-17에 나열된 기능은 Telnet 서비스 기능을 활성화/비활성화하도록 제공됩니다. [Settings] -> [Service] -> [Telnet]을 선택합니다.

표 B-17 Telnet 서비스 기능을 활성화/비활성화하는 설정

항목	요약	명령
Telnet 서비스 활성화/비활성화/설정 표시	이를 통해 Telnet 서비스를 활성화/비활성화하거나 설정을 표시할 수 있습니다.	showtelnet(8) settelnet(8)

표 B-18에 나열된 기능은 XSCF NTP 서비스 기능을 구성하도록 제공됩니다. [Settings] -> [Service] -> [NTP]를 선택합니다.

표 B-18 NTP 서비스 기능을 구성하는 설정

항목	요약	명령
NTP 서버 활성화/비활성화/설정 표시	이를 통해 XSCF가 NTP 서버로서 기능하도록 설정을 활성화, 비활성화 및 표시할 수 있습니다.	showntp(8) setntp(8)
NTP 클라이언트 활성화/비활성화/설정 표시	이를 통해 XSCF가 NTP 클라이언트로서 기능하도록 설정을 활성화, 비활성화 및 표시할 수 있습니다.	
NTP 서버 구성	이를 통해 XSCF 네트워크에 사용되는 NTP 서버의 다음 설정 항목을 표시/구성할 수 있습니다. ■ NTP 서버(최대 3개) ■ 우선순위 서버(선호) ■ 계층 값 ■ XSCF 로컬 클록 주소의 설정을 완료하려면 XSCF를 재설정해야 합니다.	

표 B-19에 나열된 기능은 XSCF SMTP 서비스 기능을 구성하도록 제공됩니다. [Settings] -> [Service] -> [SMTP]를 선택합니다.

표 B-19 SMTP 서비스 기능을 구성하는 설정

항목	요약	명령
SMTP 서버 표시/구성	이를 통해 SMTP 서버 주소, 인증 알고리즘, POP 서버 주소, 오류 이메일 회신 대상 주소 및 기타 SMTP 서버 정보를 표시/구성할 수 있습니다.	showsmtp(8) setsmtp(8)

표 B-20에 나열된 기능은 XSCF SNMP 에이전트 기능을 구성하도록 제공됩니다. [Settings] -> [Service] -> [SNMP]를 선택합니다.

표 B-20 SNMP 에이전트를 구성하는 설정

항목	요약	명령
SNMPv3 에이전트 표시/구성	이를 통해 SNMPv3 에이전트를 활성화 또는 비활성화하거나 설정을 표시할 수 있습니다. 또한 MIB 정의 파일과 시스템 관리 정보를 표시 및 구성할 수도 있습니다.	showsnmp(8) setsnmp(8)

표 B-20 SNMP 에이전트를 구성하는 설정 (계속)

항목	요약	명령
SNMPv1/v2c 에이전트 표시/구성	이를 통해 SNMPv1/v2c 에이전트를 활성화 또는 비활성화하거나 설정을 표시할 수 있습니다. 또한 커뮤니티 문자열을 표시 및 구성할 수도 있습니다.	
트랩 호스트 표시/구성	SNMPv1/v2c 트랩 호스트와 SNMPv3 트랩 호스트가 목록 형태로 표시됩니다. 트랩 호스트 이름, 포트 번호 및 기타 호스트 정보를 표시/구성할 수 있습니다.	

표 B-21에 나열된 기능은 SNMPv3의 보안 기능을 구성하도록 제공됩니다. [Settings] -> [Service] -> [SNMP Security]을 선택합니다.

표 B-21 SNMP 보안 기능 설정

항목	요약	명령
USM 관리 정보 표시/구성	이를 통해 사용자 인증 알고리즘과 같은 USM 관리 정보를 표시/구성할 수 있습니다. USM 관리 정보는 표 15-4를 참조하십시오.	showsnmpusm(8) setsnmpusm(8)
SNMPv1/v2c 에이전트 표시/구성	이를 통해 액세스 제어 그룹 및 액세스 제어 보기와 같은 VACM 관리 정보를 표시/구성할 수 있습니다. VACM 관리 정보는 표 15-4를 참조하십시오.	showsnmpvacm(8) setsnmpvacm(8)

사용자 계정 설정

표 B-22에 나열된 기능은 XSCF 로컬 사용자 계정을 설정하도록 제공됩니다. [Settings] -> [User Manage] -> [Account]을 선택합니다.

표 B-22 사용자 계정 설정

항목	요약	명령
사용자 계정 정보 표시	이를 통해 현재 등록된 사용자 계정의 정보와 상태를 표시할 수 있습니다. 이 경우 useradm 권한이 필요합니다.	showuser(8)
사용자 계정 추가/삭제	이를 통해 사용자 계정을 추가/삭제할 수 있습니다. 이 경우 useradm 권한이 필요합니다.	adduser(8) deleteuser(8)
사용자 계정 활성화/비활성화	이를 통해 현재 등록된 사용자 계정을 비활성화한 후 활성화할 수 있습니다. 이 경우 useradm 권한이 필요합니다.	disableuser(8) enableuser(8)
사용자 계정 정보 표시/변경	이를 통해 지정된 사용자 계정의 정보를 표시하고 암호, 사용자 권한 및 암호 정책을 변경할 수 있습니다. 이 경우 useradm 권한이 필요합니다.	password(8) setprivileges(8)

표 B-22 사용자 계정 설정 (계속)

항목	요약	명령
로컬 사용자 계정 정보 표시/암호 변경	사용자 계정에 useradm 이외의 권한이 있을 때 이를 통해 로컬 사용자 계정의 정보를 표시하고 암호를 변경할 수 있습니다.	showuser(8) password(8)
시스템 암호 정책 표시/구성	이를 통해 현재 시스템 암호 정책을 표시할 수 있습니다. 또한 나중에 적용하도록 시스템 암호 정책을 구성할 수도 있습니다.	showpasswordpolicy(8) setpasswordpolicy(8)

노트 - 3회 연속 로그인 실패에 사용된 사용자 계정을 잠그는 잠금 기능은 XSCF 웹에서 지원되지 않습니다. XSCF 쉘 잠금 기능에는 setloginlockout 및 showloginlockout 명령을 사용하십시오.

자동 로그아웃 설정

표 B-23에 설명된 기능은 XSCF 웹 세션 시간 초과(자동 로그아웃) 설정을 구성하도록 제공됩니다. [Settings] -> [Autologout] -> [Account]을 선택합니다. 자동 로그아웃 시간(분)이 설정되고 사용자가 XSCF 웹에 로그인하는 경우 설정된 시간 동안 액세스하지 않으면 자동 로그아웃됩니다.

표 B-23 자동 로그아웃 설정

항목	요약	명령
자동 로그아웃 시간 설정 표시/구성	이를 통해 현재 구성된 자동 로그아웃 시간(분)을 표시/구성할 수 있습니다. 기본 값은 10입니다. 허용 범위는 1 ~ 255입니다.	이는 XSCF 웹에서만 지원됩니다.

노트 - XSCF 쉘 세션 시간 초과 설정은 XSCF 웹에서 지원되지 않습니다. showautologout 및 setautologout 명령을 사용하십시오.

CoD 설정

표 B-24에 설명된 기능은 CPU 코어 활성화를 할당하도록 제공됩니다. [Settings] -> [COD Reservation]을 선택합니다.

표 B-24 CoD 예약 설정

항목	요약	명령
CPU 코어 활성화 사용량	이는 CPU 코어 활성화 사용량을 표시합니다. 다음별로 사용량을 표시할 수 있습니다. ■ 자원(CPU) ■ PPAR	showcodusage(8)

표 B-24 CoD 예약 설정 (계속)

항목	요약	명령
CPU 코어 활성화 할당 표시/구성	이는 각 PPAR마다 CPU 코어 활성화의 할당된 상태를 표시합니다. 또한 이를 통해 PPAR을 지정하고 자원에 대한 CPU 코어 활성화 수를 증가 또는 감소시킬 수도 있습니다.	showcod(8) setcod(8)

표 B-25에 설명된 기능은 CPU 코어 활성화 키를 등록하도록 제공됩니다. [Settings] -> [COD Reservation]을 선택합니다.

표 B-25 CPU 코어 활성화 키 설정

항목	요약	명령
CPU 코어 활성화 키 정보 표시/구성	이는 현재 등록된 CPU 코어 활성화 키 정보를 표시합니다.	showcodactivation (8)
CPU 코어 활성화 키 추가/삭제	이는 CPU 코어 활성화 키를 추가 또는 제거합니다.	addcodactivation (8), deletecodactivation (8)
CPU 코어 활성화 키의 등록 이력	이는 CPU 코어 활성화 키의 추가 및 삭제 이력 정보를 표시합니다.	showcodactivationhistory (8)

감사 설정

표 B-26에 나열된 기능은 XSCF 감사 설정을 구성하도록 제공됩니다. [Settings] -> [Audit]를 선택합니다.

표 B-26 감사 설정

항목	요약	명령
감사 파일 사용량 표시/데이터 전송	이를 통해 감사 파일의 활용도를 표시할 수 있습니다. 또한 감사 파일을 전송하고 2차 파일을 삭제할 수도 있습니다.	showaudit(8) setaudit(8)
감사 활성화/비활성화	이를 통해 감사를 활성화, 비활성화 및 설정을 표시할 수 있습니다.	
감사 내역 정책 표시/구성	이를 통해 데이터가 가득 찼을 때의 감사 내역 정책, 로컬 감사 파일 활용도(%)에 대한 경고 임계값 및 경고 이메일의 대상 주소를 표시/구성할 수 있습니다.	
전역 사용자 정책 표시/구성	이를 통해 전역 사용자 정책을 활성화/비활성화할 수 있습니다.	

표 B-26 감사 설정 (계속)

항목	요약	명령
사용자 감사 레코그 생성 정책 표시/추가/변경	이를 통해 사용자별 감사 레코드 생성 정책의 목록을 표시할 수 있습니다(감사 레코드 생성 활성화/비활성화). 또한 사용자별 감사 레코드 생성 정책을 추가할 수도 있습니다. 정책이 추가된 사용자의 경우 전역 사용자 정책이 비활성화됩니다. 지정된 사용자의 경우 감사 레코드 생성 정책이 활성화 또는 비활성화되고 전역 사용자 정책이 활성화됩니다.	
감사 이벤트/감사 클래스 표시/구성	이를 통해 감사 이벤트와 감사 클래스를 표시할 수 있습니다. 또한 감사 이벤트와 감사 클래스를 활성화/비활성화할 수도 있습니다.	

이메일 설정

표 B-27에 나열된 기능은 XSCF 이메일 설정을 구성하도록 제공됩니다. [Settings] -> [Email Reporting]를 선택합니다.

표 B-27 이메일 설정

항목	요약	명령
이메일 알림 기능 표시/구성	이를 통해 이메일 알림 기능 설정 정보를 표시/구성할 수 있습니다. 이메일 알림 기능을 활성화/비활성화하고 시스템 관리자로 전송되도록 대상 이메일 주소를 표시/구성할 수 있습니다.	showemailreport(8) setemailreport(8)

시간 설정

표 B-28에 나열된 기능은 시스템 시간과 표준 시간대 설정을 구성하도록 제공됩니다. [Settings] -> [Time]을 선택합니다.

표 B-28 시간 설정

항목	요약	명령
시스템 시간 표시/구성	이를 통해 현재 시스템 시간과 표준 시간대 설정을 표시/구성할 수 있습니다. 설정이 구성되면 XSCF가 재설정됩니다. 다시 로그인합니다. 시스템 시간이 NTP 서버와 동기화되면 시간 설정을 구성할 수 없습니다.	showdate(8) setdate(8) showtimezone(8) settimezone(8)

노트 - 서머 타임은 XSCF 웹을 사용하여 구성할 수 없습니다. showtimezone 및 settimezone 명령을 사용하여 구성하십시오.

소비 전력 설정

표 B-29에 나열된 기능은 시스템 소비 전력의 한계 설정을 구성하도록 제공됩니다. [Settings] -> [Power Capping]을 선택합니다.

표 B-29 소비 전력 설정

항목	요약	명령
소비 전력 한계 표시/구성	이를 통해 소비 전력 한계 설정을 구성할 수 있습니다. 또한 한계를 활성화/비활성화하고 소비 전력 상한 및 기타 설정을 구성할 수도 있습니다.	showpowercapping(8) setpowercapping(8)

전원 예약 구성

표 B-30에 나열된 기능은 시스템 전원 예약 설정을 구성하도록 제공됩니다. [Settings] -> [Power Schedule]을 선택합니다.

표 B-30 전원 예약 구성

항목	요약	명령
전원 예약 설정 표시	이를 통해 PPAR 전원 예약을 목록 형태로 표시할 수 있습니다.	showpowerschedule(8)
전원 예약 구성	이를 통해 전원 예약을 구성할 수 있습니다. 다음별로 예약을 활성화/비활성화하거나 구성할 수 있습니다. ■ PPAR ■ 모든 PPAR	setpowerschedule(8)
전원 예약 정보 표시	이를 통해 PPAR별로 다음 전원 공급 시간과 전원 차단 시간을 표시할 수 있습니다.	showpowerschedule(8)
전원 예약 세부 정보	이를 통해 세부 전원 예약 정보를 표시/구성할 수 있습니다. 다음별로 예약을 표시/추가/변경/삭제할 수 있습니다. ■ PPAR ■ 모든 PPAR	showpowerschedule(8) setpowerschedule(8) addpowerschedule(8) deletepowerschedule(8)

장치 설정

표 B-31에 나열된 기능은 서버 및 PCI 확장 장치에 연결된 카드의 정보를 구성하도록 제공됩니다. [Settings] -> [Add-In Card Manager]를 선택합니다.

표 B-31 PCI 확장 장치 정보 설정

항목	요약	명령
카드/PCI 확장 장치 센서 정보 표시	다음별로 센서 정보를 목록 형태로 표시할 수 있습니다. ■ PCI 카드(서버에 연결됨) ■ PCI 확장 장치 ■ PCI 확장 장치의 FRU	ioxadm(8)
장치 정보 표시/전원 설정 구성	이를 통해 PCI 카드, PCI 확장 장치 및 다운 링크 카드와 같은 장치의 정보를 표시할 수 있습니다. 또한 PCI 확장 장치 내 전원 장치의 전원을 차단/공급할 수도 있습니다.	
모니터링 구성요소 초기화	이를 통해 PCI 확장 장치의 모니터링 구성요소를 초기화할 수 있습니다.	
펌웨어 업데이트	이를 통해 PCI 확장 장치와 링크 카드 펌웨어를 확인, 등록 및 업데이트할 수 있습니다.	
PCI 확장 장치 LED 상태 표시/구성	이를 통해 PCI 확장 장치 내 FRU 로케이터 LED의 상태를 표시/구성할 수 있습니다.	

노트 - PCI 확장 장치 내 2개 전원 장치 둘 모두의 전원이 차단되면 XSCF 웹 또는 XSCF 쉘을 통한 PCI 확장 장치의 전원 공급이 불가능해집니다. 다시 전원을 공급하려면 물리 전원 버튼을 누르십시오.

B.3.4 서버를 유지 관리하는 페이지

XSCF 설정 정보 저장/복원

표 B-32에 나열된 기능은 XSCF 설정 정보를 저장/복원하도록 제공됩니다. [Maintenance] -> [Configuration Management]를 선택합니다.

표 B-32 XSCF 설정 정보 저장/복원

항목	요약	명령
XSCF 설정 정보 저장/복원	이를 통해 XSCF 설정 정보를 저장 및 구성할 수 있습니다. [Run] 버튼을 클릭하여 정보를 저장/구성하면 XSCF가 재설정됩니다. 다시 로그인합니다.	dumpconfig (8), restoreconfig (8)

펌웨어 업데이트

표 B-33에 나열된 기능은 XSCF 펌웨어 업데이트를 구성하도록 제공됩니다. [Maintenance] -> [Firmware Update]를 선택합니다.

표 B-33 펌웨어 업데이트 설정

항목	요약	명령
버전 표시	다음 펌웨어 버전이 표시됩니다. ■ XCP 버전 ■ XSCF 펌웨어 버전 ■ CMU 펌웨어 버전	version (8)
XCP 가져오기	이를 통해 XCP 파일을 지정하여 펌웨어를 서버로 가져올 수 있습니다.	getflashimage (8)
펌웨어 업데이트	이를 통해 XCP를 업데이트할 수 있습니다. XSCF가 재설정됩니다. 다시 로그인합니다.	flashupdate (8)
버전 조정(XSCF가 2개 이상인 시스템)	이를 통해 XSCF가 2개 이상인 시스템에서 XCP 펌웨어 버전을 일치시킬 수 있습니다. XSCF 장치, CMU 또는 캐비닛 교체 후 이를 사용합니다.	flashupdate (8)

XSCF 재설정

표 B-34에 나열된 기능은 XSCF를 재설정하도록 제공됩니다. [Maintenance] -> [Reboot XSCF]을 선택합니다.

표 B-34 XSCF 재설정

항목	요약	명령
XSCF 재설정	이를 통해 로컬 XSCF를 재설정할 수 있습니다.	rebootxscf (8)
대상 XSCF 재설정 (XSCF가 2개 이상인 시스템)	이를 통해 캐비닛 하나의 BB-ID 또는 XSCF가 있는 여러 캐비닛의 BB-ID를 지정하고 캐비닛 하나 또는 여럿을 재설정할 수 있습니다. ■ 모든 캐비닛 ■ 지정된 캐비닛	showbbstatus (8) rebootxscf (8)

XSCF 전환

표 B-35에 설명된 기능은 XSCF가 2개 이상인 시스템에서 XSCF 간을 전환하도록 제공됩니다. [Maintenance] -> [Switch Over]을 선택합니다.

표 B-35 XSCF 전환

항목	요약	명령
XSCF 간의 전환 (XSCF가 2개 이상인 시스템)	이를 통해 마스터에서 스탠바이로 또는 스탠바이에서 마스터로 XSCF를 전환할 수 있습니다.	switchscf (8)

서버 정보 저장

표 B-36에 설명된 기능은 서버 정보를 수집하고 시스템 문제를 분석/해결하도록 제공됩니다. [Maintenance] -> [Switch Over]을 선택합니다.

표 B-36 서버 정보 저장

항목	요약	명령
서버 정보 저장 대상 캐비닛 정보 저장(XSCF가 2개 이상인 시스템)	이를 통해 BB-ID 하나 또는 여러 BB-ID를 지정하고 서버 구성, 공통 시스템 로그 및 캐비닛 로그와 같은 데이터를 수집하며 데이터를 파일로 저장할 수 있습니다. ■ 모든 캐비닛 ■ 지정된 캐비닛	snapshot (8)

노트 - XSCF가 2개 이상인 시스템의 경우 스탠바이 XSCF에 로그인할 때 표시되는 페이지에서 서버 정보를 저장할 수 있습니다.

B.3.5 로그를 보는 페이지

표 B-37에 나열된 기능은 로그 정보를 보도록 제공됩니다. [Logs]를 선택합니다. 원하는 로그를 선택합니다.

표 B-37 로그

항목	요약	명령
오류 로그 표시	이를 통해 오류 로그를 볼 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), error 옵션
전원 로그 표시	이를 통해 전원 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), power 옵션
이벤트 로그 표시	이를 통해 이벤트 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), event 옵션
콘솔 로그 표시	이를 통해 콘솔 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), console 옵션
패닉 로그 표시	이를 통해 패닉 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), panic 옵션
온도 이력 로그 표시 (환경 로그)	이를 통해 지정된 BB-ID의 캐비닛 온도 이력 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), env 옵션
IPL 메시지 로그 표시	이를 통해 지정된 PPAR의 IPL 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), ipl 옵션
모니터 메시지 로그 표시	이를 통해 모니터 메시지 로그를 표시할 수 있습니다. 이를 통해 로그를 검색할 수 있습니다.	showlogs (8), monitor 옵션
감사 로그 표시	이를 통해 감사 로그를 표시할 수 있습니다. 기간, 날짜, 사용자 및/또는 클래스를 참조로 지정할 수 있습니다.	viewaudit (8)

부록 C

XSCF MIB 정보

이 부록에는 XSCF SNMP 에이전트 기능에서 지원되는 XSCF 확장 MIB(Management Information Base)의 요약이 설명되어 있습니다. SNMP 에이전트 기능의 자세한 내용은 "15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리"를 참조하십시오.

- MIB 개체 식별
- 표준 MIB
- 확장 MIB
- 트랩의 기본 정보

C.1 MIB 개체 식별

XSCF에서 지원되는 MIB 개체 식별자(OID)의 예는 아래 나열된 바와 같습니다.

```
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 }

C.2 표준 MIB

XSCF가 지원하는 표준 MIB는 다음 RFC(노트)에 부합됩니다. 표준 MIB 정의 파일은 일반 RFC 설명서를 참조하십시오.

<참조 프로토콜 및 RFC의 예>

MIB II	RFC1213
User-based Security Model（USM）	RFC3414
View-based Access Control Model (VACM)	RFC3415
SNMPv2-MIB	RFC3418

노트 - RFC: Request For Comment(의견 요청서)의 약어. RFC는 인터넷 관련 기술 표준을 수립하는 기구인 IETF(Internet Engineering Task Force)에서 발행한 기술 사양입니다.

C.3 확장 MIB

SPARC M10 시스템 XSCF는 XSCF 확장 MIB의 다음 정보를 제공합니다.

- 시스템 정보, 하드웨어/펌웨어 버전 및 시스템 구성 정보
- 환경 정보(온도, 전압, 팬 회전 등)
- 물리 분할 상태 및 물리 분할 구성 정보
- 시스템의 부품 고장 정보
- 시스템의 전원 값 정보/설정

노트 - SPARC M10 시스템에서 논리 도메인의 최대 소비 전력 및 기타 소비 전력 설정을 구성할 수 있습니다. 소비 전력 설정과 관련된 정보는 사용 버전의『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

노트 - XSCF 확장 MIB 정의 파일의 가져오기 및 설치 방법은 "15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리"를 참조하십시오.

C.3.1 XSCF 확장 MIB 개체

이 절에는 XSCF 확장 MIB의 주요 개체 그룹과 제공 정보가 설명되어 있습니다.

scfObjects

- scfInfo 그룹
  이는 마스터 XSCF 및 XSCF-LAN 정보와 같은 XSCF 관련 일반 정보를 제공합니다.
- scfState 그룹
  이는 XSCF 상태 정보, 운영 패널 모드 스위치 상태 등을 제공합니다.
- scfMonitorInfo 그룹
  이는 구성요소 이름, 온도, 전압 및 팬 회전과 같은 시스템 내 다양한 구성요소의 환경 정보를 제공합니다.
- scfSystemInfo 그룹
  이는 다음 시스템 정보를 제공합니다.
  - 호스트 이름, 일련 번호, 장착된 CPU 수 및 기타 시스템 제품 정보
  - LED 상태 정보
  - 시스템 소비 전력, 공기 배출량, 흡기 온도와 같은 시스템 환경 정보
- scfPPARInfo 그룹
  이는 다음 물리 분할(PPAR)의 정보를 제공합니다.
  - PPAR ID, 장착된 CPU 수, 메모리 용량 및 기타 PPAR 하드웨어 정보
  - OpenBoot PROM, POST, 하이퍼바이저 버전
  - Oracle Solaris 정보
  - PPAR 작동 상태, 구성 정책
- scfPsbInfo 그룹
  이는 PSB 번호, PSB 전원 상태, PSB에 PPAR 할당/설치와 같은 PSB 정보를 제공합니다.
- scfLsbInfo 그룹
  이는 LSB 번호, LSB가 속한 PPAR의 ID 및 PCL 정보와 같은 LSB 정보를 제공합니다.
- scfBoardInfo 그룹
  이는 CPU 메모리 장치(CMUL, CMUU) 이름, 번호 및 작동 상태와 같은 CMU 정보를 제공합니다.
- scfCpuInfo 그룹
  이는 CPU 번호, CPU 주파수 및 작동 상태와 같은 CPU 모듈 정보를 제공합니다.
- scfMemoryInfo 그룹
  이는 메모리 장치 번호, 용량 및 작동 상태와 같은 정보를 제공합니다.
- scfPciBoxInfo 그룹

이는 PCI 확장 장치(I/O 박스) 및 구성요소의 정보를 제공합니다. 일반 구성요소는 I/O 보드, PCI 카드, 링크 카드, 전원 장치, 팬 장치, 센서입니다. 구성요소의 자세한 내용은 『PCI Expansion Unit for SPARC M10 Systems Service Manual』의 "2장 PCI 확장 장치의 구성요소 이해"를 참조하십시오.

- scfComponentInfo 그룹
  이는 FRU 및 시스템 내 모든 구성요소의 상태와 관련된 정보를 제공합니다.
- scfDomainInfo 그룹
  이는 속한 PPAR ID, 논리 도메인 이름 및 논리 도메인 상태와 같은 논리 도메인의 정보를 제공합니다.

scfHwCtrlMIBObjects

- scfHwCtrlPowerMgmt 그룹
  이는 다음의 PPAR 전원 값 정보를 제공합니다.
  - 현재 소비 전력, 최대 소비 전력, 관리 정책 및 정격 전력 정보.
  - 소비 전력 임계값, 최소 소비 전력 한계, 최대 소비 전력 한계, 한계 초과 시 시스템 작동, 작동 시작 시까지 시간과 같은 전원 설정의 정보 샘플링 사이클 및 평균 소비 전력 등의 소비 전력 샘플링 정보.
  - 논리 도메인에서 참조/구성할 수 있는 전원 캡핑 설정의 정보.

노트 - 논리 도메인의 소비 전력 설정과 관련된 정보는 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

C.4 트랩의 기본 정보

트랩은 표준 트랩과 확장 트랩으로 분류됩니다. 표준 트랩은 SNMP 부합 장치에 일반적인 트랩입니다. 표준 트랩은 일반 설명서를 참조하십시오. 본 설명서에서 이 시스템에 특정된 이벤트를 식별하는 트랩을 확장 트랩이라고 합니다.
확장 트랩은 scfMIBTRap 개체의 다양한 정보를 제공합니다. 확장 트랩의 요약은 "15.3 SNMP 에이전트를 사용한 시스템 상태 모니터링/관리"를 참조하십시오.

부록 D

SPARC M10 시스템용 Oracle VM Server for SPARC의 특징

이 부록에는 SPARC M10 시스템에 한정된 Oracle VM Server for SPARC의 특징과 보충 정보가 설명되어 있습니다.
Oracle VM Server for SPARC 소프트웨어의 관리와 관련된 일반 정보는 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

- 도메인의 지정된 종료
- 필요 시 용량 제공 지원
- 고장인 자원 보기
- 고장인 CPU의 자동 교체
- 하이퍼바이저 덤프 수집
- 도메인 콘솔 로깅

D.1 도메인의 지정된 종료

SPARC M10 시스템의 XSCF에서 모든 논리 도메인의 지정된 종료를 수행할 수 있습니다. 지정된 종료의 시작 방법과 관련된 자세한 내용은 『SPARC M10 시스템 도메인 구성 안내서』를 참조하십시오.
ldom(1M) 명령을 사용하면 논리 도메인의 종료 그룹 번호를 설정하여 종료 순서를 수정할 수 있습니다.
도메인은 종료 그룹 번호의 내림차순으로 종료됩니다. 즉, 가장 높은 번호의 도메인이 먼저 종료됩니다. 가장 낮은 번호의 도메인은 마지막에 종료됩니다. 2개 이상의 도메인이 우선순위 하나를 공유하는 경우 마스터-슬레이브 관계가 없다면 종료 순서는 동시가 됩니다. 이 경우 슬레이브 도메인이 마스터 도메인 전에 종료됩니다.

유효 값은 1 ~ 15입니다. 기타 모든 도메인의 기본 값은 15입니다. 제어 도메인의 종료 그룹 번호는 0이며 변경할 수 없습니다.

예를 들어 2차 도메인은 기본 이외의 종료 그룹 번호를 갖습니다.

```
# ldm set-domain shutdown-group=8 secondary
```

기타 모든 게스트 도메인은 기본 종료 그룹 번호를 갖습니다. 지정된 종료 동안 2차 도메인은 모든 게스트 도메인 후와 제어 도메인 전에 종료됩니다.

노트 - 기존 도메인에 대해 종료 그룹 속성을 설정할 수 있습니다. 도메인은 비활성, 바운딩 또는 활성이 될 수 있습니다. 새 도메인을 생성하는 경우에도 속성을 설정할 수 있습니다. 하지만 XSCF는 업데이트된 종료 순서가 적용되기 전에 새 속성 값을 알고 있어야 합니다. ldm add-spconfig 명령을 사용하여 논리 도메인 구성을 XSCF에 저장하십시오. 도메인은 논리 도메인 구성에 포함되도록 바인딩 또는 활성이 되어야 합니다. 그런 다음 XSCF가 새 구성을 읽도록 서버 전원 공급/차단을 반복하십시오.

D.1.1 도메인 테이블(ldomTable)

ldomShutdownGroup 속성이 ldomTable에 추가됩니다. ldomTable은 시스템의 각 도메인을 나타내는 데 사용되며 OracleVM Server for SPARC MIB에서 검색할 수 있는 도메인 정보를 설명합니다.

표 D-1 도메인 테이블(ldomTable)

이름	데이터 유형	액세스	설명
ldomShutdownGroup	정수	읽기 전용	지정된 종료 동안 도메인의 종료 우선순위. 종료 요청은 15 ~ 0인 종료 그룹의 내림차순으로 도메인에 내려집니다. 제어 도메인의 종료 그룹은 항상 0입니다.

D.1.2 도메인 정보(ldom_info) 자원

"종료 그룹" 속성은 ldom_info 자원에 추가됩니다.

```
<Envelope>
    <References/>
    <Content xsi:type="ovf:VirtualSystem_Type" id="primary">
      <Section xsi:type="ovf:ResourceAllocationSection_type">
        <항목>
          <rasd:OtherResourceType>ldom_info</rasd:OtherResourceType>
          <uuid>c2c3d93b-a3f9-60f6-a45e-f35d55c05fb6</uuid>
          <rasd:Address>00:03:ba:d8:ba:f6</rasd:Address>
          <gprop:GenericPropertykey="hostid">83d8baf6</gprop:GenericProperty>
          <gprop:GenericProperty key="master">plum</gprop:GenericProperty>
          <gprop:GenericProperty key="failure-policy">reset</gprop:
GenericProperty>
          <gprop:GenericProperty key="extended-mapin-space">on</gprop:
GenericProperty>
          <gprop:GenericProperty key="shutdown-group">0</gprop:GenericProperty>
          <gprop:GenericProperty key="progress">45%</gprop:GenericProperty>
```

```
            <gprop:GenericProperty key="status">ongoing</gprop:GenericProperty>
            <gprop:GenericProperty key="source">dt90-319</gprop:GenericProperty>
          </Item>
        </Section>
      </Content>
</Envelope>
```

ldom_info 자원은 항상 <Content> 섹션 내에 포함됩니다. ldom_info 자원 내의 다음 속성은 옵션 속성입니다.

- 지정된 종료 동안 사용된 종료 우선순위를 나타내는 <gprop:GenericProperty key="shutdown-group"> 태그. 종료 요청은 15 ~ 0인 종료 그룹의 내림차순으로 도메인에 내려집니다. 제어 도메인의 종료 그룹은 항상 0입니다. 기타 모든 도메인의 종료 그룹에 유효한 값은 1 ~ 15입니다.

ldom_info 자원의 기타 속성은 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

D.2 필요 시 용량 제공 지원

SPARC M10 시스템은 필요 시 용량 제공을 지원합니다. 논리 도메인 관리자를 사용하여 CPU 코어에 대해 필요 시 용량 제공 허가 정보를 나열할 수 있습니다.
필요 시 용량 제공의 자세한 내용은 "14장 필요 시 용량 제공(CoD)"을 참조하십시오.

D.2.1 필요 시 용량 제공 허가 정보의 나열 방법

1. 다음 하위 명령을 실행하여 **CPU** 코어에 대해 필요 시 용량 제공 허가 정보를 나열합니다.

```
# ldm list-permits
```

PERMITS 열은 CPU에 대해 총 15개의 허가가 내려졌음을 나타냅니다. IN USE 열은 14개의 CPU 코어 허가가 현재 사용 중임을 나타냅니다. REST 열은 CPU 코어 허가를 하나만 사용할 수 있음을 나타냅니다.

```
#ldm list-permits
CPU CORE
PERMITS(PERMANENT)   IN USE      REST
15      (15)         14          1
```

도메인 자원의 기타 항목 나열과 관련된 정보는 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

D.3 고장인 자원 보기

SPARC M10 시스템은 고장인 메모리와 CPU 자원을 자동으로 감지하여 성능 저하시킵니다. ldm list-domain 및 ldm list-devices 명령에 -S 옵션을 지정하여 메모리와 CPU 자원의 상태를 생성할 수 있습니다.
도메인 자원의 나열과 관련된 정보는 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.
다음 절인 "고장인 CPU의 자동 교체"를 참조할 수도 있으며 이 절에는 사용 가능한 여유 CPU 및/또는 CPU 코어 허가가 있을 때 고장인 CPU를 자동 교체하도록 Oracle VM Server for SPARC 3.0을 구성하는 방법이 설명되어 있습니다.

D.3.1 모든 도메인에 대한 자원 상태의 생성 방법

1. 모든 도메인에 대해 긴 목록을 생성합니다.

```
primary# ldm list -l -S
```

D.3.2 사용 가능한 자원에 대한 상태 생성 방법

1. 사용 가능한 메모리 및 **CPU** 자원에 대한 상태를 생성합니다.

```
primary# ldm list-devices -S mem cpu
```

D.4 고장인 CPU의 자동 교체

SPARC M10 시스템은 고장인 CPU를 자동으로 감지하여 오프라인시킵니다. 사용 가능한 여유 CPU 및/또는 CPU 코어 허가가 있을 때 고장인 CPU를 자동 교체하도록 Oracle VM Server for SPARC 3.0을 구성할 수 있습니다.

노트 - 자동 교체가 성공하려면 특정 조건이 충족되어야 합니다.
첫 번째, 시스템의 비고장 CPU 코어 수가 총 허가 수를 넘어서야 합니다. 이 조건은 교체용으로 충분한 비고장 CPU가 시스템에 있다고 보장합니다.
두 번째, 적어도 상이한 2개 CPU 코어의 CPU 자원이 도메인에 할당되어야 합니다. 도메인에 최소 2개 CPU 코어를 할당하는 것이 좋습니다.

D.4.1 자동 교체 정책의 수정 방법

자동 교체 정책에서는 고장인 CPU 자원의 처리 방법을 지정합니다. 자동 교체 정책은 ldmd 서비스의 autoreplacement_policy_cpu 속성을 설정하여 지정합니다. Autoreplacement_policy_cpu 속성의 값은 다음과 같을 수 있습니다.

- autoreplacement_policy_cpu=1
  고장인 CPU 자원의 자동 교체를 시도하는 CPU 자동 교체 프로세스를 활성화합니다. 이는 기본 정책입니다.
- autoreplacement_policy_cpu=0
  CPU 자동 교체 프로세스를 비활성화합니다.

1. 제어 도메인에 로그인합니다.
2. 관리자, **superuser**가 되거나 동등한 역할을 하도록 합니다.
   Oracle Solaris 10의 경우 『시스템 관리 안내서: 보안 서비스』의 "RBAC 구성(작업 맵)"을 참조하십시오. Oracle Solaris 11의 경우 『Oracle Solaris 관리: 보안 서비스』의 파트 III, "역할, 권리 프로파일 및 권한"을 참조하십시오.
3. **Autoreplacement_policy_cpu** 속성 값을 봅니다.

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu
```

4. **ldmd** 서비스를 정지합니다.

```
# svcadm disable ldmd
```

5. **Autoreplacement_policy_cpu** 속성 값을 변경합니다.

```
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=value
```

6. **ldmd** 서비스를 새로고쳐 다시 시작합니다.

```
# svcadm refresh ldmd
# svcadm enable ldmd
```

이 예에는 autoreplacement_policy_cpu 속성의 현재 값을 보고 새 값으로 변경하는 방법이 나타나 있습니다. 이 속성의 원래 값은 0이며 CPU 자동 교체 프로세스의 비활성화를 의미합니다. Svcadm 명령은 ldmd 서비스를 정지 및 다시 시작하는 데 사용되며 svccfg 명령은 속성 값을 보고 설정하는 데 사용됩니다.

```
# 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
```

D.4.2 최대 재시도 카운터 및 재시도 간격의 수정 방법

자동 교체 정책의 수정 외에 CPU 자동 교체 프로세스의 최대 재시도 횟수와 재시도 사이 간격을 설정할 수도 있습니다.

- 최대 재시도 횟수는 ldmd 서비스의 autoreplacement_retry_counter 속성을 설정하여 지정합니다. 값 0에서는 재시도 횟수가 무한입니다. 기본 값은 5회 재시도입니다.
- 재시도 간격은 ldmd 서비스의 autoreplacement_retry_interval 속성을 설정하여 지정합니다. 최소 간격은 1초입니다. 기본 값은 300초입니다. 이 속성의 수정 절차는 autoreplacement_policy_cpu 속성 값의 수정 절차와 동일합니다. 이전 절 "자동 교체 정책의 수정 방법"을 참조하십시오.

D.5 하이퍼바이저 덤프 수집

하이퍼바이저가 물리 분할의 불일치를 감지하면 하이퍼바이저 중단 이벤트가 발생할 수도 있습니다. SPARC M10 시스템의 경우 하이퍼바이저 메모리의 내용이 펌웨어에 의해 보존되고 시스템이 공장 기본 구성으로 재부팅됩니다. 이 특징은 기본적으로 활성화됩니다.
ldmd는 하이퍼바이저 메모리의 보존된 내용을 /var/opt/SUNWldm/hvdump.N.gz라고 하는 제어 도메인의 파일로 복사합니다. N은 0-7 범위의 숫자입니다. 이 파일은 하이퍼바이저 중단 당시 하이퍼바이저 메모리 내용의 이진 덤프입니다.

하이퍼바이저 덤프 수집 프로세스가 완료되면 원래 논리 도메인 구성을 복원하도록 제어 도메인이 재부팅되어야 합니다. 하이퍼바이저 덤프 수집 후 자동 재부팅되도록 set-hvdump 하위 명령을 사용하여 제어 도메인을 구성할 수 있습니다. 덤프 수집 후 자동 재부팅은 기본적으로 비활성화됩니다.

D.5.1 하이퍼바이저 덤프 수집의 비활성화 방법

1. 하이퍼바이저 덤프 수집의 현재 설정을 나열합니다.

```
# ldm list-hvdump
```

2. 하이퍼바이저 덤프 수집을 비활성화합니다.

```
# ldm set-hvdump hvdump=off
```

D.5.2 하이퍼바이저 덤프 수집의 활성화 방법

1. 하이퍼바이저 덤프 수집을 활성화합니다.

```
# ldm set-hvdump hvdump=on
```

D.5.3 덤프 수집 후 자동 재부팅의 활성화 방법

1. 하이퍼바이저 덤프 수집의 현재 설정을 나열합니다.

```
# ldm list-hvdump
```

2. 하이퍼바이저 덤프 수집 후 자동 재부팅을 활성화합니다.

```
# ldm set-hvdump hvdump-reboot=on
```

D.5.4 덤프 수집 후 자동 재부팅의 비활성화 방법

1. 하이퍼바이저 덤프 수집의 현재 설정을 나열합니다.

```
# ldm list-hvdump
```

2. 하이퍼바이저 덤프 수집 후 자동 재부팅을 비활성화합니다.

```
# ldm set-hvdump hvdump-reboot=off
```

D.5.5 덤프 수집 프로세스의 수동 시작 방법

하이퍼바이저 덤프 수집 프로세스는 시스템이 공장 기본 구성으로 재부팅된 후 자동으로 이루어집니다. 하지만 자동 덤프 수집 프로세스는 너무 많은 기존 덤프 파일 또는 제어 도메인의 부족한 디스크 공간 등 여러 이유로 실패할 수도 있습니다. 문제를 해결했으면 덤프 수집 프로세스를 수동으로 시작할 수 있습니다.

1. 현재 설정을 나열하고 해결되지 않은 하이퍼바이저 덤프가 있는지 확인합니다.

```
# ldm list-hvdump
```

2. 하이퍼바이저 덤프 수집 프로세스를 수동으로 시작합니다.

```
# ldm start-hvdump
```

D.6 도메인 콘솔 로깅

논리 도메인 환경에서 1차 도메인의 콘솔 I/O는 XSCF로 디렉션됩니다. 기타 모든 도메인의 콘솔 I/O는 VCC(Virtual Console Concentrator)를 실행하는 서비스 도메인으로 리디렉션됩니다.
Solaris 11.1부터 서비스 도메인은 논리 도메인의 콘솔 로깅을 지원합니다.
도메인의 콘솔 로그는 VCC 서비스를 제공하는 서비스 도메인의 /var/log/vntsd/domain-name/console-log라고 하는 파일에 저장됩니다. 콘솔 로그 파일은 logadm(1M)에 의해 회전됩니다. 자세한 내용은 logadm.conf(4)를 참조하십시오.
Oracle VM Server for SPARC 3.0 소프트웨어를 사용하면 각 논리 도메인마다 콘솔 로깅을 선택적으로 활성화 및 비활성화할 수 있습니다. 콘솔 로깅은 기본적으로 활성화됩니다.

D.6.1 콘솔 로깅의 비활성화 방법

1. 도메인의 현재 콘솔 설정을 나열합니다.

```
# ldm list -o console domain
```

2. 콘솔 로깅을 비활성화합니다.

```
# ldm set-vcons log=off domain
```

노트 - ldm set-vcons 명령을 사용하여 콘솔 설정을 수정하려면 도메인이 언바인딩되어야 합니다. 즉, 비활성 상태에 있어야 합니다.

노트 - 도메인이 동일한 콘솔 그룹에 속하더라도 콘솔 로깅을 각 논리 도메인마다 개별적으로 활성화 또는 비활성화해야 합니다.

D.6.2 콘솔 로깅의 활성화 방법

1. 도메인의 현재 콘솔 설정을 나열합니다.

```
# ldm list -o console domain
```

2. 콘솔 로깅을 활성화합니다.

```
# ldm set-vcons log=on domain
```

D.6.3 서비스 도메인 요구 사항

서비스 도메인이 Solaris 11.1 이전의 OS 버전을 실행하는 경우 서비스 도메인에 연결된 도메인은 로깅되지 않습니다.

노트 - 도메인의 콘솔 로깅을 활성화하더라도 서비스 도메인에서 필요한 지원을 사용할 수 없으면 도메인의 가상 콘솔이 로깅되지 않습니다.

D.6.4 가상 콘솔 그룹 테이블(ldomVconsTable)

ldomVconsLog 속성이 ldomVconsTable에 추가됩니다. ldomVconsTable은 모든 가상 콘솔 서비스의 가상 콘솔 그룹을 설명합니다.

표 D-2 가상 콘솔 그룹 테이블(ldomVconsTable)

이름	데이터 유형	액세스	설명
ldomVconsLog	표시 문자열	읽기 전용	콘솔 로깅 상태. 속성 값은 ldm set-vcons 명령으로 지정하는 문자열 "on" 또는 "off"입니다.

노트 - 한 그룹에 여러 도메인이 포함된 경우 ldomVconsLog 속성은 ldm set-vcons 명령으로 최근 수정한 도메인의 콘솔 로깅 상태를 나타냅니다.

D.6.5 콘솔(콘솔) 자원

"Enable-log" 속성은 콘솔 자원에 추가됩니다.

```
<Envelope>
    <References/>
    <Content xsi:type="ovf:VirtualSystem_Type" id="ldg1">
      <Section xsi:type="ovf:VirtualHardwareSection_Type">
        <항목>
          <rasd:OtherResourceType>console</rasd:OtherResourceType>
          <gprop:GenericProperty key="port">6000</gprop:GenericProperty>
          <gprop:GenericProperty key="service_name">vcc2</gprop:GenericProperty>
          <gprop:GenericProperty key="group">group-name</gprop:GenericProperty>
          <gprop:GenericProperty key="enable-log">on</gprop:GenericProperty>
        </Item>
      </Section>
    </Content>
  </Envelope>
```

콘솔 자원은 항상 <Content> 섹션 내에 포함됩니다. 다음 키의 <gprop: GenericProperty> 태그가 있을 수 있습니다.

- enable-log – 이 콘솔의 가상 콘솔 로깅 활성화 또는 비활성화

콘솔 자원의 기타 속성은 사용 버전의 『Oracle VM Server for SPARC 관리 안내서』를 참조하십시오.

색인

D
DVD 드라이브, 143

H
HTTPS 서비스, 121

I
iSCSI, 171

O
OpenBoot PROM, 16
Oracle VM Server for SPARC, 15

P
PCI 확장 장치, 187

S
SNMP 에이전트, 207
SSH/Telnet 서비스, 116

X
XSCF 네트워크, 95
XSCF 사용자, 73
XSCF 웹, 303
XSCF 펌웨어, 4
XSCF 펌웨어, 구성, 69
XSCF 확장 MIB, 328

ㄱ
가상 CPU, 183

ㄴ
논리 도메인, 149

ㄹ
로그, 확인, 255
로그아웃, 43
로그인, 43

ㅁ
메모리 미러링, 157
메시지, 확인, 255
무정전 전원 공급 장치, 181
문제 해결, 291
물리 분할, 145

ㅅ
상태, 확인, 237
서비스 모드, 55
설정 항목, 61
소비 전력, 141
시간/날짜, 설정, 82
시스템 고도, 133
시스템 관리 터미널, 22
시스템, 시작, 27
시스템, 정지, 34

ㅇ
업데이트, 275
이중 전원 공급, 181

ㅈ
작동 모드, 전환, 55
전원 공급 연동 기능, 171

ㅍ
필요 시 용량 제공, 189

ㅎ
하드웨어 RAID, 159
하이퍼바이저, 15
활성 모니터링, 222