

SNMP 및 IPMI에 대한 Oracle® ILOM 프로토콜 관리 참조 펌웨어 릴리스 3.2.x

펌웨어 릴리스 3.2.x

ORACLE

부품 번호: E40350-03
2015년 6월

부품 번호: E40350-03

Copyright © 2014, 2015, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 합의서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 합의서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 전송, 배포, 진열, 실행, 발행 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주시기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 개인이나 법인에게 배송하는 경우, 다음 공지사항이 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.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이선스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이선스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고, 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제3자로부터 제공되는 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. 사용자와 오라클 간의 합의서에 별도로 규정되어 있지 않는 한 Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다. 단, 사용자와 오라클 간의 합의서에 규정되어 있는 경우는 예외입니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스

지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>를 참조하거나, 청각 장애가 있는 경우 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>를 방문하십시오.

목차

이 설명서 사용	9
SNMP 개요	11
Simple Network Management Protocol 정보	11
SNMP 구성 요소	12
Oracle ILOM SNMP MIB	13
SNMP 명령줄 구문 예	16
▼ SNMP 네트워크 환경 구성	16
Oracle ILOM에서 SNMP 설정 구성	19
SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리(CLI)	19
▼ SNMP 액세스 및 권한 부여 설정	19
SNMP 사용자 계정 및 커뮤니티 관리	21
Oracle ILOM을 사용하여 SNMP 트랩 경고 관리	26
SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리(웹)	28
▼ SNMP 읽기/쓰기 액세스와 권한 부여 설정	29
SNMP 사용자 계정 및 커뮤니티 관리	31
▼ SNMP 트랩 경고 관리	36
Oracle ILOM을 사용하여 SNMP MIB 다운로드	37
시작하기 전에 - SNMP MIB 다운로드	38
▼ SNMP MIB 다운로드(CLI)	38
▼ SNMP MIB 다운로드(웹)	38
SNMP를 사용하여 사용자 계정 관리	41
시작하기 전에 - 사용자 계정(SNMP)	41
Oracle ILOM 사용자 계정 구성(SNMP)	42
▼ 사용자 계정 구성	42
▼ Single Sign On 구성	43
Active Directory에 대해 Oracle ILOM 구성(SNMP)	44
▼ Active Directory 설정 관리	44

▼ Active Directory 관리자 그룹 관리	49
▼ Active Directory 운영자 그룹 관리	50
▼ Active Directory 사용자 정의 그룹 관리	51
▼ Active Directory 사용자 도메인 관리	52
▼ Active Directory 대체 서버 관리	53
▼ 서버 중복성 관리	56
▼ Active Directory DNS 로케이터 관리	57
▼ DNS 이름 서버 설정 관리(SNMP)	59
LDAP에 대해 Oracle ILOM 구성(SNMP)	60
▼ LDAP 설정 구성	60
LDAP/SSL에 대해 Oracle ILOM 구성(SNMP)	63
▼ LDAP/SSL 인증서 관리	63
▼ LDAP/SSL 관리자 그룹 관리	64
▼ LDAP/SSL 운영자 그룹 관리	65
▼ LDAP/SSL 사용자 정의 그룹 관리	66
▼ LDAP/SSL 사용자 도메인 관리	68
▼ LDAP/SSL 대체 서버 관리	69
RADIUS에 대해 Oracle ILOM 구성(SNMP)	71
▼ RADIUS 설정 구성	71
구성 요소 정보 및 전자 메일 경고 관리(SNMP)	75
시작하기 전에 - 구성 요소 정보(SNMP)	75
구성 요소 정보 보기(SNMP)	76
▼ 구성 요소 정보 보기	76
시계 설정, 이벤트 로그, Syslog 수신기 및 경고 규칙 관리(SNMP)	77
▼ 시계 설정 보기 및 설정	77
▼ Oracle ILOM 이벤트 로그 보기 및 지우기	78
▼ 원격 Syslog IP 대상 구성	79
▼ 심각도 레벨 경고 규칙 구성	80
전자 메일 경고 통지를 위한 SMTP 클라이언트 구성(SNMP)	81
▼ 경고 알림에 사용할 SMTP 클라이언트 구성	82
전자 메일 경고 설정 구성(SNMP)	83
▼ 전자 메일 경고 설정 관리	83
시스템 전원 모니터링 및 관리(SNMP)	85
시작하기 전에 - 전원 관리(SNMP)	85
전력 소비 인터페이스 모니터링(SNMP)	86
▼ 실제 전력 소비량 모니터링	86
▼ 가용 전력 모니터링	86

▼ 할당된 전력 모니터	86
▼ 허용 전력 소비량 모니터링	86
▼ 전원 관리 등록 정보 모니터링	87
▼ 전력 소비 임계값 설정	87
시스템 전원 정책 유지 보수(SNMP)	88
▼ 전원 정책 보기 및 설정	88
시스템 전력 할당 관리(SNMP)	89
▼ 시스템 전력 할당 설정	89
시스템 전원 등록 정보 관리(SNMP)	90
▼ 시스템 전원 켜기	90
▼ 시스템 전원 재설정	90
Oracle ILOM 펌웨어 업데이트 관리(SNMP)	93
▼ Oracle ILOM 펌웨어 업데이트(SNMP)	93
Oracle ILOM 백업 및 복원 구성 관리(SNMP)	97
▼ 백업 및 복원 등록 정보 확인 및 구성(SNMP)	97
SPARC 진단, POST 및 부트 모드 작업 관리(SNMP)	101
시작하기 전에 - SPARC 호스트 관리(SNMP)	101
SPARC 진단, POST 및 부트 모드 등록 정보 관리(SNMP)	102
▼ SPARC 호스트 진단 등록 정보 관리	102
▼ SPARC 호스트 POST 작업 관리	105
▼ SPARC 호스트 부트 모드 등록 정보 관리	107
▼ SPARC 호스트 키 스위치 등록 정보 관리	109
IPMI를 통한 서버 관리	111
IPMI(지능형 플랫폼 관리 인터페이스)	111
IPMI 정보	111
IPMItool	112
IPMI 경고	113
IPMI Administrator 및 Operator 역할	113
IPMI 서비스 구성	113
▼ IPMI 서비스 상태 사용(CLI)	114
▼ IPMI 서비스 상태 사용(웹)	114
IPMItool을 사용하여 ILOM CLI 명령 실행	116
시작하기 전에 - IPMItool 및 Oracle ILOM 요구 사항	116
▼ IPMItool에서 Oracle ILOM CLI 액세스	116

IPMItool을 사용하여 Oracle ILOM CLI 명령 스크립트 작성	117
시스템 관리 작업 수행(IPMItool)	118
시작하기 전에 - Oracle ILOM 및 IPMItool 요구 사항	118
▼ 센서 목록 표시	118
▼ 단일 센서 세부정보 보기	119
▼ 존재 센서 유형 값 확인 및 해석	119
▼ 호스트 전원 켜기, 전원 끄기 및 종료 기능 관리	121
▼ Oracle ILOM 전력 할당 인터페이스 관리	122
▼ 시스템 전원 정책 관리	124
▼ FRU 제조 세부정보 표시	125
▼ Oracle ILOM 이벤트 로그 표시	126
IPMItool 유틸리티 및 명령 요약	127
SNMP 명령 예	129
snmpget 명령	129
snmpwalk 명령	130
snmpbulkwalk 명령	131
snmpstat 명령	131
snmpset 명령	134
snmptrapd 명령	135
색인	137

이 설명서 사용

- **개요** - 지원되는 관리 프로토콜인 SNMP(Simple Network Management Protocol)와 IPMI(지능형 플랫폼 관리 인터페이스) 중 하나를 사용하여 원격 Oracle 하드웨어 장치를 관리하기 위한 지침을 제공합니다.
- **대상** - 이 설명서는 기술자, 시스템 관리자 및 공인 Oracle 서비스 공급자를 대상으로 합니다.
- **필요한 지식** - 사용자에게 시스템 하드웨어 관리 경험이 있어야 합니다.

제품 설명서 라이브러리

이 제품과 관련 제품에 대한 설명서 및 리소스는 http://docs.oracle.com/cd/E37444_01/index.html에서 사용할 수 있습니다.

피드백

이 설명서에 대한 피드백은 <http://www.oracle.com/goto/docfeedback>에서 보낼 수 있습니다.

SNMP 개요

설명	링크
SNMP에 대한 Oracle ILOM의 지원 기능 알아보기	■ “Simple Network Management Protocol 정보” [11]
SNMP를 사용한 관리에 대해 알아보기	■ “SNMP 구성 요소” [12]
Oracle ILOM SNMP MIB (Management Information Base) 파일에 대해 알아보기	■ “Oracle ILOM SNMP MIB” [13]
이 설명서에서 사용되는 명령줄 구문에 대해 알아보기	■ “SNMP 명령줄 구문 예” [16]

관련 정보

- [“Modifying Default Management Access Configuration Properties” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)
- [“Oracle ILOM Overview” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 3.2.x](#)

Simple Network Management Protocol 정보

Oracle ILOM은 네트워크 작업에 대한 데이터를 교환하는 데 사용되는 SNMP(Simple Network Management Protocol)를 지원합니다. SNMP는 네트워크 및 장치 또는 네트워크에 연결된 노드 관리를 지원하는 개방형 산업 표준 프로토콜 기술입니다. SNMP를 사용하면 네트워크에 액세스하여 관리 대상 장치(노드)와 관리 스테이션 간에 데이터를 전송할 수 있습니다. 호스트, 라우터, 웹 서버 또는 기타 네트워크의 서버와 같이 SNMP를 실행하는 모든 장치는 관리 대상 장치가 될 수 있습니다. SNMP 메시지는 UDP(User Datagram Protocol)를 사용하여 IP를 통해 전송됩니다. SNMP를 지원하는 모든 관리 응용 프로그램에서 서버를 관리할 수 있습니다.

SNMP는 응용 프로그램이 아니라 프로토콜이므로 SNMP 명령을 실행하려면 응용 프로그램이 필요합니다. SNMP 관리 소프트웨어에서 이 기능을 제공할 수도 있고, <http://net-snmp.sourceforge.net/>에서 제공되는 오픈 소스 도구(예: Net-SNMP)를 사용할 수도 있습니다.

SNMP에 대한 자세한 설명은 http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php에서 제공되는 5부, 소개용 SNMP 자습서를 참조하십시오.

Oracle ILOM에서는 SNMP 버전 1, 2c 및 3을 지원합니다. SNMP v3은 SNMP v1 및 v2c 보다 강력한 보안, 인증 및 프라이버시 기능을 제공하므로 SNMP v3을 사용하는 것이 좋습니다.

주 - 이 문서를 읽는 Oracle ILOM 사용자는 SNMP에 대한 실무 지식이 있는 것으로 가정합니다. 이 텍스트의 SNMP 사용 예에서는 SNMP 클라이언트측 명령을 사용합니다. SNMP에 대한 작업 지식이 없는 사용자는 http://net-snmp.sourceforge.net/wiki/index.php/Main_Page에서 자습서를 완료해야 합니다. 이 자습서는 위에 언급된 소개용 자습서보다 심층적입니다.

SNMP 구성 요소

SNMP 기능에는 다음 두 가지 구성 요소가 필요합니다.

- **네트워크 관리 스테이션** - 네트워크 관리 스테이션은 관리 대상 노드를 모니터링 및 제어하는 관리 응용 프로그램을 호스팅합니다.
- **관리 대상 노드** - 관리 대상 노드는 Oracle ILOM을 실행하는 SP(서비스 프로세서)와 같은 관리 스테이션의 요청을 전달하는 SNMP 관리 에이전트를 호스팅하는 서버, 라우터 또는 허브와 같은 장치입니다. 관리 대상 노드는 트랩 형식의 원치 않는 상태 정보를 관리 스테이션에 제공할 수도 있습니다.

SNMP는 관리 스테이션과 SNMP 에이전트 간에 관리 정보를 전달하는 데 사용되는 프로토콜입니다.

SNMP 에이전트는 Oracle 서버에 사전 설치되고 Oracle ILOM에서 실행되므로 모든 SNMP 관리는 Oracle ILOM을 통해 발생합니다. 이 기능을 사용하려면 운영체제에 SNMP 클라이언트 응용 프로그램이 설치되어 있어야 합니다.

관리 스테이션과 에이전트 모두 SNMP 메시지를 사용하여 통신합니다. 관리 스테이션에서는 정보를 보내고 받을 수 있습니다. 에이전트는 요청에 응답하고 트랩 형식의 원치 않는 메시지를 보낼 수 있습니다. 관리 스테이션과 에이전트에서 사용하는 기능은 다음과 같습니다.

- Get
- GetNext
- GetResponse
- Set
- Trap

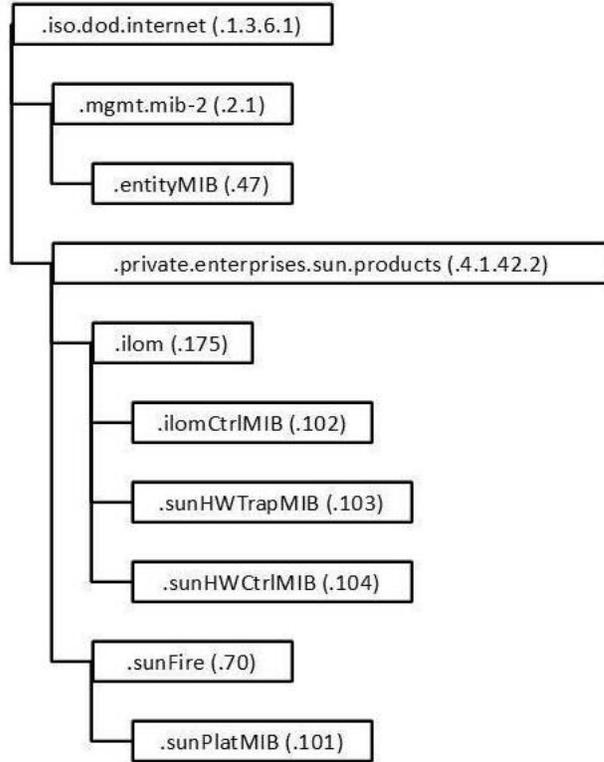
Oracle ILOM SNMP MIB

SNMP 구현의 기본 구성 요소는 MIB(Management Information Base)입니다. MIB는 관리 대상 노드의 사용 가능한 정보를 설명하는 텍스트 파일입니다. 트리와 같은 이 계층형 시스템은 각각 고유 식별자 또는 객체 ID가 있는 데이터 객체 목록으로 네트워크의 리소스에 대한 정보를 분류합니다. 따라서 MIB는 SNMP 에이전트에서 액세스할 수 있는 데이터 객체 또는 변수를 정의합니다. 관리 스테이션이 관리 대상 노드에서 정보를 요청하면 에이전트가 요청을 받아 MIB에서 적절한 정보를 검색합니다. Oracle ILOM에서는 MIB를 통해 서버의 네트워크 구성, 상태 및 통계에 액세스할 수 있습니다.

SNMP MIB는 Oracle ILOM 펌웨어의 일부입니다. Oracle ILOM에서 직접 MIB를 다운로드할 수 있습니다. MIB에 대한 자세한 내용 및 Oracle ILOM에서 MIB를 다운로드하는 것과 관련된 지침은 [“시작하기 전에 - SNMP MIB 다운로드” \[38\]](#)를 참조하십시오.

다음 그림은 표준 MIB 계층과 해당 계층에서 Oracle ILOM MIB 모듈의 위치를 보여줍니다. Oracle ILOM MIB 모듈은 다음에 나오는 표에 설명되어 있습니다.

그림 1 Oracle ILOM MIB 모듈의 위치



다음 표는 Oracle ILOM MIB 모듈 및 각 MIB 이름에 대한 객체 ID를 보여줍니다.

표 1 Oracle ILOM MIB 모듈, 객체 ID 및 MIB 이름에 대한 설명

MIB 이름	설명	MIB 객체 ID
ENTITY-MIB	단일 SNMP 에이전트에서 지원하는 여러 물리적 엔티티를 나타내는 MIB 모듈입니다. 주 - entPhysicalTable은 구현된 이 MIB에만 속합니다.	1.3.6.1.2.1.47
SUN-ILOM-CONTROL-MIB	이 MIB는 모든 Oracle ILOM 기능을 구성 및 관리할 수 있는 객체를 제공합니다. 이 MIB가 적용되는 구성에는 권한 부여, 인증, 로깅, 서비스, 네트워킹 및 펌웨어 관리와 같은 기능이 포함됩니다.	1.3.6.1.4.1.42.2.175.102
SUN-HW-TRAP-MIB	이 MIB는 Oracle Sun 서버 플랫폼에서 생성할 수 있는 하드웨어 관련 알림/트랩을 설명합니다.	1.3.6.1.4.1.42.2.175.103

MIB 이름	설명	MIB 객체 ID
	Oracle ILOM에서 SNMP 트랩을 관리하는 것과 관련된 자세한 내용은 Oracle ILOM에서 SNMP 설정 구성 을 참조하십시오.	
SUN-HW-CTRL-MIB	이 MIB를 통해 Oracle ILOM을 사용하는 모든 Oracle Sun 서버 플랫폼 장치를 제어할 수 있습니다. 주 - 이 MIB의 전원 관리 부분만 구현됩니다.	1.3.6.1.4.1.42.2.175.104
SUN-PLATFORM-MIB	이 MIB는 시스템에 모델링된 각 엔티티가 entPhysicalTable의 확장을 통해 표시되는 ENTITY-MIB(RFC 2737)에 대한 확장을 제공합니다.	1.3.6.1.4.1.42.2.70.101

다음 표에 나열된 표준 MIB의 일부가 Oracle ILOM에서 구현되었습니다.

표 2 Oracle ILOM에서 구현되는 표준 MIB

MIB 이름	설명	MIB 객체 ID
IF-MIB	네트워크 인터페이스 하위 계층의 일반 객체를 설명하는 MIB 모듈입니다. 이 MIB는 MIB-II ifTable의 업데이트된 버전으로, RFC 1229에 정의된 확장을 통합합니다.	1.3.6.1.2.1.31
IP-MIB	IP 경로 관리를 제외하고 IP 및 ICMP 구현을 관리하는 MIB 모듈입니다.	1.3.6.1.2.1.4.
SNMP-FRAMEWORK-MIB	SNMP 관리 아키텍처 MIB입니다.	1.3.6.1.6.3.10
SNMPv2-MIB	SNMP 엔티티의 MIB 모듈입니다. 주 - 이 MIB 모듈의 시스템 및 SNMP 그룹만 Oracle ILOM에 적용됩니다.	1.3.6.1.6.3.1
TCP-MIB	TCP 구현을 관리하는 MIB 모듈입니다.	1.3.6.1.2.1.49
UDP-MIB	UDP 구현을 관리하는 MIB 모듈입니다.	1.3.6.1.2.1.50

다음 표는 Oracle ILOM SNMP 구현을 지원하는 데 사용되는 MIB를 보여줍니다.

표 3 Oracle ILOM SNMP 구현을 지원하는 데 사용되는 MIB

MIB 이름	설명	MIB 객체 ID
HOST-RESOURCE-MIB	이 MIB는 호스트 시스템을 관리하는 데 사용됩니다. MIB는 UNIX 변형을 실행하는 PC 및 시스템을 포함하여 모든 인터넷 호스트에 공통적인 속성을 지원합니다.	1.3.6.1.2.1.25.1
IANAifType-MIB	이 MIB 모듈은 IANAifType Textual Convention을 정의하므로 MIB-II의 ifTable에 정의된 ifType 객체의 열거형 값을 정의합니다.	1.3.6.1.2.1.30
NOTIFICATION-LOG-MIB	이 MIB 모듈은 SNMP 알림(트랩)을 기록하는 데 사용됩니다.	1.3.6.2.1.92.1.1.3
SNMP-MPD-MIB	이 MIB 모듈은 메시지 처리 및 전달에 사용됩니다.	1.3.6.1.6.3.11
SNMPv2-TM	이 MIB 모듈은 SNMP 전송 매핑에 사용됩니다.	1.3.6.1.6.3.19
SNMPv2-SMI	이 MIB 모듈에는 버전 2 관리 정보 구조에 대한 정의가 포함되어 있습니다.	1.3.6.1.6

SNMP 명령줄 구문 예

일부 네트워크 환경에서는 SNMP 명령을 실행할 때 SNMP 버전, 커뮤니티 이름, 호스트 이름 및 기본 포트를 지정해야 합니다. 예를 들어 IPv4 환경에서 OID(객체 식별자) `sysDescr.0`의 값을 요청하려면 다음과 같이 입력할 수 있습니다.

```
%snmpget -v2c -c public 192.0.2.1:161 sysDescr.0
```

하지만 가능한 한 명령줄 인수를 사용하지 않아도 되도록 네트워크 환경을 구성할 수 있습니다. 예를 들어 SNMP v1 또는 v2c의 경우 SNMP 버전, 커뮤니티 이름 및 기본 포트에 대한 기본값을 설정하면 다음 구문이 유효한 것으로 간주됩니다.

```
%snmpget SNMP_agent sysDescr.0
```

이 설명서 전체에서 *SNMP_agent*는 질의하려는 시스템의 호스트 이름 또는 IP 주소를 나타냅니다.

주 - IPv6 주소 지정을 사용하여 장치를 질의하는 경우 `udp6:[IPv6 address]` 구문을 사용해야 합니다. 질의에 대해 `getaddrinfo: node name or service name not known` 메시지가 수신되면 SNMP 명령줄 인수에 `-YdefaultPort=<port_number>`를 추가해 보십시오.

또한 이 설명서의 예에서는 대부분의 명령줄 인수를 생략합니다. 가능한 한 명령줄 인수를 사용하지 않아도 되도록 네트워크를 구성하려면 다음 절차를 참조하십시오.

- [SNMP 네트워크 환경 구성 \[16\]](#)

▼ SNMP 네트워크 환경 구성

1. Oracle ILOM CLI(명령줄 인터페이스)에 로그인합니다.
Oracle ILOM에 로그인하는 것과 관련된 지침은 [“Log In to the Oracle ILOM CLI” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 3.2.x](#)을 참조하십시오.
2. 다음과 같이 Oracle ILOM에서 `create` 명령을 실행하여 읽기-쓰기 액세스 권한을 가지는 SNMP 커뮤니티를 만듭니다.
-> `create /SP/services/snmp/communities/community_name permission=rw`
3. 다음과 같이 `set` 명령을 실행하여 SNMP 액세스를 사용으로 설정하고 SNMP 에이전트 포트 주소를 지정합니다.
-> `set /SP/services/snmp servicestate=enabled v2c=enabled sets=enabled port=161`

4. `$HOME/mibs` 디렉토리로 Oracle ILOM MIB를 다운로드합니다.
Oracle ILOM MIB 다운로드 지침은 “[Oracle ILOM을 사용하여 SNMP MIB 다운로드](#)” [37]를 참조하십시오.
5. `$HOME/mibs` 디렉토리의 `$HOME/.snmp/snmp.conf` 파일에서 다음과 같이 지정합니다.

```
defversion      2c
defcommunity    community_name
defaultPort     161
mibs            ALL
mibdirs        +$HOME/mibs
```

6. 다음 명령을 실행하여 새 구성을 테스트합니다.

```
%snmpset SNMP_agent sysName.0 s mynewname
```

명령을 통해 시스템에 다음과 유사한 출력이 생성되어야 합니다.

```
RFC1213-MIB::sysName.0 = STRING: "mynewname"
```


Oracle ILOM에서 SNMP 설정 구성

설명	링크
SNMP 액세스, 사용자 계정 및 SNMP 트랩 경고 관리를 위한 Oracle ILOM CLI 절차에 대한 자세한 정보	<ul style="list-style-type: none">■ “SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리(CLI)” [19]■ “SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리(웹)” [28]
Oracle ILOM에서 직접 SNMP MIB를 다운로드하는 방법	<ul style="list-style-type: none">■ “Oracle ILOM을 사용하여 SNMP MIB 다운로드” [37]

관련 정보

- “Modifying Default Management Access Configuration Properties” in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- “Configuring Alert Notifications” in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리 (CLI)

- SNMP 액세스 및 권한 부여 설정 [19]
- “SNMP 사용자 계정 및 커뮤니티 관리” [21]
- “Oracle ILOM을 사용하여 SNMP 트랩 경고 관리” [26]

▼ SNMP 액세스 및 권한 부여 설정

시작하기 전에

- Oracle ILOM에서 SNMP 등록 정보를 수정하려면 Admin(a) 역할이 사용으로 설정되어 있어야 합니다.
- SNMP servicestate 등록 정보는 기본적으로 출하 시 *enabled* 상태로 제공됩니다.

- SNMP sets 쓰기 액세스 등록 정보는 기본적으로 출하 시 *disabled* 상태로 제공됩니다. Oracle ILOM에 대한 SNMP 쓰기 액세스를 허용하려면 SNMP sets 등록 정보를 사용으로 설정해야 합니다.

주 - Oracle ILOM CLI에서 작업할 때 sets 매개변수가 사용 안함으로 설정되어 있으면 모든 SNMP MIB 객체는 읽기 전용이며 `snmpset` 명령이 처리되지 않습니다.

- Oracle ILOM은 SNMP 프로토콜 버전 v1, v2c 및 v3 각각에 대해 인증 등록 정보를 제공합니다.
 - SNMP v1과 v2c의 경우 Oracle ILOM은 사용자 인증 관리를 위해 `communities` 대상 내 `public` 및 `private` 대상을 제공합니다.
 - SNMP v3의 경우 Oracle ILOM은 사용자 인증 관리를 위해 `users` 대상을 제공합니다. SNMPv3 `users` 대상은 출하 시 사용자를 위해 미리 패키징된 값으로 제공되지 않습니다.

SNMP 서비스 상태 등록 정보를 설정하려면 다음 단계를 수행하십시오.

1. Oracle ILOM CLI에 로그인합니다.
2. Oracle ILOM SNMP 등록 정보를 확인하려면 다음과 같이 입력합니다.

-> `show /SP/services/snmp`

다음과 같은 SNMP 출력이 나타납니다.

```
-> show /SP/services/snmp
/SP/services/snmp
Targets:
  communities
  mibs
  users
Properties:
  engineid = none
  port = 161
  servicestate = (enabled)
  sets = disabled
  v1 = disabled
  v2c = disabled
  v3 = enabled
Commands:
  cd
  set
  show
```

3. `set` 명령을 사용하여 SNMP 등록 정보를 변경합니다. 예를 들면 다음과 같습니다.

- 읽기 전용 액세스 권한이 있는 SNMP를 사용으로 설정하려면 다음과 같이 입력합니다.

-> `set /SP/services/snmp servicestate=enabled`

- 쓰기 액세스 권한이 있는 SNMP를 사용으로 설정하려면 다음과 같이 입력합니다.
-> `set /SP/services/snmp sets=enabled`
- SNMP 프로토콜 버전 v1, v2c 또는 v3 등록 정보를 사용으로 설정하려면 다음과 같이 입력합니다.
-> `set /SP/services/snmp v#=enabled`
여기서 #은 사용으로 설정할 SNMP 프로토콜 버전입니다.

SNMP 사용자 계정 및 읽기/쓰기 액세스 권한에 대한 자세한 내용은 [“SNMP 사용자 계정 및 커뮤니티 관리” \[21\]](#)를 참조하십시오.

4. create 명령을 사용하여 다음과 같이 SNMP v3 사용자 계정을 만듭니다.

- 권한 부여용 사용자 계정을 만들고 읽기 및 쓰기 액세스 권한을 제공하려면 다음과 같이 입력합니다.
-> `create /SP/services/snmp/users/<useraccountname> authenticationpassword=password permission=rw`
- 권한 부여용 사용자 계정을 만들고 읽기 전용 액세스 권한을 제공하려면 다음과 같이 입력합니다.
-> `create /SP/services/snmp/users/<useraccountname> authenticationpassword=password`

SNMP 사용자 계정 및 읽기/쓰기 액세스 권한에 대한 자세한 내용은 [“SNMP 사용자 계정 및 커뮤니티 관리” \[21\]](#)를 참조하십시오.

SNMP 사용자 계정 및 커뮤니티 관리

- [“시작하기 전에 - SNMP 사용자 계정” \[21\]](#)
- [“SNMP 사용자 계정 대상, 등록 정보 및 값” \[22\]](#)
- [SNMP 커뮤니티 등록 정보 보기 및 구성 \[23\]](#)
- [“SNMPv3 사용자 이름 및 암호 요구 사항” \[23\]](#)
- [SNMP v3 사용자 계정 추가 \[25\]](#)
- [SNMP v3 사용자 계정 편집 \[25\]](#)
- [SNMP v3 사용자 계정 삭제 \[25\]](#)
- [SNMP v3 사용자 계정 프라이버시 프로토콜 값 설정 \[25\]](#)
- [SNMP v1/v2c 커뮤니티 추가 또는 편집 \[26\]](#)
- [SNMP v1/v2c 커뮤니티 삭제 \[26\]](#)

시작하기 전에 - SNMP 사용자 계정

이 절의 절차를 수행하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- Oracle ILOM에서 SNMP 사용자 계정 등록 정보를 설정하려면 User Management(u) 역할이 사용으로 설정되어 있어야 합니다.
- ILOM에서 적절한 SNMP 설정이 사용으로 설정되어 있는지 확인합니다. [SNMP 액세스 및 권한 부여 설정 \[19\]](#)을 참조하십시오.

주 - Oracle ILOM CLI에서 작업할 때 sets 매개변수가 사용 안함으로 설정되어 있으면 모든 SNMP MIB 객체는 읽기 전용입니다.

- snmpset 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 SNMP v3 사용자 계정을 사용해야 합니다.

주 - 이 단원에 나와 있는 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

SNMP 사용자 계정 대상, 등록 정보 및 값

SNMP 사용자 계정 대상, 등록 정보 및 값은 /SP/services/snmp 대상 아래에서 액세스할 수 있습니다. 다음 표는 SNMP 사용자 계정에 유효한 대상, 등록 정보 및 값을 보여줍니다.

표 4 SNMP 사용자 계정 대상, 등록 정보 및 값

대상	등록 정보	값	기본값
/SP/services/snmp/ communities/ community_name	permissions	ro rw	ro
/SP/services/snmp/users/ username	authenticationprotocol	MD5 SHA	MD5
	authenticationpassword [†]	<string>	(빈 문자열)
	permissions	ro rw	ro
	privacyprotocol	none DES AES*	없음
	privacypassword [‡]	<string>	(빈 문자열)
/SP/services/snmp	engineid = none	<string>	(빈 문자열)
	port = 161	<integer>	161
	servicestate = enabled	enable disabled	enabled
	sets = enabled	enable disabled	disabled
	v1 = disabled	enable disabled	disabled
v2c = disabled	enable disabled	disabled	
v3 = disabled	enable disabled	enabled	

[†]사용자를 만들거나 수정하는 경우 인증 암호를 제공해야 합니다(SNMP v3만 해당).

*privacyprotocol 등록 정보가 none 이외의 값을 갖는 경우 프라이버시 암호를 설정해야 합니다.

*AES(고급 암호화 표준) 프라이버시 프로토콜 옵션은 Oracle ILOM 3.0.16부터 SNMPv 3에 사용할 수 있습니다.

예를 들어 사용자 a1의 privacyprotocol을 DES,로 변경하려면 다음 구문을 사용합니다.

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
privacypassword=password authenticationprotocol=SHA
authenticationpassword=password
```

다음 구문이 지정된 경우에는 변경사항이 무효화됩니다.

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
```

주 - privacy 및 authentication 등록 정보를 재설정하지 않고 SNMP 사용자 권한을 변경할 수 있습니다.

SNMPv3 사용자 이름 및 암호 요구 사항

등록 정보	설명
User Name	SNMP 사용자 이름에는 최대 32자가 포함될 수 있으며 영숫자(대문자, 소문자 및 숫자)의 조합이 사용될 수 있습니다. 공백은 허용되지 않습니다.
Authentication Password	인증 프로토콜 등록 정보가 MD5 또는 SHA로 설정된 경우 인증 암호가 필요합니다. 대/소문자를 구분하는 인증 암호를 입력합니다. 인증 암호에는 8-12자가 포함될 수 있으며 영숫자(대문자, 소문자 및 숫자)의 조합이 사용될 수 있습니다.
Privacy Password	프라이버시 프로토콜 등록 정보가 DES 또는 AES로 설정된 경우 프라이버시 암호가 필요합니다. 프라이버시 암호에는 정확히 8자가 포함되어야 하며 영숫자(대문자, 소문자 및 숫자)의 조합이 사용되어야 합니다.

▼ SNMP 커뮤니티 등록 정보 보기 및 구성

1. /SP/services/snmp 디렉토리로 이동하려면 다음과 같이 입력합니다.

```
-> cd /SP/services/snmp
```

2. 해당 디렉토리에서 show 명령을 입력하여 SNMP 설정을 확인합니다. 기본 설정은 다음과 같습니다.

```
-> show
/SP/services/snmp
Targets:
```

```

communities
mibs
users
Properties:
engineid = (none)
port = 161
servicestate = enabled
sets = disabled
v1 = disabled
v2c = disabled
v3 = enabled
Commands:
cd
set
show

```

3. 커뮤니티를 확인하려면 다음과 같이 입력합니다.

```
-> show /SP/services/snmp/communities
```

예를 들면 다음과 같습니다.

```

-> show /SP/services/snmp/communities
/SP/services/snmp/communities
Targets:
private
public
Properties:
Commands:
cd
create
delete
show

```

4. 읽기/쓰기 권한이 있는 커뮤니티를 만들려면 다음과 같이 입력합니다.

```
-> create /SP/services/snmp/communities/communityname permission=rw
```

5. 공개 커뮤니티를 확인하려면 다음과 같이 입력합니다.

```
-> show /SP/services/snmp/communities/public
```

예를 들면 다음과 같습니다.

```

-> show /SP/services/snmp/communities/public
/SP/services/snmp/communities/public
Targets:
Properties:
permission = ro
Commands:
cd
set
show

```

▼ SNMP v3 사용자 계정 추가

1. Oracle ILOM CLI에 로그인합니다.
2. SNMP v3 읽기 전용 사용자 계정을 추가하려면 다음과 같이 입력합니다.

```
-> create /SP/services/snmp/users/username authenticationpassword=password
```

주 - 암호는 대/소문자를 구분하며 콜론이나 공백 문자 없이 8~16자 이내로 입력해야 합니다.

▼ SNMP v3 사용자 계정 편집

1. Oracle ILOM CLI에 로그인합니다.
2. SNMP v3 사용자 계정을 편집하려면 다음과 같이 입력합니다.

```
-> set /SP/services/snmp/users/username authenticationpassword=password
```

주 - SNMP 사용자의 매개변수를 변경할 때는 암호를 변경하지 않은 경우에도 authenticationpassword 값을 제공해야 합니다.

▼ SNMP v3 사용자 계정 삭제

1. Oracle ILOM CLI에 로그인합니다.
2. SNMP v3 사용자 계정을 삭제하려면 다음과 같이 입력합니다.

```
-> delete /SP/services/snmp/users/username
```

▼ SNMP v3 사용자 계정 프라이버시 프로토콜 값 설정

시작하기 전에

- 사용자 계정의 프라이버시 프로토콜 등록 정보 값을 설정하기 전에 SNMP 사용자 계정을 만들어야 합니다. 자세한 내용은 [SNMP v3 사용자 계정 추가 \[25\]](#)를 참조하십시오.

1. Oracle ILOM CLI에 로그인합니다.
2. SNMP v3 사용자 계정에 지정된 `privacyprotocol` 등록 정보 값을 수정하려면 다음과 같이 입력합니다.

```
-> set /SP/services/snmp/users/username privacyprotocol=<DES|AES|None>
```

주 - Oracle ILOM 3.0.16부터 SNMPv3 AES(고급 암호화 표준) 옵션을 사용할 수 있습니다.

▼ SNMP v1/v2c 커뮤니티 추가 또는 편집

1. Oracle ILOM CLI에 로그인합니다.
2. SNMP v1/v2c 커뮤니티를 추가하려면 다음과 같이 입력합니다.
-> `create /SP/services/snmp/communities/community_name`

▼ SNMP v1/v2c 커뮤니티 삭제

1. Oracle ILOM CLI에 로그인합니다.
2. SNMP v1/v2c 커뮤니티를 삭제하려면 다음과 같이 입력합니다.
-> `delete /SP/services/snmp/communities/community_name`

Oracle ILOM을 사용하여 SNMP 트랩 경고 관리

- [SNMP 트랩 규칙 대상 및 등록 정보 구성 \[26\]](#)
- [“경고 규칙 구성 관리에 필요한 CLI 명령” \[28\]](#)

▼ SNMP 트랩 규칙 대상 및 등록 정보 구성

시작하기 전에

- Oracle ILOM에서 경고 규칙을 만들거나 편집하려면 Admin(a) 역할이 사용으로 설정되어 있어야 합니다.
- SNMP v3 트랩 경고를 정의하려면 Oracle ILOM에서 SNMPv3 사용자 이름을 정의해야 합니다. Oracle ILOM에 SNMP v3 사용자가 정의되지 않은 경우 SNMP 경고를 수신하는 SNMP v3 사용자가 SNMPv3 경고 메시지를 해독할 수 없게 됩니다. Oracle ILOM에서의 SNMPv3 권한 부여 및 SNMP v3 사용자 정의에 대한 자세한 내용은 [“SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리\(CLI\)” \[19\]](#)를 참조하십시오.
- [“경고 규칙 구성 관리에 필요한 CLI 명령” \[28\]](#)을 검토합니다.
- Oracle ILOM에서의 경고 관리 설정 구성에 대한 자세한 내용은 [“Configuring Alert Notifications” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)을 참조하십시오.

SNMP 트랩을 전송할 대상을 구성하려면 다음 단계를 수행하십시오.

1. Oracle ILOM CLI에 로그인합니다.
2. 경고 규칙의 현재 설정을 표시하려면 **show** 명령을 입력합니다.
예를 들면 다음과 같습니다.

```
-> show /SP/alertmgmt/rules/1
/SP/alertmgmt/rules/1
Targets:

Properties:
  type = snmptrap
  level = disable
  destination = 0.0.0.0
  destination_port = 0
  community_or_username = public
  snmp_version = 1
  testrule = (Cannot show property)

Commands:
  cd
  set
  show
```

3. **/SP/alertmgmt/rules** 디렉토리를 표시하려면 다음과 같이 입력합니다.

```
-> cd /SP/alertmgmt/rules
-> show
예를 들면 다음과 같습니다.
```

```
-> cd /SP/alertmgmt/rules
-> show
/SP/alertmgmt/rules
Targets:
  1
  2
  .
  .
  .
  15
Properties:

Commands:
  cd
  show
```

SNMP 트랩 대상을 구성할 규칙(대상 1~15)을 선택하고 해당 디렉토리로 이동합니다.

예를 들면 다음과 같습니다.

-> cd 4

4. 규칙 등록 정보를 변경하려면 해당 규칙 디렉토리에서 **set** 명령을 입력합니다.

예를 들어 커뮤니티 이름으로 “public”을 사용하여 SNMP v2c를 통해 중요한 트랩을 관리 클라이언트로 전송하는 규칙을 설정하려면 다음과 같이 입력합니다.

```
-> set type=snmptrap level=critical
destination=IPaddress_of_snmp_management_station destination_port=port
snmp_version=2c community_or_username=public
```

경고 규칙 구성 관리에 필요한 CLI 명령

다음 표는 Oracle ILOM CLI에서 경고 규칙 구성을 관리하는 데 필요한 CLI 명령에 대해 설명합니다.

표 5 경고 규칙 구성 관리에 필요한 CLI 명령

CLI 명령	설명
show	show 명령은 전체 경로 또는 상대 경로를 지정하여 경고 관리 명령 트리의 레벨을 표시합니다.
cd	cd 명령은 작업 디렉토리를 설정합니다. 경고 관리를 서버 SP의 작업 디렉토리로 설정하려면 명령 프롬프트에 다음 명령을 입력합니다. -> cd /SP/alertmgmt
set	set 명령은 트리의 임의 위치에서 등록 정보 값을 설정합니다. 트리 위치에 따라 등록 정보의 전체 경로 또는 상대 경로를 지정할 수 있습니다. 예를 들면 다음과 같습니다. ■ 전체 경로를 지정하려면 명령 프롬프트에 다음을 입력합니다. -> set /SP/alertmgmt/rules/1 type=snmptrap ■ 상대 경로(트리 위치: /SP/alertmgmt)를 지정하려면 명령 프롬프트에 다음 명령 경로를 입력합니다. -> set rules/1 type=snmptrap ■ 상대 경로(트리 위치: /SP/alertmgmt/rules/1)를 지정하려면 명령 프롬프트에 다음 명령 경로를 입력합니다. -> set type=snmptrap

SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리 (웹)

- [SNMP 읽기/쓰기 액세스와 권한 부여 설정 \[29\]](#)

- “SNMP 사용자 계정 및 커뮤니티 관리” [31]
- SNMP 트랩 경고 관리 [36]

▼ SNMP 읽기/쓰기 액세스와 권한 부여 설정

시작하기 전에

- Oracle ILOM에서 SNMP 등록 정보를 수정하려면 Admin(a) 역할이 사용으로 설정되어 있어야 합니다.
- SNMP service 상태는 기본적으로 출하 시 *enabled* 상태로 제공됩니다.
- SNMP set requests 상태는 기본적으로 출하 시 *disabled* 상태로 제공됩니다. Oracle ILOM에 대한 SNMP 쓰기 액세스를 허용하려면 set requests 상태를 사용으로 설정해야 합니다.

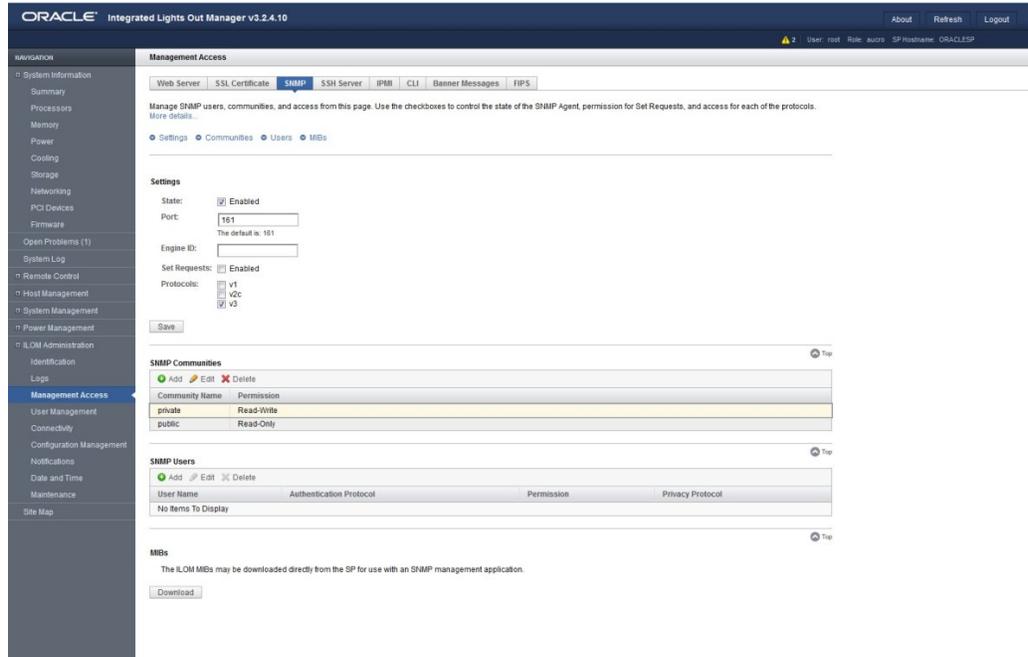
주 - Oracle ILOM에서 set requests 상태가 사용 안함으로 설정된 경우 모든 SNMP 객체는 읽기 전용이며 snmpset 명령이 처리되지 않습니다.

- Oracle ILOM은 SNMP 프로토콜 버전 v1, v2c 및 v3 각각에 대해 인증 등록 정보를 제공합니다.
 - SNMP v1 및 v2c의 경우 Oracle ILOM에서는 사용자 인증을 관리할 communities 등록 정보(값: *public* 및 *private*)를 제공합니다. 그러나 SNMP v1 및 v2c 커뮤니티에 대한 등록 정보 값은 기본적으로 출하 시 *disabled* 상태로 제공됩니다.
 - SNMP v3의 경우 Oracle ILOM에서는 사용자 인증을 관리하는 users 등록 정보를 제공합니다. users 등록 정보는 기본적으로 출하 시 *enabled* 상태로 제공됩니다. SNMP v3 users 등록 정보는 출하 시 사용자를 위해 미리 패키징된 값으로 제공되지 않습니다.

SNMP 서비스 상태 등록 정보를 설정하려면 다음 단계를 수행하십시오.

1. Oracle ILOM 웹 인터페이스에 로그인합니다.
2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. Management Access > SNMP를 누릅니다.

SNMP Management 페이지가 나타납니다.



4. **SNMP 포트를 사용으로 설정하려면 State 확인란을 누릅니다.**
State가 disabled이면 SNMP 포트가 차단되어 Oracle ILOM과 네트워크 간의 모든 SNMP 통신이 금지됩니다.
5. **Port 텍스트 필드에 포트 번호를 입력합니다.**
6. **Engine ID 필드를 빈 상태로 둡니다. 그러면 기본 설정이 사용됩니다.**
Engine ID는 SNMP 에이전트에 의해 자동으로 설정됩니다. 이 필드를 사용하여 엔진 ID를 설정할 수 있지만 이 필드를 비워 두는 것이 좋습니다. Engine ID는 SNMP 엔진을 고유하게 식별하며 사용자가 SNMP 에이전트를 질의하는 데 사용됩니다. SNMP v3 보안 및 이 설정의 사용 방법에 익숙한 경우에만 이 필드를 사용하여 Engine ID를 설정합니다.
7. **Set Requests 옵션을 사용 또는 사용 안함으로 설정하려면 Set Requests 확인란을 선택하거나 선택 해제합니다.**
Set Requests 옵션이 사용 안함으로 설정된 경우 모든 SNMP 객체는 읽기 전용이며 snmpset 명령이 처리되지 않습니다.
8. **SNMP v1, v2c 또는 v3을 사용 안함으로 설정하려면 Protocols 확인란을 누릅니다.**

SNMP v3은 기본적으로 사용으로 설정됩니다. v1, v2c 및 v3 프로토콜 버전을 사용 또는 사용 안함으로 설정할 수 있습니다.

9. **Save**를 누릅니다.

SNMP Management 페이지의 아래쪽에서 SNMP 커뮤니티나 사용자를 추가, 편집 또는 삭제할 수도 있습니다.

SNMP 사용자 계정 및 커뮤니티 관리

- [“시작하기 전에 - SNMP 사용자 계정” \[31\]](#)
- [SNMP v1/v2c 커뮤니티 추가 또는 편집 \[31\]](#)
- [SNMP v1/v2c 커뮤니티 삭제 \[33\]](#)
- [SNMP v3 사용자 계정 추가 또는 편집 \[33\]](#)
- [SNMP v3 사용자 계정 삭제 \[35\]](#)

시작하기 전에 - SNMP 사용자 계정

이 절의 절차를 수행하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- Oracle ILOM에서 사용자 계정 등록 정보를 설정하려면 User Management(u) 역할이 사용으로 설정되어 있어야 합니다.
- ILOM에서 적절한 SNMP 설정이 사용으로 설정되어 있는지 확인합니다. 자세한 내용은 [SNMP 읽기/쓰기 액세스와 권한 부여 설정 \[29\]](#)을 참조하십시오.
- snmpset 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 SNMP v3 사용자 계정을 사용해야 합니다.

▼ SNMP v1/v2c 커뮤니티 추가 또는 편집

SNMP v1 또는 v2c 커뮤니티를 추가하거나 편집하려면 다음 단계를 수행하십시오.

1. Oracle ILOM 웹 인터페이스에 로그인합니다.
2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. 그런 다음 Management Access > SNMP를 누릅니다.
SNMP Management 페이지의 중간 아래로 스크롤하여 SNMP Communities 대화 상자를 찾습니다.
4. 커뮤니티를 편집하려면 다음을 수행합니다.
 - a. 적절한 커뮤니티 라디오 버튼을 누릅니다.

- b. **Edit**를 누릅니다.
Edit Community 대화 상자가 나타납니다.
 - c. 필요한 경우 커뮤니티 등록 정보를 업데이트합니다.
 - d. **Save**를 누릅니다.
5. 커뮤니티를 추가하려면 다음을 수행합니다.
- a. **Add**를 누릅니다.
Add Community 대화 상자가 나타납니다.

Add SNMP Community

Add SNMP Community names and their associated privileges here. Click Save to complete your action.

Community Name:

Permission:

Save **Close**

- b. 새 커뮤니티를 추가하려면 **Community Name** 필드에 커뮤니티 이름을 입력합니다. 그렇지 않으면 다음 단계로 이동합니다.
커뮤니티 이름은 35자 이내로 입력할 수 있습니다. 영문자로 시작해야 하며 공백을 포함할 수 없습니다.
- c. **Permissions** 드롭다운 목록에서 읽기 전용(ro) 또는 읽기-쓰기(rw)를 선택합니다.

d. Save를 누릅니다.

▼ SNMP v1/v2c 커뮤니티 삭제

SNMP v1 또는 v2c 커뮤니티를 삭제하려면 다음 단계를 수행하십시오.

1. Oracle ILOM 웹 인터페이스에 로그인합니다.
2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. 그런 다음 Management Access > SNMP를 누릅니다.
SNMP Management 페이지가 나타납니다.
4. Communities 링크를 누르거나 아래의 커뮤니티 목록으로 스크롤합니다.
5. 삭제할 SNMP 커뮤니티의 라디오 버튼을 누릅니다.
6. Delete를 누릅니다.
확인 대화 상자가 나타납니다.
7. OK를 눌러 SNMP 커뮤니티를 삭제합니다.

▼ SNMP v3 사용자 계정 추가 또는 편집

SNMP v3 사용자 계정을 추가하거나 편집하려면 다음 단계를 수행하십시오.

주 - 커뮤니티는 액세스를 제어하는 데 사용되므로 SNMP v1 및 v2c에는 사용자 계정이 적용되지 않습니다.

1. Oracle ILOM 웹 인터페이스에 로그인합니다.
2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. 그런 다음 Management Access > SNMP를 누릅니다.
SNMP Management 페이지가 나타납니다.
4. Users 링크를 눌러 SNMP Settings 페이지를 확장하고 SNMP Users를 표시합니다.
5. SNMP 사용자를 추가하려면 Add를 누릅니다.

Add User 대화 상자가 나타납니다.

6. SNMP 사용자를 편집하려면 다음을 수행합니다.

a. 적절한 사용자 라디오 버튼을 누릅니다.

b. Edit를 누릅니다.

Edit SNMP User Information 대화 상자가 나타납니다.

The screenshot shows a dialog box titled "Edit User: JohnDoe". Inside the dialog, there is a message: "Edit SNMP user information here. Click Save to confirm your changes." Below this message are several form fields:

- User Name: JohnDoe
- Authentication Protocol: MD5 (dropdown menu)
- Authentication Password: (text input field)
- Confirm Password: (text input field)
- Permission: Read-Only (dropdown menu)
- Privacy Protocol: none (dropdown menu)
- Privacy Password: (text input field)
- Confirm Password: (text input field)

At the bottom right of the dialog, there are two buttons: "Save" and "Close".

7. 사용자를 추가하려면 User Name 텍스트 필드에 사용자 이름을 입력하고, 그렇지 않으면 다음 단계로 이동합니다.

사용자 이름은 35자 이내로 입력할 수 있습니다. 영문자로 시작해야 하며 공백을 포함할 수 없습니다.

8. Authentication Protocol 드롭다운 목록에서 Message Digest 5 (MD5) 또는 Secure Hash Algorithm (SHA)을 선택합니다.

9. Authentication Password 텍스트 필드에 암호를 입력합니다.

인증 암호는 대/소문자를 구분하며 콜론이나 공백 문자 없이 8~16자 이내로 입력해야 합니다.

10. Confirm Password 텍스트 필드에 인증 암호를 다시 입력합니다.
11. Permissions 드롭다운 목록에서 읽기 전용(ro) 또는 읽기-쓰기(rw)를 선택합니다.
12. (선택사항) 프라이버시 프로토콜을 지정하려면 다음 단계를 수행합니다.
 - a. Privacy Protocol 목록 상자에서 DES (Digital Encryption Standard) 또는 AES (Advanced Encryption Standard)를 선택합니다.

주 - AES 프라이버시 프로토콜 옵션은 ILOM 3.0.16부터 SNMPv3에만 사용할 수 있습니다.

- b. Privacy Password 입력란에 12a 단계에서 지정한 프라이버시 알고리즘의 암호를 입력합니다.
 프라이버시 암호는 대/소문자를 구분하며 콜론이나 공백 문자 없이 8~16자 이내로 입력해야 합니다.

주 - 프라이버시 암호는 12a 단계에서 DES 또는 AES를 선택한 경우에만 필요합니다.

- c. Confirm Password 필드에 12b 단계에서 지정한 프라이버시 암호와 일치하는 프라이버시 암호를 다시 입력합니다.
13. Save를 눌러 SNMP 사용자 계정 등록 정보를 적용합니다.

▼ SNMP v3 사용자 계정 삭제

SNMP v3 사용자 계정을 삭제하려면 다음 단계를 수행하십시오.

1. Oracle ILOM 웹 인터페이스에 로그인합니다.
2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. 그런 다음 Management Access > SNMP를 누릅니다.
SNMP Management 페이지가 나타납니다.
4. Users 링크를 누르거나 아래의 SNMP Users 목록으로 스크롤합니다.
5. 삭제할 SNMP 사용자 계정의 라디오 버튼을 누릅니다.
6. SNMP User's List 아래에서 Delete를 누릅니다.
확인 대화 상자가 열립니다.
7. OK를 눌러 사용자 계정을 삭제합니다.

▼ SNMP 트랩 경고 관리

시작하기 전에

- Oracle ILOM에서 SNMP 트랩 경고 규칙을 만들거나 편집하려면 Admin(a) 역할이 사용으로 설정되어 있어야 합니다.
- SNMP v3 트랩 경고를 정의하려면 Oracle ILOM에서 SNMP 사용자 이름을 정의해야 합니다. Oracle ILOM에 SNMP v3 사용자 이름이 정의되지 않은 경우 SNMP 경고를 수신하는 SNMP v3 사용자가 SNMP v3 경고 메시지를 해독할 수 없게 됩니다. Oracle ILOM에서의 SNMP v3 권한 부여 및 SNMP v3 사용자 정의에 대한 자세한 내용은 [“SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리\(웹\)” \[28\]](#)를 참조하십시오.
- Oracle ILOM에서의 경보 관리 설정 구성에 대한 자세한 내용은 [“Configuring Alert Notifications” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)을 참조하십시오.

SNMP 트랩 경고 등록 정보를 구성하려면 다음 단계를 수행하십시오.

1. Oracle ILOM 웹 인터페이스에 로그인합니다.
2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. Notifications > Alerts를 누릅니다.

Alert Settings 페이지가 나타납니다. 이 페이지에는 구성할 수 있는 경고 테이블이 표시됩니다. 최대 15개 경고를 구성할 수 있습니다.

The screenshot shows the Oracle ILOM web interface. The top navigation bar includes 'About', 'Refresh', and 'Logout'. The left sidebar shows a navigation menu with 'Notifications' highlighted. The main content area is titled 'Notifications' and contains a sub-menu with 'Alerts', 'Syslog', and 'SMTP Client'. Below this, there is a text box explaining the alert configuration process. A table titled 'Alerts' is displayed with the following data:

Alert ID	Level	Alert Type	Destination Summary
1	minor	ipmipet	0.0.0.0
2	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
3	down	ipmipet	0.0.0.0
4	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
5	minor	email	user@example.com
6	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
7	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
8	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
9	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
10	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
11	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
12	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
13	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
14	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
15	disable	snmptrap	0.0.0.0, snmp v1, community 'public'

4. 경고를 만들거나 수정하려면 경고 라디오 버튼을 누릅니다.
5. 그런 다음 Edit를 누릅니다.
Create or Modify Alert 대화 상자가 나타납니다.

6. Level 드롭다운 목록에서 경고 레벨을 선택합니다.
7. Type 드롭다운 목록에서 경고 유형을 선택합니다.
8. IP Address 필드에서 경고 대상 IP 주소를 지정합니다.
9. Save를 눌러 변경사항을 적용합니다.

Oracle ILOM을 사용하여 SNMP MIB 다운로드

- “시작하기 전에 - SNMP MIB 다운로드” [38]

- [SNMP MIB 다운로드\(CLI\) \[38\]](#)
- [SNMP MIB 다운로드\(웹\) \[38\]](#)

시작하기 전에 - SNMP MIB 다운로드

- Oracle ILOM에서 SNMP MIB를 다운로드하려면 Reset and Host Control(r) 역할이 필요합니다.
- Oracle ILOM 3.0.4 이상을 사용해야 합니다.

▼ SNMP MIB 다운로드(CLI)

1. Oracle ILOM CLI에 로그인합니다.
2. `show` 명령을 입력하여 SNMP MIB를 표시합니다.
예를 들면 다음과 같습니다.

```
-> show /SP/services/snmp/mibs
```

```
/SP/services/snmp/mibs
Targets:

Properties:
  dump_uri = (Cannot show property)

Commands:
  cd
  dump
  set
  show
```

3. 파일을 다운로드하려면 다음 명령 중 하나를 입력합니다.
-> `dump -destination URI /SP/services/snmp/mibs`
또는
-> `set /SP/services/snmp/mibs dump_uri=URI`
여기서 `URI`는 파일이 다운로드되는 대상을 지정합니다.
MIB를 포함하는 zip 파일이 대상 서버로 전송됩니다.

▼ SNMP MIB 다운로드(웹)

1. Oracle ILOM 웹 인터페이스에 로그인합니다.

2. 왼쪽 탐색 패널에서 ILOM Administration을 누릅니다.
3. Management Access > SNMP를 누릅니다.
SNMP Management 페이지가 나타납니다.
4. MIB 점프 링크를 누르거나 아래의 MIB 섹션으로 스크롤합니다.
5. Download를 누른 다음 Save를 누르고 파일을 저장할 대상을 입력합니다.
MIB를 포함하는 zip 파일이 대상 서버로 전송됩니다.

SNMP를 사용하여 사용자 계정 관리

설명	링크
SNMP를 사용하여 사용자 계정을 관리하기 위한 액세스 요구 사항 검토	■ “시작하기 전에 - 사용자 계정(SNMP)” [41]
사용자 계정을 구성하는 방법	■ “Oracle ILOM 사용자 계정 구성(SNMP)” [42]
Active Directory 설정을 구성하는 방법	■ “Active Directory에 대해 Oracle ILOM 구성(SNMP)” [44]
DNS 이름 서버를 구성하는 방법	■ DNS 이름 서버 설정 관리(SNMP) [59]
LDAP 설정을 구성하는 방법	■ “LDAP에 대해 Oracle ILOM 구성(SNMP)” [60]
LDAP/SSL 설정을 구성하는 방법	■ “LDAP/SSL에 대해 Oracle ILOM 구성(SNMP)” [63]
RADIUS 설정을 구성하는 방법	■ “RADIUS에 대해 Oracle ILOM 구성(SNMP)” [71]

관련 정보

- [“SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리\(CLI\)” \[19\]](#)
- [“SNMP 읽기 및 쓰기 액세스, 사용자 계정 및 SNMP 트랩 경고 관리\(웹\)” \[28\]](#)
- [“Modifying Default Management Access Configuration Properties” in Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x](#)
- [“Setting Up and Maintaining User Accounts” in Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x](#)

시작하기 전에 - 사용자 계정(SNMP)

이 절의 절차를 수행하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- SNMP를 사용하려면 모든 SNMP 등록 정보를 올바르게 설정합니다. 자세한 내용은 [Oracle ILOM에서 SNMP 설정 구성](#)을 참조하십시오.
사용자 계정 정보를 보려면 Read Only(o) 역할이 사용으로 설정되어 있어야 합니다.
- 사용자 계정 정보를 구성하려면 User Management(u) 역할이 사용으로 설정되어 있어야 합니다.
- snmpset 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 SNMP v3 사용자 계정을 사용해야 합니다.

주 - SNMP 명령 예는 [SNMP 명령 예](#)를 참조하십시오.

주 - 이 단원에 나와 있는 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

Oracle ILOM 사용자 계정 구성(SNMP)

- [사용자 계정 구성 \[42\]](#)
- [Single Sign On 구성 \[43\]](#)

▼ 사용자 계정 구성

주 - get 및 set 명령을 사용하여 사용자 계정 MIB 객체 설정을 구성할 수 있습니다. 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

주 - 이 절차의 구문은 tcsh 셸에 유효합니다. 사용자의 셸 환경에서는 이스케이프 문자(\)가 필요하지 않을 수도 있습니다.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. Operator 사용자 역할의 새 사용자 계정을 만들려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLocalUserRowStatus.\"user1\" i 4  
ilomCtrlLocalUserRoles.\"user1\" s \"operator\"  
ilomCtrlLocalUserPassword.\"user1\" s \"password\"
```

3. 사용자 계정을 삭제하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLocalUserRowStatus.\"user1\" i 6
```

다음 표는 사용자 계정 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLocal UserUsername	로컬 사용자 이름으로, 영문자로 시작해야 합니다. 영문자, 숫자, 하이픈 및 밑줄을 포함할 수 있지만 공백은 포함할 수 없습니다. 사용자 이름은 암호와 같을 수 없습니다.	<i>username</i>	문자열	없음
ilomCtrlLocal UserPassword	로컬 사용자의 암호입니다.	<i>password</i>	문자열	없음
ilomCtrlLocal UserRoles	사용자와 연관된 역할을 지정합니다. 기존 역할(Administrator 또는 Operator) 또는 개별 역할 ID(a, u, c, r, o, s)로 역할을 지정할 수 있습니다. 역할 ID는 함께 결합할 수 있습니다. 예를 들어 aucros와 같이 사용할 수 있습니다. 여기서 a=admin, u=user, c=console, r=reset, o=read-only, s=service를 의미합니다.	administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s)	문자열	없음
ilomCtrlLocal UserRowStatus	이 객체는 테이블에서 새 행을 만들거나 기존 행을 삭제하는 데 사용됩니다. 이 등록 정보를 createAndWait(5) 또는 destroy(6)로 설정하여 각각 사용자를 만들고 제거할 수 있습니다.	active(1), notInService(2), notReady(3), createAndGo(4), createAndWait(5), destroy(6)	정수	없음

▼ Single Sign On 구성

Single Sign On은 Oracle ILOM에 대한 액세스 권한을 얻기 위해 암호를 입력해야 하는 횟수를 줄여 주는 편리한 인증 서비스입니다. Single Sign On은 기본적으로 사용으로 설정됩니다. 다른 인증 서비스와 마찬가지로 인증 자격 증명이 네트워크를 통해 전달됩니다. 이를 원치 않는 경우 Single Sign On 인증 서비스를 사용 안함으로 설정하는 것이 좋습니다.

주 - set 명령을 사용하여 Single Sign On MIB 객체 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

Password: *password*

2. Single Sign On을 사용으로 설정하려면 다음과 같이 입력합니다.

```
ilomCtrlSingleSignonEnabled.0 i 1
```

예를 들면 다음과 같습니다.

```
% snmpset SNMP_agent ilomCtrlSingleSignonEnabled.0 i 1
```

다음 표는 Single Sign On SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlSingleSignonEnabled	장치에서 SSO(Single Sign On) 인증을 사용으로 설정해야 하는지 여부를 지정합니다. SSO를 사용하면 토큰이 전달되므로 여러 응용 프로그램 간에 암호를 다시 입력할 필요가 없습니다. SC(시스템 제어기) 웹 인터페이스와 SP(서비스 프로세서) 웹 인터페이스, SC 명령줄 인터페이스와 SP 명령줄 인터페이스, SC 및 SP 인터페이스와 Java 원격 콘솔 응용 프로그램 간에 SSO를 사용할 수 있습니다.	true(1), false(2)	정수	없음

Active Directory에 대해 Oracle ILOM 구성(SNMP)

- [Active Directory 설정 관리 \[44\]](#)
- [Active Directory 관리자 그룹 관리 \[49\]](#)
- [Active Directory 운영자 그룹 관리 \[50\]](#)
- [Active Directory 사용자 정의 그룹 관리 \[51\]](#)
- [Active Directory 사용자 도메인 관리 \[52\]](#)
- [Active Directory 대체 서버 관리 \[53\]](#)
- [서버 중복성 관리 \[56\]](#)
- [Active Directory DNS 로케이터 관리 \[57\]](#)

▼ Active Directory 설정 관리

주 - get 및 set 명령을 사용하여 Active Directory 설정을 확인하고 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- Active Directory 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryEnabled.0
```

- Active Directory를 사용으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryEnabled.0 i 1
```

- Active Directory 포트 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryPortNumber.0
```

- Active Directory 포트 번호를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryPortNumber.0 i  
portnumber
```

- Active Directory 기본 사용자 역할을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.0
```

- Active Directory 기본 사용자 역할을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.0 s acro
```

- Active Directory 인증서 파일 URI를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertFileURI.0
```

- Active Directory 인증서 파일 URI를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryCertFileURI.0 s URI
```

- Active Directory 제한 시간을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryTimeout.0
```

- Active Directory 제한 시간을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryTimeout.0 i 6
```

- Active Directory 인증서 검증 모드를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryStrictCertEnabled.0
```

- Active Directory 인증서 검증 모드를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryStrictCertEnabled.0 i 1
```

- Active Directory 인증서 파일 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertFileStatus.0
```

- 이벤트 로그로 전송되는 메시지 개수에 대한 이벤트 로그 설정을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryLogDetail.0
```

- 우선 순위가 가장 높은 메시지만 이벤트 로그에 전송되도록 이벤트 로그 설정을 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryLogDetail.0 i 2
```

- Active Directory를 통해 인증된 경우 user1에 필요한 역할을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.'user1'
```

- Active Directory를 통해 인증된 경우 user1에 대해 Admin(a) 역할을 지정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.'user1' s
```

a

- 서버와 연관된 인증서 정보가 true로 설정된 경우 이러한 정보를 확인하고 지우려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertClear.0
% snmpset SNMP_agent ilomCtrlActiveDirectoryCertClear.0 i 0
```

- 인증서 파일의 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertVersion.0
```

- 인증서 파일의 일련 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertSerialNo.0
```

- 인증서 파일의 발행인을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertIssuer.0
```

- 인증서 파일의 주체를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertSubject.0
```

- 인증서 파일의 유효 기간 시작 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertValidBegin.0
```

- 인증서 파일의 유효 기간 종료 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertValidEnd.0
```

다음 표는 Active Directory 인증서 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActiveDirectoryEnabled	Active Directory 클라이언트를 사용으로 설정할지 여부를 지정합니다.	true(1), false(2)	정수	true

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActive DirectoryIP	사용자 계정의 이름 서비스로 사용되는 Active Directory 서버의 IP 주소입니다.	<i>ipaddress</i>	문자열	없음
ilomCtrlActive Directory PortNumber	Active Directory 클라이언트의 포트 번호를 지정합니다. 포트를 0으로 지정하면 포트가 자동으로 선택되고 1부터 65535까지로 지정하면 실제 포트가 구성됩니다.	<i>portnumber</i> (범위: 0~65535)	정수	없음
ilomCtrl Active Directory DefaultRoles	Active Directory를 통해 인증된 사용자에게 필요한 역할을 지정합니다. 이 등록 정보를 기존 역할 (Administrator 또는 Operator) 또는 개별 역할 ID(a, u, c, r, o, s)로 지정하면 Active Directory 서버에 저장된 스키마가 Active Directory 클라이언트에서 무시됩니다. 또한 이 등록 정보를 none으로 설정하면 값이 지워지고 고유 Active Directory 스키마가 사용되어야 함을 나타냅니다. 역할 ID는 함께 결합할 수 있습니다. 예를 들어 aucros와 같이 사용할 수 있습니다. 여기서 a=admin, u=user, c=console, r=reset, o=read-only, s=service를 의미합니다.	administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s), none	문자열	없음
ilomCtrlActive Directory CertFileURI	Strict Certificate Mode가 사용으로 설정된 경우에 필요한 인증서 파일의 URI입니다. URI를 설정하면 인증서 인증에 해당 인증서를 즉시 사용할 수 있도록 파일이 전송됩니다.	<i>URI</i>	문자열	없음
ilomCtrlActive Directory Timeout	Active Directory 서버가 응답하지 않는 경우 시간이 초과되기 전에 대기할 시간(초)을 지정합니다.	범위: 1~20초	정수	4
ilomCtrlActive Directory StrictCert Enabled	Active Directory 클라이언트에 대해 Strict Certificate Mode를 사용으로 설정할지 여부를 지정합니다. 사용으로 설정한 경우 Active Directory 서버와 통신할 때 인증서 검증을 수행할 수 있도록 Active Directory 인증서를 SP에 업로드해야 합니다.	true(1), false(2)	정수	true
ilomCtrlActive DirectoryCert FileStatus	인증서 파일의 상태를 나타내는 문자열입니다. 인증서 파일이 있는지 여부를 확인하는 데 유용합니다.	<i>status</i>	문자열	없음

▼ Active Directory 관리자 그룹 관리

주 - Net-SNMP 샘플 응용 프로그램을 사용하는 경우 `snmpget` 및 `snmpset` 명령을 사용하여 Active Directory 관리자 그룹 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. Active Directory 관리자 그룹 ID 번호 2의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAdminGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=north,DC=oracle,DC=com
```

3. Active Directory 관리자 그룹 ID 번호 2의 이름을 `CN=spAdmins,DC=spc,DC=south,DC=oracle,DC=com`으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlActiveDirAdminGroupName.2 s CN=spAdmins,DC=spc,DC=
south,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=south,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlActiveDirAdminGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=south,DC=oracle,DC=com
```

다음 표는 Active Directory 관리자 그룹 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActiveDirAdminGroupId	Active Directory 관리자 그룹 항목의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlActiveDirAdminGroupName	이 문자열은 Active Directory 서버에 있는 그룹 이름 중 하나와 정확히 일치하는 고유 이름을 포함해야 합니다. 이 표에 있는 이러한 그룹 중 하나에 속한 사용자에게는 Administrator라는 Oracle ILOM 역할이 지정됩니다.	name (최대 255자)	문자열	없음

▼ Active Directory 운영자 그룹 관리

주 - get 및 set 명령을 사용하여 Active Directory 운영자 그룹 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. Active Directory 운영자 그룹 ID 번호 2의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
iLOMCtrlActiveDirOperatorGroupName.2
SUN-ILOM-CONTROL-MIB::iLOMCtrlActiveDirOperatorGroupName.2 =
STRING: ad-oper-group-ent-2
```

3. Active Directory 운영자 그룹 ID 번호 2의 이름을 new-name-2로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
iLOMCtrlActiveDirOperatorGroupName.2 s new-name-2
SUN-ILOM-CONTROL-MIB::iLOMCtrlActiveDirOperatorGroupName.2 =
STRING: new-name-2
% snmpget SNMP_agent
iLOMCtrlActiveDirOperatorGroupName.2
SUN-ILOM-CONTROL-MIB::iLOMCtrlActiveDirOperatorGroupName.2 =
STRING: new-name-2
```

다음 표는 Active Directory 운영자 그룹 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
iLOMCtrlActiveDirOperatorGroupName	Active Directory 운영자 그룹 항목의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
iLOMCtrlActiveDirOperatorGroupName	이 문자열은 Active Directory 서버에 있는 그룹 이름 중 하나와 정확히 일치하는 고유 이름을 포함해야 합니다. 이 표에 있는 이러한 그룹 중 하나에 속한 사용자에게는 Operator라는 Oracle ILOM 역할이 지정됩니다.	name (최대 255자)	문자열	없음

▼ Active Directory 사용자 정의 그룹 관리

주 - get 및 set 명령을 사용하여 Active Directory 사용자 정의 그룹 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. Active Directory 사용자 정의 그룹 ID 번호 2의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
iIomCtrlActiveDirCustomGroupName.2
SUN-ILOM-CONTROL-MIB::iIomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=johns,DC=oracle,DC=com
```

3. Active Directory 사용자 정의 그룹 ID 번호 2의 이름을 CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
iIomCtrlActiveDirCustomGroupName.2 s CN=SpSuperCust,OU=Groups,DC=
bills,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::iIomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com
% snmpget SNMP_agent
iIomCtrlActiveDirCustomGroupName.2
SUN-ILOM-CONTROL-MIB::iIomCtrlActiveDirCustomGroupName.2 = m
STRING: CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=co
```

4. Active Directory 사용자 정의 그룹 ID 번호 2의 역할을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
iIomCtrlActiveDirCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::iIomCtrlActiveDirCustomGroupRoles.2 =
STRING: "aucro"
```

5. Active Directory 사용자 정의 그룹 ID 번호 2의 역할을 User Management 및 Read Only(u, o)로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
iIomCtrlActiveDirCustomGroupRoles.2 s "uo"
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "uo"
% snmpget SNMP_agent
ilomCtrlActiveDirCustomGroupRole.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "uo"
```

다음 표는 Active Directory 사용자 정의 그룹 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActiveDirCustomGroup	Active Directory 사용자 정의 그룹 항목의 정수 식별자입니다.	1~5	정수	없음
Id		이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.		
ilomCtrlActiveDirCustomGroup	이 문자열은 Active Directory 서버에 있는 그룹 이름 중 하나와 정확히 일치하는 고유 이름을 포함해야 합니다. 이 테이블에 있는 이러한 그룹 중 하나에 속한 사용자에게는 항목의 역할 구성에 따라 Oracle ILOM 역할이 지정됩니다.	<i>name</i> (최대 255자)	문자열	없음
Name				
ilomCtrlActiveDirCustomGroupRoles	Active Directory를 통해 인증된 사용자에게 필요한 역할을 지정합니다. 이 등록 정보를 기존 역할 (Administrator 또는 Operator) 또는 개별 역할 ID(a, u, c, r, o, s)로 지정하면 Active Directory 서버에 저장된 스키마가 Active Directory 클라이언트에서 무시됩니다. 또한 이 객체를 none으로 설정하면 값이 지워지고 고유 Active Directory 스키마가 사용되어야 함을 나타냅니다. 역할 ID는 함께 결합할 수 있습니다. 예를 들어 aucros와 같이 사용할 수 있습니다. 여기서 a=admin, u=user, c=console, r=reset, o=read-only, s=service를 의미합니다.	administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s), none	문자열	없음

▼ Active Directory 사용자 도메인 관리

주 - get 및 set 명령을 사용하여 Active Directory 사용자 도메인 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

Password: *password*

2. Active Directory 사용자 도메인 ID 번호 2의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
  ilomCtrlActiveDirUserDomain.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@davidc.example.oracle.com
```

3. Active Directory 사용자 도메인 ID 번호 2의 이름을 <USERNAME>@johns.example.oracle.com으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
  ilomCtrlActiveDirUserDomain.2 s
  "<USERNAME>@johns.example.oracle.com"
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@johns.example.oracle.com
% snmpget SNMP_agent
  ilomCtrlActiveDirUserDomain.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@johns.example.oracle.com
```

다음 표는 Active Directory 사용자 도메인 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActiveDirUserDomain	Active Directory 도메인의 정수 식별자입니다.	1~5	정수	없음
Id		이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.		
ilomCtrlActiveDirUserDomain	이 문자열은 Active Directory 서버의 인증 도메인과 정확히 일치해야 합니다. 이 문자열에는 인증 중에 사용자의 로그인 이름으로 바뀌는 대체 문자열(<USERNAME>)이 포함되어 있어야 합니다. 기본 또는 고유 이름 형식이 허용됩니다.	name (최대 255자)	문자열	없음

▼ Active Directory 대체 서버 관리

주 - get 및 set 명령으로 MIB 객체 등록 정보 값을 설정하여 Active Directory 대체 서버 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- Active Directory 대체 서버 ID 번호 2의 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
  ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
IpAddress: 10.7.143.236
```

- Active Directory 대체 서버 ID 번호 2의 IP 주소를 10.7.143.246으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
  ilomCtrlActiveDirAlternateServerIp.2 a 10.7.143.246
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
IpAddress: 10.7.143.246
% snmpget SNMP_agent
  ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
IpAddress: 10.7.143.246
```

- Active Directory 대체 서버 ID 번호 2의 포트 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
  ilomCtrlActiveDirAlternateServerPort.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 636
```

- Active Directory 대체 서버 ID 번호 2의 포트 번호를 639로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
  ilomCtrlActiveDirAlternateServerPort.2 i 639
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 639
% snmpget SNMP_agent
  ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 639
```

- Active Directory 대체 서버 ID 번호 2의 인증서 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertStatus.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerCertStatus.
2 = STRING: certificate not present
```

- Active Directory 대체 서버 ID 번호 2의 인증서 URI를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertURI.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerCertURI.2 =
STRING: none
```

- 서버와 연관된 인증서 정보가 true로 설정된 경우 이러한 정보를 지우려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlActiveDirAlternateServerCertClear.0 i 1
```

- 대체 서버 인증서 파일의 인증서 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertVersion.0
```

- 대체 서버 인증서 파일의 일련 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertSerialNo.0
```

- 대체 서버 인증서 파일의 발행인을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertIssuer.0
```

- 대체 서버 인증서 파일의 주체를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertSubject.0
```

- 대체 서버 인증서 파일의 유효 기간 시작 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertValidBegin.0
```

- 대체 서버 인증서 파일의 유효 기간 종료 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertValidEnd.0
```

다음 표는 Active Directory 대체 서버 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActiveDirAlternateServerId	Active Directory 대체 서버 테이블의 정수 식별자입니다.	1~5 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlActiveDirAlternateServerIP	사용자 계정의 이름 서비스로 사용되는 Active Directory 대체 서버의 IP 주소입니다.	ipaddress	문자열	없음
ilomCtrlActiveDirAlternateServerPort	Active Directory 대체 서버의 포트 번호를 지정합니다. 포트를 0으로 지정하면 잘 알려진 포트 번호가 자동으로 선택됩니다. 1 - 65535를 명시적으로 지정하면 포트 번호가 설정됩니다.	portnumber(범위: 0~65535)	정수	없음
ilomCtrlActiveDirAlternateServerCertStatus	인증서 파일의 상태를 나타내는 문자열입니다. 인증서 파일이 있는지 여부를 확인하는 데 유용합니다.	status(최대 크기: 255자)	문자열	없음
ilomCtrlActiveDirAlternateServerCertURI	Strict Certificate Mode가 사용으로 설정된 경우에 필요한 인증서 파일의 URI입니다. URI를 설정하면 인증서 인증에 해당 인증서를 즉시 사용할 수 있도록 파일이 전송됩니다. 또한 직접 인증서 조작에 remove 또는 restore가 지원됩니다.	URI	문자열	없음

▼ 서버 중복성 관리

주 - get 및 set 명령을 사용하여 중복성 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 중복 구성된 서버의 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRedundancyStatus.0
```

- 서버를 활성 또는 대기 상태에서 승격할지 또는 강등할지 여부를 제어하는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRedundancyAction.0
```

- 중복 서버를 대기 상태에서 활성 상태로 승격하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRedundancyAction.0 i 2
```

- 현재 에이전트가 실행 중인 CMM(새시 모니터링 모듈)의 FRU 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRedundancyFRUName.0
```

▼ Active Directory DNS 로케이터 관리

주 - get 및 set 명령을 사용하여 Active Directory DNS 로케이터 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. Active Directory DNS 로케이터의 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorEnabled.0
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.0 =
INTEGER: false(2)
```

3. Active Directory DNS 로케이터 ID 번호 2의 상태를 **enabled**로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlActiveDirDnsLocatorEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.0 =
INTEGER: true(1)
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorEnabled.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.2 =
INTEGER: true(1)
```

4. Active Directory DNS 로케이터 ID 번호 2의 서비스 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorQueryService.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>
```

5. Active Directory DNS 로케이터 ID 번호 2의 서비스 이름 및 포트 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlActiveDirDnsLocatorQueryService.2 s
"_ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>"
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorQueryService.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>
```

다음 표는 Active Directory DNS 로케이터 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActiveDirDnsLocatorEnabled	Active Directory DNS 로케이터 기능을 사용으로 설정할지 여부를 지정합니다.	true(1), false(2)	정수	false
ilomCtrlActiveDirDnsLocatorQueryService.QueryId	Active Directory DNS 로케이터 질의 항목의 정수 식별자입니다.	1~5 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlActive DirDnsLocator QueryService	DNS 질의를 수행하는 데 사용되는 서비스 이름입니다. 이름에는 인증 시 사용자와 관련된 도메인 정보로 바뀌는 <DOMAIN>이 대체 표시자로 포함될 수 있습니다. 또한 서비스 이름에는 필요한 경우 인식된 포트 정보를 대체하는 데 사용될 수 있는 <PORT:>가 포함될 수 있습니다. 예를 들어 표준 LDAP/SSL 포트 636에 대해 <PORT:636>을 지정할 수 있습니다.	<i>name</i> (최대 255자)	문자열	없음

▼ DNS 이름 서버 설정 관리(SNMP)

주 - get 및 set 명령을 사용하여 DNS 이름 서버 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- DNS의 이름 서버를 확인하고 지정하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlDNSNameServers.0
% snmpset SNMP_agent
ilomCtrlDNSNameServers.0 s '???nameservername'
```

- DNS의 검색 경로를 확인하고 지정하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlDNSSearchPath.0
% snmpset SNMP_agent
ilomCtrlDNSSearchPath.0 s '???searchpath'
```

- DNS의 DHCP autodns 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlDNSdhcpAutoDns.0
```

- DNS의 DHCP autodns 상태를 enabled 상태로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlDNSdhcpAutoDns.0 i 1
```

- 서버가 응답하지 않는 경우 시간 초과되기 전에 대기할 시간(초)을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlDNSTimeout.0
```

- 서버가 응답하지 않는 경우 시간 초과되기 전에 대기할 시간(초)을 5로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlDNSTimeout.0 i 5
```

- 시간 초과 후 요청을 다시 시도할 횟수를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlDNSRetries.0
```

- 시간 초과 후 요청을 다시 시도할 횟수를 5로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlDNSRetries.0 i 5
```

LDAP에 대해 Oracle ILOM 구성(SNMP)

- [LDAP 설정 구성 \[60\]](#)

▼ LDAP 설정 구성

주 - get 및 set 명령을 사용하여 LDAP에 대해 Oracle ILOM을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- LDAP 사용자를 인증하도록 LDAP 서버가 사용으로 설정되어 있는지 여부를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapEnabled.0
```

- LDAP 사용자를 인증하도록 LDAP 서버 상태를 enabled 상태로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapEnabled.0 i 1
```

- LDAP 서버 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapServerIP.0
```

- LDAP 서버 IP 주소를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapServerIP.0 a ipaddress
```

- LDAP 서버 포트 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapPortNumber.0
```

- LDAP 서버 포트 번호를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapPortNumber.0 i 389
```

- LDAP 서버 고유 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapBindDn.0
```

- LDAP 서버 고유 이름을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent  
ilomCtrlLdapBindDn.0 s ou=people,ou=sales,dc=oracle,dc=com
```

- LDAP 서버 암호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapBindPassword.0
```

- LDAP 서버 암호를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapBindPassword.0 s password
```

- 사용자 검색이 완료된 LDAP 서버의 분기를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSearchBase.0
```

- 사용자를 검색할 LDAP 서버의 분기를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapSearchBase.0 s ldap_server_branch
```

- LDAP 서버 기본 역할을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapDefaultRoles.0
```

- LDAP 서버 기본 역할을 Administrator로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapDefaultRoles.0 s administrator
```

다음 표는 LDAP 설정 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdap Enabled	LDAP 클라이언트를 사용으로 설정할지 여부를 지정합니다.	true(1), false(2)	정수	false
ilomCtrlLdap ServerIP	사용자 계정의 이름 서비스로 사용되는 LDAP 서버의 IP 주소입니다.	ipaddress	문자열	없음
ilomCtrlLdap PortNumber	LDAP 클라이언트의 포트 번호를 지정합니다.	portnumber(범위: 0~65535)	정수	389
ilomCtrlLdap BindDn	LDAP 서버에 바인딩하는 데 사용되는 읽기 전용 프록시의 DN(고유 이름)입니다. 예를 들어 "cn=proxyuser, ou=people, dc=oracle, dc=com"으로 설정할 수 있습니다.	distinguished_name	문자열	없음
ilomCtrlLdap BindPassword	LDAP 서버를 바인딩하는 데 사용되는 읽기 전용 프록시 사용자의 암호입니다. 이 등록 정보는 기본적으로 쓰기 전용입니다. 쓰기 전용 액세스 레벨은 SNMP v2부터 더 이상 지원되지 않습니다. 이 등록 정보는 읽을 때 null 값을 반환해야 합니다.	password	문자열	없음
ilomCtrlLdap SearchBase	LDAP 데이터베이스에서 사용자를 찾을 검색 기준입니다. 예를 들어 "ou=people, dc=oracle, dc=com"으로 설정할 수 있습니다.	사용자를 검색할 LDAP 서버의 분기입니다.	문자열	없음
ilomCtrlLdap DefaultRoles	LDAP를 통해 인증된 사용자에게 필요한 역할을 지정합니다. 이 등록 정보는 기존 역할(Administrator 또는 Operator) 또는 개별 역할 ID(a, u, c, r, o, s)의 조합을 지원합니다. 예를 들어 aucros와 같이 사용할 수 있습니다. 여기서 a=admin, u=user, c=console, r=reset, o=read-only, s=service를 의미합니다.	administrator, operator, admin(a), user(u),	문자열	없음

MIB 객체	설명	허용되는 값	유형	기본값
		console(c), reset(r), read-only(o), service(s)		

LDAP/SSL에 대해 Oracle ILOM 구성(SNMP)

- LDAP/SSL 인증서 관리 [63]
- LDAP/SSL 관리자 그룹 관리 [64]
- LDAP/SSL 운영자 그룹 관리 [65]
- LDAP/SSL 사용자 정의 그룹 관리 [66]
- LDAP/SSL 사용자 도메인 관리 [68]
- LDAP/SSL 대체 서버 관리 [69]

▼ LDAP/SSL 인증서 관리

주 - get 및 set 명령을 사용하여 LDAP/SSL 인증서 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 서버와 연관된 인증서 정보가 true로 설정된 경우 이러한 정보를 지우려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlLdapSslCertFileClear.0 i 0
```

- 인증서 파일의 인증서 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslCertFileVersion.0
```

- 인증서 파일의 일련 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslCertFileSerialNo.0
```

- 인증서 파일의 발행인을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslCertFileIssuer.0
```

- 인증서 파일의 주체를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslCertFileSubject.0
```

- 인증서 파일의 유효 기간 시작 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslCertFileValidBegin.0
```

- 인증서 파일의 유효 기간 종료 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslCertFileValidEnd.0
```

▼ LDAP/SSL 관리자 그룹 관리

주 - get 및 set 명령을 사용하여 LDAP/SSL 관리자 그룹 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- LDAP/SSL 관리자 그룹 ID 번호 3의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslAdminGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=oracle,DC=com
```

- LDAP/SSL 관리자 그룹 ID 번호 3의 이름을 CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlLdapSslAdminGroupName.3 s CN=SpSuperAdmin,OU=Groups,DC=
tomp,DC=example,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlLdapSslAdminGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
```

다음 표는 LDAP/SSL 관리자 그룹 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdapSslAdminGroupName	LDAP/SSL AdminGroup 항목의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlLdapSslAdminGroupName	이 문자열은 LDAP/SSL 서버에 있는 그룹 이름 중 하나와 정확히 일치하는 고유 이름을 포함해야 합니다. 이 표에 있는 이러한 그룹 중 하나에 속한 사용자에게는 Administrator라는 ILOM 역할이 지정됩니다.	name (최대 255자)	문자열	없음

▼ LDAP/SSL 운영자 그룹 관리

주 - get 및 set 명령을 사용하여 LDAP/SSL 운영자 그룹 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- LDAP/SSL 운영자 그룹 ID 번호 3의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslOperatorGroupName.3SUN-ILOM-CONTROL-MIB::ilomCtrlL
```

```
dapSslOperatorGroupName.3 = STRING: CN=SpSuperOper,OU=Groups,DC=
davidc,DC=example,DC=oracle,DC=com
```

- Active Directory 운영자 그룹 ID 번호 3의 이름을 CN=SpSuperAdmin,OU=Groups, DC=tomp,DC=example,DC=oracle,DC=com으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlLdapSslOperatorGroupName.3 s CN=SpSuperOper,OU=Groups,DC=
tomp,DC=example,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
STRING: CN=SpSuperOper,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlLdapSslOperatorGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
STRING: CN=SpSuperOper,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
```

다음 표는 LDAP/SSL 운영자 그룹 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdapSslOperatorGroupId	LDAP/SSL 운영자 그룹 항목의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlLdapSslOperatorGroup Name	이 문자열은 LDAP/SSL 서버에 있는 그룹 이름 중 하나와 정확히 일치하는 고유 이름을 포함해야 합니다. 이 표에 있는 이러한 그룹 중 하나에 속한 사용자에게는 Operator라는 ILOM 역할이 지정됩니다.	name (최대 255자)	문자열	없음

▼ LDAP/SSL 사용자 정의 그룹 관리

주 - get 및 set 명령을 사용하여 LDAP/SSL 사용자 정의 그룹 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- LDAP/SSL 사용자 정의 그룹 ID 번호 2의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=johns,DC=oracle,DC=com
```

- LDAP/SSL 사용자 정의 그룹 ID 번호 2의 이름을 CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlLdapSslCustomGroupName.2 s CN=SpSuperCust,OU=Groups,DC=
bills,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com
```

- LDAP/SSL 사용자 정의 그룹 ID 번호 2의 역할을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"aucro"
```

- LDAP/SSL 사용자 정의 그룹 ID 번호 2의 역할을 User Management 및 Read Only(u,o)로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlLdapSslCustomGroupRoles.2 s "uo"
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"uo"
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"uo"
```

다음 표는 LDAP/SSL 사용자 정의 그룹 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdapSslCustomGroupId	LDAP/SSL 사용자 정의 그룹 항목의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlLdapSslCustomGroupName	이 문자열은 LDAP/SSL 서버에 있는 그룹 이름 중 하나와 정확히 일치하는 고유 이름을 포함해야 합니다. 이 테이블에 있	name (최대 255자)	문자열	없음

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdap SslCustomGroup Roles	<p>는 이러한 그룹 중 하나에 속한 사용자에게는 항목의 역할 구성에 따라 ILOM 역할이 지정됩니다.</p> <p>LDAP/SSL을 통해 인증된 사용자에게 필요한 역할을 지정합니다. 이 등록 정보를 기존 역할(Administrator 또는 Operator) 또는 개별 역할 ID(a, u, c, r, o, s)로 지정하면 LDAP/SSL 서버에 저장된 스키마가 LDAP/SSL 클라이언트에 서 무시됩니다. 또한 이 객체를 none으로 설정하면 값이 지워지고 고유 LDAP/SSL 스키마가 사용되어야 함을 나타냅니다. 역할 ID는 함께 결합할 수 있습니다. 예를 들어 aucros와 같이 사용할 수 있습니다. 여기서 a=admin, u=user, c=console, r=reset, o=read-only, s=service를 의미합니다.</p>	<p>administrator,</p> <p>operator,</p> <p>admin(a),</p> <p>user(u),</p> <p>console(c),</p> <p>reset(r),</p> <p>read-only(o),</p> <p>service(s),</p> <p>none</p>	문자열	없음

▼ LDAP/SSL 사용자 도메인 관리

주 - get 및 set 명령을 사용하여 LDAP/SSL 사용자 도메인 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- LDAP/SSL 사용자 도메인 ID 번호 3의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslUserDomain.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=davidc,DC=example,DC=oracle,DC=com
```

- LDAP/SSL 사용자 도메인 ID 번호 3의 이름을 CN=<USERNAME>, CN=Users,DC=tomp, DC=example,DC=oracle,DC=com으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlLdapSslUserDomain.3 s CN=<USERNAME>,CN=Users,DC=tomp,DC=
example,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
```

```
<USERNAME>,CN=Users,DC=tomp,DC=example,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlLdapSslUserDomain.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=tomp,DC=example,DC=oracle,DC=com
```

다음 표는 LDAP/SSL 사용자 도메인 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdapSslUserDomainId	LDAP/SSL 도메인의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlLdapSslUserDomain	이 문자열은 LDAP/SSL 서버의 인증 도메인과 정확히 일치해야 합니다. 이 문자열에는 인증 중에 사용자의 로그인 이름으로 바뀌는 대체 문자열(<USERNAME>) 이 포함되어 있어야 합니다. 기본 또는 고유 이름 형식이 허용됩니다.	name (최대 255자)	문자열	없음

▼ LDAP/SSL 대체 서버 관리

주 - get 및 set 명령을 사용하여 LDAP/SSL 대체 서버 설정을 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- LDAP/SSL 대체 서버 ID 번호 3의 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerIp.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.236
```

- LDAP/SSL 대체 서버 ID 번호 3의 IP 주소를 10.7.143.246으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
ilomCtrlLdapSslAlternateServerIp.3 a 10.7.143.246
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.246
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerIp.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.246
```

- 대체 서버와 연관된 인증서 정보가 true로 설정된 경우 이러한 정보를 확인하고 지우려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerCertClear.0
% snmpset SNMP_agent
ilomCtrlLdapSslAlternateServerCertClear.0 i 0
```

- 인증서 파일의 대체 서버 인증서 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertVersion.0
```

- 대체 서버 인증서 파일의 일련 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertSerialNo.0
```

- 대체 서버 인증서 파일의 발행인을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertIssuer.0
```

- 대체 서버 인증서 파일의 주체를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertSubject.0
```

- 대체 서버 인증서 파일의 유효 기간 시작 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerCertValidBegin.0
```

- 대체 서버 인증서 파일의 유효 기간 종료 날짜를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertValidEnd.0
```

다음 표는 LDAP/SSL 대체 서버 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlLdapSslAlternateServerId	LDAP/SSL 대체 서버 테이블의 정수 식별자입니다.	1~5 주 - 이 객체는 읽기 또는 쓰기 액세스가 허용되지 않습니다.	정수	없음
ilomCtrlLdapSslAlternateServerIP	사용자 계정의 디렉토리 서버로 사용되는 LDAP/SSL 대체 서버의 IP 주소입니다.	<i>ipaddress</i>	문자열	없음
ilomCtrlLdapSslAlternateServerPort	LDAP/SSL 대체 서버의 포트 번호를 지정합니다. 포트를 0으로 지정하면 잘 알려진 포트 번호가 자동으로 선택됩니다. 1-65535를 명시적으로 지정하면 포트 번호가 설정됩니다.	<i>portnumber</i> (범위: 0~65535)	정수	없음
ilomCtrlLdapSslAlternateServerCert	인증서 파일의 상태를 나타내는 문자열입니다. 인증서 파일이 있는지 여부를 확인하는 데 유용합니다.	<i>status</i> (최대 크기: 255 자)	문자열	없음
Status				
ilomCtrlLdapSslAlternateServerCertURI	Strict Certificate Mode가 사용으로 설정된 경우에 필요한 인증서 파일의 URI입니다. URI를 설정하면 인증서 인증에 해당 인증서를 즉시 사용할 수 있도록 파일이 전송됩니다. 또한 직접 인증서 조작에 <i>remove</i> 또는 <i>restore</i> 가 지원됩니다.	<i>URI</i>	문자열	없음

RADIUS에 대해 Oracle ILOM 구성(SNMP)

■ RADIUS 설정 구성 [71]

▼ RADIUS 설정 구성

주 - 이 절차를 완료하기 전에 RADIUS 환경에 대한 적절한 정보를 수집하십시오. *get* 및 *set* 명령을 사용하여 RADIUS를 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- RADIUS 사용자를 인증하도록 RADIUS 서버가 사용으로 설정되어 있는지 여부를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRadiusEnabled.0
```

- RADIUS 사용자를 인증하도록 RADIUS 서버 상태를 enabled 상태로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRadiusEnabled.0 i 1
```

- RADIUS 서버 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRadiusServerIP.0
```

- RADIUS 서버 IP 주소를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRadiusServerIP.0 a ipaddress
```

- RADIUS 서버 포트 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRadiusPortNumber.0
```

- RADIUS 서버 포트 번호를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRadiusPortNumber.0 i portnumber
```

- RADIUS 서버 공유 암호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRadiusSecret.0
```

- RADIUS 서버 공유 암호를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRadiusSecret.0 s secret
```

- RADIUS 서버 기본 사용자 역할을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRadiusDefaultRoles.0
```

- RADIUS 서버 기본 사용자 역할을 Console로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRadiusDefaultRoles.0 s c
```

다음 표는 RADIUS SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlRadiusEnabled	RADIUS 클라이언트를 사용으로 설정할지 여부를 지정합니다.	true(1), false(2)	정수	false
ilomCtrlRadiusServerIP	사용자 계정의 이름 서비스로 사용되는 RADIUS 서버의 IP 주소입니다.	ipaddress	문자열	없음
ilomCtrlRadiusPortNumber	RADIUS 클라이언트의 포트 번호를 지정합니다.	portnumber(범위: 0~65535)	정수	1812
ilomCtrlRadiusSecret	RADIUS 클라이언트와 서버 간의 트래픽을 암호화하는 데 사용되는 공유 암호 암호화 키입니다.	secret(최대 길이: 255자)	문자열	없음
ilomCtrlRadiusDefaultRoles	RADIUS를 통해 인증된 사용자에게 필요한 역할을 지정합니다. 이 등록 정보는 기존 역할(Administrator 또는 Operator) 또는 개별 역할 ID(a, u, c, r, o, s)의 조합을 지원합니다. 예를 들어 aucros와 같이 사용할 수 있습니다. 여기서 a=admin, u=user, c=console, r=reset, o=read-only, s=service를 의미합니다.	administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s)	문자열	없음

구성 요소 정보 및 전자 메일 경고 관리(SNMP)

설명	링크
SNMP를 사용하여 구성 요소 정보 및 전자 메일 경고를 관리하기 위한 Oracle ILOM 요구 사항 검토	■ “시작하기 전에 - 구성 요소 정보(SNMP)” [75]
구성 요소 정보를 확인하는 방법	■ “구성 요소 정보 보기(SNMP)” [76]
시계 설정, syslog 및 경고 규칙을 관리하는 방법	■ “시계 설정, 이벤트 로그, Syslog 수신기 및 경고 규칙 관리(SNMP)” [77]
전자 메일 알림 경고에 사용할 SMTP 클라이언트를 구성하는 방법	■ “전자 메일 경고 통지를 위한 SMTP 클라이언트 구성(SNMP)” [81]
경고를 구성하는 방법	■ “전자 메일 경고 설정 구성(SNMP)” [83]

관련 정보

- [“Configuring Alert Notifications, Service Requests, or Remote Logging” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)

시작하기 전에 - 구성 요소 정보(SNMP)

- SNMP를 사용하여 Oracle ILOM 설정을 확인하고 구성하려면 먼저 SNMP를 구성해야 합니다. 자세한 내용은 [Oracle ILOM에서 SNMP 설정 구성](#)을 참조하십시오.
- snmpset 명령을 실행하려면 v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 v3 사용자 계정을 사용해야 합니다.

주 - SNMP 명령 예는 [SNMP 명령 예](#)를 참조하십시오.

주 - 이 단원에 나와 있는 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

구성 요소 정보 보기(SNMP)

■ 구성 요소 정보 보기 [76]

▼ 구성 요소 정보 보기

주 - get 명령을 사용하여 구성 요소 정보를 확인할 수 있습니다. 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ip_address
```

```
Password: password
```

2. 펌웨어 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent entPhysicalFirmwareRev.1
```

다음 표는 구성 요소 정보 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	값	유형	기본값
entPhysical Name	물리적 엔티티의 텍스트 이름입니다.	크기: 0 - 255	문자열	길이가 0인 문자열
entPhysical Descr	물리적 엔티티에 대한 텍스트 설명입니다.	크기: 0 - 255	문자열	없음
entPhysical ContainedIn	이 물리적 엔티티를 포함하는 물리적 엔티티의 entPhysicalIndex 값입니다. 0 값은 물리적 엔티티가 다른 물리적 엔티티에 포함되지 않음을 나타냅니다.	범위: 0 - 2147483647	정수	없음
entPhysical Class	물리적 엔티티의 일반 하드웨어 유형을 나타냅니다.	other(1), unknown(2), chassis(3), backplane(4), container(5), powerSupply(6), fan(7), sensor(8),	정수	없음

MIB 객체	설명	값	유형	기본값
		module(9), port(10), stack(11)		
entPhysical FirmwareRev	물리적 엔티티에 대한 공급업체별 펌웨어 개정 문자열입니다.	크기: 0 - 255	문자열	길이가 0인 문 자열

시계 설정, 이벤트 로그, Syslog 수신기 및 경고 규칙 관리(SNMP)

- [시계 설정 보기 및 설정 \[77\]](#)
- [Oracle ILOM 이벤트 로그 보기 및 지우기 \[78\]](#)
- [원격 Syslog IP 대상 구성 \[79\]](#)
- [심각도 레벨 경고 규칙 구성 \[80\]](#)

▼ 시계 설정 보기 및 설정

주 - get 및 set 명령을 사용하여 NTP(Network Time Protocol) 동기화와 관련된 시계 설정을 확인하고 설정할 수 있습니다. 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ip_address
Password: password
```

2. 다른 예는 다음 SNMP 명령을 참조하십시오.

- NTP 서버 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlNTPEnabled.0
```

- NTP 서버 상태를 enabled 상태로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlNTPEnabled.0 i 1
```

- 장치의 날짜 및 시간을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlDateAndTime.0
```

- 장치의 날짜 및 시간을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlDateAndTime.0 s 2013-3-24,4:59:47.0
```

다음 표는 Oracle ILOM 시계 등록 정보에 유효한 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlDateAndTime	장치의 날짜 및 시간입니다.	date/time	문자열	없음
ilomCtrlNTP	Network Time Protocol을 사용하여 설정할지 여부를 지정합니다.	true(1), false(2)	정수	false
ilomCtrlTimezone	구성된 시간대 문자열입니다.	크기: 0 - 255	문자열	없음

▼ Oracle ILOM 이벤트 로그 보기 및 지우기

주 - get 명령을 사용하여 Oracle ILOM 이벤트를 확인하고 set 명령을 사용하여 이벤트 로그를 구성할 수 있습니다. 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ip_address
Password: password
```

2. 레코드 ID가 2인 이벤트 로그의 이벤트 로그 유형을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlEventLogType.2
```

3. 이벤트 로그를 지우려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlEventLogClear.0 i 1
```

다음 표는 Oracle ILOM 이벤트 로그 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlEventLogRecordID	지정된 이벤트 로그 항목의 레코드 번호입니다.	범위: 1 - 10000	정수	없음

MIB 객체	설명	허용되는 값	유형	기본값
	주 - 이 객체에는 액세스할 수 없습니다.			
ilomCtrlEventLogType	이벤트의 유형을 나타내는 정수입니다. 주 - 이 객체는 읽기 전용입니다.	log(1), action(2), fault(3), state(4), repair(5), other(6)	정수	없음
ilomCtrlEventLogTimestamp	이벤트 로그 항목이 기록된 날짜 및 시간입니다. 주 - 이 객체는 읽기 전용입니다.	<i>date/time</i>	문자열	없음
ilomCtrlEventLogClass	이벤트의 클래스를 나타내는 정수입니다. 주 - 이 객체는 읽기 전용입니다.	audit(1), ipmi(2), chassis(3), fma(4), system(5) pcm(6)	정수	없음
ilomCtrlEventLogSeverity	지정된 로그 항목에 해당하는 이벤트 심각도입니다. 주 - 이 객체는 읽기 전용입니다.	disable(1), critical(2), major(3), minor(4), down(5)	정수	없음
ilomCtrlEventLogDescription	이벤트에 대한 텍스트 설명입니다. 주 - 이 객체는 읽기 전용입니다.	<i>description</i>	문자열	없음
ilomCtrlEventLogClear	이 객체를 true로 설정하면 이벤트 로그가 지워집니다.	true(1), false(2)	정수	없음

▼ 원격 Syslog IP 대상 구성

주 - get 및 set 명령을 사용하여 원격 syslog 수신기의 IP 주소를 확인하고 설정할 수 있습니다. 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ip_address
```

Password: *password*

- 원격 syslog 대상 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlRemoteSyslogDestAddress1.0
```

- 원격 syslog 대상 IP 주소를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlRemoteSyslogDestAddress1.0 a ip_address
```

다음 표는 Syslog IP 대상 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	값	유형	기본값
ilomCtrlRemoteSyslogDest1	첫번째 원격 syslog 대상(로그 호스트)의 IP 주소입니다.	<i>ip_address</i>	문자열	없음
ilomCtrlRemoteSyslogDest2	두번째 원격 syslog 대상(로그 호스트)의 IP 주소입니다.	<i>ip_address</i>	문자열	없음

▼ 심각도 레벨 경고 규칙 구성

주 - get 및 set 명령을 사용하여 경고 규칙 구성을 확인하고 구성할 수 있습니다. 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

- SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ip_address
```

Password: *password*

- 경고 ID가 2인 경고 규칙의 심각도 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlAlertSeverity.2
```

- 경고 ID가 2인 경고 규칙의 심각도 레벨을 critical로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlAlertSeverity.2 i 2
```

다음 표는 경고 규칙 심각도 레벨 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	설명	허용되는 값	유형	기본값
ilomCtrlAlert ID	지정된 경고 규칙과 관련된 정수 ID입니다. 주 - 이 객체에는 액세스할 수 없습니다.	범위: 0 - 65535	정수	없음
ilomCtrlAlert Severity	지정된 클래스에 대해 경고를 트리거해야 하는 최소 이벤트 심각도를 지정합니다.	disable(1), critical(2), major(3), minor(4), down(5)	정수	없음
ilomCtrlAlert Type	지정된 경고에 대한 알림 유형을 지정합니다. 유형이 snmptrap(2) 또는 ipmipet(3)인 경우 ilomCtrlAlertDestinationIP를 지정하고, 유형이 email(1)인 경우 ilomCtrlAlert DestinationEmail을 지정해야 합니다.	email(1) snmptrap(2) ipmipet(3)	정수	없음
ilomCtrlAlert DestinationIP	경보 유형이 snmptrap(2) 또는 ipmipet(3)인 경우 경보 알림을 보낼 IP 주소를 지정합니다.	ip_address	문자열	없음
ilomCtrlAlert Destination Email	경고 유형이 email(1)인 경우 경고 알림을 보낼 전자 메일 주소를 지정합니다.	email address 크기: 0 - 255	문자열	없음
ilomCtrlAlert SNMPVersion	지정된 경고 규칙에 사용해야 하는 SNMP 트랩의 버전을 지정합니다.	v1(1), v2c(2), v3(3)	정수	없음
ilomCtrlAlert SNMPCommunity OrUsername	ilomCtrlAlertSNMPVersion 등록 정보가 v1(1) 또는 v2c(2)로 설정된 경우 사용할 커뮤니티 문자열을 지정하고, ilomCtrlAlertSNMPVersion이 v3(3)으로 설정된 경우 사용할 SNMP 사용자 이름을 지정합니다.	크기: 0 - 255	문자열	없음
ilomCtrlAlert EmailEvent ClassFilter	전자 메일로 보낸 경고를 필터링할 클래스 이름 또는 all입니다.	크기: 0 - 255	문자열	없음
ilomCtrlAlert EmailEventTypeFilter	전자 메일로 보낸 경고를 필터링할 클래스 이름 또는 all입니다.	크기: 0 - 255	문자열	없음

전자 메일 경고 통지를 위한 SMTP 클라이언트 구성(SNMP)

■ 경고 알림에 사용할 SMTP 클라이언트 구성 [82]

▼ 경고 알림에 사용할 SMTP 클라이언트 구성

시작하기 전에

- 구성된 전자 메일 알림 경고를 생성하려면 Oracle ILOM 클라이언트를 전자 메일 경고 메시지를 보낼 SMTP 클라이언트로 설정해야 합니다. Oracle ILOM 클라이언트를 SMTP 클라이언트로 설정하려면 전자 메일 알림을 처리할 보내는 SMTP 전자 메일 서버의 IP 주소 및 포트 번호를 지정해야 합니다.
- Oracle ILOM 클라이언트를 SMTP 클라이언트로 설정하기 전에 보내는 SMTP 전자 메일 서버의 IP 주소 및 포트 번호를 수집하십시오.
- `get` 및 `set` 명령을 사용하여 SMTP 클라이언트를 구성할 수 있습니다. 이 절차에 사용되는 MIB 객체에 대한 설명은 유효한 SMTP 클라이언트 MIB 객체 및 SUN-ILOM-CONTROL-MIB를 참조하십시오.

주 - 이 절차에 유효한 MIB 객체에 대한 설명은 이 절차 다음에 나오는 표를 참조하십시오.

Oracle ILOM에서 SMTP 클라이언트 등록 정보를 구성하려면 다음을 수행하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ip_address  
Password: password
```

2. 다른 예는 다음 SNMP 명령을 참조하십시오.

- SMTP 클라이언트 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSMTPEnabled.0
```

- SMTP 클라이언트 상태를 `enabled`로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSMTPEnabled.0 i 1
```

- SMTP 서버 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSMTPServerIP.0
```

- SMTP 서버 IP 주소를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSMTPServerIP.0 s ip_address
```

- SMTP 클라이언트 포트 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSMTPPortNumber.0
```

- SMTP 클라이언트 포트 번호를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSMTPPortNumber.0 i 25
```

- 보낸 사람 또는 “보낸 사람” 주소를 식별하는 선택적 형식을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSMTPCustomSender.0
```

- 보낸 사람 또는 “보낸 사람” 주소를 식별하는 선택적 형식을 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
  ilomCtrlSMTPCustomSender.0 s ???ilom-alert@HOSTNAME.abc.com'
```

다음 표는 SMTP 전자 메일 경고 알림 SNMP MIB 객체에 대해 설명합니다.

MIB 객체	등록 정보	허용되는 값	유형	기본값
ilomCtrlSMTP Enabled	SMTP 클라이언트를 사용으로 설정할지 여부를 지정합니다.	true(1), false(2)	정수	false
ilomCtrlSMTP ServerIP	사용자 계정의 이름 서비스로 사용되는 SMTP 서버의 IP 주소입니다.	ip_address	문자열	없음
ilomCtrlSMTP PortNumber	SMTP 클라이언트의 포트 번호를 지정합니다.	범위: 0 - 65535	정수	없음

전자 메일 경고 설정 구성(SNMP)

- [전자 메일 경고 설정 관리 \[83\]](#)

▼ 전자 메일 경고 설정 관리

주 - get 및 set 명령을 사용하여 전자 메일 경고 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 보낸 사람 또는 “보낸 사람” 주소를 식별하는 데 사용되는 선택적 형식을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlAlertEmailCustomSender.0
```

- 보낸 사람 또는 “보낸 사람” 주소를 식별하는 데 사용되는 선택적 형식을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent  
ilomCtrlAlertEmailCustomSender.0 s  
???ilom-alert@HOSTNAME.abc.com'
```

- 메시지 본문의 시작 부분에 추가할 수 있는 선택적 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlAlertEmailMessagePrefix.0
```

- 메시지 본문의 시작 부분에 추가할 수 있는 선택적 문자열(예: BeginMessage)을 정의하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlAlertEmailMessagePrefix.0 s  
???BeginMessage'
```

시스템 전원 모니터링 및 관리(SNMP)

설명	링크
시스템 전원 등록 정보를 관리하기 위한 SNMP 요구 사항 검토	■ “시작하기 전에 - 전원 관리(SNMP)” [85]
전력 소비 인터페이스를 모니터링하는 방법	■ “전력 소비 인터페이스 모니터링(SNMP)” [86]
시스템 전원 정책을 유지 관리하는 방법	■ “시스템 전원 정책 유지 보수(SNMP)” [88]
시스템에 전원을 적용하는 방법	■ “시스템 전원 등록 정보 관리(SNMP)” [90]

관련 정보

- [“Setting Power Alert Notifications and Managing System Power Usage” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)
- [“Real-Time Power Monitoring Through Oracle ILOM Interfaces” in Oracle ILOM User’s Guide for System Monitoring and Diagnostics Firmware Release 3.2.x](#)

시작하기 전에 - 전원 관리(SNMP)

이 절의 절차를 수행하기 전에 다음 요구 사항을 충족하는지 확인하십시오.

- SNMP를 사용하여 Oracle ILOM 설정을 확인하고 구성하려면 먼저 SNMP를 구성해야 합니다. 자세한 내용은 [Oracle ILOM에서 SNMP 설정 구성](#)을 참조하십시오.
- snmpset 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 SNMP v3 사용자 계정을 사용해야 합니다.

주 - SNMP 명령 예는 [SNMP 명령 예](#)를 참조하십시오.

주 - 이 단원에 나와 있는 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

전력 소비 인터페이스 모니터링(SNMP)

- 실제 전력 소비량 모니터링 [86]
- 가용 전력 모니터링 [86]
- 할당된 전력 모니터 [86]
- 허용 전력 소비량 모니터링 [86]
- 전원 관리 등록 정보 모니터링 [87]
- 전력 소비 임계값 설정 [87]

주 - 이 절에 설명된 전력 소비 인터페이스는 사용 중인 플랫폼에 구현되어 있지 않을 수 있습니다. 구현에 대한 자세한 내용은 시스템에 포함된 플랫폼별 Oracle ILOM 추가 안내서, 플랫폼 관리 안내서 또는 제품 안내서를 참조하십시오.

▼ 실제 전력 소비량 모니터링

- SNMP를 사용하여 실제 전력 소비량을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtActualPower.0
```

▼ 가용 전력 모니터링

- SNMP를 사용하여 총 가용 전력을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtAvailablePower.0
```

▼ 할당된 전력 모니터

- SNMP를 사용하여 시스템에 할당된 총 전력을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtAllocatedPower.0
```

▼ 허용 전력 소비량 모니터링

- SNMP를 사용하여 허용 전력 소비량을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtPermittedPower.0
```

▼ 전원 관리 등록 정보 모니터링

주 - get 명령을 사용하여 전원 관리 설정을 볼 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-HW-CTRL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 관리 대상 장치에서 다양한 전력 소비 등록 정보를 모니터링하려면 다음 SNMP 명령 예를 참조하십시오.

- PowerMgmtTable 인덱스 번호 5에 대한 전원 관리 정책의 이름을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtName.5
```

- PowerMgmtTable 인덱스 번호 5에 대한 전원 관리 정책 값의 단위를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtUnits.5
```

- PowerMgmtTable 인덱스 번호 5에 대한 전원 관리 정책의 값을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtValue.5
```

▼ 전력 소비 임계값 설정

- 하나 또는 두 개의 전력 소비 임계값을 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent sunHwCtrlPowerMgmtConsumptionThreshold1|2.0 i value
```

여기서 *value*는 전력 소비 임계값(와트)입니다.

시스템 전력 소비가 지정된 임계값을 초과하면 Oracle ILOM에서 경보를 생성합니다. 시스템에서 전자 메일 경보를 구성한 경우 경보 대상으로 알림이 전송됩니다.

시스템 전원 정책 유지 보수(SNMP)

서버 전력 소비를 줄이려면 시스템 전원 정책을 사용으로 설정합니다. 다음과 같은 시스템 전원 정책 관리 절차를 참조하십시오.

■ 전원 정책 보기 및 설정 [88]

▼ 전원 정책 보기 및 설정

시작하기 전에 시스템 전원 정책을 설정하기 전에 다음 자료에 설명된 전원 관리 기능을 검토하십시오.

<http://www.oracle.com/technetwork/articles/servers-storage-admin/ser-howto-save-pwr-sparc-1982424.html>

1. SNMP를 사용하여 Oracle의 SPARC 서버 중 하나에 대한 전원 정책을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtPolicy.0
```

다음과 같이 입력하여 Oracle의 다중 도메인 SPARC 서버 중 하나에서 지정된 도메인의 전원 정책을 확인할 수 있습니다.

```
% snmpget SNMP_agent sunHwCtrlDomainPowerMgmtPolicy.n
```

여기서 *n*은 도메인 ID에 1을 더한 값입니다.

2. Oracle의 SPARC 서버 중 하나에 대한 전원 정책을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent  
sunHwCtrlPowerMgmtPolicy.0 i disabled|performance|elastic
```

다음과 같이 입력하여 Oracle의 다중 도메인 SPARC 서버 중 하나에서 지정된 도메인의 전원 정책을 설정할 수 있습니다.

```
% snmpset SNMP_agent  
sunHwCtrlDomainPowerMgmtPolicy.n i disabled|performance|elastic
```

여기서 *n*은 도메인 ID에 1을 더한 값입니다.

시스템 전력 할당 관리(SNMP)

전력 할당을 통해 시스템 전력 소비에 대한 상한을 설정할 수 있으며, 이 경우 해당 한도가 적용됩니다. 다음과 같은 시스템 전력 할당 관리 절차를 참조하십시오.

- [시스템 전력 할당 설정 \[89\]](#)

▼ 시스템 전력 할당 설정

시작하기 전에 시스템 전력 할당을 설정하기 전에 다음 자료에 설명된 전원 관리 기능을 검토하십시오.

<http://www.oracle.com/technetwork/articles/servers-storage-admin/ser-howto-save-pwr-sparc-1982424.html>

1. 시스템에서 전력 할당을 사용으로 설정합니다.

```
% snmpset SNMP_agent sunHWCtrlPowerMgmtBudget.0 i enabled
```

2. 시스템 전력 소비에 대한 상한을 설정합니다.

```
% snmpset SNMP_agent sunHWCtrlPowerMgmtBudgetPendingPowerLimit.0 i value
sunHWCtrlPowerMgmtBudgetCommitPending.0 i true
```

여기서 *value*는 설치된 하드웨어의 최소 전력과 할당된 전력 간의 전력 한도(와트)입니다. 기본 전력 한도는 현재 허용된 피크 전력입니다.

3. 위반 조치가 수행되기 전 시스템 전력이 전력 한도(2단계 참조)를 초과할 수 있는 시간(초)을 지정합니다.

```
% snmpset SNMP_agent sunHWCtrlPowerMgmtBudgetTimelimit.0 i value
sunHWCtrlPowerMgmtBudgetCommitPending.0 i true
```

여기서 *value*는 -1과 2147483647 사이의 정수입니다. 값이 -1이면 시스템에서 출하 시 지정된 기본값을 사용합니다. 값이 0이면 하드 상한이 사용되어야 합니다. 하드 상한 설정을 지원하지 않는 시스템도 있습니다. 자세한 내용은 “[Setting SP Advanced Power Capping Policy to Enforce Power Limit](#)” in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*을 참조하십시오.

4. 지정된 시간 제한을 경과하여 전력 한도가 초과된 경우 시스템에서 수행해야 할 작업을 정의하려면 위반 조치를 설정합니다.

```
% snmpset SNMP_agent sunHWCtrlPowerMgmtBudgetTimelimitActions.0 i none|hardPowerOff
sunHWCtrlPowerMgmtBudgetCommitPending.0 i true
```

시스템 전원 등록 정보 관리(SNMP)

- 시스템 전원 켜기 [90]
- 시스템 전원 재설정 [90]

▼ 시스템 전원 켜기

주 - set 명령을 사용하여 전원 설정을 구성할 수 있습니다. 이 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

주 - 이 절차의 구문은 tcsh 셸에 유효합니다. 사용자의 셸 환경에서는 이스케이프 문자(\)가 필요하지 않을 수도 있습니다.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. '???'/SYS'라는 전원 제어 대상의 전원을 켜려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlPowerAction."/SYS/" i 1
```

▼ 시스템 전원 재설정

주 - set 명령을 사용하여 재설정 설정을 구성할 수 있습니다. 이 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

주 - 이 절차의 구문은 tcsh 셸에 유효합니다. 사용자의 셸 환경에서는 이스케이프 문자(\)가 필요하지 않을 수도 있습니다.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. '???'/SP'라는 제어 대상을 재설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlResetAction."/SP/" i 1
```


Oracle ILOM 펌웨어 업데이트 관리(SNMP)

설명	링크
SNMP를 사용하여 Oracle ILOM 펌웨어를 업데이트하는 방법	■ Oracle ILOM 펌웨어 업데이트(SNMP) [93]

관련 정보

- [“Performing Firmware Updates” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)

▼ Oracle ILOM 펌웨어 업데이트(SNMP)

시작하기 전에

- SNMP를 사용하여 Oracle ILOM 펌웨어를 확인하고 업데이트하려면 먼저 SNMP를 구성해야 합니다. 자세한 내용은 [Oracle ILOM에서 SNMP 설정 구성](#)을 참조하십시오.
- snmpset 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 SNMP v3 사용자를 사용해야 합니다.
- SNMP 명령 예는 [SNMP 명령 예](#)를 참조하십시오.

주 - get 및 set 명령을 사용하여 Oracle ILOM 펌웨어 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

주 - 이 절에 나와 있는 예제 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

SNMP를 사용하여 Oracle ILOM 펌웨어를 업데이트하려면 다음을 수행하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 현재 펌웨어 이미지의 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtVersion.0
```

- 현재 펌웨어 이미지의 빌드 번호를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareBuildNumber.0
```

- 현재 펌웨어 이미지의 빌드 날짜 및 시간을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareBuildDate.0
```

- 펌웨어 이미지를 다운로드하는 데 사용할 TFTP 서버의 IP 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareTFTPServerIP.0
```

- 펌웨어 이미지를 다운로드하는 데 사용할 TFTP 서버의 IP 주소를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlFirmwareTFTPServerIP.0 a ipaddress
```

- TFTP 서버의 새 펌웨어 이미지 파일에 대한 상대 경로를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareTFTPFileName.0
```

- TFTP 서버의 새 펌웨어 이미지 파일에 대한 상대 경로를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlFirmwareTFTPFileName.0 s '??tftpfilename'
```

- 펌웨어 업데이트 후 서버의 이전 구성을 유지할지 여부를 결정하는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwarePreserveConfig.0
```

- 펌웨어 업데이트 후 서버의 이전 구성을 유지하도록 `PreservConfig` 등록 정보를 `true`로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlFirmwarePreserveConfig.0 i 1
```

- 펌웨어 업데이트 상태를 나타내는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtStatus.0
```

- 다른 펌웨어 관리 등록 정보를 매개변수로 사용하여 펌웨어 업데이트를 초기화하는 데 사용되는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtAction.0
```

- 다른 펌웨어 관리 등록 정보를 매개변수로 사용하여 펌웨어 업데이트를 초기화할 등록 정보를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlFirmwareMgmtAction.0 i 2
```

- 펌웨어 업데이트가 초기화된 경우 및 펌웨어 업데이트를 초기화할 때 사용되는 다른 펌웨어 관리 등록 정보의 값을 지우려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlFirmwareMgmtAction.0 i 1
```

- 현재 펌웨어 관리 파일 시스템의 버전을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtFilesystemVersion.0
```

- 다음에 서버의 전원이 꺼질 때까지 BIOS 업그레이드를 연기하는 데 사용되는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlFirmwareDelayBIOS.0
```

- 다음에 서버의 전원이 꺼질 때까지 BIOS 업그레이드를 연기하는 데 사용되는 `DelayBIOS` 등록 정보를 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlFirmwareDelayBIOS.0 i 1
```


Oracle ILOM 백업 및 복원 구성 관리(SNMP)

설명	링크
Oracle ILOM 등록 정보를 백업 및 복원하는 방법	■ 백업 및 복원 등록 정보 확인 및 구성(SNMP) [97]

관련 정보

- [“Using Backup, Restore, and Reset Default Operations” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)

▼ 백업 및 복원 등록 정보 확인 및 구성(SNMP)

시작하기 전에

- SNMP를 사용하여 Oracle ILOM 설정을 확인하고 구성하려면 먼저 SNMP를 구성해야 합니다. 자세한 내용은 [Oracle ILOM에서 SNMP 설정 구성](#)을 참조하십시오.
- `snmpset` 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(`rw`) 권한을 보유한 SNMP v3 사용자를 사용해야 합니다.

주 - `get` 및 `set` 명령을 사용하여 백업 및 복원 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

주 - SNMP 명령 예는 [SNMP 명령 예](#)를 참조하십시오.

주 - 이 절에 나와 있는 예제 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

주 - 이 절차의 구문은 tcsh 셸에 유효합니다. 사용자의 셸 환경에서는 이스케이프 문자 (\)가 필요하지 않을 수도 있습니다.

SNMP를 사용하여 Oracle ILOM 백업 및 복원 등록 정보를 설정하려면 다음 단계를 수행하십시오.

1. SNMP 도구 및 ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- SNMP를 사용하여 전원 정책을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtPolicy.0
```

- 전원 등록 정보를 구성하여 ???/SYS라는 전원 제어 대상에 적용하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlPowerAction."/SYS" i 1
```

- SP 구성을 원래 출하 시 기본 상태로 복원하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlResetToDefaultsAction.0 i 3
```

- 백업 및 복원 작업 중에 구성 XML 파일의 대상을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlBackupAndRestoreTargetURI.0
```

- TFTP를 사용하여 백업 및 복원 작업 중에 구성 XML 파일의 대상을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent  
  ilomCtrlBackupAndRestoreTargetURI.0 s  
  '???tftp://tftp_server_ipaddress/remotedir/config_backup.xml'
```

- 백업 및 복원 작업 중에 중요한 데이터를 암호화하거나 해독할 암호문을 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
  ilomCtrlBackupAndRestorePassphrase.0 s ???passphrase'
```

- 백업 또는 복원 작업을 실행하는 데 사용되는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlBackupAndRestoreAction.0
```

- `ilomCtrlBackupAndRestoreAction` MIB 객체를 사용하여 복원 작업을 실행하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlBackupAndRestoreAction.0 i 2
```

- 백업 및 복원 작업의 현재 상태를 모니터링하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlBackupAndRestoreActionStatus.0
```

- 재설정 작업을 지정하여 `??/SP`라는 재설정 제어 대상에 적용하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlResetAction.\"/SP\" i 1
```


SPARC 진단, POST 및 부트 모드 작업 관리 (SNMP)

설명	링크
SPARC 구성 관리 인터페이스를 관리하기 위한 요구 사항 검토	■ “시작하기 전에 - SPARC 호스트 관리(SNMP)” [101]
SPARC 관리 인터페이스 등록 정보를 관리하는 방법	■ “SPARC 진단, POST 및 부트 모드 등록 정보 관리 (SNMP)” [102]

관련 정보

- [“Configuring Host Server Management Actions” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)
- [“Setting Diagnostic Tests to Run” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)

시작하기 전에 - SPARC 호스트 관리(SNMP)

SPARC 진단, POST 및 부트 모드 등록 정보를 관리하기 위한 SNMP 절차를 수행하기 전에 다음 요구 사항이 충족되었는지 확인해야 합니다.

- SNMP를 사용하여 Oracle ILOM 설정을 확인하고 구성하려면 먼저 SNMP를 구성해야 합니다. 자세한 내용은 [Oracle ILOM에서 SNMP 설정 구성](#)을 참조하십시오.
- snmpset 명령을 실행하려면 SNMP v1/v2c 커뮤니티 또는 읽기-쓰기(rw) 권한을 보유한 SNMP v3 사용자 계정을 사용해야 합니다.
- SNMP 명령 예는 [SNMP 명령 예](#)를 참조하십시오.

주 - 이 단원에 나와 있는 SNMP 명령은 Net-SNMP 샘플 응용 프로그램을 기반으로 하기 때문에 Net-SNMP 및 Net-SNMP 샘플 응용 프로그램이 설치되어 있는 경우에만 설명대로 작동합니다.

SPARC 진단, POST 및 부트 모드 등록 정보 관리(SNMP)

- [SPARC 호스트 진단 등록 정보 관리 \[102\]](#)
- [SPARC 호스트 POST 작업 관리 \[105\]](#)
- [SPARC 호스트 부트 모드 등록 정보 관리 \[107\]](#)
- [SPARC 호스트 키 스위치 등록 정보 관리 \[109\]](#)

▼ SPARC 호스트 진단 등록 정보 관리

주 - get 및 set 명령을 사용하여 SPARC 진단 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 호스트에 대한 내장된 진단 트리거를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsTrigger.0
```

- 호스트에 대한 내장된 진단 트리거를 power-on-reset으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsTrigger.0 i 4
```

- POST 모드를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsMode.0
```

- POST 모드를 service로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsMode.0 i 3
```

- 전원 켜기 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsPowerOnLevel.0
```

- 전원 켜기 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 `normal`로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsPowerOnLevel.0 i 3
```

- 사용자 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsUserResetLevel.0
```

- 사용자 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 `normal`로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsUserResetLevel.0 i 3
```

- 오류 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsErrorResetLevel.0
```

- 오류 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 `normal`로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsErrorResetLevel.0 i 3
```

- 하드웨어 변경 트리거를 위해 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsHwChangeLevel.0
```

- 하드웨어 변경 트리거를 위해 부트하는 동안 호스트에서 실행해야 하는 내장된 진단 레벨을 `maximum`으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsHwChangeLevel.0 i 4
```

- 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsPowerOnVerbosity.0
```

- 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 maximum으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsPowerOnVerbosity.0 i 4
```

- 사용자 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsUserResetVerbosity.0
```

- 사용자 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 maximum으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsUserResetVerbosity.0 i 4
```

- 오류 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsErrorResetVerbosity.0
```

- 오류 재설정 트리거를 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 maximum으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsErrorResetVerbosity.0 i 4
```

- 하드웨어 변경 트리거를 위해 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsHwChangeVerbosity.0
```

- 하드웨어 변경 트리거를 위해 부트하는 동안 호스트에서 실행해야 하는 내장된 진단의 상세도 레벨을 minimum으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsHwChangeVerbosity.0 i 2
```

▼ SPARC 호스트 POST 작업 관리

주 - get 및 set 명령을 사용하여 SPARC 호스트 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 호스트의 시작 MAC 주소를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostMACAddress.0
```

- OBP(OpenBoot PROM)의 버전 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostOBPVersion.0
```

- POST의 버전 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostPOSTVersion.0
```

- 치명적이지 않은 POST 오류가 발생한 경우 호스트에서 부트를 계속할지 여부를 결정하는 옵션을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostAutoRunOnError.0
```

- 치명적이지 않은 POST 오류가 발생한 경우 호스트에서 부트를 계속하도록 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostAutoRunOnError.0 i 1
```

- 호스트가 정지된 것을 발견한 경우 SP에서 수행할 작업을 결정하는 옵션을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostAutoRestartPolicy.0
```

- 호스트가 정지된 것을 발견한 경우 재설정하도록 SP를 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostAutoRestartPolicy.0 i 2
```

- 호스트 운영체제의 부트 상태를 설명하는 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostOSBootStatus.0
```

- 부트 타이머 제한 시간 값을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostBootTimeout.0
```

- 부트 타이머 제한 시간 값을 30초로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostBootTimeout.0 i 30
```

- 부트 타이머가 완료된 경우 SP에서 수행할 작업을 결정하는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostBootRestart.0
```

- 부트 타이머가 완료된 경우 재설정하도록 SP를 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostBootRestart.0 i 2
```

- SP에서 허용되는 최대 부트 실패 횟수를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostMaxBootFail.0
```

- SP에서 허용되는 최대 부트 실패 횟수를 10으로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostMaxBootFail.0 i 10
```

- 최대 부트 실패 횟수에 도달한 경우 SP에서 수행할 작업을 결정하는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostBootFailRecovery.0
```

- 최대 부트 실패 횟수에 도달한 경우 호스트 전원을 순환시키도록 SP를 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostBootFailRecovery.0 i 2
```

- 하이퍼바이저의 버전 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostHypervisorVersion.0
```

- 시스템 펌웨어(SysFw)의 버전 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostSysFwVersion.0
```

- SP에서 보낼 중단 작업을 결정하는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostSendBreakAction.0
```

- SP에서 `dumpcore` 중단 작업을 보내도록 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostSendBreakAction.0 i 3
```

- 다음에 호스트 전원을 켤 때 적용할 호스트 입출력 재구성 정책을 결정하는 등록 정보를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCHostIoReconfigurePolicy.0
```

- 다음에 전원을 켤 때 SP에서 호스트 입출력 재구성 정책을 실행하도록 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCHostIoReconfigurePolicy.0 i 3
```

▼ SPARC 호스트 부트 모드 등록 정보 관리

주 - get 및 set 명령을 사용하여 SPARC 부트 모드 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 호스트의 부트 모드 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeState.0
```

- 호스트에서 현재 NVRAM 변수 설정을 유지하도록 구성하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCBootModeState.0 i 1
```

- 부트 모드 상태를 script로 설정한 경우에 사용할 부트 스크립트를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeScript.0
```

- 부트 모드 상태를 ???setenv diag-switch로 설정한 경우에 사용할 부트 스크립트를 지정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent
  ilomCtrlSPARCBootModeScript.0 s '???setenv diag-switch'
```

- 부트 모드 구성이 완료되는 날짜 및 시간을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeExpires.0
```

- LDOM 구성 이름을 나타내는 문자열을 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeLDOMConfig.0
```

- LDOM 구성 이름을 default로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCBootModeLDOMConfig.0 s default
```

▼ SPARC 호스트 키 스위치 등록 정보 관리

주 - `get` 및 `set` 명령을 사용하여 SPARC 키 스위치 설정을 확인하고 구성할 수 있습니다. 이러한 명령에 사용되는 MIB 객체에 대한 설명은 SUN-ILOM-CONTROL-MIB를 참조하십시오.

1. SNMP 도구 및 Oracle ILOM MIB가 설치된 호스트에 로그인합니다. 예를 들어 다음과 같이 입력합니다.

```
ssh username@snmp_manager_ipaddress
```

```
Password: password
```

2. 다음 SNMP 명령 예를 참조하십시오.

- 가상 키 스위치의 현재 상태를 확인하려면 다음과 같이 입력합니다.

```
% snmpget SNMP_agent ilomCtrlSPARCKeySwitchState.0
```

- 가상 키 스위치의 상태를 `standby`로 설정하려면 다음과 같이 입력합니다.

```
% snmpset SNMP_agent ilomCtrlSPARCKeySwitchState.0 i 2
```


IPMI를 통한 서버 관리

설명	링크
IPMItool을 사용하여 Oracle 서버를 관리하는 자세한 방법	■ “IPMI(지능형 플랫폼 관리 인터페이스)” [111]
IPMItool을 사용하여 IPMI 상태를 구성하고 다양한 관리 기능을 수행하는 방법	■ “IPMI 서비스 구성” [113] ■ “IPMItool을 사용하여 ILOM CLI 명령 실행” [116] ■ “시스템 관리 작업 수행(IPMItool)” [118]
IPMI 명령에 대한 자세한 정보	■ “IPMItool 유틸리티 및 명령 요약” [127]

관련 정보

- [“Modifying Default Management Access Configuration Properties” in Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x](#)

IPMI(지능형 플랫폼 관리 인터페이스)

- [“IPMI 정보” \[111\]](#)
- [“IPMItool” \[112\]](#)
- [“IPMI 경고” \[113\]](#)
- [“IPMI Administrator 및 Operator 역할” \[113\]](#)

IPMI 정보

Oracle ILOM에서는 서버를 모니터링 및 제어하고 서버에 대한 정보를 검색할 수 있는 IPMI (지능형 플랫폼 관리 인터페이스)를 지원합니다.

IPMI는 다양한 네트워크를 통한 서버 시스템 관리를 위해 설계된 개방형 산업 표준 인터페이스입니다. IPMI 기능으로는 FRU(현장 대체 가능 장치) 부품 보고, 시스템 모니터링, 시스템 이벤트 로깅, 시스템 복구(시스템 재설정 및 전원 켜기/끄기 기능 포함) 및 경보가 있습니다.

IPMI를 통해 플랫폼 하드웨어에 기본 제공되는 관리 기능에 액세스하여 모니터링, 로깅, 시스템 복구 및 경고 기능을 사용할 수 있습니다.

Oracle ILOM은 IPMI v1.5 및 v2.0과 호환됩니다. 하지만 보안 레벨 향상을 위해 Oracle ILOM IPMI 클라이언트가 지원을 제공하고 항상 IPMI 2.0 모드로 작동해야 합니다. IPMI v2.0은 Oracle ILOM 3.2.4 및 이후 릴리스에서 기본적으로 사용으로 설정되어 있습니다.

IPMI에 대한 세부 사양을 비롯한 추가 정보는 다음 사이트에서 제공됩니다.

- <http://www.intel.com/design/servers/ipmi/spec.htm>
- <http://openipmi.sourceforge.net>

서버 및 서버 모듈(블레이드)의 SP(서비스 프로세서)는 IPMI v2.0과 호환됩니다. 대역 내(서버를 실행하는 호스트 운영체제 사용) 또는 대역 외(원격 시스템 사용)에서 IPMItool 유틸리티를 사용하여 명령줄을 통해 IPMI 기능에 액세스할 수 있습니다. 또한 Oracle ILOM 웹 인터페이스에서 IPMI 관련 트랩을 생성하거나 IPMI v1.5 또는 v2.0과 호환된 외부 관리 솔루션에서 SP의 IPMI 기능을 관리할 수 있습니다.

IPMItool

IPMItool은 IPMI 지원 장치를 관리 및 구성하는 간단한 오픈 소스 CLI(명령줄 인터페이스) 유틸리티입니다. 이 유틸리티를 사용하면 커널 장치 드라이버나 LAN 인터페이스를 통해 로컬 또는 원격 시스템의 IPMI 기능을 관리할 수 있습니다. Oracle Hardware Management Pack의 일부로 IPMItool의 특정 버전이 제공됩니다. <http://ipmitool.sourceforge.net>에서 IPMItool을 다운로드할 수 있습니다.

IPMItool을 사용하여 다음을 수행할 수 있습니다.

- SDR(Sensor Data Record) 저장소 읽기
- 센서 값 인쇄
- SEL(시스템 이벤트 로그) 콘텐츠 표시
- FRU(현장 대체 가능 장치) 부품 정보 인쇄
- LAN 구성 매개변수 읽기 및 설정
- 원격 새시 전원 제어 수행

IPMItool은 명령줄 프롬프트에서 `ipmitool help`를 입력하여 액세스할 수 있는 명령줄 도움말을 제공합니다.

IPMItool은 ILOM CLI를 직접 사용할 때와 마찬가지로 ILOM CLI(명령줄 인터페이스) 명령을 입력할 수 있는 기능을 지원합니다. CLI 명령을 스크립트로 작성한 다음 여러 SP(서비스 프로세서) 인스턴스에서 이 스크립트를 실행할 수 있습니다.

IPMI 경고

Oracle ILOM은 IPMI PET(Platform Event Trap) 경고 형식의 경고를 지원합니다. 경고는 발생 가능한 시스템 오류를 사전에 경고합니다. 경고 구성은 서버의 SP에서 사용할 수 있습니다. IPMI PET 경보는 Oracle 서버 SP에서는 지원되지만 CMM(새시 모니터링 모듈)에서는 지원되지 않습니다. IPMI 경보에 대한 자세한 내용은 [“Configuring Alert Notifications in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x”](#)을 참조하십시오.

IPMI Administrator 및 Operator 역할

IPMI Administrator 역할은 ILOM의 aucro 사용자 역할에 매핑됩니다. *IPMI Operator* 역할은 Oracle ILOM의 cro 사용자 역할에 매핑됩니다. 이러한 Oracle ILOM 역할에 대한 간단한 설명이 다음 표에 나와 있습니다.

표 6 Oracle ILOM의 IPMI Administrator 및 Operator 역할

IPMI 역할	지원되는 ILOM 역할 권한	설명
Administrator	<ul style="list-style-type: none"> ■ Admin(a) ■ User Management(u) ■ Console(c) ■ Reset and Host Console(r) ■ Read-Only(o) 	이러한 사용자 역할은 시스템 관리 구성 등록 정보, 사용자 계정 등록 정보, 원격 콘솔 관리 등록 정보, 원격 전원 관리 등록 정보, 재설정 및 호스트 컨트롤 관리 등록 정보 등의 Oracle ILOM 관리 기능에 대한 읽기/쓰기 권한을 사용으로 설정합니다.
Operator	<ul style="list-style-type: none"> ■ Console(c) ■ Reset and Host Console(r) ■ Read-Only(o) 	이러한 사용자 역할은 원격 콘솔 관리 등록 정보, 원격 전원 관리 등록 정보, 재설정 및 호스트 컨트롤 관리 등록 정보 등의 Oracle ILOM 관리 기능에 대한 읽기/쓰기 권한을 사용으로 설정합니다. 또한 Read-Only 역할은 시스템 관리 구성 등록 정보 및 사용자 관리 등록 정보에 대한 읽기 액세스를 제공합니다.

Oracle ILOM 역할 및 권한에 대한 자세한 내용은 [“Managing User Credentials” in Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x](#)를 참조하십시오.

IPMI 서비스 구성

- IPMI 서비스 상태 사용(CLI) [114]
- IPMI 서비스 상태 사용(웹) [114]

▼ IPMI 서비스 상태 사용(CLI)

1. Admin(a) 역할 권한이 있는 계정을 사용하여 Oracle ILOM CLI에 로그인합니다.
Admin(a) 역할 권한을 사용으로 설정하는 것과 관련된 자세한 내용은 “[IPMI Administrator 및 Operator 역할](#)” [113]을 참조하십시오.
2. 명령 프롬프트에서 다음 명령을 실행하여 IPMI 서비스 상태를 사용으로 설정합니다.

```
-> set /SP/services/ipmi state=enabled
Set 'state' to 'enabled'
```

3. Oracle ILOM 3.2.4 이상과 함께 서버가 제공된 경우 IPMI v1.5 연결을 사용으로 설정할지 여부를 결정합니다.
보안 향상을 위해 기본적으로 IPMI v1.5 세션이 사용 안함으로 설정되어 있습니다. IPMI v1.5의 대안으로 IPMI v2.0에서는 향상된 인증 및 IPMI 패킷 암호화를 제공합니다.
하지만 FIPS 모드가 사용 안함으로 설정된 경우 IPMI v1.5 세션을 사용으로 설정할 수도 있습니다. FIPS 모드에 대한 자세한 내용은 *Oracle ILOM* 보안 설명서를 참조하십시오.
4. Oracle ILOM 3.2.4 이상과 함께 제공된 서버에서 IPMI v1.5 연결을 사용으로 설정하려면 다음 명령을 실행합니다.

```
-> set /SP/services/ipmi v1_5_sessions=enabled
Set 'v1_5_sessions' to 'enabled'
```

IPMI 1.5 세션이 사용으로 설정된 경우 IPMItool 사용자는 -l lan 옵션을 지정해야 합니다. IPMI v1.5 세션이 사용 안함으로 설정된 경우 IPMItool 사용자는 -l lanplus 옵션을 지정해야 합니다.

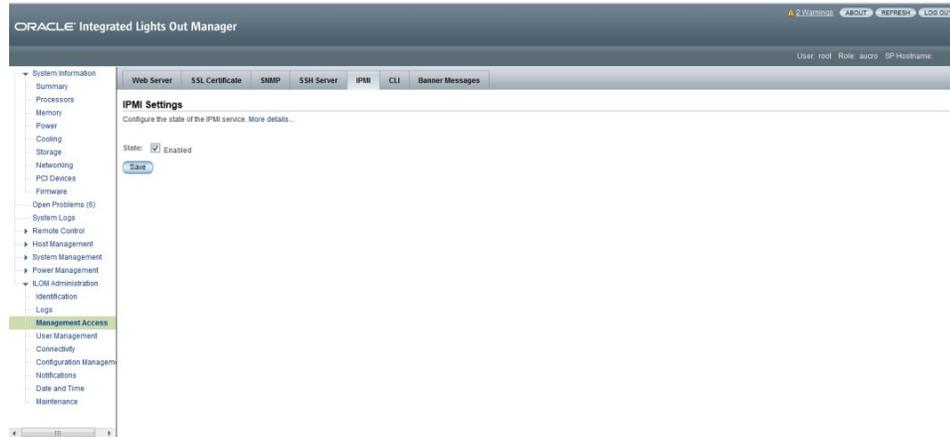


주의 - IPMI v1.5 세션에서는 향상된 인증 및 패킷 암호화를 지원하지 않습니다.

▼ IPMI 서비스 상태 사용(웹)

1. Admin(a) 역할 권한이 있는 계정을 사용하여 Oracle ILOM 웹 인터페이스에 로그인합니다.
Admin(a) 권한을 사용으로 설정하는 것과 관련된 자세한 내용은 “[IPMI Administrator 및 Operator 역할](#)” [113]을 참조하십시오.
2. ILOM Administration > Management Access > IPMI를 누릅니다.

IPMI Settings 페이지가 나타납니다.



3. State 확인란을 선택하여 IPMI 서비스 상태를 사용으로 설정합니다.
4. Oracle ILOM 3.2.4 이상과 함께 서버가 제공된 경우 IPMI v1.5 연결을 사용으로 설정할지 여부를 결정합니다.
 보안 향상을 위해 기본적으로 IPMI v1.5 세션이 사용 안함으로 설정되어 있습니다. IPMI v1.5의 대안으로 IPMI v2.0에서는 향상된 인증 및 IPMI 패킷 암호화를 제공합니다.
 하지만 FIPS 모드가 사용 안함으로 설정된 경우 IPMI v1.5 세션을 사용으로 설정할 수도 있습니다. FIPS 모드에 대한 자세한 내용을 보려면 Management Access > FIPS 페이지에서 Details 링크를 누릅니다.
5. Oracle ILOM 3.2.4 이상과 함께 제공된 서버에서 IPMI v1.5 연결을 사용으로 설정하려면 v1.5 Sessions 확인란을 선택합니다.
 IPMI 1.5 세션이 사용으로 설정된 경우 IPMITool 사용자는 -l lan 옵션을 지정해야 합니다. IPMI v1.5 세션이 사용 안함으로 설정된 경우 IPMITool 사용자는 -l lanplus 옵션을 지정해야 합니다.



주의 - IPMI v1.5 세션에서는 향상된 인증 및 패킷 암호화를 지원하지 않습니다.

IPMItool을 사용하여 ILOM CLI 명령 실행

IPMItool CLI는 Oracle ILOM CLI 명령을 실행할 수 있는 편리한 대체 방법입니다. Oracle ILOM CLI를 직접 사용할 때와 마찬가지로 명령을 입력할 수 있습니다. 대부분의 Oracle ILOM CLI 명령이 지원됩니다.

- [“시작하기 전에 - IPMItool 및 Oracle ILOM 요구 사항” \[116\]](#)
- [IPMItool에서 Oracle ILOM CLI 액세스 \[116\]](#)
- [“IPMItool을 사용하여 Oracle ILOM CLI 명령 스크립트 작성” \[117\]](#)

시작하기 전에 - IPMItool 및 Oracle ILOM 요구 사항

- IPMItool을 통해 Oracle ILOM CLI 명령을 실행하려면 IPMItool 버전 1.8.9.4 이상을 사용해야 합니다. IPMItool의 버전 번호를 확인하려면 다음과 같이 입력합니다.

```
ipmitool -v
```

- IPMItool CLI를 사용하여 명령을 실행할 때 Oracle ILOM에서 적절한 사용자 역할이 지정되었는지 확인해야 합니다. 자세한 내용은 [“IPMI Administrator 및 Operator 역할” \[113\]](#)을 참조하십시오.

▼ IPMItool에서 Oracle ILOM CLI 액세스

1. IPMItool을 사용하여 ILOM CLI를 사용으로 설정하려면 다음과 같이 입력합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -U username -P password sunoem cli
```

ILOM CLI 프롬프트가 다음과 같이 표시됩니다.

```
Connected. Use ^D to exit.
->
```

2. CLI를 사용하려면 CLI 명령을 입력합니다.

Oracle ILOM CLI 명령 스크립트를 작성하는 방법은 [“IPMItool을 사용하여 Oracle ILOM CLI 명령 스크립트 작성” \[117\]](#)을 참조하십시오.

IPMItool을 사용하여 Oracle ILOM CLI 명령 스크립트 작성

IPMItool에서 Oracle ILOM CLI를 사용하면 CLI 명령 스크립트를 작성한 다음 여러 SP 인스턴스를 이 스크립트를 실행할 수 있는 이점이 있습니다. CLI 명령을 IPMItool 명령줄에 포함하고 명령줄의 각 인수를 별도의 Oracle ILOM CLI 명령을 처리할 수 있기 때문에 스크립트 작성이 가능합니다. 각 Oracle ILOM CLI 명령의 시작 부분과 끝 부분에 큰 따옴표를 포함하여 명령을 구분합니다.

다음 예는 IPMItool 명령줄에 두 개의 CLI 명령을 포함하는 방법을 보여줍니다. 이 예에서 각 명령은 큰 따옴표로 시작하고 끝납니다.

```
# ipmitool -H SP_hostname_or_IPAddress -U username -P password sunoem cli
"show /SP/services" "show /SP/logs"
Connected. Use ^D to exit.
-> show /SP/services
/SP/services
Targets:
  http
  https
  ipmi
  kvms
  servicetag
  snmp
  ssh
  sso

Properties:

Commands:
  cd
  show

-> show /SP/logs
/SP/logs
Targets:
  audit
  event

Properties:

Commands:
  cd
  show
-> Session closed
Disconnected
```

시스템 관리 작업 수행(IPMItool)

- “시작하기 전에 - Oracle ILOM 및 IPMItool 요구 사항” [118]
- 센서 목록 표시 [118]
- 단일 센서 세부정보 보기 [119]
- 존재 센서 유형 값 확인 및 해석 [119]
- 호스트 전원 켜기, 전원 끄기 및 종료 기능 관리 [121]
- Oracle ILOM 전력 할당 인터페이스 관리 [122]
- 시스템 전원 정책 관리 [124]
- FRU 제조 세부정보 표시 [125]
- Oracle ILOM 이벤트 로그 표시 [126]

시작하기 전에 - Oracle ILOM 및 IPMItool 요구 사항

IPMItool CLI를 사용하여 Oracle ILOM 명령을 실행할 때 Oracle ILOM에서 적절한 사용자 역할이 지정되었는지 확인해야 합니다. 자세한 내용은 “[IPMI Administrator 및 Operator 역할](#)” [113]을 참조하십시오.

▼ 센서 목록 표시

- 관리 대상 장치의 센서 목록을 확인하려면 다음과 같이 입력합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -I lanplus -U username -P password
```

```
sdr list
```

다음과 같은 출력이 표시될 수 있습니다.

```
/SYS/T_AMB          | 24 degrees C      | ok
/RFM0/FAN1_SPEED   | 7110 RPM          | ok
/RFM0/FAN2_SPEED   | 5880 RPM          | ok
/RFM1/FAN1_SPEED   | 5880 RPM          | ok
/RFM1/FAN2_SPEED   | 6360 RPM          | ok
/RFM2/FAN1_SPEED   | 5610 RPM          | ok
/RFM2/FAN2_SPEED   | 6510 RPM          | ok
/RFM3/FAN1_SPEED   | 6000 RPM          | ok
/RFM3/FAN2_SPEED   | 7110 RPM          | ok
/RFM4/FAN1_SPEED   | 6360 RPM          | ok
/RFM4/FAN2_SPEED   | 5610 RPM          | ok
/RFM5/FAN1_SPEED   | 5640 RPM          | ok
/RFM5/FAN2_SPEED   | 6510 RPM          | ok
/RFM6/FAN1_SPEED   | 6180 RPM          | ok
```

```

/RFM6/FAN2_SPEED | 6000 RPM          | ok
/RFM7/FAN1_SPEED | 6330 RPM          | ok
/RFM7/FAN2_SPEED | 6330 RPM          | ok
/RFM8/FAN1_SPEED | 6510 RPM          | ok
/RFM8/FAN2_SPEED | 5610 RPM          | ok

```

주 - 이전 예에 표시된 센서 출력은 잘렸습니다. 실제 출력은 하드웨어 플랫폼에 따라 달라집니다.

▼ 단일 센서 세부정보 보기

- 관리 대상 장치의 단일 센서에 대한 세부정보를 확인하려면 다음과 같이 입력합니다.

```
sensor get /target/sensor_name
```

예를 들어 시스템 온도(/SYS/T_AMB)에 대한 센서 세부정보를 확인하려면 다음과 같이 입력합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -v -I lanplus -U username -P password
```

```
sensor get /SYS/T_AMB
```

다음과 같은 출력이 표시될 수 있습니다.

```

Locating sensor record...
Sensor ID           : /SYS/T_AMB (0x8)
Entity ID          : 41.0
Sensor Type (Analog) : Temperature
Sensor Reading     : 24 (+/- 0) degrees C
Status             : ok
Lower Non-Recoverable : 0.000
Lower Critical     : 4.000
Lower Non-Critical  : 10.000
Upper Non-Critical  : 35.000
Upper Critical     : 40.000
Upper Non-Recoverable : 45.000
Assertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
Deassertions Enabled : lnc- lcr- lnr- unc+ ucr+ unr+

```

▼ 존재 센서 유형 값 확인 및 해석

시작하기 전에

- IPMItool은 존재 센서 유형 레코드 각각에 대해 States Asserted 필드 출력을 지원합니다. 이 States Asserted 필드는 IPMItool 출력에 다음과 같이 표시될 수 있습니다.
 - States Asserted = Entity Presence

States Asserted = Entity Presence 필드가 나타나면 하드웨어 구성 요소에 대한 센서 출력에 세 가지 유효 값인 Present(=1), Absent(=2), Disabled(=4) 중 하나가 표시될 수 있습니다.

- 또는 -

■ States Asserted = Availability State

States Asserted = Availability State 필드가 나타나면 하드웨어 구성 요소에 대한 센서 출력에 두 가지 유효 값인 Device Absent(=1) 및 Device Present(=2) 중 하나가 표시될 수 있습니다.

주 - Oracle ILOM에서는 두 States Asserted 필드 모두에 대한 출력을 지원합니다. 그러나 일부 Oracle 하드웨어 플랫폼에서는 사용 가능한 States Asserted 필드 (Entity Presence 또는 Availability State)를 모두 지원하거나 둘 중 하나만 지원할 수 있습니다.

IPMI 존재 센서 유형에 대해 표시되는 값을 해석하는 방법에 대한 자세한 내용은 IPMI 2.0 Specifications의 Section 42 - Sensor and Event Code Tables를 참조하십시오. Section 42의 콘텐츠를 모두 이해하는 것이 센서 값을 해석하는 방법을 이해하는 데 중요합니다.

Oracle 하드웨어 플랫폼에만 해당하는 센서 세부정보는 해당 플랫폼의 Oracle ILOM 추가 안내서 또는 관리 안내서를 참조하십시오.

IPMITool 존재 센서 유형 값을 확인하고 해석하려면 다음 단계를 수행하십시오.

1. 하드웨어 구성 요소의 실제 센서 표시값을 확인하려면 `IPMITool sdr list` 명령을 사용합니다.

예를 들어 `sdr list` 명령을 실행하면 PCIE 하드웨어 구성 요소에 대해 다음과 같은 존재 센서 유형 표시값이 나타납니다.

```
PCIE_CC/PRSNT | 0x02 | ok
PCIE0/F20/PRSNT | 0x01 | ok
```

2. 존재 센서 유형에 대한 States Asserted 필드 값을 확인하려면 `IPMITool sensor get` 명령을 사용합니다.

IPMITool에서 `sensor get` 명령을 실행하면 다음과 같은 States Asserted 필드가 나타납니다.

■ States Asserted = Entity Presence

다음 예에서 States Asserted = Entity Presence 필드에 대해 표시된 값은 *Absent*입니다.

```
$ ipmitool sensor get PCIE_CC/PRSNT
Locating sensor record...
```

```
Sensor ID      : PCIE_CC/PRSNT (0xad)
Entity ID      : 49.0
Sensor Type (Discrete): Entity Presence
States Asserted : Entity Presence
[Absent]
```

■ States Asserted = Availability State

다음 예에서 States Asserted = Availability State 필드에 대해 표시된 값은 *Device Absent*입니다.

```
$ ipmitool sensor get PCIE1/PRSNT
Locating sensor record...
Sensor ID      : PCIE1/PRSNT (0xe6)
Entity ID      : 11.0
Sensor Type (Discrete): Entity Presence
States Asserted : Availability State
[Device Absent]
```

▼ 호스트 전원 켜기, 전원 끄기 및 종료 기능 관리

1. 관리 대상 장치에서 호스트의 전원을 켜려면 다음과 같이 입력합니다.

```
chassis power on
```

예를 들면 다음과 같습니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -v -I lanplus -U username -P password
chassis power on
```

2. 관리 대상 장치에서 호스트의 전원을 끄려면 다음과 같이 입력합니다.

```
chassis power off
```

예를 들면 다음과 같습니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -v -I lanplus -U username -P password
chassis power off
```

3. 관리 대상 장치에서 호스트의 전원을 순환시키려면 다음과 같이 입력합니다.

```
chassis power cycle
```

예를 들면 다음과 같습니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -v -I lanplus -U username -P password
chassis power cycle
```

4. 관리 대상 장치에서 호스트를 정상적으로 종료하려면 다음과 같이 입력합니다.

```
chassis power soft
```

예를 들면 다음과 같습니다.

```
$ ipmitool -H SP_hostname_or_IPAddress -v -I lanplus -U username -P password
chassis power soft
```

▼ Oracle ILOM 전력 할당 인터페이스 관리

1. 관리 대상 장치에서 전력 한도 활성화 상태를 설정하려면 다음 명령 중 하나를 사용합니다.

■ 활성화하려면

```
$ ipmitool -H SP_hostname_or_IPAddress -U username -P password raw 0x2e 0x49
0x00 0x01 0xFF 0xFF
```

명령 완료 시

```
dc
```

■ 비활성화하려면

```
$ ipmitool -H SP_hostname_or_IPAddress -U username -P password raw 0x2e 0x49
0x00 0x00 0xFF 0xFF
```

명령 완료 시

```
dc
```

다음 표는 전력 한도 활성화 상태(IPMIttool) 입력 및 출력 필드에 대해 설명합니다.

필드	바이트	설명
Input Data	1	Sun OEM 명령 그룹 번호: 0x2e
	2	명령 코드 0x49는 전력 한도 활성화 상태를 설정합니다.
	3	그룹 확장 표시: 0x00. 이 필드의 값은 무시됩니다.
	4	전력 한도 활성화 하위 명령 0x00 - 전력 한도를 비활성화합니다. 0x01 - 전력 한도를 활성화합니다.
	5-6	예약 필드: 0xFF. 이 필드의 값은 무시됩니다.
Output Data	1	IPMIttool에서 사용하는 완료 코드입니다. 성공 완료 코드 상태는 표시되지 않지만 완료 코드 결과가 'successful'이 아닌 경우 실패 메시지가 나타납니다.
	2	명령 완료 시 그룹 확장 표시 '???dc'가 나타납니다.

2. 전력 한도 할당 등록 정보를 가져오려면 다음과 같이 입력합니다.

주 - 전력 할당 할당 와트 등록 정보를 설정하기 전에 Get Power Limit Budget Wattage 명령을 사용해야 합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -U username -P password raw 0x2e 0x4A 0x00 0x00 0x00
```

명령 완료 시

```
dc 00 01 b3 00 02 fa 00 00 00 00 01 e9 00 00
```

다음 표는 전력 할당 가져오기(IPMItool) 입력 및 출력 필드에 대해 설명합니다.

필드	바이트	설명
Input Data	1	Sun OEM 명령 그룹 번호: 0x2e
	2	명령 코드 0x4A는 전력 할당 설정을 가져옵니다.
	3	그룹 확장 표시: 0x00. 이 필드의 값은 무시됩니다.
	4-5	예약 필드: 0x00. 이 필드의 값은 무시됩니다.
Output Data	1	IPMItool에서 사용하는 완료 코드입니다. 명령 완료 시 표시되지 않지만, 완료 코드 결과가 successful이 아닌 경우 명령 완료 시 실패 메시지가 나타납니다.
	2	그룹 확장 표시입니다. 위 예에서는 'dc???'로 표시됩니다.
	3	활성화 상태: 00 - 비활성화됨 01 - 활성화됨
	4	예약 필드입니다. 위 예의 b3 값은 무시해도 됩니다.
	5	전력 한도를 초과하거나 정정 시간 제한 내에 제어할 수 없는 경우 수행되는 예외 조치입니다. 반환 값: 00 - 없음 01 - 강제 전원 끄기
	6-7	전력 할당(와트)로, 위 예에서는 02 fa입니다.
	8-11	정정 시간 제한(밀리초)으로, 위 예에서는 00 00 00 00입니다.
	12	정정 시간 제한이 시스템 기본 시간 제한인지 여부를 나타내는 플래그입니다. 00 - 기본값 아님 01 - 기본값
	13	예약 필드입니다. 위 예에 표시된 값(e9)은 무시해도 됩니다.
	14-15	예약 필드입니다. 위 예에 표시된 값(00 00)은 무시해도 됩니다.

3. 전력 한도를 설정하려면 다음과 같이 입력합니다.

주 - 전력 한도 설명 명령은 시스템의 전력 할당 한도를 설정합니다. 이 명령을 사용하여 최대 시스템 전원 사용량을 설정할 수 있습니다. 전력 한도는 AC 및 DC 순환에서 항상 유지되어야 합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -U username -P password raw 0x2e 0x4B 0x00 0xff 0xff 0xff 0x01
```

명령 완료 시

```
dc 00
```

다음 표는 전력 한도 설정(IPMIttool) 입력 및 출력 필드에 대해 설명합니다.

필드	바이트	설명
Input Data	1	Sun OEM 명령 그룹 번호: 0x2e
	2	명령 코드 0x4B는 전력 할당 설정을 설정합니다.
	3	그룹 확장 표시: 0x00. 이 필드의 값은 무시됩니다.
	4-6	예약 필드: 0xff 0xff 0xff. 이 필드의 값은 무시됩니다.
	7	예외 조치: 00 - 없음, 01 - 강제 전원 끄기
	8-9	전력 한도(와트)입니다. 예: 0x2a 0xaa
	10-13	정정 시간 제한(밀리초). 예: 0x00 0x00 0x1b 0x58. 시간 제한이 기본값으로 설정된 경우 이 값은 무시됩니다. 다음 바이트를 참조하십시오.
	14	시스템 기본 시간 제한을 사용할지 여부를 나타내는 플래그입니다. 정정 시간 제한 바이트 10-13은 무시됩니다. 0x00 - 기본값 아님, 0x01 - 기본값
	15	예약 필드: 0xff. 이 필드의 값은 무시됩니다.
16-17	예약 필드: 0x00 0x00. 이 필드의 값은 무시됩니다.	
Output Data	1	IPMIttool에서 사용하는 완료 코드입니다. 성공 완료 코드 상태는 표시되지 않지만 완료 코드 결과가 successful이 아닌 경우 실패 메시지가 나타납니다.
	2	명령 완료 시 그룹 확장 표시 'dc'가 나타납니다.

▼ 시스템 전원 정책 관리

주 - 이 절차에서 정의된 설정을 모든 서버 플랫폼에 적용할 수 있는 것은 아닙니다.

1. 현재 시스템 전원 정책을 가져오려면 다음과 같이 입력합니다.

```
$ ipmitool -I lan -H SP_hostname_or_IPaddress -U username -P password raw 0x2e 0x43 4
```

2. 전원 관리 정책을 performance로 설정하려면 다음과 같이 입력합니다.

```
$ ipmitool -I lan -H SP_hostname_or_IPaddress -U username -P password raw 0x2e 0x42
2 00 00 00 00
```

3. 전원 관리 정책을 elastic으로 설정하려면 다음과 같이 입력합니다.

```
$ ipmitool -I lan -H SP_hostname_or_IPaddress -U username -P password raw 0x2e 0x42
2 00 00 00 01
```

4. 전원 관리 정책을 disabled로 설정하려면 다음과 같이 입력합니다.

```
$ ipmitool -I lan -H SP_hostname_or_IPaddress -U username -P password raw 0x2e 0x42
2 00 00 00 02
```

다음 표는 전원 관리 정책 상태(IPMIttool) 입력 필드에 대해 설명합니다.

필드	바이트	설명
Input Data	1	Sun OEM 명령 그룹 번호: 0x2e
	2	명령 코드 0x42는 전원 정책 활성화 상태를 설정합니다.
	3	그룹 확장 표시: 2.
	4-6	예약 필드입니다.
	7	전원 정책 활성화 하위 명령: 00 - Performance 정책, 01 - Elastic 정책, 02 - 정책을 사용 안함으로 설정합니다.

▼ FRU 제조 세부정보 표시

- 관리 대상 장치에 FRU 제조 세부정보를 표시하려면 `fru print` 명령을 사용합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -v -I lanplus -U username -P password fru print
```

다음과 같은 출력이 표시될 수 있습니다.

```
FRU Device Description : Builtin FRU Device (ID 0)
Board Product          : ASSY,ANDY,4SKT_PCI-E,BLADE
Board Serial           : 00000000-7001
Board Part Number      : 501-7738-01
Board Extra             : AXX_RevE_Blade
Product Manufacturer   : ORACLE
Product Name           : ILOM
```

```
FRU Device Description : /SYS (ID 4)
Chassis Type           : Rack Mount Chassis
Chassis Part Number    : 541-0251-05
Chassis Serial         : 00:03:BA:CD:59:6F
Board Product          : ASSY,ANDY,4SKT_PCI-E,BLADE
Board Serial           : 00000000-7001
```

```
Board Part Number : 501-7738-01
Board Extra      : AXX_RevE_Blade
Product Manufacturer : ORACLE
Product Name     : SUN BLADE X8400 SERVER MODULE
Product Part Number : 602-0000-00
Product Serial   : 0000000000
Product Extra    : 080020ffffffffffff0003baf15c5a
```

```
FRU Device Description : /P0 (ID 5)
Product Manufacturer  : ADVANCED MICRO DEVICES
Product Part Number   : 0F21
Product Version       : 2
```

```
FRU Device Description : /P0/D0 (ID 6)
Product Manufacturer   : MICRON TECHNOLOGY
Product Name           : 1024MB DDR 400 (PC3200) ECC
Product Part Number    : 18VDDF12872Y-40BD3
Product Version        : 0300
Product Serial         : D50209DA
Product Extra          : 0190
Product Extra          : 0400
```

```
FRU Device Description : /P0/D1 (ID 7)
Product Manufacturer   : MICRON TECHNOLOGY
Product Name           : 1024MB DDR 400 (PC3200) ECC
Product Part Number    : 18VDDF12872Y-40BD3
Product Version        : 0300
Product Serial         : D50209DE
Product Extra          : 0190
Product Extra          : 0400
```

▼ Oracle ILOM 이벤트 로그 표시

- 관리 대상 장치에서 ILOM 이벤트 로그를 확인하려면 `sel list` 명령을 사용합니다.

```
$ ipmitool -H SP_hostname_or_IPaddress -I lanplus -U username -P password sel list
```

다음과 같은 출력이 표시될 수 있습니다.

```
100 | Pre-Init Time-stamp | Power Unit #0x78 | State Deasserted
200 | Pre-Init Time-stamp | Power Supply #0xa2 | Predictive Failure Asserted
300 | Pre-Init Time-stamp | Power Supply #0xba | Predictive Failure Asserted
400 | Pre-Init Time-stamp | Power Supply #0xc0 | Predictive Failure Asserted
500 | Pre-Init Time-stamp | Power Supply #0xb4 | Predictive Failure Asserted
600 | 04/05/2007 | 12:03:24 | Power Supply #0xa3 | Predictive Failure Deasserted
700 | 04/05/2007 | 12:03:25 | Power Supply #0xaa | Predictive Failure Deasserted
800 | 04/05/2007 | 12:03:25 | Power Supply #0xbc | Predictive Failure Deasserted
900 | 04/05/2007 | 12:03:26 | Power Supply #0xa2 | Predictive Failure Asserted
a00 | 04/05/2007 | 12:03:26 | Power Supply #0xa8 | Predictive Failure Deasserted
b00 | 04/05/2007 | 12:03:26 | Power Supply #0xb6 | Predictive Failure Deasserted
```

```

c00 | 04/05/2007 | 12:03:26 | Power Supply #0xbb | Predictive Failure Deasserted
d00 | 04/05/2007 | 12:03:26 | Power Supply #0xc2 | Predictive Failure Deasserted
e00 | 04/05/2007 | 12:03:27 | Power Supply #0xb0 | Predictive Failure Deasserted
f00 | 04/05/2007 | 12:03:27 | Power Supply #0xb5 | Predictive Failure Deasserted
1000 | 04/05/2007 | 12:03:27 | Power Supply #0xba | Predictive Failure Asserted
1100 | 04/05/2007 | 12:03:27 | Power Supply #0xc0 | Predictive Failure Asserted
1200 | 04/05/2007 | 12:03:28 | Power Supply #0xa9 | Predictive Failure Deasserted
1300 | 04/05/2007 | 12:03:28 | Power Supply #0xae | Predictive Failure Deasserted
1400 | 04/05/2007 | 12:03:28 | Power Supply #0xb4 | Predictive Failure Asserted
1500 | 04/05/2007 | 12:03:28 | Power Supply #0xbe | Predictive Failure Deasserted

```

IPMItool 유틸리티 및 명령 요약

IPMItool 유틸리티는 다음 사이트에서 다운로드할 수 있습니다.

<http://ipmitool.sourceforge.net/>

IPMItool 패키지를 설치한 후 설치된 매뉴얼 페이지에서 명령 사용법 및 구문에 대한 자세한 정보에 액세스할 수 있습니다. 다음 표는 사용 가능한 IPMItool 명령을 보여줍니다.

표 7 IPMItool 명령

IPMI 명령	기능
<code>sunoem sshkey set</code>	원격 셸 사용자에게 대한 SSH 키를 구성합니다.
<code>ipmitool sunoem sshkey del</code>	원격 셸 사용자에서 SSH 키를 제거합니다.
<code>ipmitool sunoem led get</code>	LED 상태를 읽습니다.
<code>ipmitool sunoem led set</code>	LED 상태를 설정합니다.
<code>ipmitool sunoem cli</code>	ILOM CLI를 직접 사용할 때와 마찬가지로 ILOM CLI 명령을 입력합니다. LAN/LANplus 인터페이스를 사용해야 합니다.
<code>ipmitool sunoem CLI force</code>	ILOM 3.0.10부터 force 옵션을 sunoem CLI 명령의 인수로 호출할 수 있습니다.
<code>ipmitool raw</code>	원시 IPMI 명령을 실행합니다.
<code>ipmitool lan print</code>	지정된 채널의 현재 구성을 인쇄합니다.
<code>ipmitool lan set (1) (2)</code>	지정된 채널에 대해 지정된 매개변수를 설정합니다.
<code>ipmitool chassis status</code>	시스템 쏘시 및 기본 전원 부속 시스템의 상위 레벨 상태에 대한 정보를 표시합니다.
<code>ipmitool chassis power</code>	쏘시 제어 명령을 수행하여 전원 상태를 확인하고 변경합니다.
<code>ipmitool chassis identify</code>	전면 패널 표시등을 제어합니다. 기본값은 15입니다. 끄려면 0을 사용합니다.
<code>ipmitool chassis restart_cause</code>	마지막으로 시스템이 다시 시작된 원인에 대해 쏘시를 질의합니다.
<code>ipmitool chassis bootdev (1)</code>	다음 재부트 시 대체 부트 장치에서 부트하도록 시스템에 요청합니다.
<code>ipmitool chassis bootparam (1)</code>	호스트 부트 매개변수를 설정합니다.
<code>ipmitool chassis selftest</code>	BMC 자체 테스트 결과를 표시합니다.

IPMI 명령	기능
ipmitool power	BMC 자체 테스트 결과를 반환합니다.
ipmitool event	미리 정의된 이벤트를 시스템 이벤트 로그에 보냅니다.
ipmitool sdr	SDR(Sensor Data Record)에 대해 BMC를 질의하고 지정된 유형의 정보를 추출한 다음 각 센서를 질의하고 해당 이름, 표시값 및 상태를 인쇄합니다.
ipmitool sensor	넓은 테이블 형식으로 센서 및 임계값을 나열합니다.
ipmitool fru print	모든 FRU(현장 대체 가능 장치) 부품 데이터를 읽고 일련 번호, 부품 번호, 자산 태그 및 새시, 보드 또는 제품을 설명하는 간단한 문자열과 같은 정보를 추출합니다.
ipmitool sel	ILOM SP SEL(시스템 이벤트 로그)을 표시합니다.
ipmitool pef info	BMC를 질의하고 PEF 지원 기능에 대한 정보를 인쇄합니다.
ipmitool pef status	현재 PEF 상태(BMC에서 마지막으로 처리한 SEL 항목 등)를 인쇄합니다.
ipmitool pef list	현재 PEF 상태(BMC에서 마지막으로 처리한 SEL 항목 등)를 인쇄합니다.
ipmitool user	최대 사용자 ID 수, 활성 사용자 수, 정의된 고정 이름 수 등 사용자 ID에 대한 요약 정보를 표시합니다.
ipmitool session	지정된 세션에 대한 정보를 가져옵니다. ID, 핸들 번호 또는 활성 상태로 세션을 식별하거나 키워드 "all"을 사용하여 모든 세션을 지정할 수 있습니다.
ipmitool firewall (1)	개별 명령 및 명령 하위 기능을 사용 또는 사용 안함으로 설정하고, 명령 및 명령 하위 기능을 지정된 구현에서 구성할 수 있는지 여부를 결정합니다.
ipmitool set (1)	세션 호스트 이름, 사용자 이름, 암호, 권한 레벨 등의 런타임 옵션을 설정합니다.
ipmitool exec	파일 이름에서 IPMItool 명령을 실행합니다. 각 라인이 하나의 전체 명령입니다.

SNMP 명령 예

설명	링크
SNMP 명령 예	<ul style="list-style-type: none">■ “snmpget 명령” [129]■ “snmpwalk 명령” [130]■ “snmpbulkwalk 명령” [131]■ “snmpstat 명령” [131]■ “snmpset 명령” [134]■ “snmptrapd 명령” [135]

관련 정보

- [SNMP 개요](#)
- [Oracle ILOM에서 SNMP 설정 구성](#)

snmpget 명령

```
snmpget SNMP_agent sysName.0
```

SNMPv2-MIB의 sysName.0 MIB 객체에 대한 설명에서 언급한 대로 이 명령은 이 관리 대상 노드에 대해 관리용으로 지정된 이름을 반환합니다. 규약에 따라 이 이름은 노드의 정규화된 도메인 이름입니다. 이름을 알 수 없는 경우에는 길이가 0인 문자열 값이 반환됩니다.

예를 들면 다음과 같습니다.

```
% snmpget SNMP_agent sysName.0 sysObjectID.0  
ilomCtrlDateAndTime.0  
SNMPv2-MIB::sysName.0 = STRING: SUNSPHOSTNAME  
SNMPv2-MIB::sysObjectID.0 = OID: SUN-HW-TRAP-MIB::products.200.2.1.1  
SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0 = STRING: 2013-07-23,13:31:53.0
```

이 명령은 sysName.0 객체 이외에 sysObjectID.0 및 ilomCtrlDateAndTime.0 MIB 객체의 콘텐츠를 표시합니다. 각 MIB 객체에 대해 응답의 일부로 MIB 파일 이름이 제공됩니다.

MIB 파일에서 가져오는 MIB 객체에 대한 설명은 다음과 같습니다.

- `sysName` - 이 관리 대상 노드에 대해 관리용으로 지정된 이름입니다. 규약에 따라 이 이름은 노드의 정규화된 도메인 이름입니다. 이름을 알 수 없는 경우에는 길이가 0인 문자열 값이 반환됩니다.
- `sysObjectID` - 엔티티에 포함된 네트워크 관리 부속 시스템에 대한 공급업체의 인가된 표시입니다. 이 값은 SMI 엔터프라이즈 하위 트리(1.3.6.1.4.1) 내에서 할당되며 관리할 "대상"을 확인하는 쉽고 명확한 의미를 제공합니다.
- `ilomCtrlDataAndTime` - 장치의 날짜 및 시간입니다.

snmpwalk 명령

snmpwalk 명령은 연결된 GETNEXT 요청의 시퀀스를 자동으로 수행합니다. 따라서 작업 단계가 줄어듭니다. 하위 트리의 각 객체 ID 또는 노드에 한 번씩 일련의 snmpgetnext 요청을 실행할 필요 없이 하위 트리의 루트 노드에서 snmpwalk 요청을 한 번 실행하여 하위 트리의 모든 노드에 대한 값을 가져올 수 있습니다.

예를 들면 다음과 같습니다.

```
% snmpwalk SNMP_agent system
SNMPv2-MIB::sysDescr.0 = STRING: ILOM machine custom description
SNMPv2-MIB::sysObjectID.0 = OID: SUN-HW-TRAP-MIB::products.200.2.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (16439826) 1 day, 21:39:58.26
SNMPv2-MIB::sysContact.0 = STRING: set via snmp test
SNMPv2-MIB::sysName.0 = STRING: SUNSPHOSTNAME
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: RFC1213-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module to describe generic objects
for network interface sub-layers
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP
implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing IP and ICMP
implementations
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing UDP
implementations
SNMPv2-MIB::sysORDescr.6 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.7 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB for Message Processing and
Dispatching.
```

```
SNMPv2-MIB::sysORDescr.9 = STRING: The management information definitions for
the SNMP User-based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (14) 0:00:00.14
```

snmpbulkwalk 명령

snmpbulkwalk 명령은 GETBULK SNMP 프로토콜 기능을 사용하여 네트워크 엔티티 정보에 대해 전체 트리를 질의합니다. 이 명령은 "반복기"를 지정하여 추가 객체를 패킷에 압축할 수 있습니다. 따라서 snmpbulkwalk 명령은 snmpwalk 명령보다 빠릅니다.

다음은 대략적인 시작 및 종료 시간 기록이 있는 snmpwalk 명령의 예입니다.

```
% date ; snmpwalk SNMP_agent entPhysicalTable >
/dev/null ; date
Sun Jun 30 18:15:38 EDT 2013
Sun Jun 30 18:16:46 EDT 2013
```

다음은 동일한 작업을 수행하는 snmpbulkwalk 명령의 예입니다. snmpbulkwalk 명령이 snmpwalk 명령보다 빠릅니다.

```
% date ; snmpbulkwalk SNMP_agent entPhysicalTable >
/dev/null ; date
Sun Jun 30 18:19:19 EDT 2013
Sun Jun 30 18:19:38 EDT 2013
```

snmptable 명령

snmptable 명령은 SNMP 테이블의 콘텐츠를 검색하여 테이블 형식, 즉 결과 출력이 검색하는 테이블과 비슷하게 한 번에 하나의 테이블 행으로 콘텐츠를 표시합니다. 이는 테이블의 콘텐츠를 한 번에 하나의 열에 표시하는 snmpwalk 명령과 대조적입니다.

다음은 snmptable 명령의 예입니다.

```
% snmptable SNMP_agent sysORTable
```

```

SNMP table: SNMPv2-MIB::sysORTable
sysORID          sysORDescr          sysORUpTime
IF-MIB::ifMIB    The MIB module to   0:0:00:00.01
describe generic objects
SNMPv2-MIB::snmpMIB The MIB module for SNMPv2 0:0:00:00.02
for network interface
entities.
TCP-MIB::tcpMIB  The MIB module for   0:0:00:00.02
sub-layers.
managing TCP
UDP implementations.
UDP-MIB::udpMIB  The MIB module for managing 0:0:00:00.02
RFC1213-MIB::ip  The MIB module for managing 0:0:00:00.02
implementations.
SNMP-VIEW-BASED-ACM- View-based Access Control 0:0:00:00.02
SNMP-FRAMEWORK-MIB:: The SNMP Management 0:0:00:00.14
IP and ICMP implementations.
MIB::vacmBasicGroup Model for SNMP.
snmpFrameworkMIB Architecture MIB.
Compliance
SNMP-MPD-MIB::snmp The MIB for Message 0:0:00:00.14
MPDCompliance Processing and Dispatching.
SNMP-USER-BASED-SM- The management information 0:0:00:00.14
MIB::usmMIBCompliance definitions for the SNMP
User-based Security Model.

```

주 - snmpget, snmpgetnext 및 snmpwalk 명령은 모든 유형의 MIB 객체에 사용할 수 있는 반면, snmptable 명령은 MIB 테이블 객체에만 사용할 수 있습니다. 이 명령에 다른 유형의 객체 ID가 지정된 경우에는 명령이 거부됩니다. 이 제한 사항은 tableEntry 객체, 테이블 열 객체 및 기타 테이블 내의 정보를 표시하는 모든 객체에 적용됩니다. snmptable 명령에는 MIB 테이블 객체 ID만 사용할 수 있습니다.

snmptable 명령의 예에는 -ci 및 -cb 옵션이 사용됩니다. 예를 들어 다음은 -ci 옵션이 있는 snmptable 명령의 예입니다.

```

% snmptable -ci SNMP_agent sunPlatFanTable
SNMP table: SUN-PLATFORM-MIB::sunPlatFanTable
index sunPlatFanClass
10          fan
11          fan
17          fan
23          fan
29          fan
30          fan
36          fan
42          fan

```

다음은 -ci 옵션이 없는 snmptable 명령의 예입니다. 인덱스 열은 표시되어 있지 않습니다.

```
% snmptable SNMP_agent sunPlatFanTable
SNMP table: SUN-PLATFORM-MIB::sunPlatFanTable
sunPlatFanClass
fan
fan
fan
fan
fan
```

다음은 -Ci 및 -Cb 옵션이 있는 snmptable 명령의 예입니다. 출력은 축약되어 있습니다.

```
% snmptable -Ci -Cb SNMP_agent entPhysicalTable
index          Descr          VendorType  ContainedIn
SNMP table: ENTITY  ?SNMPv2-      0          chassis
-MIB::entPhysical  SMI:zeroDotZero
1
Table
```

다음은 -Ci 옵션은 있지만 -Cb 옵션은 없는 동일한 snmptable 명령의 예입니다. 여기서도 출력이 축약되어 있습니다. 각 머리글에서 MIB 객체 이름이 반복됩니다.

```
% snmptable -Ci SNMP_agent entPhysicalTable
index          entPhysicalDescr  entPhysical  entPhysical
VendorType    ContainedIn
SNMP table: ENTITY  ?SNMPv2-      0          chassis
1
-MIB::entPhysical  SMI:zeroDotZero
```

다음은 -Ci 및 -Cb 옵션이 있는 snmptable 명령의 또 다른 예입니다. 각 머리글에서 MIB 객체 이름이 반복되지 않습니다.

```
% snmptable -Cb -Ci SNMP_agent ilomCtrlAlertsTable
SNMP table: SUN-ILOM-CONTROL-MIB::ilomCtrlAlertsTable
in- Sever- Type  Destin- Destin- SNMPVer- SNMP-Comm- Email  Email
dex ity   Type  ation-  ation-  sion    unityOr-  Event  Event
1   criti- email  ?      0.0.0.0 v1      public   none   none
IP   Email                               Username  Class   Type
cal
2-15 dis- ipmi- 0.0.0.0 ?      v1      public   ?      ?
Filter Filter
able  pet
```

따라서 snmptable 명령에 -Cb 옵션을 사용한 경우 테이블 출력을 읽기가 더 쉽습니다.

다음은 SNMP 프로토콜 버전 3을 사용하는 snmptable 명령의 예입니다.

```
% snmptable -Cb -Ci -mALL -v3 -aMD5 -utestuser -Apassword -lauthNoPriv
```

```
SNMP_agent:port sunPlatPowerSupplyTable
SNMP table: SUN-PLATFORM-MIB::sunPlatPowerSupplyTable
index sunPlatPowerSupplyClass
90          powerSupply
92          powerSupply
96          powerSupply
```

다음 snmptable 명령은 빈 테이블을 반환합니다.

```
% snmptable -Cb -Ci SNMP_agent sunPlatBatteryTable
SUN-PLATFORM-MIB::sunPlatBatteryTable: No entries
```

snmpset 명령

snmpset 명령은 snmpget 명령과 구문이 비슷하지만 명령 자체는 많이 다릅니다. snmpget 명령은 지정된 객체 ID 값을 읽기만 하는 반면, snmpset 명령은 객체 ID에 지정된 값을 기록합니다. 또한 SNMP 객체는 여러 데이터 유형을 지원하므로 snmpset 명령에서 객체 ID에 쓸 값과 함께 객체 ID의 데이터 유형도 지정해야 합니다.

다음 예에서는 snmpget 및 snmpset 명령을 함께 사용하는 방법을 보여줍니다. 단계의 순서는 다음과 같습니다.

1. snmpget 명령을 사용하여 MIB 객체의 현재 값을 확인합니다.
2. snmpset 명령을 사용하여 MIB 객체의 값을 변경합니다.
3. snmpget 명령을 사용하여 MIB 객체가 실제 요청된 값으로 변경되었는지 확인합니다.

```
% snmpget SNMP_agent ilomCtrlHttpEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: false(2)
% snmpset SNMP_agent ilomCtrlHttpEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: true(1)
% snmpget SNMP_agent ilomCtrlHttpEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: true(1)
```

개인 커뮤니티 대신 공개 커뮤니티를 사용하여 이 snmpset 명령을 실행하려고 하면 명령이 작동하지 않습니다. 개인 커뮤니티는 쓰기 권한이 있지만 공개 커뮤니티는 쓰기 권한이 없기 때문입니다. 명령에서 반환되는 Reason 코드는 객체가 쓰기 가능하지 않다는 점만 나타내므로 이러한 사항을 명확히 알 수 없습니다.

예를 들면 다음과 같습니다.

```
% snmpset SNMP_agent ilomCtrlHttpEnabled.0 i 1
Error in packet.
Reason: notWritable (That object does not support modification)
```

snmptrapd 명령

snmptrapd는 SNMP 트랩 및 정보 메시지를 받아서 기록하는 SNMP 응용 프로그램입니다. 시스템에서 이러한 메시지를 받으려면 이러한 메시지를 수신할 트랩 데몬을 구성해야 합니다.

트랩 데몬을 구성하려면 다음 작업을 수행하십시오.

1. SNMP 트랩 대상을 구성합니다.

다음 예에서는 snmpset 명령을 사용하여 snmptrapd 데몬을 구성하는 방법을 보여줍니다.

```
% snmpset SNMP_agent ilomCtrlAlertType.1 i 2 ilomCtrlAlertSeverity.1 i 2
ilomCtrlAlertDestinationIP.1 a dest_ipaddress ilomCtrlAlertDestinationPort.1 i
port_number ilomCtrlAlertSNMPCommunityOrUsername.1 s private
ilomCtrlAlertSNMPVersion.1 i 2
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.1 = INTEGER: snmptrap(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.1 = INTEGER: critical(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.1 = IPAddress: dest_ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationPort.1 = INTEGER: port_number
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPCommunityOrUsername.1 = STRING: private
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.1 = INTEGER: v2c(2)
```

2. 트랩 수신기 응용 프로그램 snmptrapd를 시작합니다.
3. 테스트 트랩을 생성하여 에이전트가 관리 대상 노드에서 트랩을 전송하고 트랩 수신기가 관리 스테이션에서 트랩을 수신하는지 확인합니다.

데몬이 실행되는 동안 SNMP 에이전트를 실행하는 호스트의 Oracle ILOM CLI에 로그인하여 다음 명령을 입력합니다.

```
-> set /SP/alertmgmt/rules/n testrule=true
```

주 - 트랩 데몬을 테스트하여 제대로 구성되었는지 확인해야 합니다.

다음 화면은 관리 스테이션에 testalert 트랩이 수신된 경우의 샘플 출력을 보여줍니다.

```
SUN-ILOM-CONTROL-MIB::ilom.103.2.1.20.0 = STRING: "This is a test trap"
```


색인

#UNSORTED

Active Directory, 44

DNS 로케이터 설정

확인 및 구성, 57

관리자 그룹

확인 및 구성, 49

대체 서버

확인 및 구성, 53

사용자 도메인

확인 및 구성, 52

사용자 정의 그룹

확인 및 구성, 51

운영자 그룹

확인 및 구성, 50

IPMI

ILOM CLI에서 사용, 114

ILOM 웹 인터페이스에서 사용, 114

ILOM에서 지원되는 버전, 111

IPMI PET(Platform Event Trap) 경고, 113

IPMI 관련 트랩 생성, 112

IPMItool 정보, 112

PET 경고, 113

개요, 111

사용자 역할, 113

서버 관리에 사용, 111

세부 사양

위치, 111

IPMItool

CLI 명령 실행, 116

FRU 정보 표시, 125

ILOM CLI 액세스, 116

ILOM 이벤트 로그 표시, 126

IPMItool 사용, 112

관리 작업, 118

기능, 112, 112

다운로드 사이트

위치, 112

단일 센서 표시, 119

도움말, 112

명령, 127

명령 스크립트 작성, 117

사용에 대한 요구 사항, 116

센서 목록 표시, 118

시스템 Power Budget 관리, 122

시스템 전원 정책 관리, 124

시스템 전원 켜기/끄기 및 종료, 121

요구 사항, 118

정보, 112

LDAP, 60

구성, 60

LDAP/SSL

관리자 그룹

MIB 객체, 65

확인 및 구성, 64

대체 서버

확인 및 구성, 69

사용자 도메인

확인 및 구성, 68

사용자 정의 그룹

확인 및 구성, 66

운영자 그룹

확인 및 구성, 65

인증서 설정, 63

MIB(Management Information Base)

ILOM에서 지원하는 표준 MIB, 15

MIB 트리, 13

정의, 13

Net-SNMP

웹 사이트, 11

PET 경고, 113

PET(Platform Event Traps), 113

RADIUS

- 구성, 71
 - Single Sign On
 - 구성, 43
 - 사용, 44
 - single sign on
 - 개요, 43
 - SMTP 클라이언트
 - MIB 객체, 83
 - 구성, 82
 - SNMP
 - ILOM을 지원하는 데 사용되는 MIB, 15
 - Net-SNMP
 - 웹 사이트, 11
 - 관리 대상 노드, 12
 - 관리 스테이션 모니터링, 12
 - 구문, 16, 16
 - 네트워크 관리 스테이션, 12
 - 자습서 웹 사이트, 11
 - 지원되는 기능, 12
 - 지원되는 버전, 11
 - SNMP 사용자 계정
 - CLI로 관리, 28
 - 대상, 등록 정보 및 값, 22
 - SNMP 트랩
 - 웹 인터페이스를 사용하여 대상 구성, 36
 - SPARC 부트 모드, 107
 - SPARC 진단, 102
 - SPARC 키 스위치, 109
 - SPARC 호스트 설정, 105
- ㄱ**
- 경고
 - 경고 관리에 필요한 CLI 명령, 28
 - 전자 메일 알림 생성, 82
 - 경고 규칙
 - CLI 명령, 28
 - 구성, 80
 - 구문 예
 - SNMP, 16
 - 구성 요소 정보
 - 보기, 76
- ㄴ**
- 사용자 계정, 42
- ㅇ**
- 시계 설정
 - NTP(Network Time Protocol) 구성, 77
 - 설정, 77
 - 시스템 경고
 - 관리에 필요한 명령, 28
- ㅇ**
- 원격 syslog 수신기 IP 주소
 - 구성, 79
 - 이벤트 로그
 - 구성, 78
- ㅈ**
- 전력 소비 관리
 - 전력 모니터링
 - snmpget 명령, 86
 - 전원 정책 확인 및 설정
 - SNMP 명령, 88, 98
 - 허용 전력 모니터링
 - snmpget 명령, 86
 - 전자 메일 경고 설정
 - 구성, 83
 - 중복성 설정
 - 확인 및 구성, 56
- ㅊ**
- 펌웨어
 - 확인 및 구성, 93