



XClarity Controller 3 사용 설명서



참고: 이 정보를 사용하기 전에 [부록 B "주의사항" 167페이지](#)의 일반 정보를 읽어보십시오.

초판 (2024년 10월)

© Copyright Lenovo 2024.

권리 제한 및 계약 고지: GSA(General Services Administration) 계약에 따라 제공되는 데이터 또는 소프트웨어를 사용, 복제 또는 공개할 경우에는 계약서 번호 GS-35F-05925에 명시된 계약 사항이 적용됩니다.

목차

목차	i	SSL 개요	39
제 1 장. 소개	1	SSL 인증서 취급	40
XClarity Controller Standard 및 Premier		SSL 인증서 관리	40
수준 기능	1	Secure Shell 서버 구성	41
XClarity Controller Standard 수준 기		KCS(키보드 컨트롤러 스타일)를 통한 IPMI	
능	2	액세스	41
XClarity Controller Premier 수준 기능	4	시스템 펌웨어 하위 수준 방지	41
XClarity Controller 업그레이드	6	SKM(보안 키 관리) 구성	42
웹 브라우저 및 운영 체제 요구사항	6	Security Password Manager	42
다국어 지원	7	확장된 감사 로그	42
MIB 소개	7	사용자 계정당 동시 로그인 제한	42
이 문서에서 사용된 주의사항	8	시스템 가드	42
제 2 장. XClarity Controller 웹 인		TLS 버전 지원	43
터페이스의 열기 및 사용	9	BMC 구성 백업 및 복원	44
XClarity Controller 웹 인터페이스 액세스	9	BMC 구성 백업	44
XClarity Provisioning Manager를 통한		BMC 구성 복원	44
XClarity Controller 네트워크 연결 설정	10	BMC를 공장 출하 기본값으로 재설정	44
XClarity Controller에 로그인	12	XClarity Controller 다시 시작	45
웹 인터페이스의 XClarity Controller 기능 설		제 4 장. 서버 상태 모니터링	47
명	13	상태 요약/활성 시스템 이벤트 보기	47
제 3 장. XClarity Controller 구		시스템 정보 보기	48
성	17	시스템 사용률 보기	50
사용자 계정/LDAP 구성	17	이벤트 로그 보기	51
사용자 인증 방법	17	감사 로그 보기	51
새 역할 만들기	17	유지 관리 내역 보기	52
새 사용자 계정 만들기	19	경고 수신자 구성	52
사용자 계정 삭제	21	제 5 장. 서버 구성	53
인증에 해시 암호 사용	21	어댑터 정보 및 구성 설정 보기	53
전역 로그인 설정 구성	23	시스템 부팅 모드 및 순서 구성	53
LDAP 구성	24	1회 부팅 구성	54
네트워크 프로토콜 구성	28	서버 전원 관리	54
이더넷 설정 구성	28	전원 중복성 구성	54
DNS 구성	30	전원 최대 가용량 사용 정책 구성	55
DDNS 구성	30	전력 복구 정책 구성	55
USB를 통한 이더넷 구성	31	전원 작업	56
SNMP 구성	32	IPMI 명령으로 소비 전력 관리 및 모니터링	57
IPMI 네트워크 액세스 활성화	32	서비스 데이터 로그 다운로드	59
IPMI 명령으로 네트워크 설정 구성	33	서버 속성	59
서비스 사용 및 포트 할당	33	위치 및 담당자 설정	59
액세스 제한 구성	33	서버 제한시간 설정	60
앞면 패널 USB 관리 포트 구성	34	침입 메시지	60
보안 설정 구성	35	솔루션 서비스	60
보안 대시보드	35	XClarity Controller 날짜 및 시간 설정	61
보안 모드	35	D3 V2 재시 구성	61
보안 모드 전환	39		

제 6 장. 원격 콘솔 기능	63
원격 콘솔 기능 사용	63
원격 전원 제어	64
원격 콘솔 캡처 화면	64
원격 콘솔 키보드 지원	64
원격 콘솔 화면 모드	65
미디어 탑재 방법	65
미디어 탑재 오류 문제	68
원격 콘솔 세션 종료	70
제 7 장. 스토리지 구성	71
스토리지 세부 정보.	71
RAID 설정.	71
가상 드라이브 보기 및 구성	71
스토리지 자원 명세 보기 및 구성	72
제 8 장. 서버 펌웨어 업데이트	75
펌웨어 업데이트 개요.	75
시스템, 어댑터, PSU 펌웨어 업데이트.	75
리포지토리에서 업데이트	76
제 9 장. 라이선스 관리	79
정품 인증 키 설치	79
정품 인증 키 제거	79
정품 인증 키 내보내기	80
제 10 장. 명령줄 인터페이스	81
명령줄 인터페이스 액세스.	81
명령줄 세션에 대한 로그인	81
직렬을 SSH로 방향 재지정 구성	81
명령 구문.	82
기능 및 제한사항	82
알파벳 명령 목록	83
유틸리티 명령.	85
exit 명령.	85
help 명령.	85
history 명령	85
모니터 명령.	85
clearlog 명령.	85
fans 명령.	86
mhlog 명령.	86
led 명령	87
readlog 명령	88
servicelog 명령.	90
syshealth 명령	91
temps 명령.	92
volts 명령	92
vpd 명령	93
서버 전원 및 제어 다시 시작 명령	93
power 명령	93
reset 명령	95

fuelg 명령	95
pxeboot 명령	96
구성 명령.	96
accseccfg 명령	96
asu 명령	97
backup 명령	100
dhcpinfo 명령	100
dns 명령	101
encaps 명령	102
ethtousb 명령	102
firewall 명령	103
hashpw 명령	104
ifconfig 명령	105
keycfg 명령	107
ldap 명령.	107
ntp 명령	109
portcontrol 명령	109
ports 명령	110
rdmount 명령.	111
restore 명령	112
roles 명령	112
rtd 명령	113
seccfg 명령.	113
securityinfo 명령	114
securitymode 명령	114
set 명령	114
snmp 명령	115
snmpalerts 명령	117
sshcfg 명령	118
sslcfg 명령	119
syslock 명령	121
thermal 명령	122
tls 명령	123
trespass 명령.	123
uefipw 명령	124
usbeth 명령	124
users 명령	125
IMM 제어 명령	128
batch 명령	128
clock 명령	129
info 명령.	130
spreset 명령	130
Agent-less 명령	130
storage 명령	131
adapter 명령	138
지원 명령.	140
dbgshbmc 명령	140

제 11 장. IPMI 인터페이스.	143
IPMI로 XClarity Controller 관리	143

IPMItool 사용	143
OEM 매개 변수가 있는 IPMI 명령	144
LAN 구성 매개 변수 가져오기/설정	144
OEM IPMI 명령	153
부록 A. 도움말 및 기술 지원 얻기	163
문의하기 전에	163
서비스 데이터 수집	164
지원팀에 문의	165
부록 B. 주의사항	167

상표	167
중요 참고사항	168
미립자 오염	168
통신 규제 취급방침	169
전자 방출 주의사항	169
대만 BSMI RoHS 준수 선언	170
대만 수입 및 수출 연락처 정보	170
색인	173

제 1 장 소개

Lenovo XClarity Controller 3(XCC3)는 Lenovo ThinkSystem 서버의 차세대 관리 컨트롤러입니다.

이 컨트롤러는 서버 시스템 보드의 단일 칩에 서비스 프로세서 기능, 슈퍼 입출력(I/O), 비디오 컨트롤러 및 원격 관리 기능을 통합합니다. 다음과 같은 기능을 제공합니다.

- 시스템 관리용 전용 또는 공유 이더넷 연결의 선택
- HTML5에 대한 지원
- XClarity 모바일을 통한 액세스의 지원
- XClarity 프로비저닝 관리자
- XClarity Essentials 또는 XClarity Controller CLI를 사용하여 원격 구성.
- 원격 또는 로컬로 XClarity Controller에 액세스할 수 있는 응용프로그램과 도구의 용량
- 향상된 원격 관리 성능
- 추가 웹 관련 서비스 및 소프트웨어 응용프로그램에 대한 REST API(Redfish schema) 지원

참고:

- XClarity Controller는 현재 Redfish Scalable 플랫폼 관리 API 사양 1.16.0 및 스키마 2022.2를 지원합니다.
- XClarity Controller 웹 인터페이스에서 BMC는 XCC를 참조하는 데 사용됩니다.
- 일부 ThinkSystem 서버에서는 전용 시스템 관리 네트워크 포트를 사용할 수 없습니다. 그런 서버의 경우에는 서버 운영 체제와 공유되는 네트워크 포트를 통해서만 XClarity Controller에 액세스할 수 있습니다.

이 문서에서는 ThinkSystem 서버에서 XClarity Controller의 기능을 사용하는 방법을 설명합니다. XClarity Controller는 XClarity 프로비저닝 관리자 및 UEFI와 함께 작동하여 ThinkSystem 서버에 대한 시스템 관리 성능을 제공합니다.

펌웨어 업데이트를 확인하려면 다음 단계를 완료하십시오.

참고: 처음으로 Support Portal에 액세스할 때는 서버의 제품 범주, 제품군 및 모델 번호를 선택해야 합니다. 다음에 Support Portal에 액세스할 때는 처음에 선택한 제품이 웹 사이트에 기본 설치되며, 제품에 대한 링크만 표시됩니다. 제품 목록을 변경 또는 추가하려면, 내 제품 목록 관리 링크를 클릭하십시오. 웹 사이트는 정기적으로 변경됩니다. 펌웨어 및 문서를 찾는 프로시저가 이 문서에 설명된 내용과 약간 다를 수 있습니다.

1. <http://datacentersupport.lenovo.com>으로 이동하십시오.
2. Support(지원)에서 Data Center(데이터 센터)를 선택하십시오.
3. 내용이 로드되면 Servers(서버)를 선택하십시오.
4. Select Series(시리즈 선택)에서 먼저 특정 서버 하드웨어 시리즈를 선택한 후 Select SubSeries(서브시리즈 선택)에서 특정 서버 제품 서브시리즈를 선택하고 마지막으로 Select Machine Type(시스템 유형 선택)에서 특정 시스템 유형을 선택하십시오.

XClarity Controller Standard 및 Premier 수준 기능

XClarity Controller와 함께 Standard 및 Premier 수준의 XClarity Controller 기능이 제공됩니다. 서버에 설치되는 XClarity Controller 기능의 수준에 대한 자세한 내용은 서버에 대한 설명서를 참조하십시오. 모든 수준에서 다음이 제공됩니다.

- 서버의 24시간 원격 및 관리

- 관리 서버의 상태에 관계 없이 원격 관리
- 하드웨어 및 운영 체제의 원격 제어

XClarity Controller Standard 수준 기능

다음은 XClarity Controller Standard 수준 기능의 목록입니다.

산업 표준 관리 인터페이스

- IPMI 2.0 인터페이스
- Redfish
- DCMI 1.5
- SNMPv3

기타 관리 인터페이스

- 웹
- SSH CLI
- 앞면 패널 USB - 모바일 장치의 가상 오퍼레이터 패널

전원/재설정 제어

- 전원 켜기
- 하드/소프트 종료
- 예약된 전원 제어
- 시스템 재설정
- 부팅 순서 제어

이벤트 로그

- IPMI SEL
- 읽을 수 있는 로그
- 감사 로그
- 미니 로그

환경 모니터링

- 무에이전트 모니터링
- 센서 모니터링
- 팬 제어
- LED 제어
- 칩셋 에러(Caterr, IERR 등)
- 시스템 상태 표시
- I/O 어댑터의 OOB 성능 모니터링
- 인벤토리 표시 및 내보내기

RAS

- 가상 NMI
- 자동 펌웨어 복구

- 백업 펌웨어의 자동 프로모션
- POST 감시 장치
- OS 로더 감시 장치
- OS Watchdog
- 블루 스크린 캡처(OS 오류, FFDC 기준)
- 내장 진단 도구
- 콜 홈

네트워크 구성

- IPv4
- IPv6
- IP 주소, 서브넷 마스크, 게이트웨이
- IP 주소 할당 모드
- 호스트 이름
- 프로그래밍 가능 MAC 주소
- 듀얼 MAC 선택(서버 하드웨어에서 지원되는 경우)
- 네트워크 포트 재할당
- VLAN 태깅

네트워크 프로토콜

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SSL
- SSH
- SMTP
- LDAP 클라이언트
- NTP
- SSDP
- LLDP

경보

- PET 트랩
- SNMP v1, v2c 및 v3 트랩
- 이메일
- Redfish 알림 구독

원격 존재

- 원격 DOC(Disk-On-Chip)(RDOC)

직렬 방향 재지정

- IPMI SOL
- 직렬 포트 구성(권한 및 속도 포함)
- 직렬 콘솔 버퍼(120s)

보안

- 비호스트 프로세서 CRTM
- 디지털 서명 펌웨어 업데이트
- RBAC(역할 베이스 액세스 제어)
- 로컬 사용자 계정
- LDAP/AD 사용자 계정
- 펌웨어의 보안 롤백
- NIST SP 800-131a
- 새시 침입 감지(서버 하드웨어에서 지원하는 경우)
- 안전하고 암호화된 프로토콜만 사용
- 구성 변경 및 서버 작업의 감사 로깅
- 공개 키(PK) 인증
- 시스템 사용 중지/용도 변경(RTD/ERTD)
- PFR 지원
- FIPS 140-3
- 보안 모드 및 보안 대시보드
- 안전한 암호 저장

전원 관리

- 실시간 전력계

Features on Demand

- 활성화 키 리포지토리

배치 및 구성

- 원격 구성
- OS 통과
- 내장 배치 및 구성 도구와 드라이버 팩
- 구성 파일 백업 및 복원
- 확장 RDOC 크기(MicroSD 카드 포함)
- 구성 가능한 열전도 프로필

펌웨어 업데이트

- 무에이전트 업데이트
- 원격 업데이트

XClarity Controller Premier 수준 기능

다음은 XClarity Controller Premier 수준 기능 목록입니다.

모든 "XClarity Controller Standard 수준 기능" 2페이지.

이벤트 로그

- 구성 요소 교체 로그

RAS

- 부팅 캡처
- 크래시 비디오 캡처

경보

- Syslog

원격 존재

- 원격 KVM
- 로컬 클라이언트 ISO/IMG 파일 마운팅
- 품질/대역폭 제어
- 원격 ISO/IMG 파일 http, Samba 및 NFS의 가상 미디어 탑재

직렬 방향 재지정

- SSH-CLI를 통한 직렬 방향 재지정

보안

- 싱글 사인온
- Security Key Lifecycle Manager(SKLM/KMIP)
- IP 주소 차단
- 엔터프라이즈급 강력한 보안 모드(CNSA 준수)
- 시스템 가드

전원 관리

- 전력 상한 제한
- OOB 성능 모니터링 - 시스템 성능 매트릭스
- 실시간 전력 그래픽
- 온도 그래픽

배치 및 구성

- 원격 OS 배포

펌웨어 업데이트

- 리포지토리와 동기화
- 시스템 팩 펌웨어 번들 업데이트
- MicroSD 카드의 로컬 리포지토리에서 펌웨어 롤백

XClarity Controller 업그레이드

서버가 Standard 수준의 XClarity Controller 펌웨어 기능과 함께 제공된 경우 서버의 XClarity Controller 기능을 업그레이드할 수도 있습니다. 사용 가능한 업그레이드 수준과 순서를 배열하는 방법에 대한 자세한 내용은 제 9 장 "라이선스 관리" 79페이지의 내용을 참조하십시오.

웹 브라우저 및 운영 체제 요구사항

이 주제의 정보를 사용하여 서버의 지원되는 브라우저, 암호 세트 및 운영 체제 목록을 봅니다.

XClarity Controller 웹 인터페이스에는 다음 웹 브라우저가 필요합니다.

- Chrome 64.0 이상(원격 콘솔의 경우 64.0 이상)
- Firefox ESR 78.0 이상
- Microsoft Edge 79.0 이상
- Safari 12.0 이상(iOS 7 이상 및 OS X)

참고: 모바일 장치 운영 체제의 브라우저에서는 원격 콘솔 기능이 지원되지 않습니다.

위에 열거된 브라우저는 현재 XClarity Controller 펌웨어가 지원하는 것과 일치합니다. XClarity Controller 펌웨어를 주기적으로 확장하여 다른 브라우저에 대한 지원을 포함할 수 있습니다.

XClarity Controller의 범웨어 버전에 따라서는 웹 브라우저 지원이 이 섹션에 열거된 브라우저마다 다를 수 있습니다. 현재 XClarity Controller에 있는 펌웨어에 지원되는 브라우저 목록을 확인하려면, XClarity Controller 로그인 페이지에서 지원되는 브라우저 메뉴 목록을 클릭하십시오.

보안 강화를 위해 HTTPS를 사용하는 경우 강한 암호만 지원됩니다. HTTPS를 사용하는 경우 클라이언트 운영 체제와 브라우저의 조합이 다음 암호 세트 중 하나를 지원해야 합니다.

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

참고: 인터넷 브라우저의 캐시는 나중에 빠르게 로드할 수 있도록 방문하는 웹 페이지에 대한 정보를 저장합니다. XClarity Controller 펌웨어를 플래시 업데이트한 후에는 XClarity Controller에서 검색하지 않고도 브라우저가 계속해서 캐시의 정보를 사용할 수 있습니다. XClarity Controller 펌웨어를 업데이트 한 후에는 브라우저 캐시를 지워 XClarity Controller를 통해 사용하는 웹 페이지가 올바르게 표시되는지 확인하는 것이 좋습니다.

다국어 지원

이 주제의 정보를 사용하여 XClarity Controller에서 지원하는 언어 목록을 봅니다.

XClarity Controller 웹 인터페이스에 선택되는 언어는 영어가 기본값입니다. 인터페이스는 다국어를 표시할 수 있습니다. 포함되는 언어는 다음과 같습니다.

- 프랑스어
- 독일어
- 이탈리아어
- 일본어
- 한국어
- 포르투갈어(브라질)
- 러시아어
- 중국어(간체)
- 스페인어(국제)
- 중국어(번체)

기본 설정 언어를 선택하려면 현재 선택된 언어 옆의 화살표를 클릭하십시오. 선호 언어를 선택할 수 있는 드롭다운 메뉴가 나타납니다.

XClarity Controller 펌웨어에서 생성한 텍스트 문자열은 브라우저가 지시하는 언어로 표시됩니다. 브라우저에서 위에 나열되어 있는 번역된 언어 중 하나가 아닌 언어를 지정하는 경우 텍스트가 영어로 표시됩니다. 또한, XClarity Controller 펌웨어에서 표시하지만 생성하지는 않은 모든 텍스트 문자열(예: UEFI, PCIe 어댑터 등에서 생성한 메시지)은 영어로 표시됩니다.

영어가 아닌 언어별 텍스트 입력(예: 침입 메시지)은 현재 지원되지 않습니다. 영어로 입력된 텍스트만 지원됩니다.

MIB 소개

이 섹션에서는 관리 정보 베이스에 액세스하는 방법을 알아봅니다.

SNMP MIB는 <https://support.lenovo.com/>(포털에서 머신 유형으로 검색)에서 다운로드할 수 있습니다. 포함된 4가지 MIB는 다음과 같습니다.

- SMI MIB는 Lenovo Data Center Group의 관리 정보 구조를 설명합니다.
- 제품 MIB는 Lenovo 제품의 개체 식별자를 설명합니다.
- XCC MIB는 Lenovo XClarity Controller에 대한 인벤토리 및 모니터링 정보를 제공합니다.
- XCC 경고 MIB는 Lenovo XClarity Controller가 감지한 경고 조건에 대한 트랩을 정의합니다.

참고: 4개의 MIB에 대한 가져오기 주문은 SMI MIB → 제품 MIB → XCC MIB → XCC 경고 MIB입니다.

이 문서에서 사용된 주의사항

다음 정보를 사용하여 이 문서에서 사용되는 주의사항을 이해하십시오.

다음과 같은 주의사항이 이 설명서에서 사용됩니다.

- **참고:** 이 주의사항은 중요 제안사항, 지침 또는 조언을 제공합니다.
- **중요:** 이 주의사항은 불편함이나 문제가 있는 상황을 방지하는 데 도움이 될 수 있는 정보 또는 조언을 제공합니다.
- **주의:** 이 주의사항은 프로그램, 장치 또는 데이터에 대한 잠재적 손상을 표시합니다. 주의 사항은 손상이 발생할 수 있는 지시사항 또는 상황 바로 앞에 부착되어 있습니다.

제 2 장 XClarity Controller 웹 인터페이스의 열기 및 사용

이 주제에서는 로그인 절차 및 XClarity Controller 웹 인터페이스에서 수행할 수 있는 작업에 대한 설명합니다.

XClarity Controller는 서비스 프로세서 기능, 비디오 컨트롤러 및 원격 관리 기능을 하나의 칩에 통합합니다. 원격으로 XClarity Controller에 액세스하려면 먼저 XClarity Controller 웹 인터페이스를 사용하여 로그인해야 합니다. 이 장에서는 로그인 절차 및 XClarity Controller 웹 인터페이스에서 수행할 수 있는 작업에 대한 설명합니다.

XClarity Controller 웹 인터페이스 액세스

이 주제의 정보는 XClarity Controller 웹 인터페이스를 통해 XClarity Controller에 액세스하는 방법을 설명합니다.

XClarity Controller는 BOOTP(Static Host Configuration Protocol) 및 DHCP(Dynamic Host Configuration Protocol) IPv4 주소 사용을 지원합니다. XClarity Controller에 할당된 기본 고정 IPv4 주소는 192.168.70.125입니다. XClarity Controller는 처음에 DHCP 서버에서 주소를 얻도록 구성되어 있으며, 주소를 확보할 수 없는 경우에는 고정 IPv4 주소를 사용합니다.

XClarity Controller에서는 IPv6 또한 지원합니다. 단, 기본값으로 특정된 고정 IPv6 IP 주소는 없습니다. IPv6 환경에서 처음으로 XClarity Controller에 액세스하는 경우에는 IPv4 IP 주소 또는 IPv6 링크 로컬 주소를 사용할 수 있습니다. XClarity Controller는 RFC4291에 설명된 바와 같이 48비트 MAC의 중간에 0xFF 및 0xFE의 16진수 값과 함께 2개의 8진수를 삽입하고 MAC 주소의 첫 번째 8진수 오른쪽에서 두 번째 비트를 뒤집은 IEEE 802 MAC 주소를 사용하여 고유 링크 로컬 IPv6 주소를 생성합니다. 예를 들어 MAC 주소가 08-94-ef-2f-28-af인 경우 링크 로컬 주소는 다음과 같습니다.

fe80::0a94:efff:fe2f:28af

XClarity Controller에 액세스하면 다음 IPv6 조건이 기본값으로 설정됩니다.

- 자동 IPv6 주소 자동 구성이 활성화됩니다.
- IPv6 고정 IP 구성이 비활성화됩니다.
- DHCPv6이 비활성화됩니다.
- 상태 비저장 자동 구성이 활성화됩니다.

XClarity Controller는 전용 시스템 관리 네트워크 연결(해당되는 경우) 또는 서버와 공유되는 연결의 사용을 선택할 수 있습니다. 랙 마운트 및 타워 서버의 기본 연결은 전용 시스템 관리 네트워크 커넥터를 사용하는 것입니다.

대부분의 서버에서는 별도의 1Gbit 네트워크 인터페이스 컨트롤러를 사용하여 전용 시스템 관리 네트워크를 연결합니다. 하지만 일부 시스템에서는 NCSI(Network Controller Sideband Interface)를 사용하여 멀티 포트 네트워크 인터페이스 컨트롤러의 네트워크 포트 중 하나에 전용 시스템 관리 네트워크를 연결할 수 있습니다. 이 경우 전용 시스템 관리 네트워크 연결은 10/100 속도의 사이드밴드 인터페이스로 제한됩니다. 시스템의 관리 포트 구현에 대한 정보 및 제한 사항은 시스템 설명서를 참조하십시오.

참고: 전용 시스템 관리 네트워크 포트는 서버에서 사용 가능하지 않을 수 있습니다. 하드웨어에 전용 네트워크 포트가 없는 경우 공유 설정은 사용 가능한 유일한 XClarity Controller 설정입니다.

XClarity Provisioning Manager를 통한 XClarity Controller 네트워크 연결 설정

이 주제의 정보를 사용하여 XClarity Provisioning Manager를 통한 XClarity Controller 네트워크 연결을 설정하십시오.

서버를 시작한 후에는 XClarity Provisioning Manager를 사용하여 XClarity Controller 네트워크 연결을 구성할 수 있습니다. XClarity Controller가 설치된 서버를 DHCP 서버에 연결하거나 XClarity Controller 네트워크 IP 주소를 사용하도록 서버 네트워크를 구성해야 합니다. Setup utility를 통해 XClarity Controller 네트워크 연결을 설정하려면, 다음 단계를 완료하십시오.

단계 1. 서버를 켜십시오. ThinkSystem 시작 화면이 표시됩니다.

참고: 서버가 AC 전원에 연결된 후 전원 제어 버튼이 활성화되려면 최대 40초까지 걸릴 수 있습니다.

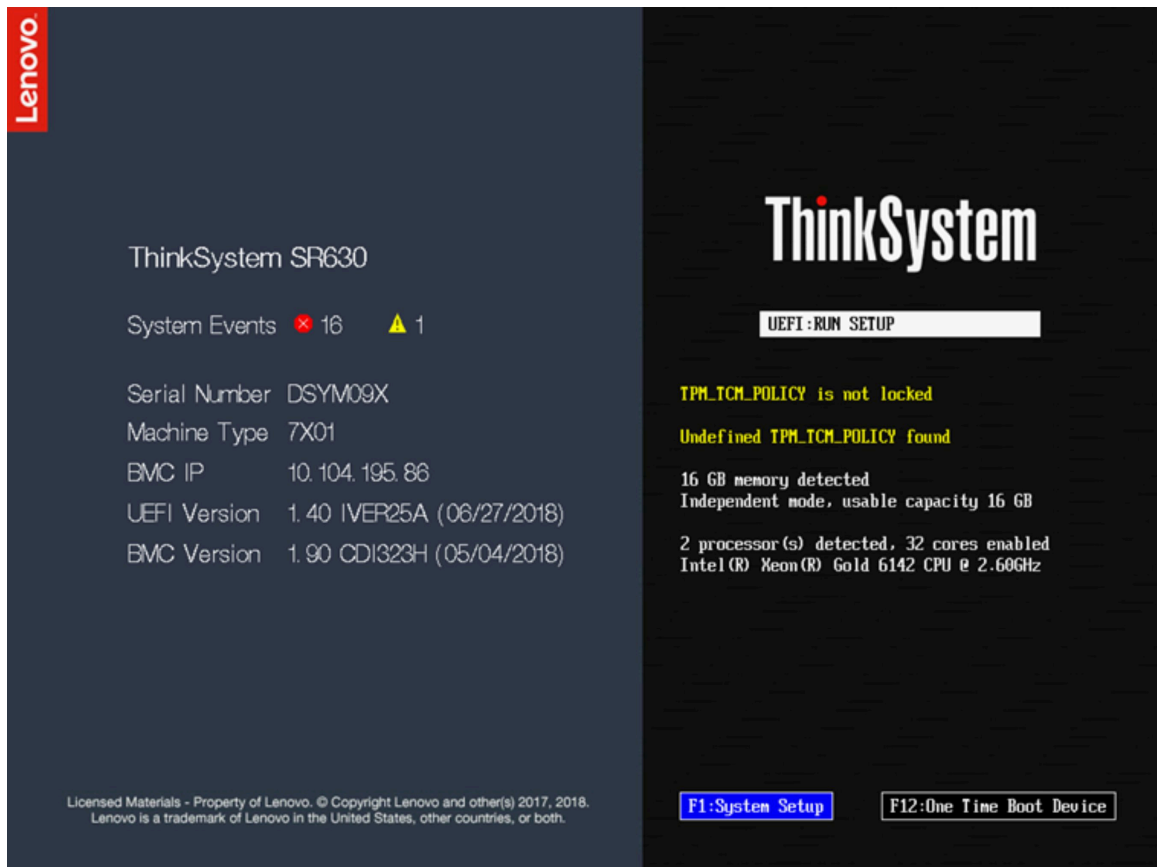


그림 1. ThinkSystem의 시작 화면

- 단계 2. <F1> System Setup 프롬프트가 표시되면 F1을 누르십시오. 시동 암호와 관리자 암호를 모두 설정한 경우 XClarity Provisioning Manager에 액세스하려면 관리자 암호를 입력해야 합니다.
- 단계 3. XClarity Provisioning Manager 기본 메뉴에서 UEFI Setup을 선택하십시오.
- 단계 4. 다음 화면에서 BMC Settings를 선택한 다음 Network Settings를 클릭하십시오.
- 단계 5. DHCP Control 필드는 3개의 XClarity Controller 네트워크 연결 선택사항이 있습니다.
 - 고정 IP

- DHCP 사용
- 폴백이 있는 DHCP

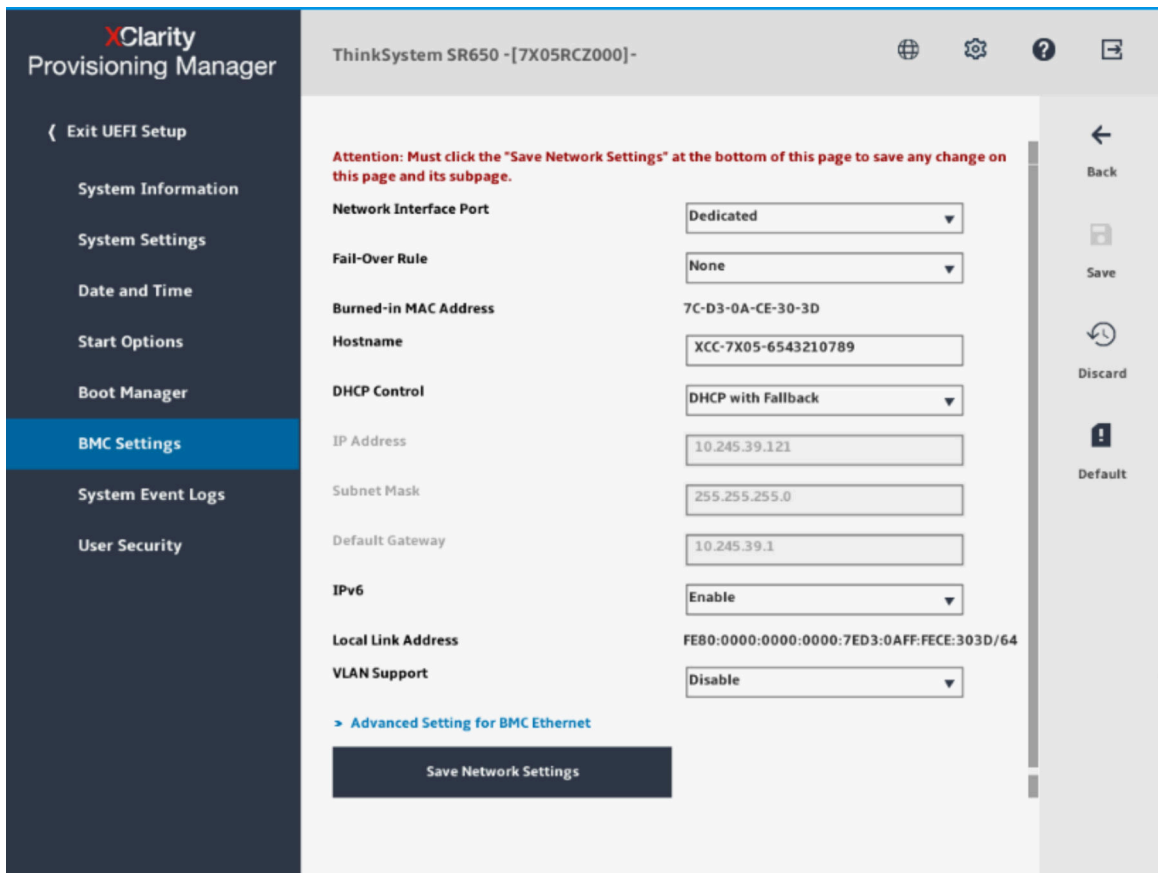


그림 2. 네트워크 연결 설정

- 단계 6. 네트워크 연결 선택사항 중 하나를 선택하십시오.
- 단계 7. 고정 IP 주소를 선택하는 경우에는 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 지정해야 합니다.
- 단계 8. 또한 Lenovo XClarity Controller Manager를 사용하여 전용 네트워크(전용 서버 네트워크 포트가 있는 경우) 또는 공유된 XClarity Controller 네트워크 연결을 선택할 수 있습니다.

참고:

- 서버에서 전용 시스템 관리 네트워크 포트를 사용 가능하지 않을 수 있습니다. 하드웨어에 전용 네트워크 포트가 없는 경우 공유 설정은 사용 가능한 유일한 XClarity Controller 설정입니다. Network Configuration 화면의 Network Interface Port 필드에서 Dedicated(해당되는 경우) 또는 Shared를 선택하십시오.
- XClarity Controller가 사용하는 서버의 이더넷 커넥터의 위치를 확인하려면, 서버와 함께 제공되는 설명서를 참조하십시오.

- 단계 9. 저장을 클릭하십시오.
- 단계 10. XClarity Provisioning Manager를 종료하십시오.

참고:

- 서버 펌웨어가 다시 작동하기 전에 약 1분 정도 기다려야 변경 사항이 적용됩니다.

- 또한 XClarity Controller 웹 인터페이스 또는 CLI(명령줄 인터페이스)를 통해 XClarity Controller 네트워크 연결을 구성할 수 있습니다. XClarity Controller 웹 인터페이스의 왼쪽 탐색 패널에서 BMC 구성을 클릭하고 네트워크를 선택하여 네트워크 연결을 구성할 수 있습니다. XClarity Controller CLI에서 설치 구성에 따라 다른 몇 개의 명령을 사용하여 네트워크를 구성할 수 있습니다.

XClarity Controller에 로그인

이 주제의 정보를 사용하여 XClarity Controller 웹 인터페이스를 통해 XClarity Controller에 액세스합니다.

중요: XClarity Controller는 처음에 사용자 이름 USERID 및 암호 PASSWORD(문자 O가 아니라 숫자 0 사용)를 사용하여 설정됩니다. 이 기본 사용자 설정은 감독자 액세스 권한을 가지고 있습니다. 보안 강화를 위해 초기 구성 중에 이 사용자 이름과 암호를 변경하십시오. 변경한 후에는 PASSWORD를 로그인 암호로 다시 설정할 수 없습니다.

XClarity Controller 웹 인터페이스를 통해 XClarity Controller에 액세스하려면 다음 단계를 완료하십시오.

- 단계 1. 웹 브라우저를 여십시오. 주소 또는 URL 필드에서 https:// 다음에 연결하려는 XClarity Controller의 IP 주소 또는 호스트 이름을 입력하십시오.
- 단계 2. 언어 드롭다운 목록에서 원하는 언어를 선택하십시오.

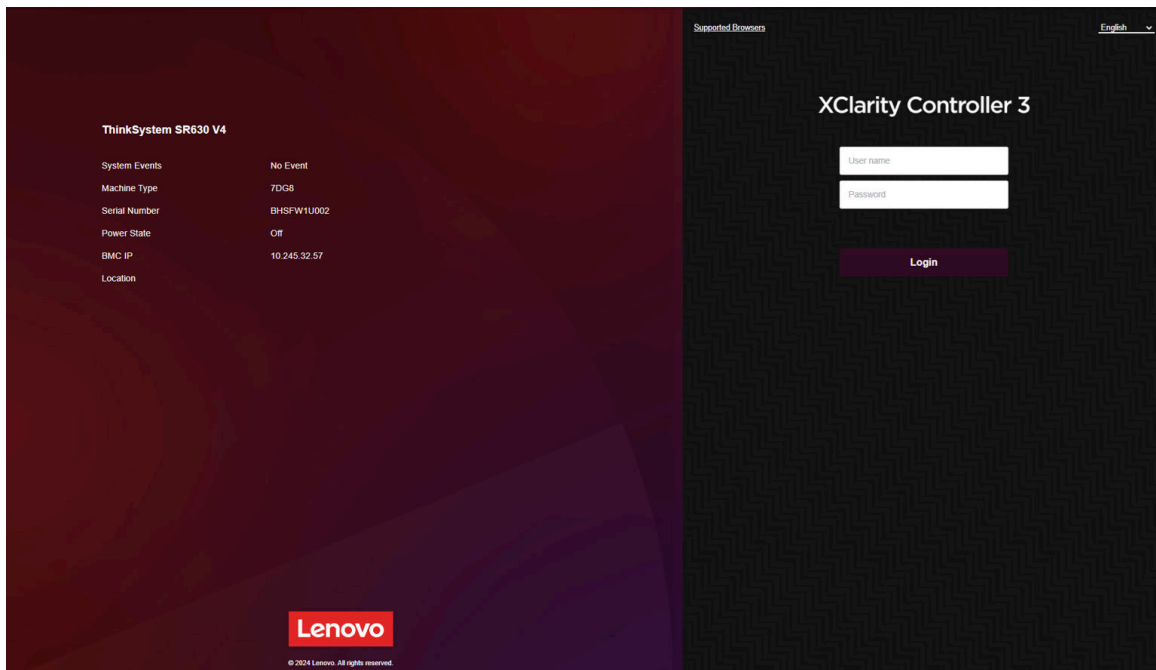




그림 3. 로그인 페이지

단계 3. XClarity Controller 로그인 창에 사용자 이름 및 암호를 입력하십시오. XClarity Controller를 처음으로 사용하는 경우 시스템 관리자로부터 사용자 이름 및 암호를 확인할 수 있습니다. 모든 로그인 시도는 이벤트 로그에 기록됩니다. 시스템 관리자가 사용자 ID를 구성하는 방법에 따라 로그인한 후에 새 암호를 입력해야 할 수 있습니다.

단계 4. 로그인을 클릭하여 세션을 시작합니다. 다음 그림에 표시된 것처럼 브라우저가 XClarity Controller 홈페이지를 엽니다. XClarity Controller가 현재 시스템에 얼마나 많은 위험

오류  및 경고 가 있는지 나타내는 플러스 아이콘을 관리하는 시스템 관련 정보가 홈페이지에 표시됩니다.

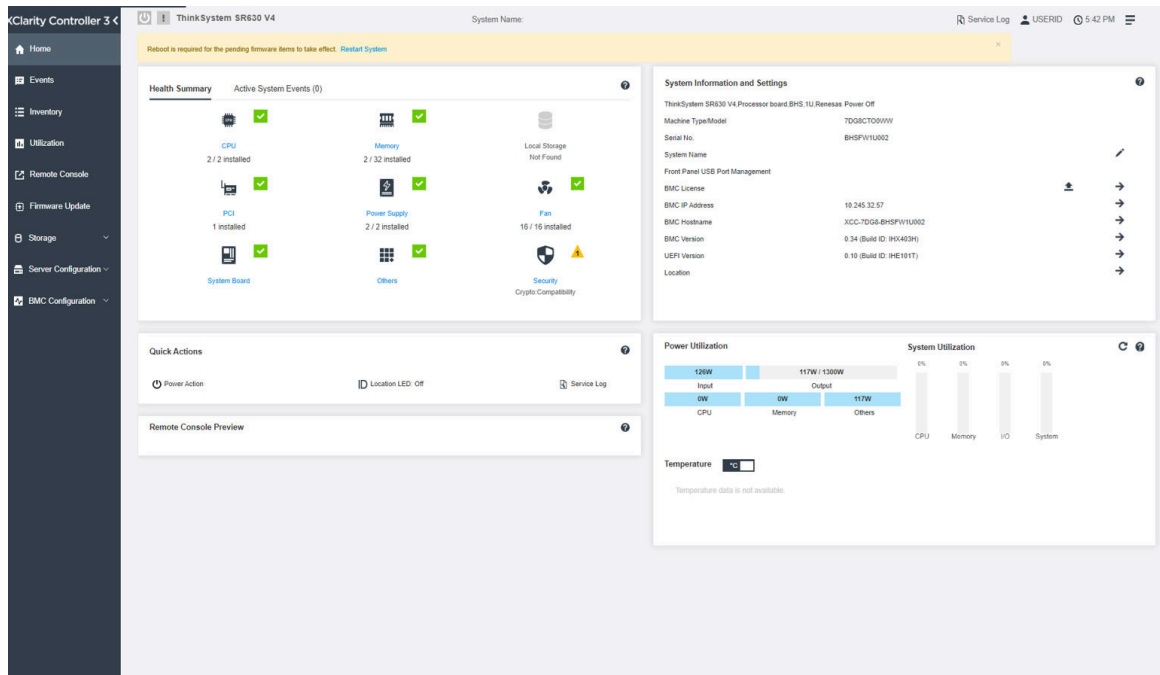


그림 4. 홈페이지

홈페이지는 기본적으로 2개의 섹션으로 나뉩니다. 첫 번째 섹션은 왼쪽 탐색 창으로 다음 작업을 수행할 수 있는 주제의 세트입니다.

- 서버 상태 모니터링
- 서버 구성
- XClarity Controller 또는 BMC 구성
- 펌웨어 업데이트

두 번째 섹션은 탐색 창의 오른쪽에 제공된 그래픽 정보입니다. 모듈 형식으로 서버 상태에 대한 간략히 보기와 수행할 수 있는 빠른 동작을 제공합니다.

웹 인터페이스의 XClarity Controller 기능 설명

이 항목의 정보는 웹 인터페이스의 XClarity Controller 기능에 대해 설명합니다.

다음은 왼쪽 탐색 창의 XClarity Controller 기능을 설명하는 표입니다.

참고: 웹 인터페이스를 탐색할 때 온라인 도움말의 물음표 아이콘을 클릭할 수도 있습니다.

탭	선택사항	설명
홈	상태 요약/활성 시스템 이벤트	시스템에서 주요 하드웨어 구성 요소의 현재 상태를 표시합니다.
	시스템 정보 및 설정	일반적인 시스템 요약 정보를 제공합니다.
	빠른 동작	서버 전원 및 위치 LED를 제어하는 빠른 링크와 서비스 데이터를 다운로드할 수 있는 버튼을 제공합니다.
	전력 사용률	현재 전력 사용률에 대한 간략한 개요를 제공합니다.
	원격 콘솔 미리보기	운영 체제 수준에서 서버를 제어하십시오. 컴퓨터에서 서버 콘솔을 보고 작동할 수 있습니다. XClarity Controller 홈 페이지의 원격 콘솔 섹션은 실행 버튼이 있는 화면 이미지를 표시합니다.
이벤트	이벤트 로그	모든 하드웨어 및 관리 이벤트의 기록 목록을 제공합니다.
	감사 로그	사용자 작업의 기록 레코드를 제공합니다.
	유지보수 내역	모든 펌웨어 업데이트, 구성 및 하드웨어 교체 기록을 표시합니다.
	경보 수신인 참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.	시스템 이벤트를 통지 받을 사람을 관리합니다. 개별 수신인을 구성하고 모든 이벤트 수신인에게 적용할 설정을 관리할 수 있습니다. 알림 구성 설정을 확인하기 위해 테스트 이벤트를 생성할 수도 있습니다.
인벤토리	CPU 페이지는 그 상태 및 키 정보와 함께 시스템의 모든 구성 요소를 표시합니다. 추가 정보를 표시할 장치를 클릭합니다. 참고: 솔루션 전원 상태에 대한 자세한 내용은 SMM3 웹 인터페이스를 참조하십시오.	
사용률	주변 온도, 구성 요소 온도, 전력 사용률, 전압 수준, 서버와 서버 구성 요소의 팬 속도 정보를 그래픽이나 표 형식으로 표시합니다.	
원격 콘솔	원격 콘솔 기능에 대한 액세스를 제공합니다. 가상 미디어 기능을 사용하여 시스템 또는 CIFS, NFS, HTTPS나 SFTP를 사용하는 BMC로 액세스할 수 있는 네트워크 위치에 있는 ISO 또는 IMG 파일 탑재할 수 있습니다. 탑재된 디스크는 서버에 연결된 USB 디스크 드라이브 또는 DVD ROM으로 나타납니다.	
펌웨어 업데이트	<ul style="list-style-type: none"> • 펌웨어 레벨을 표시합니다. • XClarity Controller 펌웨어 및 서버 펌웨어를 업데이트하십시오. • 리포지토리에서 XClarity Controller 펌웨어를 업데이트하십시오. 	
스토리지	세부사항	스토리지 장치의 물리적 구조 및 스토리지 구성이 표시됩니다.
	RAID 설정	가상 디스크 및 물리적 스토리지 장치 정보를 포함해 현재 RAID 구성을 보거나 수정합니다.

탭	선택사항	설명
서버 구성	어댑터	설치된 네트워크 어댑터 정보 및 XClarity Controller를 통해 구성될 수 있는 설정을 표시합니다.
	부팅 옵션	<ul style="list-style-type: none"> 다음에 서버가 다시 시작할 때 1회 부팅할 장치를 선택합니다. 부팅 모드 및 부팅 순서 설정을 변경합니다.
	전력 정책	<ul style="list-style-type: none"> 전원 공급 장치에 장애가 발생하면 전원 중복 장치를 구성합니다. 전력 상한 기능 정책을 구성합니다. 전력 복구 정책을 구성합니다. <p>참고: 솔루션 전원 상태에 대한 자세한 내용은 SMM3 웹 인터페이스를 참조하십시오.</p>
	서버 속성	<ul style="list-style-type: none"> 서버의 다양한 속성, 상태 조건 및 설정에 대한 액세스를 제공합니다. 서버 전원 끄기 지연을 관리합니다. 침입 메시지를 만듭니다. 침입 메시지는 사용자가 XClarity Controller에 로그인할 때 사용자에게 표시되도록 만들 수 있는 메시지입니다.
	새시 참고: 이 항목은 D3 V2 새시 호환 노드에서만 지원됩니다.	<ul style="list-style-type: none"> 새시 정보를 표시합니다. 노드를 다시 시작하거나 물리적 노드 재배포를 시뮬레이션합니다. 새시 관리자 선택 기본 설정을 표시합니다. 새시 유지보수 내역을 표시합니다.
BMC 구성	백업 및 복원	XClarity Controller의 구성을 공장 출하 기본값으로 다시 설정하거나 현재 구성을 백업 또는 파일에서 구성을 복원합니다.
	라이선스	옵션 XClarity Controller 기능의 정품 인증 키를 관리합니다.
	네트워크	XClarity Controller의 네트워크 속성, 상태 및 설정을 구성합니다.
	보안	XClarity Controller의 보안 속성, 상태 및 설정을 구성합니다.
	사용자/LDAP	<ul style="list-style-type: none"> XClarity Controller 로그인 프로파일 및 전체 로그인 설정을 구성합니다. 현재 XClarity Controller에 로그인한 사용자 계정을 봅니다. LDAP 탭은 하나 이상의 LDAP 서버에 사용할 사용자 인증을 구성합니다. 또한 LDAP 보안을 사용 또는 사용 안 함으로 설정하고 해당 인증서를 관리할 수 있습니다.
	콜 홈 참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.	콜 홈 옵션을 구성하여 시스템 관련 정보를 수집하고 서비스를 위해 Lenovo에 보냅니다.

제 3 장 XClarity Controller 구성

이 장의 정보를 사용하여 XClarity Controller 구성에 사용할 수 있는 옵션을 이해합니다.

XClarity Controller를 구성하면 다음의 주요 옵션을 사용할 수 있습니다.

- 백업 및 복원
- 라이선스
- 네트워크
- 보안
- 사용자/LDAP

사용자 계정/LDAP 구성

이 주제의 정보를 사용하여 사용자 계정을 관리하는 방법을 이해합니다.

BMC 구성의 사용자/LDAP를 클릭하여 사용자 계정을 작성, 수정 및 확인하고 LDAP 설정을 구성하십시오.

로컬 사용자는 XClarity Controller에 구성되고 현재 XClarity Controller에 로그인되어 있는 사용자 계정을 표시합니다.

LDAP 탭은 LDAP 서버에 보관되어 있는 사용자 계정에 액세스하기 위한 LDAP 구성을 표시합니다.

사용자 인증 방법

이 주제의 정보를 사용하여 XClarity Controller 서버가 로그인 시도를 인증하는 데 사용하는 모드를 이해합니다.

로그온 허용 옆의 드롭 다운 메뉴를 클릭하여 사용자 로그인 시도 인증 방법을 선택합니다. 다음 인증 방법 중 하나를 선택할 수 있습니다.

- 로컬 전용: XClarity Controller에 구성된 로컬 사용자 계정을 검색하면 사용자가 인증됩니다. 사용자 ID 및 암호가 일치하지 않는 경우 액세스가 거부됩니다.
- LDAP 전용: XClarity Controller는 LDAP 서버에 보관된 자격 증명으로 사용자를 인증하려고 시도합니다. XClarity Controller의 로컬 사용자 계정은 이 인증 방법으로 검색되지 않습니다.
- 로컬 먼저 LDAP 다음: 로컬 인증이 먼저 시도됩니다. 로컬 인증이 실패하면 LDAP 인증이 시도됩니다.
- LDAP 먼저, 로컬 사용자 다음: LDAP 인증이 먼저 시도됩니다. LDAP 인증이 실패하면 로컬 인증이 시도됩니다.

참고:

- 로컬로 관리되는 계정만 IPMI 및 SNMP 인터페이스와 공유됩니다. 이 인터페이스는 LDAP 인증을 지원하지 않습니다.
- IPMI 및 SNMP 사용자는 로그온 허용 필드를 LDAP 전용으로 설정하면 로컬로 관리되는 계정을 사용하여 로그인할 수 있습니다.

새 역할 만들기

이 주제의 정보를 사용하여 새 역할을 만듭니다.

역할 만들기

역할 탭을 클릭하고 만들기를 클릭하여 사용자 정의 역할을 만듭니다.

역할 이름 및 권한 수준 필드를 완료합니다. 권한 수준에 대한 자세한 내용은 다음 섹션을 참조하십시오.

생성된 역할은 사용자 섹션의 역할 드롭다운 메뉴에서 사용자에게 제공됩니다.

참고: 사용자 및 LDAP에 사용된 역할은 역할 이름을 편집 및 삭제할 수 없지만 해당 사용자 정의 권한을 수정할 수 있는 권한은 있습니다.

권한 수준

사용자 지정 역할은 다음 권한의 조합을 활성화할 수 있습니다.

구성 - 네트워킹 및 BMC 보안

사용자는 BMC 보안 및 네트워크 페이지에서 구성 매개 변수를 수정할 수 있습니다.

사용자 계정 관리

사용자가 사용자를 추가, 수정 또는 삭제하고 전역 로그인 설정을 변경할 수 있습니다.

원격 콘솔 액세스

사용자는 원격 콘솔에 액세스할 수 있습니다.

원격 콘솔 및 원격 디스크 액세스

사용자는 원격 콘솔 및 가상 미디어 기능에 액세스할 수 있습니다.

원격 서버 전원/다시 시작

사용자는 서버에 대한 전원 켜 및 다시 시작 기능을 수행할 수 있습니다.

구성 - 기본

사용자는 서버 속성 및 이벤트 로그에 대한 구성 매개 변수를 수정할 수 있습니다.

이벤트 로그를 지우는 기능

사용자는 이벤트 로그를 지울 수 있습니다. 누구나 이벤트 로그를 볼 수 있지만 로그를 지우려면 이 권한 수준이 필요합니다.

구성 - 고급(펌웨어 업데이트, BMC 다시 시작, 구성 복원)

사용자에게는 XClarity Controller를 구성하는 데 제한 사항이 없습니다. 또한 사용자는 관리를 위해 XClarity Controller에 액세스 권한이 있다고 할 수 있습니다. 관리 액세스 권한에는 펌웨어 업데이트, PXE 네트워크 부팅, XClarity Controller 공장 출하 기본값 복원, 구성 파일에서 XClarity Controller 설정 수정 및 복원, XClarity Controller 다시 시작/재설정과 같은 고급 기능이 포함되어 있습니다.

구성 - UEFI 보안

사용자는 UEFI 보안 설정을 수정할 수 있습니다.

사전 정의된 역할

다음 역할은 사전 정의되어 있으며 편집하거나 삭제할 수 없습니다.

관리자

관리자 역할은 제한 사항이 없으며 모든 작업을 수행할 수 있습니다.

읽기 전용

읽기 전용 역할은 서버 정보를 표시할 수 있지만 저장, 수정, 지우기, 재부팅 및 펌웨어 업데이트와 같이 시스템 상태에 영향을 주는 작업은 수행할 수 없습니다.

오퍼레이터

오퍼레이터 역할을 가진 사용자는 다음과 같은 권한을 가집니다.

- 구성 - 네트워킹 및 BMC 보안
- 원격 서버 전원/다시 시작
- 구성 - 기본
- 이벤트 로그를 지우는 기능
- 구성 - 고급(펌웨어 업데이트, BMC 다시 시작, 구성 복원)

새 사용자 계정 만들기

이 주제의 정보를 사용하여 새 로컬 사용자를 작성합니다.

사용자 작성

로컬 사용자 탭을 클릭하고 만들기를 클릭하여 새 사용자 계정을 만듭니다.

사용자 이름, 암호, 암호 확인을 완료한 후 드롭다운 메뉴에서 역할을 선택합니다. 역할에 대한 자세한 내용은 다음 섹션을 참조하십시오.

역할

다음 역할은 사전 정의되어 있으며 사용자의 필요에 따라 새로운 사용자 정의 역할을 생성할 수 있습니다.

관리자

관리자 역할은 제한 사항이 없으며 모든 작업을 수행할 수 있습니다.

읽기 전용

읽기 전용 역할은 서버 정보를 표시할 수 있지만 저장, 수정, 지우기, 재부팅 및 펌웨어 업데이트와 같이 시스템 상태에 영향을 주는 작업은 수행할 수 없습니다.

오퍼레이터

오퍼레이터 역할을 가진 사용자는 다음과 같은 권한을 가집니다.

- 구성 - 네트워킹 및 BMC 보안
- 원격 서버 전원/다시 시작
- 구성 - 기본
- 이벤트 로그를 지우는 기능
- 구성 - 고급(펌웨어 업데이트, BMC 다시 시작, 구성 복원)

SNMPv3 설정

사용자의 SNMPv3 액세스를 활성화하려면 해당 사용자 옆에 있는 편집 버튼을 클릭한 다음, 사용자 액세스 가능 인터페이스의 드롭다운 목록에서 SNMP를 체크하십시오. 다음 사용자 액세스 옵션이 설명됩니다.

액세스 유형

GET 작업만 지원됩니다. XClarity Controller는 SNMPv3 SET 작업을 지원하지 않습니다. SNMP3은 쿼리 작업만 수행할 수 있습니다.

인증 프로토콜

SNMPv3 보안 모델은 이 알고리즘을 인증하는 데 사용합니다. 지원되는 프로토콜은 다음과 같습니다.

- 없음
- HMAC-SHA(기본값)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384

- HMAC-SHA512

개인 정보 프로토콜

SNMP 클라이언트와 에이전트 간의 데이터 전송은 암호화를 사용하여 보호할 수 있습니다. 지원되는 메서드는 다음과 같습니다.

- 없음
- CBC-DES
- AES(기본값)
- AES192
- AES256
- AES192C
- AES256C

참고: SNMPv3 사용자가 반복적인 암호 문자열을 사용하는 경우에도 XClarity Controller에 계속 액세스할 수 있습니다. 참조를 위한 두 가지 예가 있습니다.

- 암호를 "11111111"(8개의 1이 포함된 8자리 숫자)로 설정한 경우 실수로 암호에 8개보다 많은 1을 입력해도 XClarity Controller에 액세스할 수 있습니다. 예를 들어 암호에 "1111111111"(10개의 1이 포함된 10자리 숫자)를 입력하는 경우 액세스가 허용됩니다. 반복되는 문자열이 동일한 키를 가진 것으로 간주됩니다.
- 암호를 "bertbert"로 설정한 경우 실수로 암호에 "bertbertbert"를 입력해도 사용자가 XClarity Controller에 액세스할 수 있습니다. 두 암호 모두 동일한 키로 간주됩니다.

자세한 내용은 Internet Standard of RFC 3414 문서의 **보안 고려사항**(<https://tools.ietf.org/html/rfc3414>)을 참조하십시오.

SSH 키

XClarity Controller는 SSH 공개 키 인증(RSA 키 유형)을 지원합니다. SSH 키를 로컬 사용자 계정에 추가하려면 해당 사용자 옆에 있는 편집 버튼을 클릭한 다음 사용자 액세스 가능 인터페이스의 드롭 다운 목록에서 SSH 키를 클릭하십시오. 다음의 두 가지 옵션이 제공됩니다.

키 파일 선택

SSH 키 파일을 선택하여 서버에서 XClarity Controller로 가져옵니다.

텍스트 필드에 키 입력

데이터를 SSH 키에서 텍스트 필드로 붙여넣거나 입력합니다.

참고:

- 일부 Lenovo 도구가 서버 운영 체제에서 실행되면 이 도구는 XClarity Controller에 액세스하기 위한 임시 사용자 계정을 만들 수 있습니다. 이 임시 계정은 볼 수 없으며 12가지 로컬 사용자 계정 위치를 사용하지 않습니다. 이 계정은 임의 사용자 이름(예: "20luN4SB") 및 암호로 만들어집니다. 이 계정은 USB를 통한 내부 이더넷 인터페이스상의 XClarity Controller에 액세스하는 데만 사용할 수 있으며 Redfish 및 SFTP 인터페이스용으로만 사용할 수 있습니다. 이 임시 계정 만들기 및 제거 작업뿐 아니라 이러한 자격 증명을 사용하는 도구에서 수행한 모든 작업은 감사 로그에 기록됩니다.
- SNMPv3 엔진 ID의 경우 XClarity Controller는 16진 문자열을 사용하여 ID를 나타냅니다. 이 16진 문자열은 기본 XClarity Controller 호스트 이름에서 변환됩니다. 다음의 예를 참조하세요.
호스트 이름 "XCC-7X06-S4AHJ300"이 먼저 ASCII 형식으로 변환됩니다. 88 67 67 45 55 88
48 54 45 83 52 65 72 74 51 48 48
ASCII 형식을 사용하여 16진 문자열이 빌드됩니다(사이의 공백은 무시). 58 43 43 2d 37 58 30 36
2d 53 34 41 48 4a 33 30 30

사용자 계정 삭제

이 주제의 정보를 사용하여 로컬 사용자 계정을 제거합니다.

로컬 사용자 계정을 삭제하려면 제거할 계정이 있는 행에서 휴지통 아이콘을 클릭하십시오. 권한이 부여된 경우 사용자 계정 관리 권한이 있는 유일한 계정만 아니면 자신의 계정 또는 다른 사용자의 계정을 제거할 수 있습니다.

인증에 해시 암호 사용

이 주제의 정보를 사용하여 인증에 해시 암호를 사용하는 방법을 이해하십시오.

암호와 LDAP/AD 사용자 계정을 사용하는 것 외에, XClarity Controller는 인증에 서드파티 해시 암호도 지원합니다. 특수 암호는 단방향 해시 (SHA256) 형식을 사용하며 XClarity Controller 웹, OneCLI 및 CLI 인터페이스에서 지원됩니다. 그러나 XCC SNMP, IPMI 및 CIM 인터페이스 인증에서는 서드파티 해시 암호를 지원하지 않습니다. OneCLI 도구 및 XCC CLI 인터페이스에서만 해시 암호가 있는 새 계정을 만들거나 해시 암호 업데이트를 수행할 수 있습니다. XClarity Controller는 해시 암호 읽기 기능을 사용하는 경우 OneCLI 도구 및 XClarity Controller CLI 인터페이스에서 해시 암호를 검색할 수도 있습니다.

XClarity Controller 웹을 통해 해시 암호 설정

BMC 구성에서 보안 을 클릭하고 Security Password Manager 섹션으로 스크롤하여 서드파티 암호 기능을 사용 또는 사용 안 함으로 설정하십시오. 이를 사용하는 경우, 서드파티 해시 암호가 로그인 인증에 사용됩니다. XClarity Controller에서 서드파티 해시 암호를 검색하는 기능도 사용 또는 사용 안 함으로 설정할 수 있습니다.

참고: 기본적으로 서드파티 암호 및 서드파티 암호 검색 허용 기능은 사용 안 함으로 설정됩니다.

사용자 암호가 기본 또는 서드파티 암호인지 확인하려면 BMC 구성에서 사용자/LDAP을 클릭하여 자세한 내용을 보십시오. 정보는 고급 속성 열에 있습니다.

참고:

- 서드파티 암호인 경우 사용자가 암호를 변경할 수 없으며, 암호 및 암호 확인 필드가 회색으로 표시됩니다.
- 서드파티 암호가 만료되면 사용자 로그인 프로세스 중에 경고 메시지가 표시됩니다.

OneCLI 기능을 통해 해시 암호 설정

- 기능 사용

```
$ sudo OneCli config set IMM.ThirdPartyPassword Enabled
```

- 해시 암호 만들기(Salt 없음). 다음은 password123 암호를 사용하여 XClarity Controller에 로그인하는 예를 보여 줍니다.

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
```

```
$ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

```
$ sudo OneCli config set IMM.Loginid.2 admin
```

```
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

- 해시 암호로 사용자 만들기(Salt 포함). 다음은 password123 암호를 사용하여 XClarity Controller에 로그인하는 예를 보여 줍니다. Salt=abc.

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
```

```
$ echo $pwhash 292bcbcb41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
```

```
$ sudo OneCli config set IMM.Loginid.3 Admin
```

```
$ sudo OneCli config set IMM.SHA256Password.3 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
```

- 해시 암호 및 salt 검색.

```
$ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled
$ sudo OneCli config show IMM.SHA256Password.3
$ sudo OneCli config show IMM.SHA256PasswordSalt.3
```

- 해시 암호 및 salt 삭제.

```
$ sudo OneCli config set IMM.SHA256Password.3 ""
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
```

- 해시 암호를 기존 계정으로 설정.

```
$ sudo OneCli config set IMM.Loginid.2 admin
$ sudo OneCli config set IMM.Password.2 Passw0rd123abc
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

참고: 해시 암호가 설정되는 동안 이 암호는 즉시 적용됩니다. 원래 표준 암호는 더 이상 유효하지 않습니다. 이 예에서는 해시 암호가 삭제될 때까지 원래의 표준 암호 Passw0rd123abc를 더 이상 사용할 수 없습니다.

CLI 기능을 통해 해시 암호 설정

- 기능 사용

```
> hashpw -sw enabled
```

- 해시 암호 만들기(Salt 없음). 다음은 password123 암호를 사용하여 XClarity Controller에 로그인하는 예를 보여 줍니다.

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
super
```

- 해시 암호로 사용자 만들기(Salt 포함). 다음은 password123 암호를 사용하여 XClarity Controller에 로그인하는 예를 보여 줍니다. Salt=abc.

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
$ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
> users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
-ssalt 'abc' -a super
```

- 해시 암호 및 salt 검색.

```
> hashpw -re enabled
> users -3 -ghp -gsalt
```

- 해시 암호 및 salt 삭제.

```
> users -3 -shp "" -ssalt ""
```

- 해시 암호를 기존 계정으로 설정.

```
> users -2 -n admin -p Passw0rd123abc -shp
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

참고: 해시 암호가 설정되는 동안 이 암호는 즉시 적용됩니다. 원래 표준 암호는 더 이상 유효하지 않습니다. 이 예에서는 해시 암호가 삭제될 때까지 원래의 표준 암호 Passw0rd123abc를 더 이상 사용할 수 없습니다.

해시 암호가 설정된 후에는 XClarity Controller에 로그인 할 때 이 암호를 사용하지 않습니다. 로그인할 때 일반 텍스트 암호를 사용해야 합니다. 아래 예에서와 같이 일반 텍스트 암호는 "password123"입니다.

```
$ pwhash = 'echo -n password123 | openssl dgst -sha256 | awk '{print $NF}''
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

```
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

전역 로그인 설정 구성

이 주제의 정보를 사용하여 모든 사용자에게 적용되는 로그인 및 암호 정책 설정을 구성합니다.

웹 비활성 세션 제한시간

이 주제의 정보를 사용하여 웹 비활성 세션 제한시간 옵션을 설정합니다.

웹 비활성 세션 제한시간 필드에서 비활성 웹 세션을 분리하기 전에 XClarity Controller가 대기하는 시간(분)을 지정할 수 있습니다. 최대 대기 시간은 1,440분입니다. 0으로 설정하면 웹 세션이 만료되지 않습니다.

XClarity Controller 펌웨어는 최대 6개의 웹 세션을 동시에 지원합니다. 다른 사람이 사용할 수 있도록 세션을 비우려면 세션을 비활성 제한시간에 의존하여 자동으로 세션을 닫기 보다는 마칠 때 웹 세션에서 로그아웃하는 것이 좋습니다.

참고: 자동으로 새로 고치는 XClarity Controller 웹 페이지에서 브라우저를 열린 상태로 두는 경우 웹 세션은 비활성으로 인해 자동으로 닫힙니다.

계정 보안 정책 설정

이 정보를 사용하여 서버의 계정 보안 정책을 이해하고 설정합니다.

다음 정보는 보안 설정의 필드에 대한 설명입니다.

처음 액세스할 때 암호 변경

기본 암호로 새 사용자를 설정한 후 이 확인란을 선택하면 해당 사용자가 처음 로그인할 때 암호를 변경하도록 요구합니다. 이 필드의 기본값은 확인란을 활성화하는 것입니다.

복잡한 암호 필요

이 옵션 상자는 기본적으로 선택되어 있으며 복잡한 암호는 다음 규칙을 준수해야 합니다.

- 다음 문자만 포함됨(공백 문자는 허용되지 않음): A-Z, a-z, 0-9, ~!@#\$%^&*()-+={}[]|:;'"<>,?/_
- 최소한 하나의 문자를 포함해야 합니다.
- 최소한 하나의 숫자를 포함해야 합니다.
- 다음 조합 중 두 개 이상이 포함되어야 합니다.
 - 하나 이상의 대문자.
 - 하나 이상의 소문자.
 - 하나 이상의 특수 문자.
- 다른 문자(특히 공백 또는 공백 문자)는 허용되지 않습니다.
- 암호에 동일한 문자를 연속해서 세 번 이상 사용해서는 안 됩니다(예: aaa).

- 암호는 사용자 이름과 동일할 수 없으며, 단순히 사용자 이름을 한 번 이상 반복하거나 사용자 이름의 역 문자 순서로 만들 수 있습니다.
- 암호는 최소 8자, 최대 255자여야 합니다.

옵션 상자를 선택하지 않은 경우 최소 암호 길이에 지정된 숫자를 0~255자로 설정할 수 있습니다. 최소 암호 길이가 0으로 설정된 경우 계정 암호가 비어 있을 수 있습니다.

암호 만료 기간(일)

이 필드에는 암호를 변경해야 하기 전에 허용되는 최대 암호 사용 기간이 포함됩니다.

암호 만료 경고 기간(일)

이 필드에는 암호가 만료되기 전에 사용자에게 경고하는 기간(일)이 포함됩니다.

최소 암호 길이(문자)

이 필드에는 암호의 최소 길이가 포함됩니다.

최소 암호 재사용 주기(횟수)

이 필드에는 다시 사용할 수 없는 이전 암호의 수가 포함됩니다.

최소 암호 변경 간격(시간)

이 필드에는 암호 변경과 변경 사이에 사용자가 기다려야 하는 기간이 포함됩니다.

최대 로그인 실패 횟수(회)

이 필드에는 사용자가 일정 기간 잠기기 전에 허용되는 로그인 시도 실패 횟수가 포함됩니다.

최대 로그인 실패 횟수 경과 후 로그아웃 시간(분)

이 필드에서는 길이(분)을 지정하며, XClarity Controller 서브시스템은 최대 로그인 실패 횟수가 된 후에 원격 로그인 시도를 비활성화합니다.

LDAP 구성

이 주제의 정보를 사용하여 XClarity Controller LDAP 설정을 보거나 변경하십시오.

LDAP 지원에는 다음이 포함됩니다.

- LDAP 프로토콜 버전 3(RFC-2251) 지원
- 표준 LDAP 클라이언트 API(RFC-1823) 지원
- 표준 LDAP 검색 필터 구문(RFC-2254) 지원
- 전송 계층 보안용 Lightweight Directory Access Protocol(v3) 확장(RFC-2830) 지원

LDAP 구현은 다음 LDAP 서버를 지원합니다.

- Microsoft Active Directory(Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode(Windows 2003, Windows 2008)
- Microsoft Lightweight Directory Service(Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Novell eDirectory Server, 버전 8.7 및 8.8
- OpenLDAP 서버 2.1, 2.2, 2.3, 2.4, 2.5 및 2.6

LDAP 탭을 클릭하여 XClarity Controller LDAP 설정을 보거나 수정하십시오.

XClarity Controller는 XClarity Controller 자체에 저장되는 로컬 사용자 계정 대신에 또는 로컬 사용자 계정 외에 중앙 LDAP 서버 통해 사용자의 액세스를 원격으로 인증할 수 있습니다. '로그인 권한 속성'

의 값을 사용하여 각 사용자 계정에 대해 권한을 지정할 수 있습니다. 또한 LDAP 서버를 사용하여 정상적인 사용자(암호 검사) 인증 외에 사용자를 그룹에 지정하고 그룹 인증을 수행할 수 있습니다. 예를 들어 XClarity Controller를 하나 이상의 그룹과 연결할 수 있으며, 사용자는 XClarity Controller와 연결된 하나 이상의 그룹에 속하는 경우에만 그룹 인증을 전달합니다.

LDAP 서버를 구성하려면 다음 단계를 완료하십시오.

1. LDAP 서버 정보에서는 항목 목록에서 다음 옵션을 사용할 수 있습니다.

- **인증의 경우에만 (로컬 인증으로) LDAP 서버 사용:** 이 옵션을 선택하면 XClarity Controller가 LDAP 서버에 대해 인증하고 그룹 구성원 정보를 검색하는 경우에만 자격 증명을 사용할 수 있습니다. 그룹 이름 및 역할은 로컬 권한 부여 그룹 섹션에서 구성할 수 있습니다.
- **인증과 권한 부여에 대해 LDAP 서버 사용:** 이 옵션을 선택하면 XClarity Controller가 LDAP 서버에 대해 인증하고 사용자 권한을 식별하는 데 모두 자격 증명을 사용할 수 있습니다.

참고: 인증에 사용할 LDAP 서버는 DNS SRV 기록을 통해 수동으로 구성하거나 동적으로 발견할 수 있습니다.

- **미리 구성된 서버 사용:** DNS가 활성화된 경우 각 서버의 IP 주소 또는 호스트 이름을 입력하여 최대 3개의 LDAP 서버를 구성할 수 있습니다. 각 서버의 포트 번호는 선택 사항입니다. 필드를 공백으로 두는 경우 비보안 LDAP 연결에 기본 값 389를 사용합니다. 보안 연결의 경우 기본 포트값은 636입니다. 하나 이상의 LDAP 서버를 구성해야 합니다.
- **DNS를 사용하여 서버 확인:** LDAP 서버를 동적으로 발견하도록 선택할 수 있습니다. RFC2782에서 설명된 메커니즘(서비스 위치 지정을 위한 DNS)을 사용하여 LDAP 서버를 찾습니다. 이를 DNS SRV라고 합니다. DNS SRV 요청에 도메인 이름으로 사용할 완전한 도메인 이름(FQDN)을 지정해야 합니다.
 - **AD 포레스트:** 교차 도메인에 유니버설 그룹이 있는 환경에서는 필수 전역 카탈로그(GC)를 검색하도록 포레스트 이름(도메인 집합)을 구성해야 합니다. 교차 도메인 그룹 멤버십이 적용되지 않는 환경에서는 이 필드를 비워둘 수 있습니다.
 - **AD 도메인:** DNS SRV 요청에 도메인 이름으로 사용할 완전한 도메인 이름(FQDN)을 지정해야 합니다.

보안 LDAP를 사용으로 설정하려는 경우 보안 LDAP 사용 확인란을 클릭하십시오. 보안 LDAP를 지원하려면 유효한 LDAP 인증서를 먼저 설치하고 하나 이상의 SSL 클라이언트에서 신뢰할 수 있는 인증서를 XClarity Controller로 가져와야 합니다. XClarity Controller 보안 LDAP 클라이언트가 호환되도록 하려면 LDAP 서버가 TLS(Transport Layer Security) 버전 1.2를 지원해야 합니다. 인증서 취급에 대한 자세한 내용은 "[SSL 인증서 취급](#)" 40페이지의 내용을 참조하십시오.

2. 추가 매개 변수에 정보를 입력하십시오. 다음은 매개 변수의 설명입니다.

LDAP 유형

LDAP 기반 인증을 위한 LDAP 서버 유형을 선택합니다. 다음 서버 유형을 사용할 수 있습니다.

- **OpenLDAP**
OpenLDAP
- **Active Directory**
디렉토리: Windows Active Directory
- **기타**
디렉토리: Apache Directory, eDirectory 등

바인딩 방법

LDAP 서버를 검색 또는 쿼리하기 전에 바인딩 요청을 보내야 합니다. 이 필드는 이 LDAP 서버 초기 바인딩을 수행하는 방법을 제어합니다. 다음 바인딩 방법을 사용할 수 있습니다.

- **구성된 자격 증명 사용**

이 방법을 사용하여 구성된 클라이언트 DN 및 암호로 바인딩합니다.

- **로그인 자격 증명 사용**

이 방법을 사용하여 로그인 프로세스 중에 제공된 자격 증명으로 바인딩합니다. 사용자 ID는 DN, 부분 DN, 정규화된 도메인 이름 또는 XClarity Controller에서 구성된 UID 검색 특성과 일치하는 사용자 ID를 통해 제공할 수 있습니다. 표시된 자격 증명이 부분 DN(예: cn=joe)과 비슷한 경우 이 부분 DN은 사용자 기록과 일치하는 DN을 만들려고 시도할 때 구성된 루트 DN에 접두어로 붙입니다. 바인딩 시도가 실패하면 로그인 자격 증명에 cn=을 접두어로 붙이고 결과 문자열을 구성된 루트 DN에 접두어로 붙여 마지막 시도를 합니다.

초기 바인딩이 성공하면 로그인하는 사용자에게 속한 LDAP 서버에서 항목을 찾기 위해 검색을 수행합니다. 필요한 경우 두 번째 바인딩 시도를 하는데, 이 때는 사용자의 LDAP 기록에서 검색한 DN과 로그인 프로세스 중에 입력한 암호를 사용합니다. 두 번째 바인딩 시도가 실패하면 사용자의 액세스가 거부됩니다. 두 번째 바인딩은 구성된 자격 증명 사용 바인딩 방법이 사용되는 경우에만 수행됩니다.

클라이언트 고유 이름

초기 바인딩에 사용할 클라이언트 고유 이름(DN)입니다. 최대 300자로 제한됩니다.

클라이언트 암호

이 고유 클라이언트의 암호입니다.

루트 DN

LDAP 서버에 있는 디렉토리 트리의 루트 항목에 대한 DN(루트 고유 이름)입니다(예: dn=mycompany,dc=com). 이 DN은 모든 검색 요청의 기본 개체로 사용됩니다.

사용자의 로그인 이름 검색 속성

바인딩 방법이 구성된 자격 증명 사용으로 설정된 경우 LDAP 서버에 대한 초기 바인딩 후 사용자의 DN, 로그인 권한 및 그룹 멤버십 등 사용자에게 대한 특정 정보를 검색하는 검색 요청을 합니다. 이 검색 요청은 해당 서버의 사용자 ID를 나타내는 속성 이름을 지정해야 합니다. 이 속성 이름은 이 필드에 구성됩니다. Active Directory 서버에서 속성 이름은 일반적으로 CN 또는 sAMAccountName입니다. Novell eDirectory 및 OpenLDAP 서버에서는 속성 이름이 일반적으로 uid입니다. 이 필드를 공백으로 둔 경우 기본값은 sAMAccountName입니다.

그룹 필터

그룹 필터: 이 필드는 그룹 인증에 사용됩니다. 사용자의 자격 증명이 확인되면 그룹 인증이 시도됩니다. 그룹 인증에 실패하면 사용자의 로그인 시도가 거부됩니다. 그룹 필터가 구성되면 XClarity Controller가 속한 그룹을 지정하는 데 사용됩니다. 즉 사용자는 그룹 인증을 위해 구성된 그룹 중 하나 이상의 그룹에 속해야 성공할 수 있습니다. 그룹 필터 필드를 공백으로 두는 경우 그룹 인증이 자동으로 성공합니다. 그룹 필터가 구성되면 목록의 그룹 하나 이상을 사용자가 속한 그룹과 일치시키는 시도를 합니다. 일치하지 않으면 사용자는 인증에 실패하고 액세스가 거부됩니다. 하나 이상 일치되는 경우 그룹 인증에 성공합니다.

비교는 대소문자를 구분합니다. 필터는 511자로 제한되며 하나 이상의 그룹 이름으로 구성할 수 있습니다. 여러 그룹 이름을 구분하려면 콜론(:) 문자를 사용해야 합니다. 앞 공백과 뒤 공백이 무시되지만 다른 공백은 그룹 이름의 일부로 취급됩니다.

참고: 기존의 와일드카드 문자(*)는 더 이상 와일드카드로 취급하지 않습니다. 와일드카드 개념은 보안 노출을 방지하기 위해 중단되었습니다. 그룹 이름은 전체 DN으로 또는 cn 부분만 사용하여 지정할 수 있습니다. 예를 들어 실제 DN 또는 adminGroup을 사용하여 DN이 cn=adminGroup, dc=mycompany, dc=com인 그룹을 지정할 수 있습니다.

그룹 멤버십 검색 속성

그룹 검색 속성 필드는 사용자가 속한 그룹을 식별하는 데 사용되는 속성 이름을 지정합니다. Active Directory 서버에서 속성 이름은 일반적으로 memberOf입니다. Novell eDirectory 서버에서 속성 이름은 groupMembership입니다. OpenLDAP 서버에서 사용자는 일반적으로 objectClass가 PosixGroup과 같은 그룹에 할당됩니다. 그러한 맥락에서 이 필드

는 PosixGroup의 멤버를 식별하는 데 사용되는 특성 이름을 지정합니다. 이 특성 이름이 memberUid입니다. 이 필드를 비워 두면 필터의 속성 이름은 기본적으로 memberOf가 됩니다.

로그인 권한 속성

사용자가 LDAP 서버를 통해 성공적으로 인증된 경우 해당 사용자에 대해 로그인 권한을 검색해야 합니다. 로그인 권한을 검색하려면 서버에 보낸 검색 필터가 로그인 권한과 연결된 특성 이름을 지정해야 합니다. 로그인 권한 속성 필드는 속성 이름을 지정합니다. 인증과 권한 부여에 대해 LDAP 서버를 사용하면서 이 필드를 공백으로 두면 해당 사용자는 액세스가 거부됩니다. LDAP 서버 검색에서 반환되는 속성 값은 13개의 연속된 0 또는 1로 입력된 비트 문자열이거나 총 13개의 연속된 0 또는 1로 입력된 비트 문자열이어야 합니다. 각 비트는 기능 집합을 나타냅니다. 비트는 위치에 따라 번호를 부여합니다. 가장 왼쪽 비트는 비트 위치 0이고 가장 오른쪽 비트는 비트 위치 12입니다. 비트 위치에 1이라는 값이 오면 해당 비트 위치와 관련된 기능을 활성화합니다. 비트 위치에 0이라는 값이 오면 해당 비트 위치와 관련된 기능을 비활성화합니다. 010000000000 문자열이 유효한 예이며, 어떤 필드에도 배치되도록 하는 데 사용됩니다. 사용되는 특성은 자유 형식 문자열이 가능해야 합니다. 속성이 성공적으로 검색되면 LDAP 서버가 반환하는 값은 다음 표의 정보에 따라 해석됩니다.

표 1. 권한 비트

비트 위치 설명이 포함된 3열 표.

비트 위치	기능	설명
0	항상 거부	사용자는 항상 인증에 실패합니다. 이 기능을 사용하여 특정 사용자를 차단하거나 특정 그룹과 연관된 사용자를 차단할 수 있습니다.
1	감독자 액세스	사용자에게 관리자 권한을 부여합니다. 사용자는 모든 기능에 대한 읽기/쓰기 권한을 가집니다. 이 비트가 설정된 경우 아래의 다른 비트를 개별적으로 설정할 필요가 없습니다.
2	읽기 전용 액세스	사용자는 읽기 전용 액세스 권한을 가지며, 유지보수 절차(예: 다시 시작, 원격 작업 또는 펌웨어 업데이트) 또는 수정 작업(저장, 지우기 또는 복원 기능)을 수행할 수 없습니다. 비트 위치 2 및 다른 모든 비트는 상호 배타적이며 비트 위치 2의 우선 순위가 가장 낮습니다. 다른 비트가 설정되면 이 비트는 무시됩니다.
3	구성 - 네트워크 및 BMC 보안	사용자는 보안, 네트워크 프로토콜, 네트워크 인터페이스, 포트 할당 및 직렬 포트 구성의 구성을 수정할 수 있습니다.
4	사용자 계정 관리	사용자는 사용자를 추가/수정/삭제하고 로그인 프로파일 창에서 전역 로그인 설정을 변경할 수 있습니다.
5	원격 콘솔 액세스	사용자는 원격 서버 콘솔에 액세스할 수 있습니다.
6	원격 콘솔 및 원격 디스크 액세스	사용자는 원격 서버 콘솔과 원격 서버의 원격 디스크 기능에 액세스할 수 있습니다.
7	원격 서버 전원/다시 시작 액세스	사용자는 원격 서버에 대한 전원 켜기 및 다시 시작 기능에 액세스할 수 있습니다.
8	구성 - 기본	사용자는 시스템 설정과 경고 패널에서 구성 매개 변수를 수정할 수 있습니다.
9	이벤트 로그를 지우는 기능	사용자는 이벤트 로그를 지울 수 있습니다. 참고: 모든 사용자가 이벤트 로그를 볼 수 있지만, 이벤트 로그를 지우려면 사용자에게 이 수준의 권한이 있어야 합니다.
10	구성 - 고급(펌웨어 업데이트, BMC 다시 시작, 구성 복원)	사용자에게는 XClarity Controller를 구성하는 데 제한 사항이 없습니다. 또한 사용자는 관리를 위해 XClarity Controller에 액세스할 수 있습니다. 사용자는 펌웨어 업그레이드, PXE 네트워크 부팅, 어댑터 공장 출하 기본값 복원, 구성 파일에서 어댑터 구성 수정 및 복원, 어댑터 다시 시작/재설정과 같은 고급 기능을 수행할 수 있습니다.

표 1. 권한 비트 (계속)

비트 위치	기능	설명
11	구성 - UEFI 보안	사용자는 UEFI 보안 관련 설정을 구성할 수 있습니다(UEFI F1 보안 설정 페이지에서도 구성 가능).
12	예약됨	나중에 사용하도록 예약되어 있으며 현재 무시됩니다.

비트가 설정되지 않은 경우 사용자 액세스가 거부됩니다

참고: 사용자 레코드에서 직접 검색한 로그인 권한에는 우선 순위가 부여됩니다. 사용자에게 해당 레코드에 대한 로그인 권한 속성이 없으면 사용자가 속한 그룹에서 사용 권한을 검색하고, 이 속성이 구성된 경우 그룹 필터와 일치하는 사용 권한을 검색합니다. 이 경우, 모든 그룹에 대한 모든 비트의 포함적 OR이 사용자에게 할당됩니다. 이와 마찬가지로 읽기 전용 액세스는 다른 모든 비트가 0인 경우에만 설정됩니다. 또한 어느 그룹에 항상 거부 비트가 설정된 경우 사용자는 액세스가 거부됩니다. 항상 거부 비트는 항상 다른 비트에 우선합니다.

중요: 사용자에게 기본, 네트워킹 및/또는 보안 관련 어댑터 구성 매개 변수를 수정하는 기능을 제공하는 경우 이 동일한 사용자에게 XClarity Controller를 다시 시작하는 기능(비트 위치 10)도 제공해야 합니다. 그렇게 하지 않으면 이 기능 없이 사용자는 매개 변수(예: 어댑터의 IP 주소)를 변경할 수 있지만 적용할 수 없습니다.

- 인증의 경우에만 (로컬 인증으로) LDAP 서버 사용 모드가 사용되는 경우 로컬 권한 부여 그룹을 구성합니다. 그룹 이름, 그룹 도메인 및 역할은 사용자 그룹에 대해 로컬 권한 부여를 제공하도록 구성됩니다. 각 그룹은 로컬 사용자의 역할에 구성된 것과 동일한 역할(권한)이 할당될 수 있습니다. 사용자 계정은 LDAP 서버의 다양한 그룹에 할당됩니다. BMC에 로그인하면 이 사용자 계정이 속한 그룹의 역할(권한)이 사용자 계정에 할당됩니다. 그룹 도메인은 고유 이름과 동일한 형식이어야 하며(예: dc=mycompany,dc=com) 그룹 검색의 기본 개체로 사용됩니다. 필드를 비워 두면 '루트 DN' 필드와 동일한 값이 사용됩니다. 추가 그룹은 '+' 아이콘을 클릭하여 추가하거나 'x' 아이콘을 클릭하여 삭제할 수 있습니다.
- 사용자 이름 표시에 사용되는 속성 지정 드롭 다운 메뉴에서 사용자 이름 표시에 사용되는 속성을 선택합니다.

네트워크 프로토콜 구성

이 주제의 정보를 사용하여 XClarity Controller의 네트워크 설정을 보거나 설정합니다.

이더넷 설정 구성

이 주제의 정보를 사용하여 XClarity Controller가 이더넷 연결을 통해 통신하는 방법을 보거나 변경합니다.

참고: AMD 서버는 이더넷 장애 조치 기능을 지원하지 않습니다.

XClarity Controller는 네트워크 컨트롤러 두 개를 사용합니다. 네트워크 컨트롤러 하나는 전용 관리 포트에 연결되고, 다른 네트워크 컨트롤러는 공유 포트에 연결됩니다. 각 네트워크 컨트롤러는 자체 번인(burn-in)된 MAC 주소로 할당됩니다. DHCP를 사용하여 XClarity Controller에 IP 주소를 할당하는 경우 사용자가 네트워크 포트 간에 전환하거나 전용 네트워크 포트에서 공유 네트워크 포트에 장애 조치 발생하면 DHCP 서버가 XClarity Controller에 다른 IP 주소를 할당할 수 있습니다. DHCP를 사용하는 경우 사용자는 IP 주소를 사용하는 대신 호스트 이름을 사용하여 XClarity Controller에 액세스해야 합니다. XClarity Controller 네트워크 포트가 변경되지 않은 경우에도 DHCP 임대가 만료되거나 XClarity Controller가 재부팅되면 DHCP 서버가 XClarity Controller에 다른 IP 주소를 할당할 수 있습니다. 사용자가 변경되지 않는 IP 주소를 사용하여 XClarity Controller에 액세스해야 하는 경우 XClarity Controller는 DHCP가 아닌 고정 IP 주소로 구성되어야 합니다.

BMC 구성의 네트워크를 클릭하여 XClarity Controller 이더넷 설정을 수정하십시오.

XClarity Controller 호스트 이름 구성

기본 XClarity Controller 호스트 이름은 문자열 "XCC -"에 서버 시스템 유형 및 서버 일련 번호의 조합을 사용하여 생성됩니다(예, "XCC-7X03-1234567890"). 이 필드에 최대 63자를 입력하여 XClarity Controller 호스트 이름을 변경할 수 있습니다. 호스트 이름에는 마침표가 포함되어서는 안 되며 알파벳, 숫자, 하이픈 및 밑줄 문자만 포함됩니다.

이더넷 포트

이 설정은 공유 및 전용 포트를 포함하여 관리 컨트롤러에서 사용하는 이더넷 포트의 활성화를 제어합니다.

사용 안 함으로 설정 시, 모든 이더넷 포트에 IPv4 또는 IPv6 주소가 할당되지 않으며 이더넷 구성에 대한 추가 변경을 방지합니다.

참고: 이 설정은 USB LAN 인터페이스 또는 서버 앞면의 USB 관리 포트에 영향을 주지 않습니다. 이러한 인터페이스에는 고유한 전용 활성화 설정이 있습니다.

IPv4 네트워크 설정 구성

IPv4 이더넷 연결을 사용하려면 다음 단계를 완료하십시오.

1. IPv4 옵션을 활성화하십시오.

참고: 이더넷 인터페이스를 비활성화하면 외부 네트워크에서 XClarity Controller에 액세스할 수 없습니다.

2. 방법 필드에서 다음 옵션 중 하나를 선택하십시오.

- DHCP에서 IP 확보: XClarity Controller는 DHCP 서버에서 IPv4 주소를 확보합니다.
- 고정 IP 주소 사용: XClarity Controller는 IPv4 주소의 사용자 지정값을 사용합니다.
- DHCP 먼저, 고정 IP 주소 다음: XClarity Controller는 DHCP 서버에서 IPv4 주소를 확보하려고 시도하지만, 그러한 시도가 실패하면 XClarity Controller는 IPv4 주소의 사용자 지정값을 사용합니다.

3. 고정 IPv4 주소 필드에서 XClarity Controller에 할당할 IP 주소를 입력하십시오.

참고: IP 주소에는 공백이 없고 마침표로 분리된 0~255 사이의 정수 4개가 포함되어야 합니다. 방법이 DHCP에서 IP 확보로 설정되면 이 필드를 구성할 수 없습니다.

4. 네트워크 마스크 필드에서 XClarity Controller가 사용하는 서브넷 마스크를 입력하십시오.

참고: 서브넷 마스크에는 공백이나 연속적인 마침표가 없고 마침표로 분리된 0~255 사이의 정수 4개가 포함되어야 합니다. 기본 설정은 255.255.255.0입니다. 방법이 DHCP에서 IP 확보로 설정되면 이 필드를 구성할 수 없습니다.

5. 기본값 게이트웨이 필드에서 네트워크 게이트웨이 라우터를 입력하십시오.

참고: 게이트웨이 주소에는 공백 또는 연속적인 마침표가 없고 0~255 사이의 정수 4개가 포함되어야 합니다. 방법이 DHCP에서 IP 확보로 설정되면 이 필드를 구성할 수 없습니다.

고급 이더넷 설정 구성

고급 이더넷 탭을 클릭하여 추가 이더넷 설정을 설정합니다.

VLAN(Virtual LAN) 태깅을 활성화하려면 VLAN 사용 확인란을 선택하십시오. VLAN이 활성화되고 VLAN ID가 구성되면, XClarity Controller는 지정된 VLAN ID가 있는 패킷만 수락합니다. VLAN ID는 1~4094의 숫자값으로 구성할 수 있습니다.

MAC 주소 목록에서 다음 선택사항 중 하나를 선택할 수 있습니다.

- 번인(burned-in) MAC 주소 사용

변인 MAC 주소 옵션은 제조업체에 의해 이 XClarity Controller에 할당된 고유 물리적 주소입니다. 이 주소는 읽기 전용 필드입니다.

- 사용자 지정 MAC 주소 사용

값이 지정되면, 로컬로 관리되는 주소가 변인 MAC 주소를 대체합니다. 로컬로 관리되는 주소는 hexadecimal value from 000000000000~FFFFFFFFFFFF의 진수 값입니다. 이 값은 xx:xx:xx:xx:xx:xx 형식이어야 하며, 여기서 x는 0~9 또는 "a"~"f"의 진수값입니다. XClarity Controller는 멀티캐스트 주소의 사용을 지원하지 않습니다. 멀티캐스트 주소의 첫 번째 바이트는 홀수이며(최소의 유의미한 비트는 1로 설정됩니다), 따라서 첫 번째 바이트는 짝수이어야 합니다.

데이터 전송 속도 및 양방향 필드에서 자동 교섭 또는 사용자 지정을 선택하여 데이터 전송 속도 및 양방향을 지정합니다.

MTU(최대 전송 단위) 필드에서 네트워크 인터페이스의 패킷의 최대 전송 단위(바이트 단위)를 지정하십시오. 최대 전송 단위 범위는 1000~1500입니다. 이 필드의 기본값은 1500입니다.

IPv6 네트워크 설정 구성

1. IPv6 옵션을 활성화하십시오.
2. 다음 할당 방법 중 하나를 사용하여 IPv6 주소를 인터페이스에 할당할 수 있습니다.
 - 상태 비저장 주소 자동 구성 사용
 - 상태 저장 주소 구성 사용(DHCPv6)
 - 정적으로 할당된 IP 주소 사용

참고: 통계적으로 할당된 IP 주소 사용을 선택하면, 다음 정보를 입력해야 합니다.

- IPv6 주소
- 접두사 길이
- 게이트웨이

DNS 구성

이 주제의 정보를 사용하여 XClarity Controller DNS(Domain Name System) 설정을 보거나 변경합니다.

BMC 구성의 네트워크를 클릭하여 XClarity Controller DNS 설정을 보거나 수정하십시오.

추가 DNS 주소 서버 사용 확인란을 클릭한 경우 네트워크에서 도메인 이름 시스템 서버 최대 3개의 IP 주소를 지정하십시오. 각 IP 주소에는 마침표로 분리된 0~255 사이의 정수 4개가 포함되어야 합니다. 이 DNS 서버 주소를 검색 목록 상단에 추가하기 때문에 호스트 이름 조회는 DHCP 서버가 자동으로 할당하는 DNS 서버에서 이루어지기 전에 이러한 서버에서 이루어집니다.

DNS를 사용해 Lenovo XClarity Administrator 검색 확인란을 클릭한 경우 XClarity Manager를 선택해야 합니다.

DDNS 구성

이 주제의 정보를 사용하여 XClarity Controller의 DDNS(Dynamic Domain Name System) 프로토콜을 활성화 또는 비활성화합니다.

BMC 구성의 네트워크를 클릭하여 XClarity Controller DDNS 설정을 보거나 수정하십시오.

DDNS 활성화 확인란을 클릭하여 DDNS를 활성화하십시오. DDNS가 사용되면 XClarity Controller는 XClarity Controller가 구성한 호스트 이름의 활성 도메인 이름 서버 구성, 도메인 이름 서버에 저장된 주소 또는 기타 정보를 실시간으로 변경할 도메인 이름 서버를 알립니다.

XClarity Controller의 도메인 이름을 선택하는 방법을 결정하려면 항목 목록에서 옵션을 선택하십시오.

- 사용자 지정 도메인 이름 사용: XClarity Controller가 속하는 도메인 이름을 지정할 수 있습니다.
- DHCP 서버에서 얻은 도메인 이름 사용: DHCP 서버로 XClarity Controller가 속하는 도메인 이름을 지정할 수 있습니다.

USB를 통한 이더넷 구성

이 주제의 정보를 사용하여 서버와 XClarity Controller 사이의 대역 내 통신에 사용되는 USB 인터페이스를 통한 이더넷을 제어합니다.

BMC 구성의 네트워크를 클릭하여 XClarity Controller USB를 통한 이더넷 설정을 보거나 수정하십시오.

USB를 통한 이더넷은 XClarity Controller에 대한 대역 내 통신에 사용됩니다. 확인란을 클릭하여 USB를 통한 이더넷 인터페이스를 활성화 또는 비활성화합니다.

중요:

- USB를 통한 이더넷을 비활성화하면 XClarity Essentials 대역 내 업데이트 유틸리티를 사용하는 서버 펌웨어 또는 XClarity Controller 펌웨어의 대역 내 업데이트를 수행할 수 없습니다. XClarity Controller 웹 인터페이스의 펌웨어 업데이트 옵션 또는 XClarity Essentials 대역 외 업데이트 유틸리티를 사용하여 펌웨어를 업데이트하십시오.
- USB 대역 내 인터페이스가 비활성화된 경우, 서버가 예기치 않게 다시 시작되는 것을 방지하려면 Watchdog 시간 제한을 비활성화하는 것이 중요합니다.
- 이 인터페이스를 사용하려면 이 기능을 지원하는 운영 체제 드라이버를 설치해야 합니다(Windows의 경우 RNDIS, Linux의 경우 cdc_ether 및 usbnet). XClarity Controller는 Windows에서 XClarity Controller USB 장치를 RNDIS 장치로 인식하도록 하는 Windows용 INF 파일을 제공합니다.

XClarity Controller가 USB 인터페이스를 통한 이더넷의 엔드포인트에 주소를 할당하는 데 사용하는 방법을 선택하십시오.

- USB를 통한 이더넷에 IPv6 링크 로컬 주소 사용: 이 방법은 USB 인터페이스를 통한 이더넷의 엔드포인트에 할당된 MAC 주소의 범위를 벗어난 IPv6 주소 사용입니다. 일반적으로 IPv6 링크 로컬 주소는 MAC 주소(RFC 4862)로 생성되지만, Windows 2008 및 새로운 2016 운영 체제는 인터페이스의 호스트 이름에 대한 고정 링크 로컬 IPv6 주소를 지원하지 않습니다. 대신에 기본 Windows 행동은 실행하는 동안 무작위 링크 로컬 주소를 다시 생성합니다. IPv6 링크 로컬 주소 모드를 사용하기 위해 XClarity Controller USB 인터페이스를 통한 이더넷을 구성하는 경우에는 XClarity Controller가 Windows를 인터페이스에 할당한 주소를 알지 못하기 때문에 이 인터페이스를 사용하는 다양한 기능이 작동하지 않습니다. 서버가 실행 중인 경우 Windows는 다른 USB를 통한 이더넷 주소 구성 방법 중 하나를 사용하거나, 다음 명령을 사용하여 기본 Windows 동작을 비활성화합니다.
`netsh interface ipv6 set global randomizeidentifiers=disabled`
- USB를 통해 이더넷에 IPv4 설정 구성: 이 방법을 사용하면 XClarity Controller와 USB 인터페이스를 통한 이더넷의 서버 측면에 할당되는 IP 주소와 서브넷 마스크를 지정합니다.

참고:

- XClarity Controller IP 주소, OS IP 주소 및 네트워크 마스크를 구성한 후 로컬 운영 체제에서 USB를 통한 이더넷 인터페이스의 IP 주소를 수동으로 구성해야 합니다.
- OS IP 주소 설정은 XClarity Controller가 Watchdog 상태 모니터링 또는 대역 내 펌웨어 업데이트와 같은 통신 목적으로 USB를 통한 이더넷 네트워크의 반대쪽 끝(운영 체제)을 인식하도록 하는 데 사용됩니다.

USB를 통한 이더넷 포트 번호와 외부 이더넷 포트 번호 간 매핑은 USB를 통한 이더넷 포트 전달에 외부 이더넷 사용 확인란을 클릭하고 관리 네트워크 인터페이스에서 서버로 전달할 포트에 대한 매핑 정보를 작성하여 제어합니다.

SNMP 구성

이 주제의 정보를 사용하여 SNMP 에이전트를 구성합니다.

다음 단계를 완료하여 XClarity Controller SNMP 정보 설정을 구성하십시오.

1. BMC 구성에서 네트워크를 클릭하십시오.
2. 해당하는 확인란을 선택하여 SNMPv3 에이전트, SNMPv1 트랩, SNMPv2 트랩 및/또는 SNMPv3 트랩을 활성화합니다.

참고:

- SNMPv3 에이전트를 활성화하려면 BMC 연락처 및 위치를 지정해야 합니다.
 - SNMPv3 에이전트가 활성화되면 각 XClarity Controller 사용자 계정에 대해 SNMPv3를 구성할 수 있습니다.
 - 트랩을 수신하려면 SNMP 트랩 및 SNMPv3 에이전트를 모두 활성화해야 합니다
3. SNMPv1 트랩 또는 SNMPv2 트랩을 사용하는 경우 다음 필드를 완료하십시오.
 - a. 커뮤니티 이름 필드에 커뮤니티 이름을 입력합니다. 커뮤니티 이름은 비워둘 수 없습니다.
 - b. 호스트 필드에 호스트 주소를 입력합니다.
 4. SNMPv3 트랩을 사용 설정하면 다음 필드를 완료하십시오.
 - a. 엔진 ID 필드에 엔진 ID를 입력합니다. 엔진 ID는 비워둘 수 없습니다.
 - b. 트랩 수신기 포트 필드에 포트 번호를 입력합니다. 기본 포트 번호는 162입니다.
 5. SNMP 트랩을 활성화하면 경고하려고 하는 다음 이벤트 유형을 선택하십시오.
 - 위험
 - 주의
 - 시스템

참고: 각 주요 범주를 클릭하여 알림을 받고자 하는 하위 범주 이벤트 유형을 추가로 선택하십시오.

6. SNMPv3 에이전트를 활성화한 경우 다음을 완료하십시오.
 - a. BMC 구성에서 사용자/LDAP를 클릭합니다.
 - b. 해당 사용자 옆에 있는 편집 버튼을 클릭한 다음 사용자 액세스 가능 인터페이스의 드롭 다운 목록에서 SNMP를 선택하십시오.

참고: 테스트 트랩 전송 옆에 있는 전송 버튼을 클릭하여 SNMP 설정을 확인합니다.

IPMI 네트워크 액세스 활성화

이 주제의 정보를 사용하여 XClarity Controller에 대한 IPMI 네트워크 액세스를 제어합니다.

LAN을 통한 IPMI 액세스를 활성화하려면 다음 단계를 완료하십시오.

1. BMC 구성의 네트워크를 클릭하여 XClarity Controller IPMI 설정을 보거나 수정하십시오.
2. 서비스 활성화 및 포트 할당에서 LAN을 통한 IPMI를 클릭하여 XClarity Controller에 대한 IPMI 네트워크 액세스를 활성화합니다.
3. BMC 구성에서 사용자/LDAP를 클릭합니다.
4. 해당 사용자 옆에 있는 편집 버튼을 클릭한 다음 사용자 액세스 가능 인터페이스의 드롭 다운 목록에서 LAN을 통한 IPMI를 체크하십시오.

중요:

- IPMI 프로토콜을 사용하는 네트워크를 통해 XClarity Controller에 액세스하는 도구 또는 응용프로그램을 사용하지 않는 경우 보안 향상을 위해 IPMI 네트워크 액세스를 비활성화하는 것이 좋습니다.

- XClarity Controller에서는 LAN을 통한 IPMI 액세스가 기본적으로 사용 안 함으로 설정되어 있습니다.

IPMI 명령으로 네트워크 설정 구성

이 주제의 정보를 사용하여 IPMI 명령을 사용하는 네트워크 설정을 구성합니다.

BMC 네트워크 설정은 각각 별도의 IPMI 요청을 사용하여 특정 순서 없이 구성되기 때문에, BMC를 다시 시작하여 보류 중인 네트워크 변경 사항을 적용하기 전까지는 BMC에 모든 네트워크 설정이 완전히 표시되지 않습니다. 네트워크 설정 변경을 위한 요청은 이 요청이 이루어지는 당시에는 성공할 수 있지만 추가 변경이 요청되는 경우 부적합한 것으로 판별될 수 있습니다. BMC가 다시 시작될 때 보류 중인 네트워크 설정이 호환되지 않으면 새 설정이 적용되지 않습니다. BMC를 다시 시작한 다음 새 설정을 사용하여 BMC에 액세스하여 예상대로 적용되었는지 확인해 보아야 합니다.

서비스 사용 및 포트 할당

이 주제의 정보를 사용하여 일부 서비스가 XClarity Controller에서 사용하는 포트 번호를 보거나 변경합니다.

BMC 구성의 네트워크를 클릭하여 XClarity Controller 포트 할당을 보거나 수정하십시오. 포트 할당을 보거나 수정하려면 다음 필드를 완료하십시오.

HTTPS(웹/Redfish)

이 항목은 항상 활성화됩니다. 이 필드에서 HTTPS를 통한 웹의 포트 번호를 지정하십시오. 기본값은 443입니다.

원격 존재

이 항목은 항상 활성화됩니다. 포트 번호는 443입니다.

LAN을 통한 IPMI

포트 번호는 623입니다. 이 필드는 사용자가 구성할 수 없습니다.

참고: 사용자/LDAP 페이지의 해당 사용자에게 대한 사용자 액세스 가능 인터페이스 필드에서 LAN을 통한 IPMI가 선택되고 적용되어야 합니다.

SSDP

포트 번호는 1900입니다. 이 필드는 사용자가 구성할 수 없습니다.

SSH

이 필드에서 SSH 프로토콜을 통해 명령줄 인터페이스에 액세스하도록 구성되는 포트 번호를 지정합니다. 기본값은 22입니다.

SNMP 에이전트

이 필드에서 XClarity Controller에서 실행되는 SNMP의 포트 번호를 지정하십시오. 기본값은 161입니다. 유효한 포트 번호값은 1~65535입니다.

참고: 사용자/LDAP 페이지의 해당 사용자에게 대한 사용자 액세스 가능 인터페이스 필드에서 SNMP가 선택되고 적용되어야 합니다.

액세스 제한 구성

이 주제의 정보를 사용하여 IP 주소 또는 MAC 주소에서 XClarity Controller에 액세스하는 것을 차단하는 설정을 보거나 변경합니다.

BMC 구성의 네트워크를 클릭하여 XClarity Controller 액세스 제어 설정을 보거나 수정하십시오.

차단 목록 및 시간 제한

이 옵션을 사용하면 특정 기간 동안 특정 IP/Mac 주소를 차단할 수 있습니다.

• 차단된 IP 주소 목록

- 쉽표로 구분된 IPv4 주소 또는 범위 및 IPv6 주소 또는 범위를 최대 3개씩 입력할 수 있으며, XClarity Controller로 액세스할 수 없습니다. 아래의 IPv4 예를 참조하십시오.
- 단일 IPv4 주소 샘플: 192.168.1.1
- 수퍼넷 단일 IPv4 주소 샘플: 192.168.1.0/24
- IPv4 범위 샘플: 192.168.1.1~192.168.1.5

• 차단된 MAC 주소 목록

- 쉽표로 구분된 MAC 주소를 최대 3개까지 입력할 수 있으며, XClarity Controller로 액세스할 수 없습니다. 예: 11:22:33:44:55:66.

• 제한적 액세스(1회)

- XClarity Controller가 액세스할 수 없는 시간 간격을 한 번 예약할 수 있습니다. 지정하는 시간 간격은 다음 요건을 충족해야 합니다.
- 시작 날짜와 시간은 현재 XCC 시간 이후여야 합니다.
- 종료 날짜와 시간은 시작 날짜와 시간 이후여야 합니다.

• 제한적 액세스(일일)

- XClarity Controller가 액세스할 수 없는 하나 이상의 일일 시간 간격을 예약할 수 있습니다. 지정하는 시간 간격마다 다음 요건을 충족해야 합니다.
- 종료 날짜와 시간은 시작 날짜와 시간 이후여야 합니다.

외부 트리거 차단 목록

이러한 옵션을 사용하면 클라이언트가 잘못된 사용자 이름 또는 암호를 사용하여 XClarity Controller에 연속적으로 로그인을 시도한 특정 IP 주소(IPv4 및 IPv6)의 자동 차단을 설정할 수 있습니다.

자동 차단은 특정 IP 주소에서 과도한 로그인 실패가 발생하는 시기를 동적으로 결정하고 해당 주소가 미리 결정된 시간 동안 XClarity Controller에 액세스하지 못하도록 차단합니다.

• 특정 IP의 최대 로그인 실패 수

- 최대 개수는 특정 IP 주소의 잘못된 암호를 가진 사용자가 잠기기 전에 허용되는 로그인 실패 횟수를 나타냅니다.
- 0으로 설정하면 로그인 실패로 인해 IP 주소가 잠기지 않습니다.
- 특정 IP 주소에 대해 실패한 로그인 카운터는 해당 IP 주소에서 성공적으로 로그인한 후 0으로 재설정됩니다.

• IP 차단을 위한 잠금 기간

- 사용자가 잠긴 IP 주소에서 다시 로그인을 시도하기 전에 경과해야 하는 최소 시간(분)입니다.
- 0으로 설정하면 잠긴 IP 주소에서의 액세스는 관리자가 명시적으로 잠금을 해제할 때까지 차단된 상태로 유지됩니다.

• 차단 목록

- 차단 목록 표에는 잠긴 모든 IP 주소가 표시됩니다. 차단 목록에서 하나 또는 모든 IP 주소를 잠금 해제할 수 있습니다.

앞면 패널 USB 관리 포트 구성

이 주제의 정보를 사용하여 XClarity Controller 앞면 패널 USB 관리 포트를 구성합니다.

XClarity Controller에 대한 연결은 주로 Lenovo XClarity 모바일 앱을 실행하는 모바일 장치에 사용하기 위한 것입니다. USB 케이블로 모바일 장치와 서버의 앞면 패널이 연결되면 장치와 XClarity Controller를 USB를 통한 이더넷으로 연결할 수 있습니다.

일부 서버에서는 앞면 패널 USB 포트를 서버 호스트 또는 XClarity Controller에 연결하도록 전환할 수 있습니다.

참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.

보안 설정 구성

이 주제의 정보를 사용하여 보안 프로토콜을 구성합니다.

참고: 기본 최소 TLS 버전 설정은 TLS 1.2이지만, 브라우저 또는 관리 응용프로그램에 필요한 다른 TLS 버전을 사용하도록 XClarity Controller를 구성할 수 있습니다. 자세한 정보는 "[tls 명령](#)" 123페이지의 내용을 참조하십시오.

BMC 구성의 보안을 클릭하여 XClarity Controller의 보안 속성, 상태 및 설정을 액세스 및 구성하십시오.

보안 대시보드

이 주제에서는 보안 대시보드의 개요를 다룹니다.

보안 대시보드는 전반적인 보안 평가 및 시스템 상태에 관한 정보를 제공합니다.

- BMC 보안 이벤트는 새시 침입, PFR에서 감지된 손상, 시스템 가드에서 감지된 하드웨어 불일치, 플래너에서 열린 보안 점퍼 등과 같은 보안 문제에서 제기된 이벤트를 보고합니다.
- BMC 보안 모드는 보안 모드의 전반적인 준수 상태에 관한 정보를 제공합니다.
- BMC 서비스 및 포트에는 활성화되었지만 현재 보안 모드를 준수하지 않는 모든 비보안 서비스/포트가 나열됩니다.
- BMC 인증서에는 XCC에서 사용하는 모든 비준수 인증서가 나열됩니다.
- BMC 사용자 계정에서는 계정 및 암호 관리를 보다 안전하게 설정하는 방법에 대한 일반적인 추천을 제공합니다.

참고: XCC에서 검색한 이러한 보안 영역에 위험이 있는 경우 대시보드에 경고 아이콘이 표시됩니다. 각 범주 아래의 세부사항 링크를 통해 사용자가 문제를 해결할 수 있는 설정 페이지로 이동할 수도 있습니다.

보안 모드

이 주제에서는 보안 모드의 개요를 다룹니다.

XCC 표준 라이선스를 사용하면 사용자는 표준 모드와 호환성 모드의 두 가지 보안 모드 중 하나로 서버를 구성할 수 있습니다. 모든 V4 서버에서 사용할 수 있습니다.

Lenovo XClarity Controller 3 Premier 업그레이드 라이선스는 세 번째 보안 모드인 엔터프라이즈급 강력한 모드가 제공됩니다. 이 모드는 높은 수준의 보안 요건이 필요할 때 가장 적합합니다.

참고: 기본적으로 XCC는 ECDSA 자체 서명된 인증서를 사용하며 ECDSA 기반 알고리즘만 사용할 수 있습니다. RSA 기반 인증서를 사용하려면 CSR을 생성하고 내부 또는 외부 CA로 서명된 다음 서명된 인증서를 XCC로 가져옵니다.

엔터프라이즈급 강력한 보안 모드

- 엔터프라이즈급 강력한 보안 모드는 가장 안전한 모드입니다.
- BMC에서 사용하는 모든 암호화 알고리즘은 CNSA 1.0을 준수합니다.

- BMC는 FIPS 140-3 검증 모드에서 작동합니다.
- 엔터프라이즈급 강력한 등급 인증서가 필요합니다.
- CNSA 1.0 암호화를 지원하는 서비스만 활성화할 수 있습니다.
- 활성화하려면 FoD(Features on Demand) 키가 필요합니다.

표준 보안 모드

- 표준 모드는 기본 보안 모드입니다.
- BMC에서 사용하는 모든 암호화 알고리즘은 FIPS 140-3를 준수합니다.
- 활성화된 모든 서비스가 FIPS 140-3 준수 암호화를 사용하는 경우 BMC가 FIPS 140-3 검증 모드에서 작동합니다.
- 표준 등급 인증서가 필요합니다.
- FIPS 140-3 준수 암호화를 지원하지 않는 암호화가 필요한 서비스는 기본적으로 비활성화됩니다.

호환성 모드

- 호환성 모드는 서비스와 클라이언트가 엔터프라이즈급 강력한 수준/표준을 준수하지 않는 암호화를 요구할 때 사용하는 모드입니다.
- 보다 광범위한 암호화 알고리즘이 지원됩니다.
- 이 모드가 활성화되면 BMC가 표준 검증 모드에서 작동하지 않습니다.
- 모든 서비스를 활성화할 수 있습니다.

지원되는 TLS 암호 세트

TLS 암호화 설정은 BMC 서비스에 대해 지원되는 TLS 암호 세트를 제한하는 것입니다.

TLS 암호 세트	보안 모드	TLS 버전
TLS_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • 엔터프라이즈급 강력한 • 표준* • 호환성* 	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	<ul style="list-style-type: none"> • 호환성 	TLS 1.3
TLS_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • 표준 • 호환성 	TLS 1.3
TLS_AES_128_CCM_SHA256	<ul style="list-style-type: none"> • 표준 • 호환성 	TLS 1.3
TLS_AES_128_CCM_8_SHA256	<ul style="list-style-type: none"> • 표준 • 호환성 	TLS 1.3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • 엔터프라이즈급 강력한 • 표준* • 호환성* 	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • 엔터프라이즈급 강력한 • 호환성* 	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> • 엔터프라이즈급 강력한 	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> • 표준 • 호환성 	TLS 1.2

TLS 암호 세트	보안 모드	TLS 버전
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	<ul style="list-style-type: none"> 호환성 	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	<ul style="list-style-type: none"> 호환성 	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> 표준 호환성 	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> 표준 	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> 표준 	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> 표준 	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> 표준 	TLS 1.2

참고: 표에서 별표(*)가 표시된 보안 모드는 Lenovo XClarity Controller 3 Premier 업그레이드 라이선스가 필요합니다.

세 가지 보안 모드의 서비스 매트릭스

기능/서비스	암호화 사용	기본 상태 즉시 사용 가능	강력한 모드에서 지원됨	표준 모드에서 지원됨	호환 모드에서 지원됨
KCS를 통한 IPMI	미지원	사용	지원	지원	지원
LAN을 통한 IPMI	지원	사용 안 함	미지원	지원	지원

기능/서비스	암호화 사용	기본 상태 즉시 사용 가능	강력한 모드에서 지원됨	표준 모드에서 지원됨	호환 모드에서 지원됨
SNMPv1 TRAP	미지원	구성 안 됨	미지원	지원	지원
SNMPv3 트랩	지원	구성 안 됨	미지원	지원 활성화된 경우 비 FIPS 암호화 사용에 대해 경고합니다.	지원
SNMPv3 에이전트	지원	구성 안 됨	미지원	지원 활성화된 경우 비 FIPS 암호화 사용에 대해 경고합니다.	지원
이메일 알림	지원	구성 안 됨	지원 CRAM-MD5 인증으로 활성화할 수 없음	지원 CRAM-MD5가 필요한 경우 비 FIPS 암호화 사용에 대해 경고합니다.	지원
시스템 로그 경고	미지원	구성 안 됨	미지원	지원	지원
TLS 1.2	지원	사용	지원	지원	지원
TLS 1.3	지원	사용	지원	지원	지원
HTTPS를 통한 웹	지원	사용	지원	지원	지원
HTTPS를 통한 Redfish	지원	사용	지원	지원	지원
SSDP	미지원	사용	지원	지원	지원
SSH-CLI	지원	사용	지원	지원	지원
SFTP	지원	사용 안 함	지원	지원	지원
LDAP	미지원	구성 안 됨	미지원	지원	지원
보안 LDAP	지원	구성 안 됨	지원	지원	지원
보안 키 관리	지원	구성 안 됨	지원	지원	지원
원격 콘솔	지원	사용	지원	지원	지원
가상 미디어 - CIFS	지원	구성 안 됨	미지원	지원	지원
가상 미디어 - NFS	미지원	구성 안 됨	미지원	지원	지원
가상 미디어 - HTTPFS	지원	구성 안 됨	지원	지원	지원
RDOC - 로컬	지원	구성 안 됨	지원	지원	지원
RDOC - CIFS	지원	구성 안 됨	미지원	지원	지원
RDOC - HTTP	미지원	구성 안 됨	미지원	지원	지원

기능/서비스	암호화 사용	기본 상태 즉시 사용 가능	강력한 모드에서 지원됨	표준 모드에서 지원됨	호환 모드에서 지원됨
RDOC - HTTPS	지원	구성 안 됨	지원	지원	지원
RDOC - FTP	미지원	구성 안 됨	미지원	지원	지원
RDOC - SFTP	지원	구성 안 됨	지원	지원	지원
FFDC 업로드 (SFTP)	지원	사용	지원	지원	지원
FFDC 업로드 (TFTP)	미지원	사용	미지원	지원	지원
리포지토리에 서 업데이트 - CIFS	지원	구성 안 됨	미지원	지원	지원
리포지토리에 서 업데이트 - NFS	미지원	구성 안 됨	미지원	지원	지원
리포지토리에 서 업데이트 - HTTP	미지원	구성 안 됨	미지원	지원	지원
리포지토리에 서 업데이트 - HTTPS	지원	구성 안 됨	지원	지원	지원
콜 홈	지원	사용 안 함	지원	지원	지원
서드파티 암호	지원	구성 안 됨	미지원	지원	지원
포트 전달	해당사항 없음	사용 안 함	지원	지원	지원

보안 모드 전환

이 주제의 정보를 사용하여 보안 모드를 전환하고 검증하십시오.

표준 모드는 기본 보안 모드입니다.

일반적으로 XCC에서 표준 모드와 호환되지 않는 설정이 감지되면 XCC에 알림이 표시되지만 사용자가 모드를 변경할 필요는 없습니다. 이 경우 XCC는 재정의(비준수)와 함께 표준 보안 모드를 시작합니다.

사용자는 드롭 다운 메뉴를 열어 다른 모드를 선택하고 검증 기능을 사용하여 XCC에서 얼마나 많은 비준수 항목이 감지되었는지 확인할 수 있습니다.

적용을 클릭하면 XCC에서 준수 항목도 검증합니다.

SSL 개요

이 주제는 SSL 보안 프로토콜의 개요입니다.

SSL은 통신 개인 정보를 제공하는 보안 프로토콜입니다. SSL은 클라이언트/서버 응용 프로그램을 활성화 하여 도청, 변조 및 메시지 위조를 방지하도록 설계된 방식으로 통신할 수 있습니다. XClarity Controller를 구성하여 보안 웹 서버(HTTPS), 보안 LDAP 연결(LDAPS), HTTPS를 통한 CIM 및 SSH 서버 같은 여러 가지 유형의 연결에 대한 SSL 지원을 사용하고 SSL에 필요한 인증서를 관리할 수 있습니다.

SSL 인증서 취급

이 주제에서는 SSL 보안 프로토콜로 사용할 수 있는 인증서의 관리에 대한 정보를 제공합니다.

WEB, Redfish 및 LDAP 클라이언트는 동일한 인증서 구성을 사용합니다. SSL 인증서 구성을 변경할 때마다 SSL 연결을 다시 설정해야 합니다. SSL은 자체 서명된 인증서 또는 서드파티 인증 기관에서 서명한 인증서와 함께 사용할 수 있습니다. 자체 서명된 인증서를 사용하는 것이 SSL을 사용하는 가장 간단한 방법이지만 약간의 보안 위험이 있습니다. 이러한 위험이 발생하는 이유는 클라이언트와 서버 간에 처음 연결을 시도하는 경우 SSL 클라이언트가 SSL 서버의 ID를 검증할 방법이 없기 때문입니다. 악의적인 제3자가 서버를 가장하여 XClarity Controller와 브라우저 간의 데이터 흐름을 가로채는 것이 가능합니다. (브라우저와 XClarity Controller 간에 첫 연결 시) 자체 서명된 인증서를 브라우저의 인증서 스토어에 가져오는 경우 해당 브라우저에 대해 향후 모든 통신의 보안이 유지됩니다(초기 연결이 공격에 의해 손상되었다고 가정 시). SSL 인증서 관리 페이지를 사용하여 키 쌍과 자체 서명된 인증서를 생성한 후 SSL이 활성화될 수도 있습니다.

더욱 완벽한 보안을 위해 인증 기관(CA)에서 서명한 인증서를 사용하십시오. 서명된 인증서를 받으려면 다음을 수행합니다.

- SSL 인증서 관리의 생성 아이콘에서 CSR(인증서 서명 요청) 생성을 선택합니다.
- 필수 필드를 채우고 생성을 선택합니다.
- 자체 서명된 인증서가 생성되면 해당 인증서가 SSL 인증서 관리에 표시됩니다.
- 다운로드 아이콘에서 CSR(인증서 서명 요청) 다운로드를 선택하여 서명된 인증서를 다운로드합니다.
- 서명된 인증서가 다운로드되면 CA 인증서 관리에서 서명된 인증서 가져오기 아이콘을 선택하여 XClarity Controller로 인증서를 가져옵니다.

CA의 기능은 XClarity Controller의 ID를 확인하는 것입니다. 인증서에는 CA 및 BMC에 대한 디지털 서명이 포함되어 있습니다. 잘 알려진 CA에서 인증서를 발급하거나 CA의 인증서를 이미 웹 브라우저로 가져온 경우에는 브라우저가 인증서의 유효성을 검증하고 BMC 웹 서버를 확실하게 식별할 수 있습니다.

참고로 SSL은 인증서의 XClarity Controller 호스트 이름(또는 일반 이름)을 웹 브라우저에 표시되는 호스트 이름과 비교합니다.

SSL 인증서 관리

이 주제에서는 SSL 보안 프로토콜을 사용한 인증서 관리를 위해 선택할 수 있는 일부 작업에 대한 정보를 제공합니다.

BMC 구성에서 보안을 클릭하여 SSL 인증서 관리를 구성하십시오.

XClarity Controller 인증서를 관리할 때 다음 작업이 제공됩니다.

서명된 인증서 다운로드

이 링크를 사용하여 현재 설치된 인증서의 복사본을 다운로드합니다. 인증서를 PEM 또는 DER 형식으로 다운로드할 수 없습니다. 인증서의 내용은 OpenSSL(<http://www.openssl.org>) 등의 서드파티 도구를 사용하여 볼 수 있습니다. OpenSSL를 사용하여 인증서의 내용을 볼 수 있는 명령줄은 다음과 같을 것입니다.

```
openssl x509 -in cert.der -inform DER -text
```

CSR(인증서 서명 요청) 다운로드

이 링크를 사용하여 인증서 서명 요청서 복사본을 다운로드합니다. CSR을 PEM 또는 DER 형식으로 다운로드할 수 없습니다.

서명된 인증서 생성

자체 서명된 인증서를 생성하십시오. 작업이 완료되면 새 인증서를 사용하여 SSL을 활성화할 수 있습니다.

참고: 서명된 인증서 생성 작업을 수행하면 HTTPS에 대한 자체 서명된 인증서 생성 창이 열립니다. 필수 또는 옵션 필드를 완료하라는 메시지를 받습니다. 필수 필드를 완료해야 합니다. 정보를 입력한 후에는 생성을 클릭하여 작업을 완료합니다.

CSR(인증서 서명 요청)을 생성

CSR(인증서 서명 요청)을 생성하십시오. 작업이 완료되면 CSR 파일을 다운로드한 후 인증 기관(CA)에 보내 서명을 받을 수 있습니다.

참고: 인증서 서명 요청(CSR) 생성 작업을 수행하면 HTTPS에 대한 인증서 서명 요청 생성 창이 열립니다. 필수 또는 옵션 필드를 완료하라는 메시지를 받습니다. 필수 필드를 완료해야 합니다. 정보를 입력한 후에는 생성을 클릭하여 작업을 완료합니다.

서명된 인증서 가져오기

이 기능을 사용하여 서명된 인증서를 가져옵니다. 서명된 인증서를 얻으려면 SSL 인증서 관리 페이지를 사용하여 인증 기관(CA)에 보야 합니다.

Secure Shell 서버 구성

이 주제의 정보를 사용하여 SSH 보안 프로토콜을 이해 및 활성화합니다.

BMC 구성의 네트워크를 클릭하여 Secure Shell 서버를 구성하십시오.

SSH 프로토콜을 사용하려면 SSH 서버를 활성화할 수 있도록 먼저 키를 생성해야 합니다.

참고:

- 이 옵션을 사용하는 데 인증서 관리는 필요하지 않습니다.
- XClarity Controller가 처음에 SSH 서버 키를 만듭니다. 새 SSH 서버 키를 생성하려면 BMC 구성에서 네트워크를 클릭한 다음 SSH 서버에서 키 생성을 클릭하십시오.
- 작업을 완료한 후 변경 사항을 적용하려면 XClarity Controller를 다시 시작해야 합니다.

KCS(키보드 컨트롤러 스타일)를 통한 IPMI 액세스

이 주제의 정보를 사용하여 XClarity Controller에 대한 KCS(Keyboard Controller Style)를 통한 IPMI 액세스를 제어합니다.

XClarity Controller는 인증이 필요하지 않은 KCS 채널을 통해 IPMI 인터페이스를 제공합니다.

BMC 구성에서 보안을 클릭하여 KCS를 통한 IPMI 액세스를 활성화 또는 비활성화합니다.

참고:

- 설정을 변경한 후 변경 사항을 적용하려면 XClarity Controller를 다시 시작해야 합니다.
- **사용 안 함(요청 시 사용)** 옵션은 대부분의 경우 KCS 채널을 비활성화하지만, 시스템 펌웨어 업데이트 중 일부 Lenovo 도구가 XClarity Controller와 정보를 교환할 수 있도록 허용합니다. 이 경우에는 KCS 채널이 몇 분 동안 잠깐 활성화된 다음, 완료 시 또는 시간 초과 시 비활성화됩니다.

중요: IPMI 프로토콜을 통해 XClarity Controller에 액세스하는 서버에서 도구 또는 응용프로그램을 실행하지 않는 경우 보안 향상을 위해 IPMI KCS 액세스를 비활성화하는 것이 좋습니다. XClarity Essentials는 KCS 인터페이스가 아닌 XClarity Controller로 연결되는 IPMI를 사용합니다. KCS를 통한 IPMI 인터페이스를 비활성화하는 경우 서버에서 XClarity Essentials를 실행하기 전에 다시 활성화하십시오. 마친 후에는 인터페이스를 비활성화하십시오.

시스템 펌웨어 하위 수준 방지

이 주제의 정보를 사용하여 시스템 펌웨어를 이전 펌웨어 수준으로 변경하는 것을 방지합니다.

이 기능으로 시스템 펌웨어를 이전 펌웨어 수준으로 되돌릴 것인지 여부를 결정할 수 있습니다.

BMC 구성에서 네트워크를 클릭하여 시스템 펌웨어 하위 수준 방지를 활성화 또는 비활성화하십시오.

XClarity Controller를 다시 시작하지 않아도 변경 사항이 즉시 적용됩니다.

SKM(보안 키 관리) 구성

이 주제의 정보를 사용하여 보안 키를 만들고 관리하십시오.

이 기능은 중앙 집중식 키 관리 서버를 사용해 스토리지 하드웨어를 잠금 해제하는 키를 제공함으로써 ThinkSystem 서버의 SED에 저장된 데이터에 액세스할 수 있게 합니다. 키 관리 서버에는 SKLM - IBM SED 키 관리 서버 및 KMIP - Thales/Gemalto SED 키 관리 서버(KeySecure 및 CipherTrust)가 포함됩니다.

참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.

Security Password Manager

이 주제의 정보를 사용하여 서드파티 암호를 허용합니다.

이 기능을 사용하면 사용자는 서드파티 암호 사용을 허용할지 여부를 결정할 수 있습니다.

- 서드파티 암호: 활성화되고 나면 BMC는 사용자가 제공한 암호 해시를 사용하여 인증을 진행할 수 있습니다.
- 서드파티 암호 검색 허용: 사용자는 BMC에서 서드파티 암호 해시 검색을 활성화하거나 비활성화할 수도 있습니다.

확장된 감사 로그

이 항목의 정보를 사용하여 확장 감사 로그를 제어하십시오.

이 기능으로 LAN 및 KCS 채널에서 IPMI set 명령(원시 데이터)의 로그 항목을 감사 로그에 포함할지 여부를 결정할 수 있습니다.

확장 감사 로그를 사용/사용 안 하려면 XCC 웹의 BMC 구성에서 보안을 클릭합니다.

참고: IPMI set 명령이 LAN 채널에서 오는 경우 사용자 이름과 소스 IP 주소가 로그 메시지에 포함됩니다. 그리고 민감한 보안 정보(예: 암호)가 있는 모든 IPMI 명령은 제외됩니다.

사용자 계정당 동시 로그인 제한

이 주제의 정보를 사용하여 사용자 계정당 동시 세션 수를 제한합니다.

이 기능을 사용하면 사용자는 사용자 계정당 허용되는 동시 세션 수를 결정할 수 있습니다.

- 웹 동시 세션 수: 1~10개의 세션 수까지 설정할 수 있습니다.
- 명령줄 동시 세션 수: 1~2개의 세션 수 중 설정할 수 있습니다.
- Redfish 동시 세션 수: 1~16개의 세션 수까지 설정할 수 있습니다.

참고: 총 세션 수가 설정한 수를 초과하면 사용자는 더 이상 새 세션을 생성할 수 없습니다.

시스템 가드

이 주제에서는 시스템 가드에 대한 개요를 다룹니다.

시스템 가드 기능은 하드웨어 구성 요소 인벤토리의 스냅샷을 신뢰할 수 있는 참조로 취한 다음 참조 스냅샷과의 편차를 모니터링합니다. 편차가 발생하면 사용자에게 이벤트를 보고할 수 있으며 필요에 따라 서버가 OS로 부팅되는 것을 방지하고 사용자에게 응답을 요청할 수도 있습니다.

사용자는 기능이 비활성화되어 있어도 언제든지 스냅샷을 찍을 수 있습니다. 스냅샷 생성에는 약 1분이 소요됩니다. 사용자는 시행할 하드웨어 구성 요소의 하위 집합을 선택하고 편차가 감지될 때 취할 해당 조치를 선택할 수 있습니다.

참고: 편차 감지는 서버 전원 켜기(POST) 또는 시스템 재부팅 시 실행됩니다. 예를 들어 OS가 계속 실행되는 동안 디스크 드라이브를 뽑았다가 잠시 후에 다시 연결하면 시스템 가드에서는 이벤트를 기록하거나 조치를 취하지 않습니다. 빼낸 디스크 드라이브가 다음에 재부팅할 때까지 남아 있으면 시스템 가드가 작동합니다.

참고: AC 복원 후 처음 전원을 켜는 동안 다음 조건을 충족하면 XCC는 OS 부팅을 방지하기 위해 UEFI에 알리지 않을 수 있습니다.

- 다음 조건에서 시스템 가드 활성화:
 - CPU 또는 DIMM 하드웨어 선택됨
 - OS 부팅 방지 옵션 선택됨
- 하드웨어 구성 변경이 신뢰할 수 있는 스냅샷과 일치하지 않음.

XCC는 POST 후 구성 불일치를 보고하며, 이 제한 사항은 후속 OS 재부팅에서 지속되지 않습니다.

시스템 가드 활성화

이 주제의 정보를 사용하여 시스템 가드를 사용 설정합니다.

시스템 가드 기능은 기본적으로 비활성화되어 있습니다. 최종 사용자의 요구 조건에 따라 출하 전에 활성화됩니다.

또한 XCC 기본값으로 재설정 옵션은 시스템 가드를 비활성화하고 스냅샷 기록을 제외한 설정을 지웁니다.

시스템 가드를 활성화하는 동안 사용자는 시스템 가드 보호 기능을 켜기 전에 설정을 확인하거나, 기존의 신뢰할 수 있는 스냅샷을 사용하거나, 인벤토리를 새로운 신뢰할 수 있는 스냅샷으로 캡처하라는 메시지를 받게 됩니다. 기능이 켜지면 다음이 예상됩니다.

- 시스템 전원이 꺼지면 시스템 가드가 하드웨어 인벤토리 수집을 즉시 시작합니다.
- 시스템 전원이 켜져 있으면 시스템 가드는 구성 요소 인벤토리 데이터를 신뢰할 수 있는 스냅샷과 비교합니다.

비교 결과가 신뢰할 수 있는 스냅샷과 편차가 있는 경우 XCC에는 하드웨어 구성 불일치로 인한 비준수 경고가 표시됩니다. 신뢰할 수 있는 스냅샷과 비교하여 위치/식별자/설명 속성이 포함된 각 누락/변경/신규 하드웨어 구성 요소의 불일치 목록이 나열됩니다.

사용자는 시스템 가드의 범위 및 조치를 구성하고 범위 및 조치 패널을 통해 시스템이 규정을 준수하지 않을 때 취할 조치를 결정할 수 있습니다.

TLS 버전 지원

이 항목의 정보를 사용하여 지원되는 다른 TLS 버전에 대해 알아보십시오.

다음 TLS 버전이 지원됩니다.

- TLS 1.2 이상
- TLS 1.3

지원되는 TLS 암호 세트의 전체 목록은 "[지원되는 TLS 암호 세트](#)" 36페이지 섹션을 참조하십시오.

BMC 구성 백업 및 복원

이 주제의 정보는 BMC 구성을 복원 또는 수정하는 방법을 설명합니다.

BMC 구성에서 백업 및 복원을 선택하여 다음 작업을 수행합니다.

- 관리 컨트롤러 구성 요약 보기
- 관리 컨트롤러 구성 백업 또는 복원
- 백업 보기 또는 상태 복구
- 관리 컨트롤러 구성을 공장 출하 기본값으로 다시 설정
- 관리 컨트롤러 초기 설정 마법사에 대한 액세스

BMC 구성 백업

이 주제의 정보는 BMC 구성을 백업하는 방법을 설명합니다.

BMC 구성에서 백업 및 복원을 선택합니다. 백업 BMC 구성 섹션은 맨 위에 있습니다.

이전에 백업이 만들어진 경우에는 마지막 백업 필드에서 자세한 내용을 확인합니다.

현재 BMC 구성을 백업하려면 아래에 표시된 단계를 완료하십시오.

1. BMC 백업 파일의 암호를 지정하십시오.
2. 전체 파일을 암호화할 것인지 민감한 데이터만 암호화할 것인지 선택하십시오.
3. 백업 시작을 클릭하여 백업 프로세스를 시작하십시오. 프로세스 중에는 복원/재설정 작업을 수행할 수 없습니다.
4. 프로세스가 완료되면 파일을 다운로드 및 저장할 수 있는 버튼이 나타납니다.

참고: 사용자가 새 XClarity Controller 사용자/암호를 설정하고 구성 백업을 수행하면 기본 계정/암호(USERID/PASSWORD)도 포함됩니다. 이후 백업에서 기본 계정/암호를 삭제하면 시스템에 XClarity Controller 계정/암호 복원에 실패했음을 알리는 메시지가 표시됩니다. 사용자는 이 메시지를 무시할 수 있습니다.

BMC 구성 복원

이 주제의 정보는 BMC 구성을 복원하는 방법을 설명합니다.

BMC 구성에서 백업 및 복원을 선택합니다. 구성 파일에서 BMC 복원 섹션은 백업 BMC 구성 아래에 있습니다.

BMC 이전에 저장된 구성으로 복원하려면 아래에 표시된 단계를 완료하십시오.

1. 백업 파일을 찾아 선택한 후 메시지가 표시되면 암호를 입력하고 다음 >을 클릭하십시오.
2. 세부 정보 보기를 클릭하여 파일을 확인합니다.
3. 내용을 확인한 후 복원 시작을 클릭하십시오.

BMC를 공장 출하 기본값으로 재설정

이 주제의 정보에서는 BMC를 공장 출하 기본값으로 재설정하는 방법을 설명합니다.

BMC 구성에서 백업 및 복원을 선택합니다. BMC를 공장 출하 기본값으로 재설정 섹션은 구성 파일에서 BMC 복원 아래에 있습니다.

BMC를 공장 출하 기본값으로 다시 설정하려면 아래에 표시된 단계를 따르십시오.

1. BMC를 공장 출하 기본값으로 재설정 작업을 클릭하십시오.

참고:

- 감독자 사용자 권한 레벨을 가진 사용자만 이 작업을 수행할 수 있습니다.
- 인터넷 연결은 일시적으로 끊어집니다. 재설정 작업이 완료되면 다시 XClarity Controller 웹 인터페이스에 로그인해야 합니다.
- BMC를 공장 출하 기본값으로 재설정 작업을 클릭하면 확인 창이 표시됩니다. 확인란을 선택하여 다음 설정을 유지할 수 있습니다.
 - 로컬 사용자 설정 유지: 현재 사용자/역할/전역 설정이 백업됩니다. 콘텐츠 CLI 명령 'users'/'roles'/'accesscfg'를 복원합니다. 예: 사용자 이름/역할 이름/암호 만료 경고 기간/암호 복잡성 규칙 활성화 등.
 - 네트워크 설정 유지: 현재 네트워크 설정이 백업됩니다. 'ifconfig' CLI 명령의 네트워크 출력을 복원합니다. 예: 호스트 이름/IPv4 주소/IPv6 주소/게이트웨이 등
- 확인을 클릭하면 유지하도록 선택한 변경 사항을 제외하고 이전의 모든 구성 변경 사항이 손실됩니다.
- BMC 구성을 복원할 때 LDAP를 사용하려면 먼저 신뢰할 수 있는 보안 인증서를 가져와야 합니다.
- BMC 로컬 시스템에서 작업하는 경우 TCP/IP 연결이 끊기게 됩니다. 연결을 복원하려면 BMC 네트워크 인터페이스를 재구성해야 합니다.
- 프로세스가 완료되면, XClarity Controller가 다시 시작됩니다.
- BMC를 공장 출하 기본값으로 재설정해도 UEFI 설정 및 원격 콘솔의 액세스 모드(단일/다중 사용자)에는 영향을 주지 않습니다(브라우저 쿠키에 저장됨).

XClarity Controller 다시 시작

이 주제의 정보는 XClarity Controller를 다시 시작하는 방법을 설명합니다.

XClarity Controller를 다시 시작하는 방법에 대한 세부 정보는 "[전원 작업](#)" 56페이지의 내용을 참조하십시오.

제 4 장 서버 상태 모니터링

이 주제의 정보를 사용하여 액세스하는 서버에 대한 정보를 보고 모니터링하는 방법을 이해하십시오.

XClarity Controller에 로그인하면 시스템 상태 페이지가 표시됩니다. 이 페이지에서 서버 하드웨어 상태, 이벤트 및 감사 로그, 시스템 상태, 관리 이력 및 경보 수신자를 볼 수 있습니다.

상태 요약/활성 시스템 이벤트 보기

이 주제의 정보를 사용하여 상태 요약/활성 시스템 이벤트를 확인하는 방법을 이해합니다.

XClarity Controller 홈페이지에 액세스하면 **상태 요약**이 기본적으로 표시됩니다. 그래픽 표현이 표시되어 설치된 하드웨어 구성 요소의 수와 각 상태를 나타냅니다. 모니터링되는 하드웨어 구성 요소는 다음이 포함됩니다.

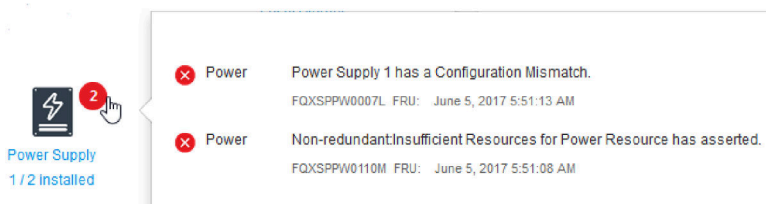
- CPU(프로세서)
- 메모리
- 로컬 저장 장치
- PCI 어댑터
- 전원 공급 장치
- 팬
- 시스템 보드
- 기타
- 보안

참고: 로컬 스토리지는 심플 스왑 백플레인 구성이 있는 시스템의 상태 아이콘에 사용할 수 없음을 표시할 수도 있습니다.



 CPU 1 / 2 installed	 Memory 1 / 32 installed	 Local Storage Not Found
 PCI Not Found	 Power Supply 2 / 2 installed	 Fan Not Found
 System Board	 Others	 Security Crypto:Standard

하드웨어 구성 요소가 정상적으로 작동하지 않는 경우 위험 또는 경고 아이콘으로 표시됩니다. 위험 조건은 빨간색 아이콘으로 표시되며, 경고 상태는 노란색 삼각형 아이콘으로 표시됩니다. 위험 또는 경고 표시 위에 마우스를 대면 해당 구성 요소의 현재 활성 이벤트가 최대 3개까지 표시됩니다.



다른 이벤트를 보려면 **활성 시스템 이벤트** 탭을 클릭합니다. 시스템에서 현재 활성 상태인 이벤트를 보여주는 창이 표시됩니다. 전체 이벤트 내역을 보려면 **모든 이벤트 로그 보기**를 클릭합니다.

하드웨어 구성 요소가 녹색 확인 표시로 표시되면 정상적으로 작동하고 있으며 활성 이벤트가 없습니다.

하드웨어 구성 요소 아래의 텍스트는 설치된 구성 요소의 수를 기술합니다. 텍스트(링크)를 클릭하면 **인벤토리** 페이지에 연결됩니다.

참고: D3 V2 새시 호환 노드에서 전원 공급 장치 링크는 관리자 노드에서만 사용할 수 있습니다.

시스템 정보 보기

이 주제에서는 공통 서버 정보의 요약 을 얻을 수 있는 방법을 설명합니다.

홈페이지 오른쪽에 있는 **시스템 정보 및 설정** 패널은 일반적인 서버 정보를 요약하여 제공하며, 다음 사항이 포함됩니다.

- 컴퓨터 이름, 전원 및 운영 체제 상태
- 시스템 유형/모델
- 일련 번호
- 시스템 이름
- 앞면 패널 USB 포트 관리

참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.

- BMC 라이선스
- BMC IP 주소
- BMC 호스트 이름
- 활성 새시 관리자

참고: 이 항목은 D3 V2 새시 호환 노드에서만 지원됩니다.

- BMC 버전
- UEFI 버전
- 위치

서버는 다음 표에 나열된 시스템 상태 중 하나일 수 있습니다.

표 2. 시스템 상태 설명

서버의 시스템 상태를 설명하는 제목이 있는 2열 표입니다.

상태	설명
시스템 전원 꺼짐/상태를 알 수 없음	서버의 전원이 꺼져 있습니다.
시스템 전원 켜짐/UEFI 시작	서버의 전원이 켜져 있지만 UEFI가 실행 중이 아닙니다.
UEFI에서 시스템 실행 중	서버의 전원이 켜져 있고 UEFI가 실행 중입니다.
부팅 중인 운영 체제 또는 지원되지 않는 운영 체제(OS가 ping에 응답하지 않는 경우 시스템이 이 상태일 수 있음)	해당 서버 상태의 원인은 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> • 운영 체제 로더가 시작되었지만 운영 체제가 실행 중이 아닙니다. • USB를 통한 BMC 이더넷 인터페이스를 사용 안 함으로 설정합니다. • 운영 체제에 USB를 통한 이더넷 인터페이스를 지원하는 드라이버가 로드되지 않았습니다.
운영 체제 부팅됨	서버 운영 체제가 실행 중입니다.
메모리 테스트에서 실행 중인 시스템	서버의 전원이 켜져 있고 메모리 진단 도구를 실행 중입니다.
시스템이 설정에서 실행 중	서버의 전원이 켜져 있고 시스템이 UEFI F1 설정 메뉴 또는 LXPM 메뉴로 부팅되었습니다.
시스템이 LXPM 유지보수 모드로 실행 중	서버의 전원이 켜져 있고 시스템이 사용자가 LXPM 메뉴를 통해 탐색할 수 없는 LXPM 유지 관리 모드로 부팅되었습니다.

시스템 이름을 변경하려고 하는 경우에는 연필 아이콘을 클릭하십시오. 사용하려는 시스템 이름을 입력한 후 녹색 체크 표시를 클릭하십시오.

서버에 XClarity Controller Premier 수준 라이선스 이외의 라이선스가 있는 경우 라이선스 업그레이드를 구매하여 향상된 기능을 활성화할 수 있습니다. 업그레이드 라이선스를 얻은 후에 업그레이드 라이선스를 설치하려면, 위로 화살표 아이콘을 클릭하십시오.

BMC License



라이선스를 추가, 삭제하거나 내보내려면 오른쪽 화살표 아이콘을 클릭하십시오.

BMC License



BMC IP 주소, BMC 호스트 이름, UEFI 버전, BMC 버전 및 위치 항목에 대한 관련 설정을 변경하려면 오른쪽 화살표를 클릭하십시오.

- IP 주소 및 호스트 이름의 경우에는 네트워크의 이더넷 구성 섹션으로 이동합니다.
- UEFI 및 BMC 버전 항목의 경우에는 펌웨어 업데이트 페이지로 이동합니다.
- 위치 항목의 경우에는 서버 구성 페이지의 서버 속성 섹션으로 이동합니다.

BMC IP Address	10.245.32.57
BMC Hostname	XCC-7DG8-BHSFW1U002
BMC Version	0.34 (Build ID: IHX403H)
UEFI Version	0.10 (Build ID: IHE101T)
Location	



시스템 사용률 보기

왼쪽 패널의 사용률을 클릭하면 일반적인 서버 사용률 정보가 요약되어 제공됩니다.

시스템 사용률은 프로세서, 메모리, I/O 하위 시스템의 실시간 사용률을 기반으로 하는 복합 메트릭입니다. 사용률 데이터는 그래픽 보기 또는 표 보기에서 볼 수 있으며, 다음을 포함합니다.

- 온도
 - 실시간 주변 온도와 주요 구성 요소 온도를 표시합니다.
 - 메모리 모듈 위로 마우스 커서를 가져가면 현재 온도가 표시됩니다.
- 전력 사용률
 - 현재 소비 전력 파이 차트를 표시합니다.
 - 파이 차트 위로 마우스 커서를 가져가면 현재 소비 전력이 표시됩니다.
 - 현재 소비 전력 파이 차트는 CPU, 메모리, 기타 및 예비의 네 가지 범주로 구성됩니다. "기타"는 총 시스템 소비 전력에서 CPU 및 메모리 소비 전력을 뺀 값을 의미합니다. "예비"는 총 사용 가능한 할당 전력에서 총 시스템 소비 전력을 뺀 값을 의미합니다.
 - 전압 탭에는 하드웨어에서 지원하는 모든 전압 센서의 현재 전압 판독 값과 상태가 표시됩니다.
- 시스템 사용률
 - 시스템, 프로세서, 메모리 및 I/O 하위 시스템의 현재 사용률 스냅샷을 의미합니다.

참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.
- 팬 속도 (RPM)
 - 팬 속도 섹션에는 팬 속도가 최대 속도의 백분율로 표시됩니다.
 - 사용자는 기어 아이콘을 클릭하여 팬 속도 부스트 옵션에 액세스할 수 있습니다.

- 이 설정을 사용하면 주변 온도에 따라 서버를 추가로 냉각시킬 수 있습니다. 제어된 열전도 알고리즘으로 정상 속도보다 팬 속도를 높일 수 있습니다. 팬이 이미 최대 속도로 실행 중인 경우에는 변경되지 않습니다.

이벤트 로그 보기

이벤트 로그는 모든 하드웨어 및 관리 이벤트의 기록 목록을 제공합니다.

이벤트의 이벤트 로그 탭을 선택하여 이벤트 로그 페이지를 표시합니다. 로그의 모든 이벤트에는 XClarity Controller 날짜 및 시간 설정을 사용하여 타임스탬프가 있습니다. 일부 이벤트는 경고 수신인에 경고를 생성하도록 구성되어 있는 경우 이벤트가 발생할 때 경고도 생성합니다. 또한 이벤트 로그의 이벤트를 정렬하고 필터링할 수 있습니다.

다음은 이벤트 로그 페이지에서 수행할 수 있는 작업의 설명입니다.

- **테이블 사용자 지정:** 이 작업 항목을 선택하여 표에 표시하려고 하는 정보의 유형을 선택합니다. 일련 번호를 표시하여 2개 이상의 이벤트에 동일한 타임스탬프가 있을 때 이벤트의 순서에 대한 결정을 지원할 수 있습니다.

참고: 내부 BMC 프로세스로 일부 일련 번호를 결정할 수 있으며, 따라서 일련 번호로 이벤트를 정렬할 때 일련 번호에 차이가 있는 것은 정상적입니다.

- **로그 지우기:** 이 작업 항목을 선택하여 이벤트 로그를 삭제하십시오.
- **새로 고치기:** 이 작업 항목을 선택하여 페이지가 마지막으로 표시된 이후 발생했을 수 있는 이벤트 로그 항목이 있는 디스플레이를 업데이트하십시오.
- **유형:** 표시할 이벤트 유형을 선택합니다. 이벤트 유형에는 다음이 포함됩니다.



- 로그의 오류 항목 표시



- 로그의 경고 항목 표시



- 로그의 정보 항목 표시

각 아이콘을 클릭하여 표시할 오류의 유형을 끄거나 켜십시오. 아이콘을 연속해서 클릭하면 이벤트 표시와 표시하지 않는 것 사이에서 전환됩니다. 아이콘을 둘러싼 검은색 상자는 이벤트 유형이 표시됨을 나타냅니다.

- **소스 유형 필터:** 드롭다운 메뉴에서 항목을 선택하여 표시하려고 하는 이벤트 로그 항목의 유형만 표시합니다.
- **시간 필터:** 이 작업 항목을 선택하여 표시하려는 이벤트의 간격을 지정합니다.
- **검색:** 특정 유형의 이벤트 또는 키워드를 검색하려면, 확대경 아이콘을 클릭한 후 검색 상자에서 검색할 단어를 입력하십시오. 입력은 대소문자를 구분합니다.

참고: 최대 이벤트 로그 레코드 수는 1024입니다. 이벤트 로그가 가득 차면 새 로그 항목이 가장 오래된 로그 항목을 자동으로 덮어씁니다.

감사 로그 보기

감사 로그는 XClarity Controller에 로그인, 새 사용자 만들기, 사용자 암호 변경과 같은 사용자 작업에 대한 기록 레코드를 제공합니다.

감사 로그를 사용하여 인증, 변경 사항 및 시스템 작업을 추적 및 문서화할 수 있습니다.

이벤트 로그와 감사 로그는 모두 유사한 관리 및 보기 작업을 지원합니다. 감사 로그 페이지에서 수행할 수 있는 디스플레이 및 필터링 작업의 설명을 확인하려면 "[이벤트 로그 보기](#)" 51 페이지의 내용을 확인하십시오.

참고:

- 서버 운영 체제에서 Lenovo 도구를 실행하면 감사 로그에 사용자가 인식할 수 없는 사용자 이름(예: "20luN4SB")이 수행한 작업을 보여주는 레코드가 포함될 수 있습니다. 일부 도구가 서버 운영 체제에서 실행되는 경우 이 도구는 XClarity Controller 액세스에 사용할 수 있는 임시 사용자 계정을 만들 수 있습니다. 이 계정은 임의 사용자 이름 및 암호로 만들어지며 USB 인터페이스를 통한 내부 이더넷상의 XClarity Controller에 액세스하는 데만 사용할 수 있습니다. 이 계정은 XClarity Controller Redfish 및 SFTP 인터페이스에 액세스하는 데만 사용할 수 있습니다. 이 임시 계정 만들기 및 제거 작업뿐 아니라 이 자격 증명을 사용하는 도구에서 수행한 모든 작업은 감사 로그에 기록됩니다.
- 최대 감사 로그 레코드 수는 1024입니다. 감사 로그가 가득 차면 새 로그 항목이 가장 오래된 로그 항목을 자동으로 덮어씁니다.

유지 관리 내역 보기

유지보수 내역 페이지에는 펌웨어 업데이트, 구성 및 하드웨어 교체 기록에 대한 정보가 포함되어 있습니다.

유지보수 내역의 내용을 필터링하여 일정 유형의 이벤트 또는 일정 시간 간격을 표시할 수 있습니다.

참고: 최대 유지 관리 내역 레코드 수는 250입니다. 유지 관리 내역 로그가 가득 차면 새 로그 항목이 가장 오래된 로그 항목을 자동으로 덮어씁니다.

경고 수신자 구성

이 항목의 정보를 사용하여 이메일 및 syslog 알림 또는 SNMP 트랩 수신인을 추가 및 수정하십시오.

참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.

제 5 장 서버 구성

이 장의 정보를 사용하여 서버 구성에 사용할 수 있는 옵션을 이해합니다.

서버를 구성하면 다음 옵션을 사용할 수 있습니다.

- 어댑터
- 부팅 옵션
- 전력 정책
- 서버 속성
- 새시

참고: 이 항목은 D3 V2 새시 호환 노드에서만 지원됩니다.

어댑터 정보 및 구성 설정 보기

이 주제의 정보를 사용하여 서버에 설치된 어댑터에 관한 정보를 봅니다.

서버 구성에서 어댑터를 클릭하여 서버에 설치된 어댑터에 대한 정보를 보십시오.

참고: 어댑터가 상태 모니터링을 지원하지 않는 경우 모니터링 또는 구성을 볼 수 없습니다. 설치된 모든 PCI 어댑터의 자원 명세 관련 정보는 [자원 명세 페이지](#)를 참조하십시오.

시스템 부팅 모드 및 순서 구성

시스템 부팅 모드 및 순서를 구성하려면 이 주제의 정보를 사용하십시오.

서버 구성에서 부팅 옵션을 선택하는 경우 시스템 부팅 순서를 구성할 수 있습니다.

참고: 미인증 대역 내 방법은 보안 관련 시스템 설정을 변경할 수 없습니다. 예를 들어 보안 부팅은 OS 또는 UEFI 셸에서 미인증 대역 내 API를 통해 구성할 수 없어야 합니다. 여기에는 대역 내에서 실행되는 OneCLI와 IPMI를 사용하여 임시 자격 증명을 얻거나 보안 부팅, TPM, UEFI 설정 암호 관련 설정을 구성하는 도구 및 API가 포함됩니다. 모든 보안 관련 설정에는 충분한 권한이 있는 적절한 인증이 필요합니다.

시스템 부팅 순서를 구성하려면 **사용 가능한 장치** 목록에서 장치를 선택하고 오른쪽 화살표를 클릭하여 부팅 순서에 장치를 추가하십시오. 부팅 순서에서 장치를 제거하려면 부팅 순서 목록에서 장치를 선택하고 왼쪽 화살표를 클릭하여 사용 가능한 장치 목록으로 장치를 다시 이동하십시오. 부팅 순서를 변경하려면 장치를 선택하고 위쪽 또는 아래쪽 화살표를 클릭하여 장치를 우선순위의 위쪽 또는 아래쪽으로 이동하십시오.

부팅 순서를 변경하는 경우 변경 사항을 적용하기 전에 다시 시작 옵션을 선택해야 합니다. 다음 옵션이 제공됩니다.

- **즉시 서버 다시 시작:** 부팅 순서 변경이 저장되고 운영 체제를 종료하지 않고도 서버가 즉시 다시 시작됩니다.
- **서버 정상적으로 다시 시작:** 부팅 순서 변경이 저장되고 서버를 다시 시작하기 전에 운영 체제가 종료됩니다.
- **나중에 수동으로 다시 시작:** 부팅 순서 변경이 저장되지만 다음에 서버가 재부팅될 때까지 변경이 적용되지 않습니다.

1회 부팅 구성

구성된 부팅을 일시적으로 무시하고 지정된 장치로 1회 부팅을 실행하려면 이 주제의 정보를 사용하십시오.

서버 구성에서 부팅 옵션을 클릭하고 드롭다운 메뉴에서 장치를 선택하여 시스템이 다음에 서버가 다시 시작할 때 1회 부팅할 장치를 구성하십시오. 다음 선택 사항이 제공됩니다.

PXE 네트워크

PXE(Preboot eXecution Environment) 네트워크 부팅을 시도할 서버를 설정합니다.

기본 이동식 미디어

서버가 기본 USB 장치에서 부팅됩니다.

기본 CD/DVD

서버가 기본 CD/DVD 드라이브에서 부팅됩니다.

F1 시스템 설치

서버가 Lenovo XClarity Provisioning Manager로 부팅됩니다.

진단 파티션

서버가 Lenovo XClarity Provisioning Manager의 진단 섹션으로 부팅됩니다.

기본 하드 디스크

서버가 기본 디스크 드라이브에서 부팅됩니다.

기본 원격 미디어

서버는 탑재된 가상 미디어에서 부팅됩니다.

탑재됨

구성된 부팅 순서가 사용됩니다. 구성된 부팅 순서를 대체하는 1회 부팅이 없습니다.

1회 부팅 없음

구성된 부팅 순서가 사용됩니다. 구성된 부팅 순서를 대체하는 1회 부팅이 없습니다.

부팅 순서에 대해 1회 변경을 선택하는 경우 변경 사항을 적용하려면 다시 시작 옵션을 선택해야 합니다.

- 즉시 서버 다시 시작: 부팅 순서 변경이 저장되고 운영 체제를 종료하지 않고도 서버가 즉시 다시 시작됩니다.
- 서버 정상적으로 다시 시작: 부팅 순서 변경이 저장되고 서버를 다시 시작하기 전에 운영 체제가 종료됩니다.
- 나중에 수동으로 다시 시작: 부팅 순서 변경이 저장되지만 다음에 서버가 재부팅될 때까지 변경이 적용되지 않습니다.

서버 전원 관리

전원 관리 정보를 보고 및 전원 관리 기능을 수행하려면 이 주제의 정보를 사용하십시오.

전원 관리 정보를 확인하고 전원 관리 기능을 수행하려면 서버 구성에서 전력 정책을 선택하십시오.

참고: 고밀도 서버 노드가 포함된 엔클로저에서 새시 냉각 및 전원은 XClarity Controller 대신 SMM에 의해 제어됩니다. 솔루션 전원 상태에 대한 자세한 내용은 SMM3 웹 인터페이스를 참조하십시오.

전원 중복성 구성

전원 중복성을 구성하려면 이 주제의 정보를 사용하십시오.

참고:

- AMD 서버는 전원 정책 기능 구성을 지원하지 않습니다.

- 2개의 전원 공급 장치가 설치된 경우 중복 모드가 중복(N+N)으로 설정됩니다. 이러한 2개의 전원 공급 장치 구성을 사용하면 전원 공급 장치 중 하나에 장애가 발생하거나 AC가 손실 또는 제거된 경우 XCC 이벤트 로그에 중복 손실 이벤트가 보고됩니다.
- 출하 후 전원 공급 장치가 1개만 설치된 경우에는 중복 모드가 비중복 모드로 자동 설정됩니다.

전원 중복성 섹션의 사용 가능 필드에는 다음이 포함됩니다.

- **중복성(N+N):** 시스템에 동시에 전원을 공급할 수 있는 두 개 이상의 독립적인 전원이 있습니다. 즉, 하나 이상의 전원 소스에 장애가 발생해도 어떠한 중단 없이 시스템에 전원 소스를 계속 공급할 수 있습니다. N+N 중복성은 고수준의 내결함성을 제공하고 여러 오류가 발생한 경우에도 시스템이 계속 작동하도록 합니다.
 - **제로 출력 모드:** 중복 구성에서 사용되면 일부 PSU는 경부하 조건에서 자동으로 대기 상태로 전환됩니다. 이러한 방식으로 나머지 PSU는 전체 전력 부하를 전달하여 효율성을 높입니다.
- **비중복 모드:** 이 모드에서는 전원 공급 장치가 손실된 경우 서버가 작동 가능 상태 유지가 보장되지 않습니다. 전원 공급 장치가 실행 중 상태를 유지하지 못하는 경우 서버가 스로틀링됩니다.

구성을 변경한 후 적용을 클릭하십시오.

전원 최대 가용량 사용 정책 구성

전력 제한 정책을 구성하려면 이 주제의 정보를 사용하십시오.

참고:

- AMD 서버는 전원 최대 가용량 사용 정책 기능 구성을 지원하지 않습니다.
- 고밀도 서버 노드가 포함된 엔클로저에서 새시 냉각 및 전원은 XClarity Controller 대신 SMM에 의해 제어됩니다. 솔루션 전원 상태에 대한 자세한 내용은 SMM3 웹 인터페이스를 참조하십시오.

전원 최대 가용량 사용 기능을 사용 또는 사용 안 함으로 설정하도록 선택할 수 있습니다. 전원 최대 가용량 사용을 사용하면 서버에서 사용하는 전원의 양을 제한하도록 선택할 수 있습니다. 전원 최대 가용량 사용을 사용 안 함으로 설정하면 전원 중복성 정책으로 서버가 사용하는 최대 전원이 결정됩니다. 설정을 변경하려면 먼저 재설정을 클릭하십시오. 원하는 설정을 선택한 다음 적용을 클릭하십시오.

총 전원 용량은 전원 중복 모드와 시스템에 설치된 PSU 수를 기준으로 계산됩니다. 최대 전원 한계의 수동 설정은 실제 전원 용량을 초과할 수 있습니다.

전원 최대 가용량 사용이 활성화되면 전원 한계를 유지하기 위해 시스템이 스로틀링될 수도 있습니다.

참고: 전원 최대 가용량 사용이 비활성화된 경우에도 전원 공급 장치 장애, 냉각 문제 등의 특정 결합 조건에서 시스템이 스로틀링될 수도 있습니다.

전원 최대 가용량 사용은 입력 측정 또는 출력 측정을 사용하여 활성화될 수 있습니다. 드롭다운 메뉴에서 전원 최대 가용량 사용 제한을 결정하는 데 사용할 측정값 유형을 선택하십시오. 측정값 간에 전환하면 그에 따라 슬라이더의 숫자가 변경됩니다.

전원 최대 가용량 값을 변경하는 방법은 두 가지입니다.

- **방법 1:** 슬라이더 표시를 원하는 와트로 이동하여 전체 서버 전원 제한을 설정합니다.
- **방법 2:** 입력 상자에 값을 입력합니다. 슬라이더 표시가 해당 위치로 자동으로 이동합니다.

구성을 변경한 후 적용을 클릭하십시오. 변경 사항은 즉시 적용됩니다.

전력 복구 정책 구성

전원 손실 후 전력이 복구된 경우 서버가 반응하는 방법을 구성하려면 이 주제의 정보를 사용하십시오.

전력 복구 정책을 구성하는 경우 다음 세 가지 옵션이 제공됩니다.

항상 끄기

전력이 복구되면 서버의 전원이 꺼진 상태로 유지됩니다.

복원

전원 장애가 발생한 시간에 서버의 전원이 켜져 있었으면 전력이 복구될 때 서버의 전원이 자동으로 켜집니다. 그렇지 않은 경우 전력이 복구되면 서버의 전원이 꺼진 상태로 유지됩니다.

참고: 전원 장애가 발생하기 전에 서버가 켜져 있던 경우 전원 켜기에 대해 1~15초의 무작위 지연 시간을 설정하려면 이 확인란을 선택합니다.

항상 켜기

전력이 복구되면 서버의 전원이 자동으로 켜집니다.

구성을 변경한 후 적용을 클릭하십시오.

전원 작업

이 주제의 정보를 사용하여 서버에 대해 이루어질 수 있는 전원 작업을 이해합니다.

XClarity Controller 홈페이지의 빠른 동작 섹션에서 전원 동작을 클릭하십시오.

다음 표에는 서버에서 수행할 수 있는 전원 및 다시 시작 동작에 대한 설명이 나와 있습니다.

표 3. 전원 동작 및 설명

서버 전원 및 다시 시작 동작에 대한 설명이 포함되어 있는 2열 표입니다.

전원 동작	설명
서버 전원 켜기	서버 전원을 켜고 운영 체제를 부팅하려면 이 작업 항목을 선택하십시오.
서버 전원 정상적으로 끄기	운영 체제를 시스템 종료하고 서버 전원을 끄려면 이 작업 항목을 선택하십시오.
서버 전원 즉시 끄기	운영 체제를 시스템 종료하지 않고 서버 전원을 끄려면 이 작업 항목을 선택하십시오.
서버 정상적으로 다시 시작	운영 체제를 시스템 종료하고 서버를 껐다 켜려면 이 작업 항목을 선택하십시오.
서버 즉시 다시 시작	운영 체제를 시스템 종료하지 않고 서버 전원을 바로 껐다 켜려면 이 작업 항목을 선택하십시오.
서버를 시스템 설정으로 부팅	서버 전원을 켜거나 서버를 재부팅하고 부팅 중 F1을 누르지 않아도 시스템 설정으로 자동으로 부팅되도록 하려면 이 항목을 선택하십시오.
NMI(Non-Maskable Interrupt) 트리거	이 작업 항목을 선택하여 "정지된" 시스템에서 NMI(Non-maskable Interrupt)를 강제로 수행합니다. 이 작업 항목을 선택하면 플랫폼 운영 체제가 시스템 정지 조건의 디버그 목적으로 사용할 수 있는 메모리 덤프를 수행할 수 있습니다. F1 시스템 설정 메뉴의 NMI에 대한 자동 재부팅 설정은 XClarity Controller가 NMI 후 서버를 재부팅할 것인지를 결정합니다.
전원 동작 예약	서버의 일일 및 주간 전원 및 다시 시작 동작을 예약하려면 이 작업 항목을 선택합니다.

표 3. 전원 동작 및 설명 (계속)

전원 동작	설명
관리 컨트롤러 다시 시작	XClarity Controller를 다시 시작하려면 이 작업 항목을 선택합니다.
AC 전원 주기 서버	서버의 전원을 껐다 켜려면 이 작업을 선택합니다.
참고: <ul style="list-style-type: none"> 운영 체제가 화면 보호기가 작동 중인 상태이거나 운영 체제를 종료할 때 잠긴 모드인 경우 XClarity Controller는 정상적인 종료를 시작할 수 없습니다. 전원 끄기 지연 주기가 만료되면 XClarity Controller에서 하드 재설정 또는 종료를 수행하며, 그 동안 운영 체제는 계속 실행 중일 수 있습니다. 앞면 패널의 전원 LED가 빠르게 깜박이는 경우 XClarity Controller가 정상적인 전원 켜기 순서를 시작하지 못할 수 있습니다. 전원 LED가 천천히 깜박이기 시작하면 XClarity Controller가 시스템 전원을 켤 수 있습니다. 	

IPMI 명령으로 소비 전력 관리 및 모니터링

이 주제의 정보를 사용하여 IPMI 명령을 사용하는 전원 소모량 관리 및 모니터링합니다.

이 주제는 IPMI(Intelligent Platform Management Interface) 전원 관리 명령을 사용하여 서버에 대한 전원 및 열 모니터링 및 정책 기반 전원 관리를 제공하는 데 Intel 지능형 전원 노드 관리자 및 DCMI(데이터센터 관리 인터페이스)를 사용하는 방법에 대해 설명합니다.

Intel 노드 관리자 SPS 3.0을 사용하는 서버의 경우 XClarity Controller 사용자는 Intel ME(Management Engine)에서 제공하는 IPMI 전원 관리 명령을 사용하여 노드 관리자 기능을 제어하고 서버 소비 전력을 모니터링할 수 있습니다. DCMI 전원 관리 명령을 사용하여 서버 전원을 관리할 수도 있습니다. 이 주제에서는 노드 관리자 예제 및 DCMI 전원 관리 명령에 대해 다룹니다.

노드 관리자 명령을 사용하여 서버 전원 관리

이 주제의 정보를 사용하여 노드 관리자를 사용하는 서버 전원을 관리합니다.

Intel 노드 관리자 펌웨어에는 외부 인터페이스가 없기 때문에 XClarity Controller에서 노드 관리자 명령을 먼저 수신한 다음 Intel 노드 관리자로 전송해야 합니다. XClarity Controller는 표준 IPMI 브리징을 사용하여 IPMI 명령에 대한 릴레이 및 전송 장치 역할을 합니다.

참고: 노드 관리자 IPMI 명령을 사용하여 노드 관리자 정책을 변경하면 XClarity Controller 전원 관리 기능과 충돌이 발생할 수 있습니다. 기본적으로 노드 관리자의 브리징 명령은 충돌을 방지하기 위해 사용 안 함으로 설정됩니다.

XClarity Controller가 아닌 노드 관리자를 사용하여 서버 전원을 관리하려는 사용자의 경우 (네트워크 기능: 0x3A) 및 (명령: 0xc7)으로 구성된 OEM IPMI 명령을 사용할 수 있습니다.

고유 노드 관리자 IPMI 명령 유형을 사용하려는 경우: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x01`

고유 노드 관리자 IPMI 명령 유형을 사용 안 함으로 설정하려는 경우: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x00`

다음 정보는 노드 관리자 전원 관리 명령의 예입니다.

참고:

- IPMI 채널 0 및 0x2c의 대상 주소를 지정하면 IPMITOOL을 사용하여 Intel 노드 관리자에 명령을 처리하도록 전송할 수 있습니다. 요청 메시지는 작업을 시작하는 데 사용되며 응답 메시지는 요청자에게 반환됩니다.
- 명령은 공간 제한으로 인해 다음 형식으로 표시됩니다.

전역 시스템 전원 통계 가져오기를 사용하여 전원 모니터링(명령 코드 0xC8): 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00 응답:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Intel 노드 관리자 정책 설정을 사용하여 전원 최대 가용량 사용(명령 코드 0xC1): 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00 응답:57 01 00

Intel 노드 관리자 정책 설정을 사용하여 전원 절약(명령 코드 0xC1): 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00

Intel 관리 엔진 장치 ID 가져오기를 사용하여 장치 ID 기능 가져오기: 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x06 0x01 응답:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

더 많은 Intel 노드 관리자 명령을 보려면 <https://businessportal.intel.com>에서 Intel 지능형 전원 노드 관리자, IPMI를 사용하는 외부 인터페이스 사양의 최신 릴리스를 참조하십시오.

DCMI 명령을 사용하여 서버 전원 관리

이 주제의 정보를 사용하여 DCMI 명령을 사용하는 서버 전원을 관리합니다.

DCMI는 표준 관리 소프트웨어 인터페이스를 통해 표시할 수 있는 모니터링 및 제어 기능을 제공합니다. 서버 전원 관리 기능은 DCMI 명령을 사용하여 수행할 수도 있습니다.

다음 정보는 일반적으로 사용되는 DCMI 전원 관리 기능 및 명령의 예입니다. 요청 메시지는 작업을 시작하는 데 사용되며 응답 메시지는 요청자에게 반환됩니다.

참고: 명령은 공간 제한으로 인해 다음 형식으로 표시됩니다.

전원 읽기 가져오기: 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x02 0xdc 0x01 0x00 0x00 응답:dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40

전원 제한 설정: 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03 응답:dc

전원 최대 가용량 사용 가져오기: 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x03 0xdc 0x00 0x00 응답:dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00

전원 제한 활성화: 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x01 0x00 0x00 응답:dc

전원 제한 비활성화: 요청:ipmitool -H <\$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x00 0x00 0x00 응답:dc

참고: 일부 서버의 경우 전원 제한 설정 명령에 대한 예외 작업이 지원되지 않을 수 있습니다. 예를 들어 시스템 강제 전원 끄기 및 SEL에 대한 로그 이벤트 매개 변수가 지원되지 않을 수 있습니다.

DCMI 사양에서 지원하는 전체 명령 목록은 <https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf>에서 데이터센터 관리 인터페이스 사양의 최신 릴리스를 참조하십시오.

서비스 데이터 로그 다운로드

이 주제의 정보를 사용하여 서버에 대한 서비스 정보를 수집합니다. 이 프로세스는 일반적으로 서버 문제를 해결하는 데 도움이 되도록 서비스 담당자가 요청하는 경우에만 수행됩니다.

XClarity Controller 홈페이지에서 빠른 동작 섹션의 서비스 로그 옵션을 클릭하고 서비스 데이터 로그를 선택합니다.

기본적으로 서비스 로그에는 시스템 정보, 시스템 인벤토리, 시스템 사용자, SMBIOS 테이블, 센서 읽기, 이벤트 로그, FOD 키, SLP 키, UEFI 구성 및 XClarity Controller 3 구성 등의 데이터가 포함됩니다.

기본 정보 옵션 위로 마우스를 이동하고 플로팅 창을 클릭하면 내보낼 실제 데이터 중 일부를 볼 수 있습니다.

기본 정보는 필수 항목이며 다음 정보를 내보낼 수도 있습니다.

- 네트워크 정보(IP, 호스트 이름)
- 원격 분석(24시간 데이터)
- 감사 로그(사용자 이름 포함)
- 최신 오류 화면

서비스 데이터 로그를 다운로드하려면 내보내기를 클릭하십시오.

서비스 수집 프로세스 및 지원 데이터가 완료되기까지 몇 분 정도 걸릴 수 있습니다. 이 파일은 기본 다운로드 폴더에 저장됩니다. 서비스 데이터 파일의 이름 지정 규칙은 다음 규칙을 따릅니다. <machine type and model>_<serial number>_xcc3_ServiceData_<date>-<time>.zip

예: 7X2106Z01A_2345678_xcc3_ServiceData_240517-112857.zip.

.zip 형식의 서비스 데이터 외에도 탐색 기록...을 통해 .tar.zst 파일 형식으로 디버그 로그를 다운로드할 수도 있습니다. 디버그 lodf 파일의 이름 지정 규칙은 다음 규칙을 따릅니다. <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst

예: 7X2106Z01A_2345678_xcc3_DebugLog_240517-112857.zip.

참고:

- 또한 탐색 기록...에는 최근에 내보낸 서비스 로그가 포함됩니다.
- .tar.zst 파일 형식은 다른 압축 알고리즘을 사용하며 'zstd' 패키지로 추출될 수 있습니다. 예:
tar --use-compress-program=unzstd -xvf <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst

서버 속성

이 주제의 정보를 사용하여 관련 서버 속성을 변경하거나 보십시오.

위치 및 담당자 설정

이 주제의 정보를 사용하여 운영 및 지원 담당자가 시스템을 식별하는 데 도움이 되는 다양한 매개 변수를 설정합니다.

위치 및 담당자 정보를 구성하려면 서버 구성에서 서버 속성을 선택하십시오.

담당자

시스템에 문제가 발생한 경우 연락해야 하는 담당자의 이름 및 전화 번호를 지정할 수 있습니다.

참고: 이 필드는 SNMPv3 구성의 담당자 필드와 동일하며 SNMPv3을 사용하려면 필수 사항입니다.

랙 이름

서버가 어떤 랙에 있는지를 지정하여 서버를 더욱 쉽게 찾을 수 있습니다.

룸 번호

서버가 어떤 룸에 있는지를 지정하여 서버를 더욱 쉽게 찾을 수 있습니다.

빌딩

서버가 어떤 빌딩에 있는지를 지정하여 서버를 더욱 쉽게 찾을 수 있습니다.

최저 U

랙의 위치를 지정하여 서버를 더욱 쉽게 찾을 수 있습니다.

주소

서버가 있는 장소의 전체 주소를 지정할 수 있습니다.

참고: 관련 정보가 입력되어 있는 경우 SNMPv3 섹션 및 XClarity Controller 홈페이지의 위치 필드에 한 행으로 표시됩니다.

서버 제한시간 설정

이 주제의 정보를 사용하여 서버의 제한 시간을 설정합니다.

이러한 시간 제한은 정지된 서버에 대한 작업을 복원하는 데 사용됩니다.

서버 구성에서 서버 속성을 선택하여 서버 시간 제한을 구성하십시오. 다음과 같은 서버 시간 제한 선택 사항이 제공됩니다.

전원 끄기 지연 사용

이 필드를 사용하여 BMC 서브시스템이 시스템 전원을 끄기 전에 운영 체제가 종료될 때까지 대기하는 시간(분 단위)을 지정합니다.

전원 끄기 지연 시간 제한 값을 설정하려면 드롭다운에서 시간 간격을 선택하고 **적용**을 클릭하십시오. XClarity Controller의 전원을 강제로 끄지 않도록 하려면 드롭다운 선택 항목에서 **없음**을 선택하십시오.

침입 메시지

사용자가 XClarity Controller에 로그인할 때 표시되는 메시지를 만들려면 이 주제의 정보를 사용하십시오.

서버 구성에서 서버 속성을 선택합니다. 사용자에게 표시할 메시지를 구성하려면 **침입 메시지** 옵션을 사용합니다. 완료되면 **적용**을 클릭합니다.

메시지 텍스트는 사용자가 로그인할 때 XClarity Controller 로그인 페이지의 메시지 영역에 표시됩니다.

솔루션 서비스

이 항목의 정보를 사용하여 솔루션 서비스를 활성화 또는 비활성화합니다.

참고: 이 기능은 향후 업데이트에서 지원될 예정입니다.

XClarity Controller 날짜 및 시간 설정

이 주제의 정보를 사용하여 XClarity Controller 날짜와 시간 설정을 이해합니다. XClarity Controller 날짜 및 시간을 구성하기 위한 지시사항이 제공됩니다. XClarity Controller 날짜 및 시간은 이벤트 로그에 기록된 모든 이벤트 및 전송된 경고를 타임스탬프하는 데 사용됩니다.

XClarity Controller 홈페이지에서 오른쪽 위에 있는 시계 아이콘을 클릭하여 XClarity Controller 날짜 및 시계를 보거나 변경합니다. XClarity Controller에는 고유 실시간 시계가 없습니다. XClarity Controller를 구성하여 네트워크 타임 프로토콜 서버 또는 서버의 실시간 시계 하드웨어와 시간 및 날짜를 동기화할 수 있습니다.

NTP와 동기화

다음 단계를 완료하여 XClarity Controller 시계를 NTP 서버와 동기화하십시오.

- 시간을 NTP와 동기화를 선택하고 NPT 서버 주소를 지정합니다.
- "+" 아이콘을 클릭하여 추가 NTP 서버를 지정할 수 있습니다.
- XClarity Controller가 NTP 서버와 동기화하는 빈도를 지정합니다.
- NTP 서버에서 가져온 시간은 UTC(Coordinated Universal Time) 형식입니다.
 - XClarity Controller에서 로컬 영역의 시간 및 날짜를 조정하도록 하려면 드롭다운 메뉴에서 사용자 로케일에 대한 시간대 오프셋을 선택합니다.
 - 사용 중인 지역에서 일광 절약 시간을 준수하는 경우 일광 절약 시간(DST)에 맞게 자동으로 조정 확인란을 선택합니다.
- 구성 변경이 완료되면 적용을 클릭합니다.

호스트와 동기화

서버의 실시간 시계 하드웨어에서 유지되는 시간은 UTC(Coordinated Universal Time) 형식이거나 로컬 시간 형식으로 조정 및 저장되었을 수 있습니다. 일부 운영 체제는 실시간 시계를 UTC 형식으로 저장하지만 기타 운영 체제는 로컬 시간으로 시간을 저장합니다. 서버 실시간 시계는 시간이 어떤 형식으로 되어 있는지를 표시하지 않습니다. 따라서 XClarity Controller가 호스트의 실시간 시계와 동기화하도록 구성된 경우 사용자는 XClarity Controller에서 실시간 시계에서 가져온 시간 및 날짜를 사용하는 방법을 선택할 수 있습니다.

- 로컬(예: Windows): 이 모드에서 XClarity Controller는 실시간 시계에서 가져온 시계 및 날짜를 적용 가능한 모든 시간대 및 DST 오프셋이 적용된 로컬 시간으로 처리합니다. 사용자의 위치에서 일광 절약 시간을 준수하는 경우 일광 절약 시간(DST)에 맞게 자동으로 조정 확인란을 선택할 수도 있습니다.
- UTC(예: Linux): 이 모드에서 XClarity Controller는 실시간 시계에서 가져온 시계 및 날짜를 시간대가 적용되지 않았거나 DST 오프셋이 적용된 Coordinated Universal Time으로 처리합니다. 이 모드에서는 드롭다운 메뉴에서 사용자의 로케일에 대한 시간대 오프셋을 선택하여 로컬 영역의 시간 및 날짜를 조정하도록 선택할 수 있습니다. 사용자의 위치에서 일광 절약 시간을 준수하는 경우 일광 절약 시간(DST)에 맞게 자동으로 조정 확인란을 선택할 수도 있습니다.
- 구성 변경이 완료되면 적용을 클릭합니다.

참고: 일광 절약이 발생하는 경우 시계가 앞으로 이동하는 간격 중에 XClarity Controller에서 수행하도록 예약된 모든 작업이 수행되지 않습니다. 예를 들어 미국 일광 시작 시간이 3월 12일 오전 2시이고 전월 동작이 3월 12일 오전 2시 10분에 예약되어 있으면 이 동작은 발생하지 않습니다. 오전 2시가 되면 XClarity Controller는 시간을 오전 3시로 읽습니다.

D3 V2 새시 구성

이 항목의 정보를 사용하여 D3 V2 새시 설정에 대해 알아보십시오.

D3 V2 새시에 대한 정보를 보려면 서버 구성에서 새시를 클릭하십시오.

새시 정보

이 섹션에는 UUID, 일련 번호, 시스템 유형 및 펌웨어 버전을 포함한 새시 정보가 표시됩니다. 또한 폼 팩터, 전원 상태 및 IP 주소를 포함한 노드 정보도 표시됩니다.

참고:

- 해당 노드 옆에 있는 재설정/재배치 버튼을 클릭하여 노드를 다시 시작하거나 물리적 노드 재배치를 시뮬레이션합니다.
- 관리자 노드만 다른 노드를 재설정하거나 재배치할 수 있습니다.

새시 관리자 역할

이 섹션에서는 새시 관리자 선택 기본 설정이 표시됩니다.

참고:

- 노드가 관리자 선택 프로세스에 참여할 수 있도록 하려면 새시 관리자 역할에 참여를 선택합니다. 영구 관리자로 지정된 다른 노드가 있다면 그 노드가 없지 않는 한 선택 프로세스가 발생하지 않습니다.
- 하나의 노드만 관리자로 지정하려면 이 노드를 영구 새시 관리자로 지정을 선택합니다. 이 경우 관리자 역할의 고가용성은 없습니다. 새시에 영구 관리자 노드가 없으면 다음으로 적합한 관리자를 선택하기 위해 관리자 선택 프로세스가 발생합니다.

새시 유지보수 내역

새시 유지보수 내역에는 새시에서 추가되거나 제거된 노드의 기록과 한 노드에서 다른 노드로 변경되는 관리자 역할의 기록이 유지됩니다.

제 6 장 원격 콘솔 기능

이 주제의 정보를 사용하여 서버 콘솔로 원격으로 보고 서버 콘솔과 상호 작용하는 방법을 이해합니다.

XClarity Controller 웹 인터페이스의 원격 콘솔 기능을 사용하여 서버 콘솔을 보고 서버 콘솔과 상호 작용할 수 있습니다. 디스크 이미지(ISO 또는 IMG 파일)를 서버의 가상 드라이브로 할당할 수 있습니다. 원격 콘솔 기능은 XClarity Controller Premier 수준 기능에서 사용할 수 있으며 웹 인터페이스를 통해서만 사용 가능합니다. 원격 콘솔 기능을 사용하려면 감독자 액세스 또는 원격 콘솔 액세스 권한이 있는 사용자 ID로 XClarity Controller에 로그인해야 합니다. XClarity Controller Standard 수준에서 XClarity Controller Premier 수준으로 업그레이드하는 방법에 대한 자세한 정보는 "[XClarity Controller 업그레이드](#)" 6페이지의 내용을 참조하십시오.

원격 콘솔 기능을 사용하려면 다음을 수행하십시오.

- 서버 상태에 관계없이 최대 1920x1200 32bpp@60Hz의 그래픽 해상도로 비디오를 원격으로 봅니다.
- 원격 클라이언트의 키보드 및 마우스를 사용하여 서버에 원격으로 액세스합니다.
- 로컬 시스템 또는 원격 시스템에 있는 ISO 또는 IMG 파일을 서버에서 사용할 수 있는 가상 드라이브로 탑재합니다.
- XClarity Controller 메모리에 IMG 또는 ISO 이미지를 업로드하고 이를 서버에 가상 드라이브로 탑재합니다. 전체 크기가 최대 100MB인 파일을 최대 2개까지 XClarity Controller 메모리에 업로드할 수 있습니다.

참고:

- 원격 콘솔 기능이 다중 사용자 모드(XClarity Controller Premier 수준 기능 세트가 포함된 XClarity Controller는 최대 6개의 동시 세션을 지원함)에서 시작된 경우 원격 디스크 기능은 한 번에 하나의 세션에서만 실행할 수 있습니다.
- 원격 콘솔은 시스템 보드의 비디오 컨트롤러에서 생성한 비디오만 표시할 수 있습니다. 별도의 비디오 컨트롤러 어댑터가 설치되어 있고 시스템의 비디오 컨트롤러 대신 사용되는 경우 XClarity Controller 원격 콘솔은 추가된 어댑터의 비디오 내용을 표시할 수 없습니다.
- 네트워크에 방화벽이 있는 경우 원격 콘솔 기능을 지원하려면 네트워크 포트가 열려 있어야 합니다. 원격 콘솔 기능에서 사용하는 네트워크 포트 번호를 보거나 변경하려면 "[서비스 사용 및 포트 할당](#)" 33페이지를 참조하십시오.
- 원격 콘솔 기능은 웹 페이지에서 서버 비디오를 표시하는 데 HTML5를 사용합니다. 이 기능을 사용하려면 브라우저에서 HTML5 요소를 사용하는 비디오 내용 표시를 지원해야 합니다.
- Internet Explorer에서 BMC에 액세스하는 데 자체 서명된 인증서 및 IPv6 주소를 사용하는 경우 원격 콘솔 세션은 인증서 오류로 인해 시작되지 않을 수 있습니다. 이 문제를 방지하기 위해 Internet Explorer 신뢰 루트 인증서 기관에 자체 서명된 인증서를 추가할 수 있습니다.
 - BMC 구성에서 보안을 선택하고 자체 서명된 인증서를 다운로드합니다.
 - 인증서 파일 확장자를 *.crt로 변경하고 웹 인증서 파일을 두 번 클릭합니다.
 - IE11 브라우저 캐시를 지웁니다.
 - 다음 인증서 가져오기 마법사 단계를 따라 인증서 설치를 클릭하여 인증서 저장소에 인증서를 설치합니다.

원격 콘솔 기능 사용

이 주제에서는 원격 콘솔 기능에 관한 정보를 제공합니다.

XClarity Controller 원격 콘솔 기능은 XClarity Controller Premier 수준 기능에서만 사용할 수 있습니다. 원격 콘솔을 작동할 수 있는 권한이 없으면 잠금 아이콘이 표시됩니다.

XClarity Controller Premier 수준 업그레이드용 정품 인증 키를 구입 및 획득했다면 "[정품 인증 키 설치](#)" 79페이지에 나와 있는 지시사항에 따라 설치하십시오.

원격 콘솔 기능을 사용하려면 XClarity Controller 홈 페이지 또는 원격 콘솔 웹 페이지의 원격 콘솔 미리 보기 섹션에서 흰색 대각선 화살표가 있는 이미지를 클릭합니다.

원격 전원 제어

이 주제에서는 원격 콘솔 창에서 서버 전원 및 다시 시작 명령을 전송하는 방법에 대해 설명합니다.

기본 웹 페이지로 돌아가지 않고 원격 콘솔 창에서 서버 전원 및 다시 시작 명령을 보낼 수 있습니다. 원격 콘솔에서 서버 전원을 제어하려면 전원을 클릭하고 다음 명령 중 하나를 선택하십시오.

서버 전원 켜기

서버 전원을 켜고 운영 체제를 부팅하려면 이 작업 항목을 선택하십시오.

서버 전원 정상적으로 끄기

운영 체제를 시스템 종료하고 서버 전원을 끄려면 이 작업 항목을 선택하십시오.

서버 전원 즉시 끄기

운영 체제를 시스템 종료하지 않고 서버 전원을 끄려면 이 작업 항목을 선택하십시오.

서버 정상적으로 다시 시작

운영 체제를 시스템 종료하고 서버를 껐다 켜려면 이 작업 항목을 선택하십시오.

서버 즉시 다시 시작

운영 체제를 시스템 종료하지 않고 서버 전원을 바로 껐다 켜려면 이 작업 항목을 선택하십시오.

서버를 시스템 설정으로 부팅

서버 전원을 켜거나 서버를 재부팅하고 부팅 중 F1을 누르지 않아도 시스템 설정으로 자동으로 부팅되도록 하려면 이 항목을 선택하십시오.

원격 콘솔 캡처 화면

이 주제의 정보를 사용하여 원격 콘솔 화면 캡처 기능을 사용하는 방법을 이해합니다.

원격 콘솔 창의 화면 캡처 기능은 서버의 비디오 디스플레이 내용을 캡처합니다. 화면 이미지를 캡처하고 저장하려면 다음 단계를 완료하십시오.

단계 1. 원격 콘솔 창에서 **캡처 화면**을 클릭합니다.

단계 2. 팝업 창에서 **파일 저장**을 클릭하고 **확인**을 누릅니다. 파일 이름이 rpvviewer.png로 지정되고 기본 다운로드 폴더에 이 파일이 저장됩니다.

참고: 화면 캡처 이미지는 JPG 파일 유형으로 저장됩니다.

원격 콘솔 키보드 지원

키보드의 원격 콘솔 창에는 다음 옵션 항목이 제공됩니다.

- 가상 키보드를 실행하려면 **가상 키보드**를 클릭하십시오. 이 기능은 실제 키보드가 없는 태블릿 장치를 사용 중인 경우 유용합니다. 서버에 전송할 수 있는 매크로 및 키 조합을 만드는 데 다음 옵션을 사용할 수 있습니다. 사용 중인 클라이언트 시스템의 운영 체제는 Ctrl+Alt+Del과 같은 특정 키 조합을 서버에 전송하지 않고 트랩핑할 수 있습니다. 사용 중인 프로그램이나 브라우저에서 F1 또는

Esc와 같은 기타 키를 인터셉트할 수 있습니다. 매크로는 사용자가 전송할 수 없는 키 입력을 서버에 전송하는 메커니즘을 제공합니다.

- 서버 정의 매크로를 사용하려면 서버 매크로를 클릭하십시오. 일부 서버 매크로는 XClarity Controller 펌웨어에 미리 정의되어 있습니다.

원격 콘솔 화면 모드

이 주제의 정보를 사용하여 원격 콘솔 화면 모드를 구성합니다.

원격 콘솔 화면 모드를 구성하려면 **화면 모드**를 클릭하십시오.

다음 메뉴 옵션을 사용할 수 있습니다.

전체 화면

이 모드는 클라이언트 바탕 화면을 비디오 디스플레이로 채웁니다. 이 모드에서 Esc 키를 누르면 전체 화면 모드가 종료됩니다. 원격 콘솔 메뉴는 전체 화면 모드에서 표시되지 않기 때문에 키보드 매크로와 같은 원격 콘솔 메뉴에서 제공하는 기능을 사용하려면 전체 화면 모드를 종료해야 합니다.

화면에 맞춤

원격 콘솔이 실행되는 경우 기본 설정입니다. 이 설정에서는 대상 바탕 화면이 스크롤 막대 없이 완전히 표시되며, 가로 세로 비율이 유지됩니다.

미디어 탑재 방법

이 주제의 정보를 사용하여 미디어 탑재를 수행하는 방법을 이해합니다.

ISO 및 IMG 파일을 가상 드라이브로 탑재할 수 있는 세 가지 메커니즘이 제공됩니다.

- 미디어를 클릭하여 원격 콘솔 세션의 서버에 가상 드라이브를 추가할 수 있습니다.
- 원격 콘솔 세션을 설정하지 않고 원격 콘솔 웹 페이지에서 직접 탑재합니다.
- 독립형 도구.

가상 미디어 기능을 사용하려면 사용자에게 원격 콘솔과 원격 디스크 액세스 권한이 있어야 합니다.

파일은 로컬 시스템 또는 원격 서버에서 가상 미디어로 탑재할 수 있으며, 네트워크를 통해 액세스하거나 RDOC 기능을 사용하여 XClarity Controller 메모리로 업로드할 수 있습니다. 이러한 메커니즘은 아래에 설명되어 있습니다.

- 로컬 미디어는 XClarity Controller에 액세스하는 데 사용 중인 시스템에 위치한 ISO 또는 IMG 파일입니다. 이 메커니즘은 원격 콘솔 웹 페이지에서 직접 사용할 수 있는 것이 아니라 원격 콘솔 세션을 통해 서만 사용할 수 있으며 XClarity Controller Premier 수준 기능에서만 제공됩니다. 로컬 미디어를 마운트하려면 로컬 미디어 파일 마운트 섹션에서 모든 로컬 미디어 마운트를 클릭합니다. 최대 4개의 파일을 서버에 동시 탑재할 수 있습니다.
- 원격 시스템에 있는 파일도 가상 미디어로 탑재할 수 있습니다. 최대 4개의 파일을 가상 드라이브로 동시에 탑재할 수 있습니다. XClarity Controller는 다음 파일 공유 프로토콜을 지원합니다.
 - CIFS - Common Internet File System:
 - 원격 시스템에 있는 파일을 찾을 수 있는 URL을 입력합니다.
 - 파일이 서버에 읽기 전용 가상 미디어로 표시되도록 하려면 확인란을 선택합니다.
 - 원격 시스템에 있는 파일에 액세스하려면 XClarity Controller에 필요한 자격 증명을 입력합니다.

참고: XClarity Controller는 공백이 포함된 사용자 이름, 암호 또는 URL을 지원하지 않습니다. CIFS 서버에 사용자 이름 또는 암호에 공백으로 구성된 로그인 자격 증명 없이 그리고 URL에 공백이 포함되어 있지 않은지를 확인하십시오.

- 탑재 옵션은 선택 사항이며 CIFS 프로토콜이 정의합니다.
- 원격 서버가 보안이 중앙에서 처리되는 서버 모음에 속하는 경우 원격 서버가 속하는 도메인 이름을 입력합니다.
- NFS - 네트워크 파일 시스템:
 - 원격 시스템에 있는 파일을 찾을 수 있는 URL을 입력합니다.
 - 파일이 서버에 읽기 전용 가상 미디어로 표시되도록 하려면 확인란을 선택합니다.
 - 탑재 옵션은 선택 사항이며 NFS 프로토콜이 정의합니다. NFSv3과 NFSv4가 모두 지원됩니다. 예를 들어 NFSv3을 사용하려면 "nfsvers = 3" 옵션을 지정해야 합니다. NFS 서버가 AUTH_SYS 보안 특성을 사용하여 NFS 작업을 인증하는 경우, "sec = sys" 옵션을 지정해야 합니다.
- HTTPFS - HTTP Fuse-based File System:
 - 원격 시스템에 있는 파일을 찾을 수 있는 URL을 입력합니다.
 - 파일이 서버에 읽기 전용 가상 미디어로 표시되도록 하려면 확인란을 선택합니다.

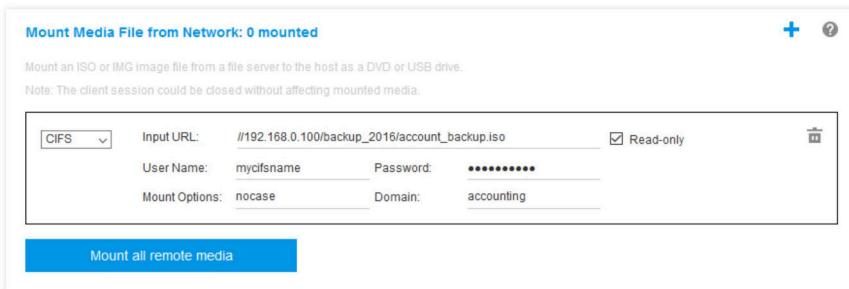
참고: Microsoft IIS에서 생성한 보안 인증서로 인해 탑재 프로세스 중에 오류가 발생할 수 있습니다. 이러한 경우에는 "미디어 탑재 오류 문제" 68페이지에서 문제 해결 방법을 찾아볼 수 있습니다.

파일을 가상 미디어로 탑재하려면 모든 원격 미디어 탑재를 클릭하십시오. 가상 미디어를 제거하려면 탑재된 미디어 오른쪽에 있는 휴지통 아이콘을 클릭하십시오.

- XClarity Controller 메모리에 파일을 최대 2개까지 업로드할 수 있으며 XClarity Controller RDOC 기능을 사용하여 가상 미디어로 탑재할 수 있습니다. 두 파일의 총 크기는 100MB를 초과할 수 없습니다. 이러한 파일은 원격 콘솔 세션이 종료된 경우에도 제거될 때까지 XClarity Controller 메모리에 유지됩니다. RDOC 기능은 파일 업로드 시 다음 메커니즘을 지원합니다.

- CIFS - Common Internet File System: 세부 정보는 위 설명을 참조하십시오. 예:

IP 주소가 192.168.0.100인 CIFS 서버의 backup_2016 디렉토리에 있는 account_backup.iso라는 ISO 파일을 서버의 읽기 전용 가상 드라이브로 탑재하려면 아래 그림과 같이 필드를 채웁니다. 이 예에서 192.168.0.100에 있는 서버는 "accounting" 도메인 아래에 있는 서버 모음의 구성원입니다. 도메인 이름은 옵션입니다. CIFS 서버가 도메인의 일부가 아닌 경우 도메인 필드를 비워 둡니다. CIFS "nocase" 탑재 옵션은 CIFS 서버에 파일 이름의 대문자/소문자 확인을 무시해야 한다는 점을 알려주는 이 예의 탑재 옵션 필드에서 지정됩니다. 탑재 옵션 필드는 옵션입니다. 이 필드에 사용자가 입력한 정보는 BMC에서 사용하지 않으며, 탑재 요청이 이루어지면 CIFS 서버로 전달되기만 합니다. CIFS 서버가 지원하는 옵션을 확인하려면 CIFS 서버 구현에 대한 설명서를 참조하십시오.

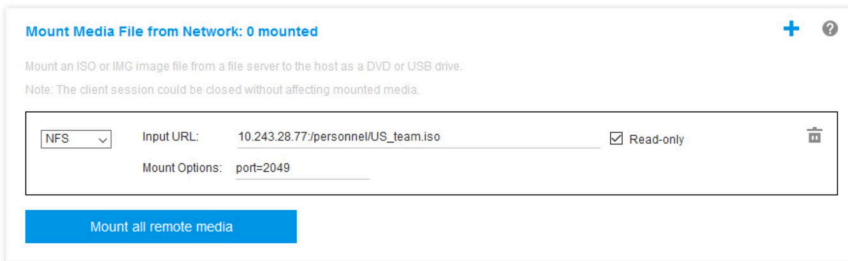


BMC는 URL 지정 시 지침을 제공합니다. 입력된 URL이 유효하지 않으면 탑재 버튼이 회색으로 표시되고, URL 필드 아래에 URL에 적합한 형식을 보여주는 빨간색 텍스트가 표시됩니다.

URL address in the form of //ipaddress/path/to/file or //domain-name/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items.

- NFS - 네트워크 파일 시스템: 세부 정보는 위 설명을 참조하십시오. 예:

IP 주소가 10.243.28.77인 NFS 서버의 "personnel" 디렉토리에 있는 US_team.iso라는 ISO 파일을 서버의 읽기 전용 가상 드라이브로 탑재하려면 아래 그림과 같이 필드를 채웁니다. NFS "port = 2049" 탑재 옵션은 네트워크 포트 2049를 사용하여 데이터를 전송하도록 지정합니다. 탑재 옵션 필드는 옵션입니다. 이 필드에 사용자가 입력한 정보는 탑재 요청이 이루어지면 NFS 서버로 전달됩니다. NFS 서버가 지원하는 옵션을 확인하려면 NFS 서버 구현에 대한 설명서를 참조하십시오.



BMC는 URL 지정 시 지침을 제공합니다. 입력된 URL이 유효하지 않으면 탑재 버튼이 회색으로 표시되고, URL 필드 아래에 URL에 적합한 형식을 보여주는 빨간색 텍스트가 표시됩니다.

URL address in the form of ipaddress:/path/to/file or domain-name:/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items.

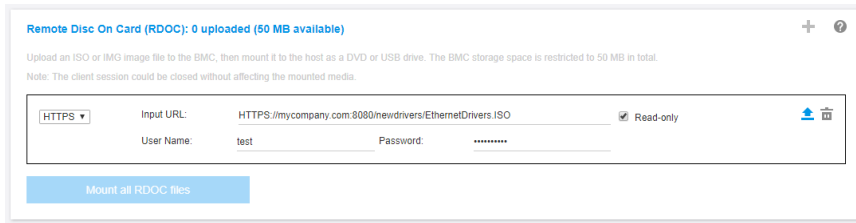
- HTTPS - Hypertext Transfer Protocol Secure:

- 원격 시스템에 있는 파일을 찾을 수 있는 URL을 입력합니다.
- 파일이 서버에 읽기 전용 미디어로 표시되도록 하려면 확인란을 선택합니다.
- 원격 시스템에 있는 파일에 액세스하려면 XClarity Controller에 필요한 자격 증명을 입력합니다.

참고:

- Microsoft IIS에서 생성한 보안 인증서로 인해 탑재 프로세스 중에 오류가 발생할 수 있습니다. 이러한 경우에는 "미디어 탑재 오류 문제" 68페이지에서 문제 해결 방법을 찾아볼 수 있습니다.
- XClarity Controller는 공백이 포함된 사용자 이름, 암호 또는 URL을 지원하지 않습니다. CIFS 서버에 사용자 이름 또는 암호에 공백으로 구성된 로그인 자격 증명 없이 그리고 URL에 공백이 포함되어 있지 않은지를 확인하십시오. 예:

네트워크 포트 8080을 사용하여 도메인 이름이 "mycompany.com"인 HTTPS 서버의 "newdrivers" 디렉토리에 있는 EthernetDrivers.ISO라는 ISO 파일을 서버의 읽기 전용 가상 드라이브로 탑재하려면 아래 그림과 같이 필드를 채웁니다.



BMC는 URL 지정 시 지침을 제공합니다. 입력된 URL이 유효하지 않으면 탑재 버튼이 회색으로 표시되고, URL 필드 아래에 URL에 적합한 형식을 보여주는 빨간색 텍스트가 표시됩니다.

URL address in the form of `https://ipaddress[:port]/path/to/file` or `HTTPS://domain-name[:port]/path/to/file`. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- SFTP - SSH 파일 전송 프로토콜

- 원격 시스템에 있는 파일을 찾을 수 있는 URL을 입력합니다.
- 파일이 서버에 읽기 전용 가상 미디어로 표시되도록 하려면 확인란을 선택합니다.
- 원격 시스템에 있는 파일에 액세스하려면 XClarity Controller에 필요한 자격 증명을 입력하십시오.

참고:

- XClarity Controller는 공백이 포함된 사용자 이름, 암호 또는 URL을 지원하지 않습니다. CIFS 서버에 사용자 이름 또는 암호에 공백으로 구성된 로그인 자격 증명 없이 그리고 URL에 공백이 포함되어 있지 않은지를 확인하십시오.
- XClarity Controller가 HTTPS 서버에 연결할 때 HTTPS 서버에서 사용하는 보안 인증서 정보를 보여주는 팝업 창이 표시됩니다. XClarity Controller는 보안 인증서의 진위 여부를 확인할 수 없습니다.

- 로컬 - Common Internet File System:

- 시스템에서 탑재할 ISO 또는 IMG 파일을 찾아봅니다.
- 파일이 서버에 읽기 전용 가상 미디어로 표시되도록 하려면 확인란을 선택합니다.

파일을 가상 미디어로 탑재하려면 모든 RDOC 파일 탑재를 클릭하십시오. 가상 미디어를 제거하려면 탑재된 미디어 오른쪽에 있는 휴지통 아이콘을 클릭하십시오.

독립형 도구

XClarity Controller를 사용하여 장치 또는 이미지(.iso / .img)를 탑재해야 하는 사용자의 경우 OneCLI 패키지의 rdmount 독립형 코드 부분을 사용할 수 있습니다. 특히 rdmount는 XClarity Controller에 대한 연결을 열어 호스트에 장치나 이미지를 탑재합니다.

rdmount의 구문은 다음과 같습니다.

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Iso 파일을 탑재하는 예:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

미디어 탑재 오류 문제

이 항목의 정보를 사용하여 미디어 탑재 오류 문제를 해결하십시오.

Microsoft IIS에서 생성한 보안 인증서 사용 시, 탑재 프로세스 중에 오류가 발생할 수 있습니다. 이 경우 보안 인증서를 openssl에서 생성한 새 인증서로 변경하십시오. 새로 생성한 pfx 파일은 별도로 Microsoft IIS 서버에 로드됩니다.

다음은 Linux 운영 체제에서 openssl을 통해 새 보안 인증서를 생성하는 방법을 보여 주는 예시입니다.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....+*****
.....+*****
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt server.csr server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt server.csr server.key server.pfx
```

원격 콘솔 세션 종료

이 주제에서는 원격 콘솔 세션을 종료하는 방법을 설명합니다.

원격 콘솔 세션을 종료하려면 원격 콘솔 및 가상 미디어 세션 창을 닫으십시오.

제 7 장 스토리지 구성

이 장의 정보를 사용하여 스토리지 구성에 사용할 수 있는 옵션을 이해합니다.

스토리지를 구성하면 다음 옵션을 사용할 수 있습니다.

- 스토리지 세부 정보
- RAID 설정

스토리지 세부 정보

스토리지 세부 정보 기능을 사용하려면 이 항목에 있는 정보를 사용하십시오.

이 기능은 위치, 제조업체, 제품 이름, 상태, 용량, 인터페이스, 미디어, 폼 팩터 및 기타 정보와 같은 세부 정보와 함께 저장 장치의 물리적 구조 및 저장 구성을 표시합니다.

SSD 드라이브 남은 수명 값이 임계값에 도달하거나 더 낮은 경우 경고 또는 위험 이벤트가 트리거됩니다. 경고 및 위험 이벤트의 기본 잔여 수명 값은 각각 8%와 4%입니다. 스토리지 세부 정보 옆의 톱니바퀴 아이콘을 클릭하여 임계값을 설정합니다.

PCIe 레인 x1 모드를 지원하는 SAS/SATA/NVMe(AnyBay) 백플레인을 구성하려면 백플레인 옆의 톱니바퀴 아이콘을 클릭한 다음 드라이브 베이 그룹을 선택하고 적용 버튼을 클릭하여 구성을 저장하십시오.

RAID 설정

RAID 기능을 수행하려면 이 주제의 정보를 사용하십시오.

이 주제의 정보를 사용하여 RAID 어댑터의 스토리지 풀, 관련 가상 디스크 및 드라이브를 보고 구성합니다. 시스템의 전원이 꺼져 있는 경우 전원을 켜야 RAID 정보를 볼 수 있습니다.

가상 드라이브 보기 및 구성

이 주제의 정보를 사용하여 가상 드라이브를 보고 구성합니다.

서버 구성에서 RAID 설정을 선택하면 배열 구성 탭이 선택되고 기존 가상 디스크가 기본적으로 표시됩니다. 논리 드라이브는 디스크 배열 및 컨트롤러별로 정렬됩니다. 가상 디스크에 대한 자세한 내용(예: 가상 디스크 스트립 크기) 및 부팅 가능 정보가 표시됩니다.

RAID 설정을 구성하려면 편집 모드 사용을 클릭하십시오.

편집 모드에서 컨트롤러 작업 메뉴를 클릭하고 현재 RAID 가상 디스크를 보고 새 RAID 가상 디스크를 만들 수 있습니다.

컨트롤러 작업 메뉴에서 다음 작업을 수행할 수 있습니다.

RAID 구성 지우기

선택한 컨트롤러에 대한 모든 구성 및 데이터를 지웁니다.

외부 드라이브 가져오기

감지된 외부 드라이브를 모두 가져옵니다. 외부 드라이브는 다른 RAID 구성에서 현재 RAID 컨트롤러로 이동된 드라이브입니다.

참고: 감지된 외부 드라이브가 없으면 통보됩니다.

외부 구성 관리

감지된 외부 드라이브를 모두 가져옵니다. 외부 드라이브는 다른 RAID 구성에서 현재 RAID 컨트롤러로 이동된 드라이브입니다.

참고: 감지된 외부 드라이브가 없으면 통보됩니다.

특정 컨트롤러에 대한 현재 RAID 가상 디스크 정보는 각각의 '가상 디스크 카드'로 표시됩니다. 각 카드에는 가상 디스크 이름, 상태, 용량 및 작업과 같은 정보가 표시됩니다. 연필 아이콘을 사용하면 정보를 편집할 수 있고, 휴지통 아이콘을 사용하면 '가상 디스크 카드'를 삭제할 수 있습니다.

참고: 용량 및 RAID 수준은 변경할 수 없습니다.

가상 디스크 이름을 클릭하면 가상 디스크 속성 창이 표시됩니다.

새 RAID 가상 디스크 만들기

새 RAID 가상 디스크를 만들려면 아래에 나와 있는 단계를 따르십시오.

참고: 남아 있는 스토리지 용량이 없으면 새 가상 디스크를 만들 수 없습니다.

1. 사용 가능한 스토리지 용량이 있는 드라이브 또는 디스크 배열 선택

- a. 새 디스크 배열에서 가상 디스크를 만드는 경우 RAID 수준을 지정해야 합니다.

참고: 선택할 드라이브가 부족한 경우 다음을 클릭하면 RAID 수준 필드에 오류 메시지가 표시됩니다.

- b. 일부 RAID 수준의 경우 스팬이 필요합니다. 최소 드라이브 양도 스팬에 표시되어야 합니다. 이러한 유형의 상황에서는 스팬 번호 필드에 스팬 번호를 지정하고, 드라이브 옆의 드롭 다운 메뉴에서 구성원 또는 핫 스패어를 선택한 다음, 가상 디스크를 만드는 데 사용할 드라이브 옆에 있는 확인란을 선택합니다.
- c. 기존 디스크 배열에서 가상 디스크를 만들려면 사용 가능한 용량이 있는 디스크 배열을 선택해야 합니다.

2. 가상 디스크 만들기

- a. 기본적으로 가상 디스크를 만드는 데 모든 스토리지 용량이 사용됩니다. 모든 스토리지가 사용되면 추가 아이콘이 사용 안 함으로 설정됩니다. 연필 아이콘을 클릭하여 용량 또는 기타 속성을 변경할 수 있습니다.
- b. 스토리지 용량 일부만 사용하도록 첫 번째 가상 디스크를 편집하는 경우 추가 아이콘이 사용으로 설정됩니다. 가상 디스크 추가 창을 표시하려면 이 아이콘을 클릭합니다.
- c. 제거 아이콘을 클릭하여 가상 디스크를 제거합니다. 가상 디스크가 한 개만 있는 경우에는 이 아이콘이 표시되지 않습니다. 제거 아이콘을 클릭하면 선택한 행이 바로 삭제됩니다. 가상 디스크가 아직 만들어지지 않았기 때문에 확인 창이 표시되지 않습니다.
- d. 만들기 시작을 클릭하여 프로세스를 시작합니다.

참고: 컨트롤러가 지원되지 않는 경우 메시지가 표시됩니다.

스토리지 자원 명세 보기 및 구성

이 주제의 정보를 사용하여 스토리지 인벤토리를 보고 구성합니다.

스토리지 자원 명세 탭에서 디스크 배열, RAID 컨트롤러에 대한 연관 가상 드라이브 및 드라이브를 보고 구성할 수 있습니다.

• RAID 구성을 지원하는 스토리지 장치의 경우:

1. 컨트롤러에 구성된 디스크 배열이 포함되어 있는 경우 디스크 배열을 기반으로 설치된 드라이브가 표시됩니다. 다음에는 창에 표시되는 항목에 대한 설명이 나와 있습니다.

- 테이블 제목: 디스크 배열 ID, RAID 수준 및 총 드라이브 수를 표시합니다.
 - 테이블 내용: 드라이브 이름, 드라이브 상태, 유형, 제품, 제조업체, 일련 번호 및 작업과 같은 기본 속성을 나열합니다. 자원 명세 페이지로 이동하여 XClarity Controller에서 검색할 수 있는 모든 속성을 볼 수 있습니다.
 - 작업: 다음에는 수행할 수 있는 작업 항목이 표시됩니다. 일부 작업은 드라이브가 다른 상태인 경우 사용할 수 없습니다.
 - 핫 스페어 할당: 드라이브를 전역 핫 스페어 또는 전용 핫 스페어로 지정합니다.
 - 핫 스페어 제거: 핫 스페어에서 드라이브를 제거합니다.
 - 디스크 드라이브를 오프라인 상태로 만들기: 드라이브를 오프라인 상태로 설정합니다.
 - 디스크 드라이브를 온라인 상태로 만들기: 드라이브를 온라인 상태로 설정합니다.
 - 재구축 시작: RAID를 재구축합니다.
 - 디스크 드라이브를 재사용 가능으로 만들기: 드라이브를 재사용 가능으로 설정합니다.
 - 디스크 드라이브를 누락으로 만들기: 드라이브를 누락으로 설정합니다.
 - 드라이브 양호 상태를 JBOD로 만들기: JBOD 디스크 배열에 드라이브를 추가합니다.
 - 드라이브를 구성되지 않은 양호 상태로 만들기: 드라이브를 배열로 구성할 수 있도록 만들거나 비상 핫 스페어로 사용할 수 있도록 만듭니다.
 - 드라이브를 구성되지 않은 비정상 상태로 만들기: 드라이브를 배열에서 사용되거나 비상 핫 스페어로 사용되지 않도록 비정상 상태로 표시합니다.
 - 디스크 드라이브를 제거 준비로 만들기: 제거를 위해 드라이브를 설정합니다.
2. 컨트롤러에 아직 구성되지 않은 드라이브가 포함되어 있는 경우 해당 드라이브가 비RAID 디스크 드라이브 테이블에 표시됩니다. JBOD를 구성 준비로 변환 옵션을 클릭하면 이 작업 항목을 지원하는 모든 드라이브를 보여주는 창이 표시됩니다. 변환할 드라이브를 한 개 이상 선택할 수 있습니다.

RAID 구성을 지원하지 않는 스토리지 장치의 경우: XClarity Controller는 일부 드라이브의 속성을 검색하지 못할 수 있습니다.

제 8 장 서버 펌웨어 업데이트

서버 펌웨어를 업데이트하려면 이 주제의 정보를 사용하십시오.

펌웨어 업데이트 개요

서버 펌웨어 업데이트에 대한 일반 정보입니다.

왼쪽 창에서 펌웨어 업데이트를 클릭하면 펌웨어 정보의 개요가 제공됩니다.

- 리포지토리에서 업데이트: 일괄 업데이트를 위해 서버 펌웨어를 원격 CIFS/NFS 리포지토리와 동기화합니다("리포지토리에서 업데이트" 76페이지 참조).
- 시스템 펌웨어: 시스템 펌웨어 상태, 버전 및 시스템 펌웨어 업데이트에 대한 개요입니다.

참고: 자동 동기화를 클릭하여 백업할 기본 BMC 자동 승격을 활성화 또는 비활성화합니다. 이 설정이 활성화되면 기본 백크가 ISM(이미지 안정성 메트릭) 측정을 통과한 후 보류 중인 백업 백크 펌웨어가 기본 백크에서 동기화됩니다.

- 어댑터 펌웨어: 설치된 어댑터 펌웨어, 상태, 버전 및 어댑터 펌웨어 업데이트에 대한 개요입니다.
- 전원 공급 장치 펌웨어: 전원 공급 장치 펌웨어 버전 및 PSU 펌웨어 업데이트에 대한 개요입니다.
- 드라이브 백플레인 PSoc 펌웨어: 백플레인 펌웨어 버전의 개요입니다. 시스템 펌웨어 업데이트를 수행합니다.

BMC 기본 및 백업 버전을 포함하여 BMC, UEFI, LXPM, LXPM 드라이버, 내장 OS, FPGA 및 어댑터의 현재 상태 및 펌웨어 버전이 표시됩니다. 펌웨어 상태에는 다음 세 가지 범주가 있습니다.

- 활성화: 펌웨어가 활성화 상태입니다.
- 비활성: 펌웨어가 활성화 상태가 아닙니다.
- 다시 시작 보류 중: 펌웨어 이미지가 업데이트되었으며 BMC의 서버가 다시 시작된 후에 적용됩니다.
- 해당사항 없음: 이 구성 요소에 대한 펌웨어가 설치되어 있지 않습니다.

주의:

- UEFI를 업데이트하기 전에 XCC 및 IMM을 최신 버전으로 업데이트해야 합니다. 다른 순서로 업데이트하면 잘못된 동작이 발생할 수 있습니다.
- 잘못된 펌웨어 업데이트를 설치하면 서버가 오작동할 수도 있습니다. 펌웨어 또는 장치 드라이버 업데이트를 설치하기 전에 모든 추가 정보 파일과 다운로드된 업데이트와 함께 제공된 히스토리 파일을 변경하십시오. 이러한 파일에는 이전 펌웨어 또는 장치 드라이버 버전에서 최신 버전으로 업데이트하는 데 필요한 특별한 절차를 포함하여 업데이트에 관한 중요한 정보와 업데이트 설치에 대한 절차가 들어 있습니다. 웹 브라우저에 XCC 캐시 데이터가 포함되어 있을 수 있으므로 XCC 펌웨어가 업그레이드된 후에는 웹 페이지를 다시 로드하는 것이 좋습니다.
- SATA M.2 어댑터를 제외하고 AMD 프로세서 서버는 대역 외 어댑터 펌웨어 업데이트를 지원하지 않습니다.
- 일부 펌웨어 업데이트는 펌웨어 활성화 또는 내부 업데이트를 수행하는 시스템 재시작이 필요합니다. 시스템 부팅에서 이 프로세스를 '시스템 유지 관리 모드'라고 하며 이는 사용자 전원 작업을 일시적으로 허용하지 않습니다. 이 모드는 펌웨어 업데이트 중에도 활성화됩니다. 사용자는 시스템이 유지 관리 모드로 전환될 때 AC 전원을 분리해서는 안 됩니다.

시스템, 어댑터, PSU 펌웨어 업데이트

시스템 펌웨어, 어댑터 펌웨어, PSU 펌웨어를 업데이트하는 단계입니다.

시스템 펌웨어, 어댑터 펌웨어, PSU 펌웨어 업데이트를 수동으로 적용하려면 다음 단계를 완료하십시오.

1. 각 기능 내에서 펌웨어 업데이트를 클릭합니다. 서버 펌웨어 업데이트 창이 열립니다.
2. **찾아보기...**를 클릭하여 사용할 펌웨어 업데이트 파일을 선택합니다.
3. 선택하려고 하는 파일로 이동하여 열기를 클릭하십시오. 선택된 파일이 표시되면 서버 펌웨어 업데이트 창으로 되돌아갑니다.
4. 다음을 클릭하여 업로드를 시작하고 선택된 파일의 프로세스를 확인하십시오. 파일을 업로드하면서 확인하는 동안 진행계가 표시됩니다. 이 상태 창을 보고 업로드하려고 선택한 파일이 올바른 파일인지 확인할 수 있습니다. 시스템 펌웨어의 경우, 상태 창에 BMC, UEFI 또는 LXPM과 같은 업데이트할 펌웨어 파일의 유형과 관련된 정보가 표시됩니다. 펌웨어 파일을 성공적으로 업로드 및 확인하고 다음을 클릭하여 업데이트할 장치를 선택하십시오.
5. 업데이트를 클릭하여 펌웨어 업데이트를 시작하십시오. 진행계에는 업데이트의 진행 상태가 표시됩니다. 펌웨어 업데이트가 성공적으로 완료되면 **마침**을 클릭하십시오. 업데이트를 적용하기 위해 XClarity Controller를 다시 시작해야 하는 경우에는 경고 메시지가 표시됩니다. XClarity Controller를 다시 시작하는 방법에 대한 세부 정보는 "[전원 작업](#)" 56페이지의 내용을 참조하십시오.

리포지토리에서 업데이트

원격 리포지토리에서 서버 펌웨어 업데이트

개요

참고: CIFS/NFS/HTTPS/Onboard 펌웨어 기록 기능을 사용하려면 XCC Premier 라이선스가 필요합니다.

XCC에는 업데이트 번들(서비스 팩) 패키지를 사용하여 서버에서 펌웨어를 업데이트하는 프로세스가 도입되었습니다. 이 기능은 단일 API 또는 Redfish 클라이언트 도구를 사용하여 OOB 및 IB 펌웨어 패키지 등 시스템의 모든 펌웨어를 업데이트함으로써 프로세스를 간소화합니다. 이 프로세스의 예로는 적용 가능한 펌웨어 패키지 식별, 원격 HTTP/HTTPS 서버에서 다운로드 및 추출, 웹 브라우저를 통해 BMC 내부 스토리지에 업로드, CIFS 또는 NFS 공유 디렉토리에서 마운트가 있습니다.

CIFS 또는 NFS 마운트를 사용하는 경우, 메타데이터에 지정된 펌웨어 페이로드와 함께 메타데이터(JSON 형식) 파일을 네트워크 공유 파일 시스템의 루트 디렉토리에 배치해야 합니다. 서버의 microSD 장치는 기록 리포지토리를 저장할 수 있으므로 사용자가 펌웨어 수준을 롤백할 수 있습니다.

펌웨어 패키지에 대역외 펌웨어 업데이트를 지원하지 않는 페이로드가 포함된 경우 BMC는 서버를 시작하고 업데이트를 수행하기 전에 BMC에 설치된 내장 OS 이미지에서 부팅하도록 서버를 구성합니다.

번들 및 메타데이터 업데이트

업데이트 번들(서비스 팩)은 펌웨어 번들이 압축된 파일입니다. 여기에는 시스템 구성 요소에 적합한 하나 이상의 펌웨어 패키지가 포함됩니다. 리포지토리에서 XCC의 업데이트 기능에서는 업데이트 번들 파일을 사용합니다. 압축을 푼 번들 파일에는 메타데이터와 페이로드 바이너리가 포함됩니다. JSON 메타데이터 파일은 번들 파일에 포함된 펌웨어 이미지 종류에 대한 정보를 XCC에 제공하고 페이로드 바이너리는 펌웨어 이미지를 제공합니다.

XCC 내부의 펌웨어 리포지토리

업데이트 번들에는 여러 펌웨어 패키지가 포함될 수 있으며 XCC는 새로운 기능을 위해 플래시에 2GB 공간을 예약합니다. 새 번들이 수신되면 XCC는 이전 데이터를 정리합니다. 일부 플랫폼은 MicroSD 카드를 사용하여 추가 스토리지를 제공하고 XCC는 마지막 업데이트된 번들을 SD 카드의 기록 리포지토리로 이동시킵니다. 펌웨어 기록 리포지토리에는 최대 3개의 번들을 저장할 수 있으며 사용자는 펌웨어 롤백 기능을 사용하여 이전 번들로 되돌릴 수 있습니다.



참고:

- 업데이트 번들에 시스템에서 사용할 수 있는 OOB 펌웨어 패키지만 포함된 경우 XCC는 시스템 전원 상태를 변경하지 않습니다. PCI 장치 펌웨어를 업데이트하려면 시스템 전원이 켜져 있어야 합니다.
- 업데이트 번들에 시스템에서 사용할 수 있는 IB 펌웨어 패키지가 포함된 경우 XCC는 업데이트 전에 시스템 전원 상태를 저장하고 업데이트 번들이 업데이트된 후 전원 상태를 복원합니다. 업데이트 프로세스 중에 XCC는 호스트를 내장 OS로 재부팅합니다.
- 업데이트 번들에 전제 조건 수준의 UEFI 펌웨어가 포함되어 있고 현재 설치된 UEFI 버전이 해당 수준을 충족하지 않거나 그보다 낮은 경우, XCC는 먼저 UEFI 펌웨어 업데이트를 수행하기 위해 시스템 전원을 끕니다.
- 업데이트 번들에 전제 조건 수준의 XCC 펌웨어가 포함되어 있고 현재 설치된 XCC 버전이 해당 수준을 충족하지 않거나 그보다 낮은 경우, XCC는 자체 업그레이드 후 먼저 재부팅합니다.

WebGUI로 업데이트

리포지토리에서 업데이트를 통해 사용자가 XCC를 구성하여 서버 펌웨어를 내부 스토리지와 동기화할 수 있습니다. 펌웨어 리포지토리에 2진 및 메타데이터 파일 또는 업데이트 번들 메타데이터 JSON 및 해당 2진 파일을 비롯한 패키지가 포함되어야 합니다. XCC는 메타데이터 JSON 파일을 구문 분석하여 이 특정 시스템 하드웨어에 대한 OOB 업데이트를 지원하는 펌웨어 패키지를 선택한 다음 배치 업데이트를 시작합니다.

리포지토리에서 업데이트하려면 다음 단계를 완료하십시오.

1. 내부 스토리지를 사용하는 경우 펌웨어 패키지 가져오기를 클릭하고 펌웨어 패키지(.tgz 또는 zip 형식)를 찾습니다.
2. 시스템 업데이트를 클릭하여 배치 업데이트를 시작합니다.
3. 세부 정보 보기를 클릭하여 업데이트 상태를 확인합니다.
 - 녹색 확인 표시  : 펌웨어 업그레이드가 완료된 상태입니다.
 - 빨간색 X 표시  : 펌웨어 업그레이드에 실패한 상태입니다.
 - 업데이트 중: 펌웨어 업그레이드를 진행 중인 상태입니다.
 - 취소: 펌웨어 업그레이드가 취소된 상태입니다.
 - 대기 중: 펌웨어 업그레이드 배포 대기 중입니다.

참고: 업데이트 중지를 클릭하면 현재 설치 패키지 업데이트가 완료된 후 대기열에서 업데이트가 취소됩니다.

4. CIFS 또는 NFS를 사용하는 경우 마운트 해제를 클릭하여 원격 리포지토리 연결을 해제합니다.
5. 업데이트를 적용하기 위해 XClarity Controller를 다시 시작해야 하는 경우에는 경고 메시지가 표시됩니다. XClarity Controller를 다시 시작하는 방법에 대한 세부 정보는 "[전원 작업](#)" 56페이지의 내용을 참조하십시오.

참고: 시스템에 MicroSD 카드가 설치되어 있는 경우 업데이트 번들의 업데이트 기록을 확인하고 업데이트 번들의 인덱스를 선택하여 펌웨어 롤백을 수행할 수 있습니다. 이 프로세스는 기록 업데이트 번들이 MicroSD 내부에 배치된다는 점을 제외하면 리포지토리에서 업데이트하는 방식과 유사합니다.

제 9 장 라이선스 관리

Lenovo XClarity Controller 라이선스 관리에서는 옵션 서버 및 시스템 관리 기능을 설치 및 관리할 수 있습니다.

다양한 수준의 XClarity Controller 펌웨어 기능 및 서버에 사용할 수 있는 기능이 있습니다. 서버에 설치된 펌웨어 기능의 수준은 하드웨어 유형에 따라 다릅니다.

정품 인증 키를 구입 및 설치하면 XClarity Controller 기능을 업그레이드할 수 있습니다.

정품 인증 키를 주문하려면 영업 담당자 또는 비즈니스 파트너에게 문의하십시오.

XClarity Controller 웹 인터페이스 또는 XClarity Controller CLI를 사용하여 구입한 옵션 기능을 사용할 수 있는 정품 인증 키를 수동으로 설치합니다. 키를 활성화하기 전에:

- XClarity Controller에 로그인하는 데 사용하는 시스템에 정품 인증 키가 있어야 합니다.
- 라이선스 키를 주문해서 우편이나 이메일을 통해 인증 코드를 받았어야 합니다.

XClarity Controller 웹 인터페이스를 사용한 정품 인증 키 관리에 대한 정보는 "[정품 인증 키 설치](#)" 79페이지, "[정품 인증 키 제거](#)" 79페이지 또는 "[정품 인증 키 내보내기](#)" 80페이지를 참조하십시오. XClarity Controller CLI를 사용한 정품 인증 키 관리에 대한 정보는 "[keycfg 명령](#)" 107페이지의 내용을 참조하십시오.

XClarity Controller 라이선스 관리 시 ID를 등록하려면 다음 링크를 클릭하십시오.

<https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome>

Lenovo 서버의 라이선스 관리에 대한 추가 정보는 다음 Lenovo Press 웹 사이트에서 확인할 수 있습니다.

<https://lenovopress.com/redp4895-using-lenovo-features-on-demand>

정품 인증 키 설치

이 주제의 정보를 사용하여 옵션 기능을 서버에 추가합니다.

정품 인증 키를 설치하려면 다음 단계를 완료하십시오.

단계 1. BMC 구성에서 라이선스를 클릭하십시오.

단계 2. 라이선스 업그레이드를 클릭하십시오.

단계 3. 새 라이선스 추가 창에서 찾아보기를 클릭한 후 파일 업로드 창에 추가할 정품 인증 키를 선택하고 열기를 클릭하여 파일을 추가하십시오. 키 추가를 마치려면 정품 인증 키 추가 창에서 가져오기를 클릭합니다.

참고: 정품 인증 키가 유효하지 않으면 오류 창이 나타납니다.

정품 인증 키 제거

이 주제의 정보를 사용하여 서버에서 옵션 기능을 삭제합니다.

정품 인증 키를 제거하려면 다음 단계를 완료하십시오.

단계 1. BMC 구성에서 라이선스를 클릭하십시오.

단계 2. 제거할 정품 인증 키를 선택한 후 삭제를 클릭하십시오.

단계 3. 정품 인증 키 삭제 확인 창에서 확인을 클릭하여 정품 인증 키 삭제를 확인합니다. 선택한 정품 인증 키가 서버에서 제거되며 더 이상 라이선스 관리 페이지에 나타나지 않습니다.

정품 인증 키 내보내기

이 주제의 정보를 사용하여 서버에서 옵션 기능을 내보냅니다.

정품 인증 키를 내보내려면 다음 단계를 완료하십시오.

단계 1. BMC 구성에서 라이선스를 클릭하십시오.

단계 2. 라이선스 관리 페이지에서 내보낼 정품 인증 키를 선택한 후 내보내기를 클릭하십시오.

단계 3. 선택한 라이선스 내보내기 창에서 내보내기를 클릭하여 정품 인증 키 내보내기 요청을 확인합니다.

단계 4. 파일을 저장할 디렉토리를 선택하십시오. 선택한 정품 인증 키가 서버에서 내보내집니다.

제 10 장 명령줄 인터페이스

이 주제의 정보를 사용하여 XClarity Controller 웹 인터페이스를 사용할 필요 없이 XClarity Controller를 관리 및 모니터링하는 명령을 입력합니다.

XClarity Controller CLI(명령줄 인터페이스)를 사용하여 웹 인터페이스를 사용할 필요 없이 XClarity Controller에 액세스합니다. 웹 인터페이스가 제공하는 관리 기능의 서브세트를 제공합니다.

SSH 세션을 통해 CLI에 액세스할 수 있습니다. CLI 명령을 실행하기 전에 XClarity Controller로 인증을 해야 합니다.

명령줄 인터페이스 액세스

이 주제의 정보를 사용하여 CLI에 액세스합니다.

CLI에 액세스하려면 XClarity Controller IP 주소에 대한 SSH 세션을 시작하십시오(자세한 내용은 "[직렬을 SSH로 방향 재지정 구성](#)" 81페이지 참조).

명령줄 세션에 대한 로그인

이 주제의 정보를 사용하여 명령줄 세션에 로그인합니다.

명령줄에 로그인하려면 다음 단계를 완료하십시오.

- 단계 1. XClarity Controller 연결을 설정하십시오.
- 단계 2. 사용자 이름 메시지에서 사용자 ID를 입력하십시오.
- 단계 3. 암호 프롬프트에서 XClarity Controller에 로그인하는 데 사용하는 암호를 입력하십시오.

참고: 명령줄 프롬프트는 system>입니다. 명령줄 세션은 명령줄에 exit을 입력할 때까지 계속됩니다. 로그오프되면 세션이 끝납니다.

직렬을 SSH로 방향 재지정 구성

이 주제는 XClarity Controller를 직렬 터미널 서버로 사용하는 것에 대한 정보를 제공합니다.

직렬을 SSH로 방향 재지정하면 시스템 관리자가 XClarity Controller를 직렬 터미널 서버로 사용할 수 있습니다. 직렬 방향 재지정을 사용하면 SSH 연결에서 서버 직렬 포트에 액세스할 수 있습니다.

참고: CLI console 1 명령은 COM 포트로 직렬 포트 방향 재지정 세션을 시작하는 데 사용됩니다.

세션 예

```
$ ssh USERID@10.240.1.12  
Password:
```

```
system>
```

SSH 세션의 모든 트래픽은 COM2로 라우팅됩니다.

```
ESC (
```

종료 키 키 순서를 입력하여 CLI로 되돌아가십시오. 이 예에서는 Esc를 누른 후 왼쪽 괄호를 입력하십시오. IMM CLI로 리턴을 나타내는 CLI 프롬프트가 표시됩니다.

```
system>
```

명령 구문

이 주제에서 제공하는 지침을 확인하고 CLI에 명령을 입력하는 방법을 알아보십시오.

명령을 사용하기 전에 다음의 내용을 읽어보십시오.

- 각 명령의 형식은 다음과 같습니다.
command [arguments] [-options]
- 명령 구문은 대소문자를 구분합니다.
- 명령 이름은 모두 소문자입니다.
- 모든 인수는 명령 바로 다음에 표시해야 합니다. 옵션은 인수 바로 다음에 표시해야 합니다.
- 각 옵션 앞에는 항상 하이픈(-)을 표시해야 합니다. 옵션은 짧은 옵션(단일 문자) 또는 긴 옵션(여러 개의 문자)가 될 수 있습니다.
- 옵션에 인수가 있는 경우에는 인수가 필수입니다, 예,
ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
여기서 ifconfig는 명령이고 eth0은 인수이며 -i, -g 및 -s는 옵션입니다. 이 예에서는 모든 옵션에 인수가 있습니다.
- 대괄호는 인수 또는 옵션이 선택적이라는 것을 나타냅니다. 대괄호는 입력하는 명령의 일부가 아닙니다.

기능 및 제한사항

다음에는 CLI 기능 및 제한에 대한 정보가 포함되어 있습니다.

CLI에는 다음과 같은 기능 및 제한사항이 있습니다.

- 여러 동시 CLI 세션은 SSH를 통해 허용됩니다.
- 라인당 명령 한 개가 허용됩니다(공백을 포함하여 1024자로 제한).
- 긴 명령에 연속 문자는 없습니다. 유일한 편집 기능은 방금 입력한 문자를 삭제할 수 있는 Backspace 키입니다.
- 위 화살표 및 아래 화살표 키를 사용하여 마지막 8개의 명령을 통해 찾아볼 수 있습니다. history 명령은 마지막 명령 8개에 대한 목록을 표시하며 다음 예에서와 같이 명령을 실행하기 위한 단축키로 사용할 수 있습니다.

```
system > history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
```


-l 00:00:00:00:00:00

system >

- CLI에서 출력 버퍼 제한은 2KB입니다. 버퍼링은 없습니다. 개별 명령의 출력은 2,048자 이하여야 합니다. 직렬 방향 재지정 모드에는 이 제한이 적용되지 않습니다(직렬 방향 재지정하는 동안 데이터가 버퍼됨).

- 간단한 텍스트 메시지는 예를 들어 다음과 같이 명령 실행 상태를 표시하는 데 사용됩니다.

```
system> power on
```

```
ok
```

```
system> power state
```

```
Power: On
```

```
State: System power off/State unknown
```

```
system>
```

- 명령 구문은 대소문자를 구분합니다.

- 옵션과 인수 사이에는 최소한 1개의 공백이 있어야 합니다. 예를 들어 `ifconfig eth0 -i192.168.70.133`은 올바른 구문입니다. 올바른 구분은 `ifconfig eth0 -i 192.168.70.133`입니다.

- 모든 명령에는 구문 도움말을 제공하는 `-h`, `-help` 및 `?` 옵션이 있습니다. 다음에 제시된 예의 결과는 모두 동일합니다.

```
system> power -h
```

```
system> power -help
```

```
system> power ?
```

- 다음 섹션에서 설명되는 일부 명령은 시스템 구성에 사용하지 못할 수 없습니다. 구성에서 지원하는 명령 목록을 보려면 다음 예에 나와 있는 것과 같이 `help` 또는 `?` 옵션을 사용합니다.

```
system> help
```

```
system> ?
```

알파벳 명령 목록

이 주제에는 알파벳 순서로 CLI 명령의 목록이 포함되어 있습니다. 각 명령의 주제로 연결되는 링크가 제공됩니다. 각 명령 주제는 명령, 기능, 구문 및 사용에 대한 정보를 제공합니다.

모든 XClarity Controller CLI 명령의 전체 목록(알파벳 순서)은 다음과 같습니다.

- ["accsecfg 명령" 96페이지](#)
- ["adapter 명령" 138페이지](#)
- ["asu 명령" 97페이지](#)
- ["backup 명령" 100페이지](#)
- ["batch 명령" 128페이지](#)
- ["clearlog 명령" 85페이지](#)
- ["clock 명령" 129페이지](#)
- ["dbgshbmc 명령" 140페이지](#)
- ["dhcinfo 명령" 100페이지](#)
- ["dns 명령" 101페이지](#)
- ["encaps 명령" 102페이지](#)
- ["ethtousb 명령" 102페이지](#)
- ["exit 명령" 85페이지](#)
- ["fans 명령" 86페이지](#)
- ["firewall 명령" 103페이지](#)
- ["fuelg 명령" 95페이지](#)
- ["hashpw 명령" 104페이지](#)

- "help 명령" 85페이지
- "history 명령" 85페이지
- "ifconfig 명령" 105페이지
- "info 명령" 130페이지
- "keycfg 명령" 107페이지
- "ldap 명령" 107페이지
- "led 명령" 87페이지
- "mhlog 명령" 86페이지
- "ntp 명령" 109페이지
- "portcontrol 명령" 109페이지
- "ports 명령" 110페이지
- "power 명령" 93페이지
- "pxeboot 명령" 96페이지
- "rdmount 명령" 111페이지
- "readlog 명령" 88페이지
- "reset 명령" 95페이지
- "restore 명령" 112페이지
- "roles 명령" 112페이지
- "rtd 명령" 113페이지
- "seccfg 명령" 113페이지
- "securityinfo 명령" 114페이지
- "securitymode 명령" 114페이지
- "servicelog 명령" 90페이지
- "snmp 명령" 115페이지
- "snmpalerts 명령" 117페이지
- "spreset 명령" 130페이지
- "sshcfcg 명령" 118페이지
- "sslcfcg 명령" 119페이지
- "storage 명령" 131페이지
- "syshealth 명령" 91페이지
- "syslock 명령" 121페이지
- "temps 명령" 92페이지
- "thermal 명령" 122페이지
- "tls 명령" 123페이지
- "trespass 명령" 123페이지
- "uefipw 명령" 124페이지
- "usbeth 명령" 124페이지
- "users 명령" 125페이지
- "volts 명령" 92페이지
- "vpd 명령" 93페이지

유틸리티 명령

이 주제에서는 Utility CLI 명령의 목록을 알파벳 순서로 제공합니다.

현재 3가지 유틸리티 명령이 있으며 다음과 같습니다.

exit 명령

이 명령을 사용하여 CLI 세션에서 로그오프합니다.

exit 명령을 사용하여 CLI 세션에서 로그오프 및 종료합니다.

help 명령

이 명령은 모든 명령의 목록을 표시합니다.

help 명령을 사용하여 각 명령에 대한 간단한 설명을 포함해 모든 명령의 목록을 표시합니다. 또한 명령 프롬프트에서 ?을 입력할 수 있습니다.

history 명령

이 명령은 이전에 실행된 명령의 목록을 제공합니다.

history 명령을 사용하여 실행된 명령 중 마지막 8개의 색인된 이력 목록을 표시합니다. 색인을 단축키(앞에 ! 표시)로 사용하여 이 이력 목록의 명령을 다시 실행할 수 있습니다.

예:

```
system> history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-L 00:00:00:00:00:00
system>
```

모니터 명령

이 주제에서는 CLI 모니터 명령의 목록을 알파벳 순서로 제공합니다.

현재 11가지 모니터 명령이 있으며 다음과 같습니다.

clearlog 명령

이 명령은 IMM 이벤트 로그를 지우는 데 사용됩니다.

IMM의 이벤트 로그를 지우려면 `clearlog` 명령을 사용하십시오. 이 명령을 사용하려면 이벤트 로그를 지울 수 있는 권한이 있어야 합니다.

참고: 이 명령은 지원 담당자만 사용할 수 있습니다.

구문:
`clearlog [-options]`

표 4. clearlog 옵션

옵션	설명	값
-t	이벤트 유형, 삭제할 이벤트 유형을 선택 하십시오. 별도로 지정하지 않으면 모든 이벤트 유형이 선택됩니다.	전체, 플랫폼, 감사 <ul style="list-style-type: none"> 전체: 플랫폼 이벤트와 감사 이벤트를 포함한 모든 이벤트 유형. 플랫폼: 플랫폼 이벤트 유형. 감사: 감사 이벤트 유형.

예:
`system> clearlog`
 All event log cleared successfully
`system>`
`system> clearlog -t all`
 All event log cleared successfully
`system>`
`system> clearlog -t platform`
 Platform event log cleared successfully
`system>`
`system> clearlog -t audit`
 Audit event log cleared successfully
`system>`

fans 명령

이 명령은 서버 팬의 속도를 표시하는 데 사용됩니다.

fans 명령을 사용하여 각 서버 팬의 속도를 표시합니다.

예:
`system> fans`
 fan1 75%
 fan2 80%
 fan3 90%
`system>`

mhlog 명령

이 명령을 사용하여 유지보수 내역 활동 로그 항목을 표시 및 구성합니다.

구문:
`mhlog [-options]`

표 5. mhlog 옵션

옵션	설명	값
-c	카운트 항목 표시	1~250
-i	인덱스의 시작 항목 표시	1~250

표 5. mhlog 옵션 (계속)

옵션	설명	값
-f	로그 파일의 원격 파일 이름	로그 파일의 파일 이름에 유효한 파일 이름
-ip	TFTP/SFTP 서버의 주소	TFTP/SFTP 서버에 유효한 IP 주소
-pn	tftp/sftp 서버의 포트 번호	TFTP/SFTP 서버의 유효한 포트 번호(기본값 69/22).
-u	SFTP 서버의 사용자 이름	SFTP 서버의 유효한 사용자 이름
-pw	SFTP 서버의 암호	SFTP 서버의 유효한 암호

예:

```
system> mhlog
Type      Message                                     Time
-----
Hardware  SAS Backplane1(SN: XXXX9CE009L) is added.    05/08/2020,04:23:18
Hardware  CPU 1(SKU NO: 50844440) is added.           05/08/2020,04:23:22
Hardware  CPU 2(SKU NO: 50844440) is added.           05/08/2020,04:23:22
Hardware  M2 Card(SN: R1SH9AJ0037) is added.          05/08/2020,04:23:22
Firmware  Primary XCC firmware is updated to TGBT99T by XCC Web. 05/08/2020,06:40:37
Firmware  Primary XCC firmware is activated to TGBT99T. 05/08/2020,06:41:26
Hardware  PSU1(SN: D1D694C0075) is added.            05/08/2020,06:43:28
system>
```

led 명령

이 명령을 사용하여 LED 상태를 표시 및 설정합니다.

led 명령은 서버 LED 상태를 표시 및 설정합니다.

- 옵션이 없이 led 명령을 실행하면 전면 패널 LED의 상태를 표시합니다.
- led -d 명령 옵션은 led -identify on 명령 옵션과 함께 사용됩니다.

다음 표는 옵션의 인수를 보여줍니다.

구문:

```
led [-options]
```

표 6. led 옵션

옵션	설명	값
-l	모든 시스템의 상태 및 시스템 하위 구성 요소 LED를 가져오십시오.	
-identify	엔클로저 식별 LED의 변경 상태	꺼짐, 켜짐, 깜박임
-d	지정된 시간 동안 식별 LED 켜짐	시간(초)

예:

```
system> led
Fault      Off
Identify   On       Blue
Chklog     Off
Power      Off
```

```
system> led -l
Label      Location      State      Color
```

```

Battery          Planar          Off
BMC Heartbeat   Planar          Blink    Green
BRD              Lightpath Card Off
Channel A       Planar          Off
Channel B       Planar          Off
Channel C       Planar          Off
Channel D       Planar          Off
Channel E       Planar          Off
Chklog          Front Panel     Off
CNFG            Lightpath Card Off
CPU             Lightpath Card Off
CPU 1           Planar          Off
CPU 2           Planar          Off
DASD            Lightpath Card Off
DIMM            Lightpath Card Off
DIMM 1          Planar          Off
DIMM 10         Planar          Off
DIMM 11         Planar          Off
DIMM 12         Planar          Off
DIMM 13         Planar          Off
DIMM 14         Planar          Off
DIMM 15         Planar          Off
DIMM 16         Planar          Off
DIMM 2          Planar          Off
DIMM 3          Planar          Off
DIMM 4          Planar          Off
DIMM 5          Planar          Off
DIMM 6          Planar          Off
DIMM 7          Planar          Off
DIMM 8          Planar          Off
DIMM 9          Planar          Off
FAN             Lightpath Card Off
FAN 1           Planar          Off
FAN 2           Planar          Off
FAN 3           Planar          Off
Fault           Front Panel (+) Off
Identify        Front Panel (+) On      Blue
LINK            Lightpath Card Off
LOG             Lightpath Card Off
NMI             Lightpath Card Off
OVER SPEC      Lightpath Card Off
PCI 1           FRU             Off
PCI 2           FRU             Off
PCI 3           FRU             Off
PCI 4           FRU             Off
Planar          Planar          Off
Power           Front Panel (+) Off
PS             Lightpath Card Off
RAID           Lightpath Card Off
Riser 1        Planar          Off
Riser 2        Planar          Off
SAS ERR        FRU             Off
SAS MISSING    Planar          Off
SP             Lightpath Card Off
TEMP           Lightpath Card Off
VRM            Lightpath Card Off
system>

```

readlog 명령

이 명령은 IMM 이벤트 로그를 표시합니다.

readlog 명령을 사용하여 IMM 이벤트 로그 항목을 표시합니다. 한 번에 5개의 이벤트 로그가 표시됩니다. 항목은 가장 최근 것부터 가장 오래된 것까지 표시됩니다.

참고:

- R - 올바르지 않음
- I - 정보
- W - 경고
- E - 위험

구문:

readlog [-options]

표 7. readlog 옵션

옵션	설명	값
-a	이벤트 로그의 모든 항목을 가장 최근 항목부터 표시합니다.	
-f	카운터를 재설정하고 이벤트 로그의 처음 5개 항목을 가장 최근 항목부터 표시합니다.	
-date	지정된 날짜의 이벤트 로그 항목을 표시합니다	다음 형식을 사용하십시오: mm/dd/yyyy.
-sev	지정된 심각도 수준의 이벤트 로그 항목을 표시합니다.	R, I, W, E
-i	이벤트 로그가 저장되는 TFTP 또는 SFTP 서버의 IPv4 또는 IPv6 IP 주소를 설정합니다. -i 및 -l 명령 옵션을 함께 사용하여 위치를 지정합니다.	유효한 IP 주소
-l	이벤트 로그 파일의 파일 이름을 설정합니다. -i 및 -l 명령 옵션을 함께 사용하여 위치를 지정합니다.	유효한 파일 이름
-pn	TFTP 또는 SFTP 서버의 포트 번호를 표시하거나 설정합니다.	유효한 포트 번호(기본값 69/22)
-u	SFTP 서버의 사용자 이름을 지정합니다.	유효한 사용자 이름
-pw	SFTP 서버의 암호를 지정합니다.	유효한 암호
-di	확장된 감사 로그 기능	none, ipmi

예:

```
system> readlog -f
1 I 2017-06-17T09:31:59.217 Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685 Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581 Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174 Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5 I 2017-06-16T10:40:14.352 Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
```

```
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

servicelog 명령

이 명령은 새 서비스 데이터 파일을 생성하는 데 사용됩니다.

참고: 이 명령은 ffdc 명령이었습니다.

servicelog 명령을 사용하여 서비스 데이터를 생성하고 Support에 전송합니다.

다음 목록은 servicelog 명령과 함께 사용할 수 있는 명령으로 구성되어 있습니다.

다음 표는 옵션의 인수를 보여줍니다.

구문:

```
servicelog [subset_command] [-options]
```

표 8. servicelog 서브세트 명령

옵션	설명
generate	새 서비스 데이터 파일 만들기
status	서비스 데이터 파일 상태 확인
copy	기존 서비스 데이터 복사
delete	기존 서비스 데이터 삭제

표 9. servicelog 옵션

옵션	설명	값
-t	서비스 로그 유형	1, 2, 3 <ul style="list-style-type: none"> 1: 디버그 로그(FFDC, 기본값) 2: 서비스 데이터 로그 3: 서비스 데이터 로그 결합 디버그 로그이며 로그 파일을 복사할 때만 유효함
generate 명령에 대한 추가 옵션		
-c	데이터 범주 선택을 덤프합니다. 이 옵션을 통해 지정하지 않으면 데이터 범주가 포함되지 않습니다.	<ul style="list-style-type: none"> 유형 1(ffdc)의 경우: corefile 유형 2(서비스 데이터 로그)의 경우: network, audit, telemetry, osscreen
generate 및 copy 명령의 추가 옵션		
-f	원격 파일 이름 또는 sftp 대상 디렉토리.	sftp의 경우에는 전체 경로 또는 뒤/디렉토리 이름에 대해 사용합니다 (~ / 또는 /tmp/). 기본값은 시스템 생성 이름입니다.
-ip	tftp/sftp 서버의 주소.	유효한 IP 주소
-pn	tftp/sftp 서버의 포트 번호.	유효한 포트 번호(기본값 69/22)
-u	sftp 서버의 사용자 이름.	유효한 사용자 이름
-pw	sftp 서버의 암호.	유효한 암호
-timeout	포그라운드 복사 허용 시간(분).	1~5(기본값 1)


```

예:
system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz

```

```

system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -ip 192.168.70.230
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>

```

syshealth 명령

이 명령에서는 상태 또는 활성 이벤트의 요약을 제공합니다.

syshealth 명령을 사용해 서버의 상태 또는 활성 이벤트에 대한 요약을 제공합니다. 전원 상태, 시스템 상태, 하드웨어 상태(팬, 전원 공급 장치, 스토리지, 프로세서, 메모리 포함), 다시 시작 카운트, IMM 소프트웨어 상태가 표시됩니다.

구문:
syshealth [arguments]

표 10. syshealth 인수

인수	설명
summary	시스템 상태 요약을 표시합니다.
activeevents	활성 이벤트를 표시합니다.
냉각	냉각 장치 상태를 표시합니다.
전원	전원 모듈 상태를 표시합니다.
스토리지	로컬 스토리지 상태를 표시합니다.
processors	프로세서 상태를 표시합니다.
메모리	메모리 상태를 표시합니다.

```

예:
system> syshealth summary
Power On
State OS booted

```

Restarts 29

```
system> syshealth activeevents  
No Active Event Available!
```

temps 명령

이 명령은 모든 온도 및 온도 임계값 정보를 표시합니다.

temps 명령을 사용하여 모든 온도 및 온도 임계값을 표시합니다. 웹 인터페이스와 동일한 온도 세트가 표시됩니다.

구문:
temps

예:
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

	WR	W	T	SS	HS
Ambient Temp	109.40/43	N/A	78.80/26.00	109.40/43.00	122.00/50.00
Exhaust Temp	N/A	N/A	32.00/0.00	116.60/47.00	N/A

system>

참고:

1. 출력에는 다음과 같은 열 머리글이 있습니다.

WR: warning reset(상승 임계 이력값)

W: warning high(위험하지 않게 높은 임계값)

T: 온도(현재 온도)

SS: hard shutdown(상단 위험 임계값)

HS: 하드 종료(상단 복구 불가능 임계값)

2. 모든 온도값의 단위는 화씨/섭씨입니다.

3. N/A는 적용할 수 없음을 나타냅니다.

volts 명령

이 명령을 서버 전압 정보를 표시합니다.

volts 명령을 사용하여 모든 전압 및 전압 임계값을 표시합니다. 웹 인터페이스와 동일한 전압 세트가 표시됩니다.

구문:
volts

예:
system> volts

	HSL	SSL	WL	WRL	V	WRH	WH	SSH	HSH
CMOS Battery	N/A	2.25	2.39	0.03	3.12	0.03	N/A	N/A	N/A

system>

참고: 출력에는 다음과 같은 열 머리글이 있습니다.

- HSL: 하드 종료 낮음(하단 복구 불가능 임계값)
- SSL: 소프트 종료 낮음(하단 위험 임계값)
- WL: 경고 낮음(위험하지 않게 낮은 임계값)
- WRL: 경고 재설정 낮음(하강 임계 이력값)
- V: 전압(현재 값)
- WRH: 경고 재설정 높음(상승 임계 이력값)
- WL: 경고 높음(위험하지 않게 높은 임계값)
- SSH: 소프트 종료 높음(상단 위험 임계값)
- HSH: 하드 종료 높음(상단 복구 불가능 임계값)

vpd 명령

이 명령은 서버의 하드웨어 및 소프트웨어와 관련된 구성 및 정보 데이터(필수 제품 데이터)를 표시합니다.

vpd 명령을 사용하여 시스템(sys), IMM(bmc), 서버 BIOS(uefi), Lenovo XClarity Provisioning Manager(lxpm), 서버 펌웨어(fw), 서버 구성 요소(comp), PCIe 장치(pcie)에 대한 필수 제품 데이터를 표시합니다. 웹 인터페이스와 동일한 정보가 표시됩니다.

구문:
vpd [arguments]

표 11. vpd 인수

인수	설명
vpd sys	시스템에 대한 필수 제품 데이터를 표시합니다.
vpd bmc	관리 컨트롤러에 대한 필수 제품 데이터를 표시합니다.
vpd uefi	시스템 BIOS에 대한 필수 제품 데이터를 표시합니다.
vpd lxpm	시스템 LXPM에 대한 필수 제품 데이터를 표시합니다.
vpd fw	시스템 펌웨어에 대한 필수 제품 데이터를 표시합니다.
vpd comp	시스템 구성 요소에 대한 필수 제품 데이터를 표시합니다.
vpd pcie	PCIe 장치에 대한 필수 제품 데이터를 표시합니다.

예:
system> vpd bmc
Type Status Version Build ReleaseDate

BMC (Primary) Active 0.00 DVI399T 2017/06/06
BMC (Backup) Inactive 1.00 TEI305J 2017/04/13
system>

서버 전원 및 제어 다시 시작 명령

이 주제에서는 전원 및 다시 시작 CLI 명령의 목록을 알파벳 순서로 제공합니다.

현재 4가지 서버 전원 및 다시 시작 명령이 있으며 다음과 같습니다.

power 명령

이 명령은 서버 전원을 제어하는 방법을 설명합니다.

power 명령을 사용하여 서버 전원을 켜십시오. power 명령을 실행하려면, 원격 서버 전원/다시 시작 액세스 권한 수준이 있어야 합니다.

구문:

power on [-options]
 power off [-options]
 power cycle [-options]
 power uefi
 power state

표 12. power 명령

명령	설명
power on	이 명령을 사용하여 서버 전원을 켭니다.
power off	이 명령을 사용하여 서버 전원을 끕니다.
power cycle	이 명령을 사용하여 서버 전원을 끄고 켭니다.
power uefi	이 명령을 사용하여 UEFI의 F1 설정으로 부팅합니다.
power state	이 명령을 사용하여 서버 전원 상태 및 서버의 현재 상태를 표시합니다.

표 13. power 옵션

옵션	설명	값
-s	이 옵션을 사용하여 서버를 끄기 전에 운영 체제를 종료합니다. 참고: -s 옵션은 power off 및 power cycle 명령에 대한 -every 옵션을 사용하는 경우에 표시됩니다.	
-every	power on, power off 및 power cycle 명령으로 이 옵션을 사용하여 서버 전원을 제어하십시오. 날짜, 시간 및 빈도(일일 또는 주간)를 설정하여 서버의 전원을 켜거나 끄기 또는 순환할 수 있습니다.	Sun, Mon, Tue, Wed, Thu, Fri, Sat, Day, clear
-t	이 옵션을 사용하여 운영 체제의 전원 켜기, 종료 및 서버의 전원 끄기 또는 다시 시작을 위한 시간(시간 및 분)을 지정합니다.	다음 형식을 사용하십시오: hh:mm.
-d	이 옵션을 사용하여 서버의 전원을 켜는 날짜를 지정하십시오. 이 매개 변수는 power on 명령에 대한 추가 옵션입니다. 참고: -d 및 -every 옵션은 동일한 명령으로 함께 사용할 수 없습니다.	다음 형식을 사용하십시오: mm/dd/yyyy.
-clear	이 옵션을 사용하여 예정된 전원 켜는 날짜를 지우십시오. 이 매개 변수는 power on 명령에 대한 추가 옵션입니다.	

다음 정보는 power 명령의 예입니다.

매주 일요일 1시 30분에 운영 체제를 종료하고 서버 전원을 끄려면, 다음 명령을 입력하십시오.
 system> power off -every Sun -t 01:30

매주 일요일 1시 30분에 운영 체제를 종료하고 서버를 다시 시작하려면, 다음 명령을 입력하십시오.
 system> power cycle -every Day -t 01:30

매주 월요일 1시 30분에 서버의 전원을 켜려면, 다음 명령을 입력하십시오.

```
system> power on -every Mon -t 1:30
```

2013년 12월 31일 오후 11시 30분에 서버의 전원을 켜려면, 다음 명령을 입력하십시오.

```
system> power on -d 12/31/2013 -t 23:30
```

주간 전원 주기를 지우려면, 다음 명령을 입력하십시오.

```
system> power cycle -every clear
```

reset 명령

이 명령은 서버를 재설정하는 방법을 설명합니다.

reset 명령을 사용하여 서버를 다시 시작합니다. 이 명령을 사용하려면 전원이 있어야 하여 액세스 권한을 다시 시작해야 합니다.

구문:

```
reset [-options]
```

표 14. reset 옵션

옵션	설명	값
-s	서버를 재설정하기 전에 운영 체제를 종료합니다.	
-d	지정된 시간(초) 동안 재설정 수행을 지연합니다.	0 - 120
-nmi	서버에서 NMI(Non-Maskable Interrupt)를 생성합니다.	

fuelg 명령

이 명령은 서버 전원에 대한 정보를 표시합니다.

fuelg 명령을 사용하여 서버 전원 사용에 대한 정보를 표시하고 서버 전원 관리를 구성합니다. 이 명령은 또한 전원 중복 손실에 대한 정책을 구성합니다.

구문:

```
fuelg [-options]
```

표 15. fuelg 옵션

옵션	설명	값
-pme	서버의 전원 관리 및 제한을 활성화 또는 비활성화합니다.	on, off
-pcapmode	서버의 전원 제한 모드를 설정합니다.	출력, 입력
-pcap	옵션이 없이 대상에서 fuelg 명령을 실행할 때 표시되는 전원 제한 값의 범위 내에 있는 숫자 값	숫자 와트 값
-history	소비 전력 또는 성능 내역을 표시합니다.	pc, perf
-period	내역을 표시할 숫자 값입니다.	1, 6, 12, 24시간
-pm	보조 전원의 손실에 대한 정책 모드를 설정합니다.	<ul style="list-style-type: none">bt- 스로틀링 포함 기본rt- 스로틀링 포함 보조(기본값)

표 15. fuelg 옵션 (계속)

옵션	설명	값
-zm	제로 출력 모드를 사용 또는 사용하지 않습니다. 이 설정은 정책 모드가 스토틀링 포함 보조로 설정된 경우에만 설정할 수 있습니다.	on, off
-perf	시스템, 프로세서, 메모리 모듈 및 I/O를 포함해 현재 컴퓨터 사용률을 표시합니다.	
-pc	현재 소비 DC 전력 표시	<ul style="list-style-type: none"> 출력 - 시스템, 프로세서, 메모리 모듈 및 기타 구성 요소의 현재 출력 소비 전력을 표시합니다. input - 시스템 소비 전력을 포함하여 현재 입력 소비 전력을 표시합니다. 참고: AMD 서버의 경우 현재 출력 소비 전력에 일부 구성 요소가 표시되지 않습니다.

pxeboot 명령

이 명령은 PXE(Preboot eXecution Environment)의 상태를 표시 및 설정합니다.

구문:

pxeboot [-options]

표 16. pxeboot 옵션

옵션	설명	값
-en	다음 시스템을 재시작에 대한 PXE(Preboot eXecution Environment) 상태를 설정합니다.	enabled, disabled

구성 명령

이 주제에서는 구성 CLI 명령의 목록을 알파벳 순서로 제공합니다.

현재 41가지 구성 명령이 있으며 다음과 같습니다.

accseccfg 명령

이 명령을 사용하여 계정 보안 설정을 표시 및 구성합니다.

구문:

accsecfg [-options]

표 17. accseccfg 옵션

옵션	설명	값
-am	사용자 인증 방법을 설정합니다.	local, ldap, localldap, ldaplocal
-lp	최대 로그인 실패 횟수 경과 후 로그아웃 시간(분)	0~2880, 0 = 잠금 기간이 만료되지 않음
-pe	암호 만료 기간(일).	0~365, 0 = 만료되지 않음

표 17. accseccfg 옵션 (계속)

옵션	설명	값
-pew	암호 만료 경고 기간 참고: 암호 만료 경고 기간은 암호 만료 기간보다 짧아야 합니다.	0~30, 0 = 만료되지 않음
-pc	암호 복잡성 규칙이 사용 설정되었습니다.	on, off
-pl	암호 길이.	암호 복잡성 규칙을 사용하는 경우 암호 길이는 8~32 사이입니다. 그렇지 않으면 0~32 사이입니다.
-ci	최소 암호 변경 간격(시간).	0~240, 0 = 즉시 변경
-lf	최대 로그인 실패 횟수.	0~10, 0 = 잠기지 않음
-chgnew	처음 로그인한 후 새 사용자 암호 변경.	on, off
-rc	암호 재사용 주기.	0~10, 0 = 즉시 재사용
-wt	웹 및 SSH(Secure Shell) 비활성 세션 제한 시간 초과(분).	0~1440

예:
system> accseccfg
 -am: local
 -lp: 60
 -pe: none
 -pew: 0
 -pc: on
 -pl: 10
 -ci: 0
 -lf: 5
 -chgnew: on
 -rc: 5
 -wt: 20
system>

asu 명령

이 명령은 UEFI 설정을 구성하는 데 사용됩니다.

ASU(Advanced Settings Utility) 명령은 UEFI 설정을 구성하는 데 사용됩니다. UEFI 설정 변경 내용이 적용하려면 호스트 시스템을 재부팅해야 합니다.

구문:
asu [subset_command]

표 18. asu 서브세트 명령

명령	설명	값
help	이 명령은 1개 이상의 설정에 대한 도움말 정보를 표시합니다.	setting_name
설정	이 명령을 사용하여 설정이 값을 변경합니다. UEFI 설정을 입력값으로 설정합니다. 참고: <ul style="list-style-type: none"> 1개 이상의 설정/값 쌍을 설정하십시오. 설정이 단일 설정으로 확장하면 와일드카드가 포함될 있습니다. 	setting_name=value

표 18. asu 서브세트 명령 (계속)

명령	설명	값
	<ul style="list-style-type: none"> 공백을 포함하고 있는 경우에는 값을 따옴표로 묶어야 합니다. 정렬된 목록값은 등호 기호(=)로 분리됩니다. 예를 들어 B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network"를 설정합니다. 	
show	이 명령을 사용하여 1개 이상의 설정에 대한 현재 값을 표시합니다.	setting_name
showvalues	<p>이 명령을 사용하여 1개 이상의 설정에 대한 모든 가능한 값을 표시합니다.</p> <p>참고:</p> <ul style="list-style-type: none"> 이 명령은 설정의 허용 가능한 값에 대한 정보를 표시합니다. 설정에서 허용된 인스턴스의 최소 수 및 최대 수가 표시됩니다. 사용하지 않으면 기본값이 표시됩니다. 괄호 (< 및 >)를 열고 닫기 하여 기본값을 묶습니다. 텍스트 값은 최소 및 최대 길이 및 정규 표현식을 표시합니다. 	setting_name
showgroups	이 명령을 사용하여 사용 가능한 설정 그룹을 표시합니다. 이 명령을 사용하여 알려진 그룹의 이름을 표시합니다. 그룹 이름은 설치된 장치에 따라 다를 수 있습니다.	
<p>참고:</p> <ul style="list-style-type: none"> 명령 구문에서 setting_name은 확인하거나 변경하려는 설정의 이름이며, value는 설정에 배치하는 값입니다. setting_name은 set 명령을 사용하는 경우를 제외하고 2개 이상의 이름이 될 수 있습니다. setting_name에는 와일드카드(예: 별표(*) 또는 물음표(?))가 포함될 수 있습니다. setting_name은 그룹, 설정 이름 또는 all이 될 수 있습니다. 		

예:

- 모든 asu 명령 옵션을 표시하려면 asu help를 입력하십시오.
- 하나의 명령에 대한 도움말을 표시하려면 asu help setting_name을 입력하십시오.
- 값을 변경하려면 asu set setting_name=value를 입력하십시오.
- 현재 값을 표시하려면 asu show setting_name을 입력하십시오.
- 설정에서 가능한 모든 값을 표시하려면 asu showvalues setting_name을 입력하십시오. show values 명령 예:

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```
- 사용 가능한 설정 그룹을 표시하려면 asu showgroups를 입력하십시오.

다음 표는 옵션의 인수를 보여줍니다.

표 19. asu 옵션

다음 표는 옵션, 옵션 설명 및 옵션에 대한 관련 값으로 구성되어 있는 멀티 행 3열 표입니다.

표 19. asu 옵션 (계속)

옵션	설명	값
-b	배치 형식으로 표시하십시오.	
-help ¹	명령 사용 및 옵션을 표시하십시오. -help 옵션은 예를 들어 asu -help show 명령 앞에 위치합니다.	
-l	긴 형식 설정 이름(구성 설정 포함)	
-m	혼합 형식 설정 이름(구성 id 사용)	
-v ²	자세한 정보 출력.	

1. -help 옵션은 어떤 명령으로도 사용할 수 있습니다.
2. -v 옵션은 asu 및 명령 사이에서만 사용됩니다.

구문:

asu [-options] command [cmdopts]

options:

- v verbose output
- help display main help

cmdopts:

- help help for the command

참고: 자세한 명령 옵션은 개별 명령을 참조하십시오.

asu 트랜잭션 명령을 사용하여 여러 개의 UEFI 설정을 설정하고 배치 모드 명령을 만들어 실행하십시오. tropen 및 trset 명령을 사용하여 적용할 설정이 여러 개 포함되어 있는 트랜잭션 파일을 만드십시오. tropen 명령을 사용하여 지정된 id가 있는 트랜잭션을 엽니다. trset 명령을 사용하여 이러한 설정을 사용하도록 설정을 추가합니다. trcommit 명령을 사용하여 완료된 트랜잭션을 엽니다. 트랜잭션으로 완료하는 경우에는 trrm 명령을 삭제할 수 있습니다.

참고: UEFI 설정 복구 작업에서는 임의의 3자리 숫자를 사용하는 id로 트랜잭션을 만듭니다.

다음 표에는 asu 명령으로 사용할 수 있는 트랜잭션 명령이 포함되어 있습니다.

표 20. asu 트랜잭션 명령

다음 표는 트랜잭션 명령, 명령 설명 및 명령에 대한 관련 값으로 구성되어 있는 멀티 행 3열 표입니다.

명령	설명	값
tropen id	이 명령은 설정할 몇 개의 설정이 포함되어 있는 새로운 트랜잭션 파일을 만듭니다.	Id는 식별 문자열(1~3개의 영숫자 문자)입니다.
trset id	이 명령을 사용하여 1개 이상의 설정 또는 값 쌍을 트랜잭션에 추가하십시오.	Id는 식별 문자열(1~3개의 영숫자 문자)입니다.
trlist id	이 명령은 먼저 트랜잭션 파일의 내용을 표시합니다. 이 명령은 CLI 셸에 트랜잭션 파일을 만들 때 유용할 수 있습니다.	Id는 식별 문자열(1~3개의 영숫자 문자)입니다.
trcommit id	이 명령은 먼저 트랜잭션 파일의 내용을 커밋 및 실행합니다. 실행의 결과 및 오류가 표시됩니다.	Id는 식별 문자열(1~3개의 영숫자 문자)입니다.
trrm id	이 명령은 커밋된 트랜잭션 파일을 제거합니다.	Id는 식별 문자열(1~3개의 영숫자 문자)입니다.

여러 개의 UEFI 설정을 설정한 예:

```

asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1

```

backup 명령

이 명령을 사용하여 현재 시스템 보안 설정이 포함된 백업 파일을 만듭니다.

구문:

backup [-options]

표 21. backup 옵션

옵션	설명	값
-f	백업 파일의 파일 이름	유효한 파일 이름
-pp	암호 또는 따옴표로 구분된 암호구(백업 파일 내에서 암호를 암호화하는 데 사용)	유효한 암호 또는 따옴표로 구분된 암호구
-ip	TFTP/SFTP 서버의 IP 주소	유효한 IP 주소
-pn	TFTP/SFTP 서버의 포트 번호	유효한 포트 번호(기본값 69/22)
-u	SFTP 서버의 사용자 이름	유효한 사용자 이름
-pw	SFTP 서버의 암호	유효한 암호
-fd	백업 CLI 명령의 XML 설명에 대한 파일 이름	유효한 파일 이름

예:

```

system> backup -f xcc-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>

```

dhcpinfo 명령

이 명령을 사용하여 eth0에 대한 DHCP 서버 지정 IP 구성을 봅니다.

DHCP 서버가 인터페이스를 자동으로 구성하는 경우에는 dhcpinfo 명령을 사용하여 eth0에 대한 DHCP 서버 지정 IP 구성을 봅니다. ifconfig 명령을 사용하여 DHCP를 활성화 또는 비활성화할 수 있습니다.

구문:

dhcpinfo [ethernet_number]

예:

```
dhcpinfo eth1
```

다음 표에는 예의 출력에 대한 설명이 나와 있습니다.

표 22. dhcpinfo 출력

필드	설명
-server	구성을 할당한 DHCP 서버
-n	할당된 호스트 이름
-i	할당된 IPv4 주소
-i6	할당된 IPv6 주소
-g	할당된 게이트웨이 주소
-s	할당된 서브넷 마스크
-d	할당된 IPv4 도메인 이름
-d6	할당된 IPv6 도메인 이름
-dns1	기본 IPv4 DNS 서버 IP 주소
-dns2	보조 IPv4 DNS IP 주소
-dns3	3차 IPv4 DNS 서버 IP 주소
-i6	IPv6 주소
-d6	IPv6 도메인 이름
-dns61	기본 IPv6 DNS 서버 IP 주소
-dns62	보조 IPv6 DNS IP 주소
-dns63	3차 IPv6 DNS 서버 IP 주소

dns 명령

이 명령을 사용하여 IMM의 DNS 구성을 보고 설정합니다.

구문:

dns [-options]

표 23. dns 옵션

옵션	설명	값
-state	DNS의 상태	on, off
-i1	기본 IPv4 DNS 서버 IP 주소	점으로 구분된 십진수 IP 주소 형식의 IP 주소.
-i2	보조 IPv4 DNS IP 주소	점으로 구분된 십진수 IP 주소 형식의 IP 주소.
-i3	3차 IPv4 DNS 서버 IP 주소	점으로 구분된 십진수 IP 주소 형식의 IP 주소.
-i61	기본 IPv6 DNS 서버 IP 주소	IPv6 형식의 IP 주소.
-i62	보조 IPv6 DNS IP 주소	IPv6 형식의 IP 주소.
-i63	3차 IPv6 DNS 서버 IP 주소	IPv6 형식의 IP 주소.
-ddns	DDNS의 상태	enabled, disabled
-dnsrc	기본 설정 DDNS 도메인 이름	dhcp, manual
-ddn	수동으로 지정된 DDN	
-ddncur	현재 DDN(읽기 전용)	
-p	기본 설정 DNS 서버(ipv4, ipv6)	ipv4, ipv6

표 23. dns 옵션 (계속)

옵션	설명	값
-dscvry	LXCA 주소 검색	enabled, disabled
-dsclist	DNS SRV의 LXCA 목록	
-dscxm	XClarity Manager 구성	

다음 예는 DNS를 비활성화한 경우 IMM 구성을 보여줍니다.

```
system> dns
-state : disabled
-i1 : 0.0.0.0
-i2 : 0.0.0.0
-i3 : 0.0.0.0
-i61 : ::
-i62 : ::
-i63 : ::
-ddns : enabled
-dnsrc : DHCP
-ddn :
-ddncur : labs.lenovo.com
-p : ipv6
-dscvry : enabled
system>
```

encaps 명령

이 명령을 사용하여 BMC가 encapsulation 모드를 종료하도록 합니다.

```
구문:
encaps [arguments]
```

표 24. encaps 인수

인수	설명
lite off	BMC가 encapsulation 모드를 종료하고 모든 사용자에게 대한 전역 액세스를 열도록 합니다.

ethtousb 명령

ethtousb 명령을 사용하여 이더넷을 USB 포트를 통한 이더넷 매핑을 표시 및 구성합니다.

명령을 사용하면 외부 이더넷 포트 번호를 USB를 통한 이더넷에 대한 다른 포트 번호로 매핑할 수 있습니다.

```
구문:
ethtousb [-options]
```

표 25. ethtousb 명령

옵션	설명	값
-en	USB를 통한 이더넷 상태.	enabled, disabled 참고: <usbeth>를 통해 USB를 통한 이더넷 인터페이스를 활성화하여 포트 매핑을 효과적으로 만듭니다.
-m[x] port1:port2	색인 x의 포트 매핑을 구성합니다.	변수 설명: • 포트 색인 번호 x는 명령 옵션의 1~10의 정수로 지정합니다. • 포트 쌍의 port1은 외부 이더넷 포트 번호입니다. • 포트 쌍의 port2는 USB를 통한 이더넷 포트 번호입니다.
-rm map_index	지정된 색인의 포트 매핑을 제거합니다.	포트 색인 번호 map_index는 명령 옵션에서 1~10의 정수로 지정됩니다. 참고: 포트 맵 색인은 옵션이 없이 ethtousb 명령을 사용하여 표시됩니다.

예:
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 ethtousb : On
 =====
 1: 100: 200
 2: 101: 201
system>

firewall 명령

이 명령을 사용하여 특정 주소의 액세스를 제한하고 선택적으로 액세스 시간 프레임을 제한하도록 방화벽을 구성합니다. 옵션을 지정하지 않으면 현재 설정이 표시됩니다.

구문:
firewall [-options]

표 26. firewall 옵션

옵션	설명	값
IP 주소 화이트리스트에 대한 옵션		
-wips	화이트리스트 IP 주소를 표시/구성합니다.	<유효한 IP 주소>, clr <ul style="list-style-type: none"> 유효한 IP 주소: 1~3개의 IP 주소 허용 (쉼표로 구분, CIDR 또는 범위) 참고: IPv4 및 IPv6 주소는 CIDR 형식을 사용하여 주소 범위를 차단할 수 있습니다. <ul style="list-style-type: none"> -clr: 화이트리스트 지우기
차단 목록 및 시간 제한에 대한 옵션		
-bips	IP 주소 1~3개 차단(쉼표로 구분, CIDR 또는 범위)	유효한 IP 주소 참고: IPv4 및 IPv6 주소는 CIDR 형식을 사용하여 주소 범위를 차단할 수 있습니다.
-bmacs	MAC 주소 1~3개 차단(쉼표로 구분)	유효한 MAC 주소 참고: MAC 주소 필터링은 특정 주소에만 작동합니다.

표 26. firewall 옵션 (계속)

옵션	설명	값
-bbt	차단 시작 시간 - 현재 시간 이후여야 함	시간 형식 <YYYY-MM-DD HH:MM>
-bet	차단 종료 시간 - 시작 시간 이후여야 함	시간 형식 <YYYY-MM-DD HH:MM>
-bti	1~3번의 시간대별 차단(쉼표로 구분) 예: firewall - bti 01:00-02:00,05:05-10:30은 매 일 01:00~02:00 및 05:05-10:30에 액세스를 차단합니다.	시간 범위의 형식 <HH:MM-HH:MM>
-clr	지정된 유형에 대한 방화벽 규칙을 지웁니다.	ip, mac, datetime, interval, all
다음은 IP 주소 차단 옵션입니다.		
-iplp	IP 주소 잠금 기간(분)입니다.	0~2,880 사이의 숫자 값, 0 = 만료되지 않음
-iplf	IP 주소가 잠기기 전의 로그인 실패 최대 개수입니다.	0~32 사이의 숫자 값, 0 = 잠기지 않음 참고: 이 값이 0이 아니면 <accseccfg -lf>에서 설정한 <최대 로그인 실패 횟수>보다 크거나 같아야 함
-ipbl	잠긴 IP 주소 목록을 표시/구성합니다.	del, clrall, show • -del: 차단 목록에서 IPv4 또는 IPv6 주소 삭제 • -clrall: 모든 차단 IP 삭제 • -show: 모든 차단 IP 표시

다음 목록에 firewall 명령의 구문에 대한 예가 나와있습니다.

- 모든 옵션의 값과 IP 주소 차단 목록을 표시하려면 firewall을 입력합니다.
- 다중 IP에서 액세스를 차단하려면 firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5를 입력합니다.
- 매일 01:00-02:00,05:05-10:30,14:15-20:00 동안 모든 액세스를 차단하려면 firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00을 입력합니다.
- 차단 목록 및 시간 제한의 모든 규칙을 지우려면 firewall -clr all을 입력합니다.
- IP 주소 잠금 기간을 60분으로 설정하려면 firewall -iplp 60을 입력합니다.
- 최대 로그인 실패 횟수를 5회로 설정하려면 firewall -iplf 5를 입력합니다.
- IP 주소 차단 목록에서 192.168.100.1을 삭제하려면 firewall -ipbl -del 192.168.100.1을 입력합니다.
- IP 주소 차단 목록에서 3fcc:1234::2를 삭제하려면 firewall -ipbl -del 3fcc:1234::2를 입력합니다.
- 모든 차단 IP 주소를 삭제하려면 firewall -ipbl -clrall을 입력합니다.
- 모든 차단 IP 주소를 표시하려면 firewall -ipbl -show를 입력합니다.

hashpw 명령

이 명령을 -sw 옵션과 함께 사용하여 타사 암호 기능을 사용/사용 안 함 또는 -re 옵션과 함께 사용하여 타사 암호 검색 허용을 사용/사용 안 합니다.

구문:
hashpw [-options]

표 27. hashpw 옵션

옵션	설명	값
-sw	타사 암호 스위치 상태	enabled, disabled
-re	타사 암호 읽기 상태 참고: 스위치를 사용하는 경우 읽기를 설정할 수 있습니다.	enabled, disabled

예:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account  Login ID  Advanced Attribute  Role  Password Expires
-----
1        USERID   Native              Administrator  Password doesn't expire
5        guest5   Third-party Password Administrator  90 day(s)
```

ifconfig 명령

이 명령을 사용하여 이더넷 인터페이스를 구성합니다.

ifconfig 명령을 사용하여 현재 이더넷 인터페이스 구성을 표시합니다. 이더넷 인터페이스 구성을 변경하려면, 다음에 값이 표시되는 옵션을 입력하십시오. 인터페이스 구성을 변경하려면 최소한 어댑터 네트워킹 및 보안 구성 권한이 있어야 합니다.

구문:

```
ifconfig [ethernet_number] [-options]
```

예:

```
dhcpcinfo eth1 -b
```

표 28. Ifconfig 옵션

옵션	설명	값
-state	인터페이스 상태	disabled, enabled
-c	구성 방법	dhcp, static, dthens(dthens는 웹 인터페이스의 dhcp 서버를 사용하고, 실패하면 정적 config 구성 사용 옵션과 일치)
-ghn	DHCP에서 호스트 이름 얻기	disabled, enabled
-i	정적 IP 주소	올바른 형식의 주소.
-g	게이트웨이 주소	올바른 형식의 주소.
-s	서브넷 마스크	올바른 형식의 주소.
-n	호스트 이름	최대 63자의 문자열. 문자열에는 문자, 숫자, 마침표, 밑줄 및 하이픈이 포함될 수 있습니다.
-auto	데이터 전송률 및 양방향 네트워크 설정을 구성할 수 있는지 여부를 결정하는 자동 협상 설정	true, false
-vlan	VLAN 태깅 활성화 또는 비활성화	enabled, disabled

표 28. Ifconfig 옵션 (계속)

옵션	설명	값
-vlanid	VLAN ID	1과 4094 사이의 숫자값
-r	레이터 속도	10, 100, 1000
-d	양방향 모드	full, half
-m	MTU	60과 1500 사이의 숫자
-l	LAA	MAC 주소 형식. 멀티캐스트 주소는 허용되지 않습니다(첫 번째 바이트는 짝수이어야 함).
-b	번인(burn-in) MAC 주소(읽기 전용)	
-dn	도메인 이름(읽기 전용)	
-ipv6	IPv6 상태	disabled, enabled
-ipv6static	정적 IPv6 상태	disabled, enabled
-i6	정적 IP 주소	이더넷 채널 0의 정적 IP 주소(IPv6형식).
-p6	주소 접두사 길이	1과 128 사이의 숫자값
-g6	게이트웨이 또는 기본 루트	게이트웨이에 대한 IP 주소 또는 IPv6의 이더넷 채널 0에 대한 기본 라우트.
-dhcp6	IPv6 DHCP 모드	enabled, disabled
-sa6	IPv6 상태 비저장 모드	enabled, disabled
-lla	링크-로컬 주소(읽기 전용)	
-ncsi	NCSI NIC 포트 선택	nic[x]:port[y] 참고: 두 개 이상의 설정이 있는 경우 구분 기호로 쉼표를 사용합니다.
-nic	NIC 모드 전환 ¹	shared, dedicated, shared:nic[x] ²
-failover ²	장애 조치	none, shared, shared:nic[x]
-nssync ³	네트워크 설정 동기화	enabled, disabled
-address_table	자동으로 생성된 IPv6 주소 및 접두사 길이 표(읽기 전용) 참고: 옵션은 IPv6 및 상태 비저장 자동 구성을 활성화하는 경우에만 표시됩니다.	

참고:

- nic는 nic의 상태도 표시합니다. [active]는 현재 사용 중인 nic XCC를 나타냅니다.
예:
-nic: shared:nic3
nic1: dedicate
nic2: ext card slot #3
nic3: ext card slot 5 [active]
nic3가 공유 모드, 슬롯 5, nic2가 슬롯 3, nic1이 XCC 전용 포트, XCC가 nic3를 사용 중임을 나타냅니다.
- shared:nic[x] 값은 옵션인 메자닌 네트워크 카드가 설치된 서버에서 사용할 수 있습니다. 이 메자닌 네트워크 카드는 IMM에서 사용할 수 있습니다.
- IMM가 전용 관리 네트워크 포트를 사용하도록 구성된 경우 -failover 옵션은 전용 포트가 분리되어 있으면 공유 네트워크 포트로 전환하도록 IMM에 지시합니다.
- 장애 조치 모드가 활성화된 경우 -nssync 옵션은 전용 관리 네트워크 포트에 사용되는 것과 동일한 네트워크 설정을 공유 네트워크 포트에 사용하도록 IMM에 지시합니다.

예:

```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

keycfg 명령

이 명령을 사용하여 정품 인증 키를 표시, 추가 또는 삭제합니다.

정품 인증 키는 옵션인 IMM 기능에 대한 액세스를 제어합니다.

참고:

- 파일 전송을 통해 새 정품 인증 키를 추가합니다.
- 키의 수 또는 키 유형을 지정하여 이전 키를 삭제하십시오. 유형별로 키를 삭제하는 경우에는 지정된 유형의 첫 번째 키만 삭제됩니다.

구문:

keycfg [-options]

표 29. Keycfg 옵션

옵션	설명	값
-add	정품 인증 키 추가	ip, pn, u, pw, f <ul style="list-style-type: none"> • -ip: 추가할 정품 인증 키가 있는 TFTP/SFTP 서버의 IP 주소 • -pn: 추가할 정품 인증 키가 있는 TFTP/SFTP 서버의 포트 번호(기본값 69/22) • -u: 추가할 정품 인증 키가 있는 SFTP 서버의 사용자 이름 • -pw: 추가할 정품 인증 키가 있는 SFTP 서버의 암호 • -f: 추가할 정품 인증 키의 파일 이름
-del	색인 번호별 정품 인증 키 삭제	keycfg 목록의 유효한 정품 인증 키 색인 번호
-deltype	키 유형별 정품 인증 키 삭제	유효한 키 유형 값

옵션이 없이 keycfg 명령을 실행하면, 설치된 정품 인증 키 목록이 표시됩니다. 표시된 키 정보에는 각 정품 인증 키, 정품 인증 키의 유형, 키가 유효한 날짜, 남아 있는 사용 횟수, 키 상태 및 키 설명이 포함됩니다.

예:

```
system> keycfg
ID Type Valid Uses Status Description
1 4 10/10/2010 5 "valid" "IMM remote presence"
2 3 10/20/2010 2 "valid" "IMM feature"
3 32796 NO CONSTRAINTS NO CONSTRAINTS "valid" "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

참고: ID 번호 3의 설명 필드는 공간 한계로 인해 별도의 라인에 제공됩니다.

ldap 명령

이 명령을 사용하여 LDAP 프로토콜 구성 매개 변수를 표시 및 구성합니다.

구문:

ldap [-options]

표 30. ldap 옵션

옵션	설명	값
-aom	Active Directory 사용 사용 인증 전용 모드	enabled, disabled
-a	사용자 인증 방법	<ul style="list-style-type: none"> • loc: 로컬 전용 • ldap: LDAP 전용 • locld: 로컬 먼저 LDAP 다음 • ldloc: LDAP 먼저 로컬 다음
-b	바인딩 방법	<ul style="list-style-type: none"> • anon: 익명 • client: ClientDN 및 암호로 바인딩 • login: 로그인 자격 증명으로 바인딩
-c	클라이언트 고유 이름	client_dn의 최대 127자로 구분된 문자열
-d	도메인 검색	search_domain의 최대 63자로 구분된 문자열
-fn	포레스트 이름	Active Directory 환경의 경우. 최대 127자의 문자열.
-f	그룹 필터	group_filter의 최대 127자로 구분된 문자열
-g	그룹 검색 속성	group_search_attr의 최대 63자로 구분된 문자열
-l	로그인 권한 속성	string의 최대 63자로 구분된 문자열
-p	클라이언트 암호	client_pw의 최대 15자로 구분된 문자열
-pc	클라이언트 암호 확인	confirm_pw의 최대 15자로 구분된 문자열 명령 사용: ldap -p client_pw -pc confirm_pw 이 옵션은 클라이언트 암호를 바꿀 때 필요합니다. confirm_pw 인수와 client_pw 인수를 비교합니다. 인수가 일치하지 않으면 명령이 실패합니다.
-r	루트 항목 DN(고유 이름)	root_dn의 최대 127자로 구분된 문자열
-s1ip	서버 1 호스트 이름/IP 주소	호스트 이름/ip_addr에 대한 최대 127자의 문자열 또는 IP 주소
-s2ip	서버 2 호스트 이름/IP 주소	호스트 이름/ip_addr에 대한 최대 127자의 문자열 또는 IP 주소
-s3ip	서버 3 호스트 이름/IP 주소	호스트 이름/ip_addr에 대한 최대 127자의 문자열 또는 IP 주소
-s4ip	서버 4 호스트 이름/IP 주소	호스트 이름/ip_addr에 대한 최대 127자의 문자열 또는 IP 주소
-s1pn	서버 1 포트 번호	port_number에 대한 최대 5자리의 숫자 포트 번호
-s2pn	서버 2 포트 번호	port_number에 대한 최대 5자리의 숫자 포트 번호
-s3pn	서버 3 포트 번호	port_number에 대한 최대 5자리의 숫자 포트 번호
-s4pn	서버 4 포트 번호	port_number에 대한 최대 5자리의 숫자 포트 번호
-u	사용자의 로그인 이름 검색 속성	search_attr의 최대 63자로 구분된 문자열
-v	DNS를 통해 LDAP 서버 주소 가져오기	꺼짐, 켜짐
-h	명령 사용 및 옵션을 표시합니다.	

```

예:
system> ldap
-aom enable
-a loclld
-b client
-c cn=admin,dc=lenovo,dc=com
-d
-fn
-f example.com
-g cn
-l XCC3RBSPermissions
-r
-s1ip 10.241.99.94
-s2ip
-s3ip
-s4ip
-s1pn 389
-s2pn 389
-s3pn 389
-s4pn 389
-u uid
-v off
system>

```

ntp 명령

이 명령을 사용하여 NTP(네트워크 타임 프로토콜)를 표시 및 구성합니다.

구문:
ntp [-options]

표 31. ntp 명령

옵션	설명	값
-en	네트워크 타임 프로토콜을 활성화 또는 비활성화합니다.	enabled, disabled
-i[x]	색인 x의 NTP(Network Time Protocol) 서버 이름 또는 IP 주소.	시계 동기화에 사용할 NTP 서버의 이름. NTP 서버의 색인 번호 범위는 -i1~-i4입니다. 참고: -i는 i1와 동일합니다.
-f	IMM 시계가 NTP(Network Time Protocol) 서버와 동기화되는 빈도(분 단위).	3~1,440분
-synch	네트워크 타임 프로토콜 서버와 즉시 동기화해야 합니다.	이 매개 변수에는 어떤 값도 사용되지 않습니다.

```

예:
system> ntp
-en: disabled
-f: 3 minutes
-i: not set

```

portcontrol 명령

이 명령을 사용하여 네트워크 서비스 포트를 켜거나 끕니다.

구문:
portcontrol [-options]

표 32. portcontrol 옵션

옵션	설명	값
-ipmi	LAN을 통한 IPMI 액세스 사용 또는 사용 안 함	on, off
-ipmi-kcs	서버에서 IPMI 액세스를 요청 시 사용, 사용 또는 사용 안 함	auto, on, off
-rest	REST 검색 사용 또는 사용 안 함	on, off
-snmp	SNMP 검색 사용 또는 사용 안 함	on, off
-ssdp	SSDP 검색 사용 또는 사용 안 함	on, off
-cli	CLI 검색 사용 또는 사용 안 함	on, off
-web	WEB 검색 사용 또는 사용 안 함	on, off
-all	모든 인터페이스 및 검색 프로토콜 사용 또는 사용 안 함	on, off

예:

```
system> portcontrol
ipmi : on
ipmi-kcs : on
rest : on
snmp : off
ssdp : on
cli : on
web : on
system>
```

ports 명령

이 명령을 사용하여 IMM 포트를 표시하고 구성합니다.

구문:

```
ports [-options]
```

표 33. ports 옵션

옵션	설명	값
-open	열린 포트 표시(읽기 전용)	
-reset	포트를 기본 설정으로 재설정(읽기 전용)	
-http	HTTP 포트 번호	기본 포트 번호: 80
-https	HTTPS 포트 번호	기본 포트 번호: 443
-ssh	SSH 레거시 CLI 포트 번호	기본 포트 번호: 22
-snmpa	SNMP 에이전트 포트 번호	기본 포트 번호: 161
-snmpt	SNMP 트랩 포트 번호	기본 포트 번호: 162
-rp	원격 관리 포트 번호	기본 포트 번호: 3900

```

예:
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>

```

rdmount 명령

이 명령을 사용하여 원격 디스크 이미지 또는 네트워크 공유를 탑재합니다.

참고:

- XClarity Controller 메모리에 파일을 최대 2개까지 업로드할 수 있으며 XClarity Controller RDOC 기능을 사용하여 가상 미디어로 탑재할 수 있습니다. 두 파일의 총 크기는 50MB를 초과할 수 없습니다. 업로드된 이미지는 `-rw` 옵션을 사용하지 않는 한 읽기 전용입니다.
- HTTP, SFTP 또는 FTP 프로토콜을 사용하여 이미지를 탑재하거나 매핑할 때 모든 이미지의 총 크기는 50MB를 초과하지 않아야 합니다. NFS 또는 SAMBA 프로토콜이 사용되는 경우에는 크기 제한이 없습니다.

구문:

```
rdmount [-options]
```

표 34. rdmount 옵션

옵션	설명
<code>-r</code>	rdoc 작업(사용되는 경우, 첫 번째 옵션이어야 함) <code>-r -map</code> : RDOC 이미지 탑재 <code>-r -unmap<filename></code> : 탑재된 RDOC 이미지 탑재 해제 <code>-r -maplist</code> : XClarity Controller 웹 브라우저 및 CLI 인터페이스를 통해 탑재된 RDOC 이미지를 표시합니다.
<code>-map</code>	<code>-t <samba nfs http sftp ftp></code> 파일 시스템 유형 <code>-ro</code> 읽기 전용 <code>-rw</code> 읽기-쓰기 <code>-u</code> 사용자 <code>-p</code> 암호 <code>-l</code> 파일 위치(URL 형식) <code>-o</code> 옵션 (samba 및 nfs 탑재에 대한 기타 옵션 문자열) <code>-d</code> 도메인 (samba 탑재에 대한 도메인)
<code>-maplist</code>	매핑된 이미지 표시
<code>-unmap</code>	<id fname>은 네트워크 이미지에 ID를 사용하고 rdoc에 파일 이름을 사용함
<code>-mount</code>	매핑된 이미지 마운트
<code>-unmount</code>	마운트된 이미지 마운트 해제

restore 명령

이 명령을 사용하여 백업 파일에서 시스템 설정을 복원합니다.

구문:

```
restore [-options]
```

표 35. restore 옵션

옵션	설명	값
-f	백업 파일 이름	유효한 파일 이름
-pp	암호 또는 백업 파일 내에서 암호를 암호화하는 데 사용되는 암호구	유효한 암호 또는 따옴표로 구분된 암호구
-ip	TFTP/SFTP 서버의 IP 주소	유효한 IP 주소
-pn	TFTP/SFTP 서버의 포트 번호	유효한 포트 번호(기본값 69/22)
-u	SFTP 서버의 사용자 이름	유효한 사용자 이름
-pw	SFTP 서버의 암호	유효한 암호

예:

```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

roles 명령

이 명령을 사용하여 역할을 표시하거나 구성합니다.

구문:

```
roles role_account[3-31] [-options]
```

표 36. roles 옵션

옵션	설명	값
-n	역할 이름	32자로 제한
-p	권한 설정	<p>custom:am, rca, rcvma, pr, cel, bc, nsc, ac, us</p> <ul style="list-style-type: none"> • am: 사용자 계정 관리 액세스 • rca: 원격 콘솔 액세스 • rcvma: 원격 콘솔 및 원격 디스크(가상 미디어) 액세스 • pr: 원격 서버 전원/다시 시작 액세스 • cel: 이벤트 로그를 지우는 기능 • bc: 어댑터 구성(기본) • nsc: 어댑터 구성(네트워크와 보안) • ac: 고급 어댑터 구성(고급) • us: UEFI 보안 <p>참고: 위의 사용자 지정 권한 플래그는 조합하여 사용할 수 있음</p>
-d	행 삭제	

예:
system> roles -3 -n test1 -p custom:am|rcal|rcvma
ok

```
system> roles
Account      Role           Privilege      Assigned To
-----
0            Administrator  all            USERID
1            ReadOnly      none
2            Operator      custom:pr|cel|bc|nsc
3            test1        custom:am|rcal|rcvma
```

rtd 명령

이 명령을 사용하여 모든 BMC 설정을 공장 출하 기본값으로 복원합니다.

참고: 이 명령은 `restoredefaults` 및 `clearcfg` 명령이었습니다.

구문:
rtd [-options]

표 37. rtd 옵션

옵션	설명
-all	모든 BMC 설정을 공장 기본값으로 재설정합니다.
-eu	사용자 설정을 제외한 모든 BMC 설정을 공장 기본값으로 재설정합니다.
-en	네트워크 설정을 제외한 모든 BMC 설정을 공장 기본값으로 재설정합니다.
-eun	사용자 및 네트워크 설정을 제외한 모든 BMC 설정을 공장 기본값으로 재설정합니다.

예:
system> rtd -all

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

```
Proceed? (y/n)
Y
Restoring defaults
```

seccfg 명령

이 명령을 사용하여 방화벽 롤백을 수행합니다.

구문:
seccfg [-options]

표 38. secctfg 옵션

옵션	설명	값
-fwrb	이전 버전으로의 펌웨어 롤백을 허용합니다.	enabled, disabled
-aubp	기본 승격에 대한 자동 백업 기능을 활성화 또는 비활성화합니다.	enabled, disabled

securityinfo 명령

이 명령은 보안 관련 정보를 표시하는 데 사용됩니다.

구문:

securityinfo [-options]

표 39. securityinfo 옵션

옵션	설명
-event	보안 이벤트를 표시합니다.
-cryptomode	보안 cryptomode 상태를 표시합니다.
-service	서비스 및 포트의 보안 상태를 표시합니다.
-cert	인증서의 보안 상태를 표시합니다.
-account	사용자 계정의 보안 상태를 표시합니다.

securitymode 명령

이 명령은 새 서비스 데이터 파일을 생성하는 데 사용됩니다.

구문:

securitymode [-options]

표 40. securitymode 옵션

옵션	설명	값
-mode	보안 모드를 선택합니다. <ul style="list-style-type: none"> CNSA - 엔터프라이즈급 강력한 FIPS - 표준 COMPAT- 호환성 	CNSA, FIPS, COMPAT <ul style="list-style-type: none"> CNSA: 엔터프라이즈급 강력한 수준 암호화를 지원하는 서비스만 허용되며, 이를 활성화하려면 FoD(Features on Demand) 키가 필요합니다. FIPS: 표준 수준 암호화를 지원하지 않는 암호화가 필요한 서비스는 기본적으로 비활성화되어 있습니다. COMPAT: 이 모드가 활성화되면 XCC는 표준 검증 모드에서 작동하지 않습니다. 모든 서비스를 활성화할 수 있습니다.
-h	사용 및 옵션을 나열합니다.	

set 명령

이 명령을 사용하여 일부 IMM 설정을 변경합니다.

- 일부 IMM 설정은 간단한 set 명령을 사용하여 변경할 수 있습니다.
- 이 설정 중 환경 변수 같은 것은 CLI가 사용됩니다.

다음 표는 옵션의 인수를 보여줍니다.

표 41. set 명령

다음 표는 명령, 설명 및 관련 정보로 구성되어 있는 단일 행 3열 표입니다.

옵션	설명	값
변수	지정된 경로 또는 설정에 대한 값을 설정하십시오.	지정된 경로 또는 설정에 대한 적절한 값.

구문:
 set [-options]
 option:
 value

snmp 명령

이 명령을 사용하여 SNMP 인터페이스 정보를 표시 및 구성합니다.

구문:
 snmp [-options]

표 42. snmp 옵션

옵션	설명	값
-a3	SNMPv3 에이전트	on, off 참고: SNMPv3 에이전트를 활성화하려면 다음 기준이 충족되어야 합니다. • -cn 명령 옵션을 사용하여 지정된 IMM 담당자. • -l 명령 옵션을 사용하여 지정된 IMM 위치.
-t	SNMPv3 트랩	on, off
-tn	SNMPv3 트랩 사용자 이름	유효한 사용자 이름
-tauth	SNMPv3 트랩 인증 프로토콜	none, HMAC-SHA
-tapw	SNMPv3 트랩 인증 암호	유효한 암호
-tpriv	SNMPv3 트랩 개인 프로토콜	none, CBC-DES, AES
-tppw	SNMPv3 트랩 개인 암호	유효한 암호
-tix	커뮤니티 IP 주소 또는 호스트 이름 x	유효한 IP 주소 또는 호스트 이름(63자로 제한, x의 범위는 1~3일 수 있음). 참고: • IP 주소 또는 호스트 이름에는 마침표, 밑줄, 마이너스 기호, 문자, 숫자만 포함할 수 있습니다. 공백이나 연속 마침표는 사용할 수 없습니다. • 인수 없음을 지정하여 커뮤니티 IP 주소 또는 호스트 이름을 지웁니다.

표 42. snmp 옵션 (계속)

옵션	설명	값
-l	IMM 위치	문자열(47자로 제한). 참고: <ul style="list-style-type: none"> 공백을 포함하고 있는 인수의 경우에는 따옴표로 묶어야 합니다. 인수에서는 앞 공백 또는 뒤 공백이 허용됩니다. 인수 없음을 지정하거나 빈 문자열을 인수로 지정(예: "")하여 IMM 위치를 지웁니다.
-cn	IMM 담당자 이름	문자열(47자로 제한). 참고: <ul style="list-style-type: none"> 공백을 포함하고 있는 인수의 경우에는 따옴표로 묶어야 합니다. 인수에서는 앞 공백 또는 뒤 공백이 허용됩니다. 인수 없음을 지정하거나 빈 문자열을 인수로 지정(예: "")하여 IMM 연락처 이름을 지웁니다.
-t1	SNMPv1 TRAP	on, off
-c	SNMP 커뮤니티 이름	문자열(15자로 제한). 참고: <ul style="list-style-type: none"> 공백을 포함하고 있는 인수의 경우에는 따옴표로 묶어야 합니다. 인수에서는 앞 공백 또는 뒤 공백이 허용됩니다. 인수 없음을 지정하거나 "" 같이 빈 문자열을 인수로 지정하여 SNMP 커뮤니티 이름을 지웁니다.
-ci	커뮤니티 IP 주소/호스트 이름 1	유효한 IP 주소 또는 호스트 이름(63자로 제한). 참고: <ul style="list-style-type: none"> IP 주소 또는 호스트 이름에는 마침표, 밑줄, 마이너스 기호, 문자, 숫자만 포함할 수 있습니다. 공백이나 연속 마침표는 사용할 수 없습니다. 인수 없음을 지정하여 커뮤니티 IP 주소 또는 호스트 이름을 지웁니다.
-cliy	커뮤니티 IP 주소/호스트 이름 y	유효한 IP 주소 또는 호스트 이름(63자로 제한, y의 범위는 2~3일 수 있음). 참고: <ul style="list-style-type: none"> IP 주소 또는 호스트 이름에는 마침표, 밑줄, 마이너스 기호, 문자, 숫자만 포함할 수 있습니다. 공백이나 연속 마침표는 사용할 수 없습니다. 인수 없음을 지정하여 커뮤니티 IP 주소 또는 호스트 이름을 지웁니다.
-t2	SNMPv2 트랩	on, off
-ct	SNMPv2 트랩 커뮤니티 이름	문자열(15자로 제한). 참고: <ul style="list-style-type: none"> 공백을 포함하고 있는 인수의 경우에는 따옴표로 묶어야 합니다. 인수에서는 앞 공백 또는 뒤 공백이 허용됩니다. 인수 없음을 지정하거나 빈 문자열을 인수로 지정(예: "")하여 IMM 연락처 이름을 지웁니다.

표 42. snmp 옵션 (계속)

옵션	설명	값
-cti	SNMPv2 트랩 커뮤니티 IP 주소/호스트 이름 1	유효한 IP 주소 또는 호스트 이름 (63자로 제한). 참고: <ul style="list-style-type: none"> IP 주소 또는 호스트 이름에는 마침표, 밑줄, 마이너스 기호, 문자, 숫자만 포함할 수 있습니다. 공백이나 연속 마침표는 사용할 수 없습니다. 인수 없음을 지정하여 SNMP 커뮤니티 IP 주소 또는 호스트 이름을 지웁니다.
-eid	SNMP 엔진 ID	문자열 (1~27자로 제한)
-send	테스트 트랩 정보 전송	

예:

```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

snmpalerts 명령

이 명령을 사용하여 SNMP를 통해 전송되는 경보를 관리합니다.

구문:

```
snmpalerts [-options]
```

표 43. snmpalerts 옵션

옵션	설명	값
-status	SNMP 경고 상태	on, off
-crt	경보를 보내는 위험 이벤트 설정	all, none, custom:tel vo po di fa cp me in re ot pc 사용자 지정 위험 경고 설정은 snmpalerts -crt custom:tel vo 형식의 값에 대한 파이프 분리 목록을 사용하여 지정되며, 여기서 사용자 지정 값은 다음과 같습니다. <ul style="list-style-type: none"> te: 위험 온도 임계값 초과 vo: 위험 전압 임계값 초과 po: 위험 전원 장애 di: 하드 디스크 드라이브 장애 fa: 팬 장애 cp: 마이크로프로세서 실패 me: 메모리 장애 in: 하드웨어 비호환성 re: 전원 중복 장애

표 43. snmpalerts 옵션 (계속)

옵션	설명	값
		<ul style="list-style-type: none"> ot: 기타 모든 위험 이벤트 pc: PCIe 위험 이벤트
-wrn	경보를 보내는 경고 이벤트 보내기	<p>all, none, custom:rp te vo po falcp me ot pw 사용자 지정 경고 경보 설정은 snmpalerts -wrn custom:rp te 형식의 값에 대한 파이프 분리 목록을 사용하여 지정되며, 사용자 지정 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> rp: 전원 중복 경고 te: 경고 온도 임계값 초과 vo: 경고 전압 임계값 초과 po: 경고 전원 임계값 초과 fa: 비위험 팬 이벤트 cp: 저하된 상태의 마이크로프로세서 me: 메모리 경고 ot: 기타 모든 경고 이벤트 pw: PCIe 경고 이벤트
-sys	경보를 보내는 일상적인 이벤트 보내기	<p>all, none, custom:lo tio ot po bf til pf el ne nl dh oa 사용자 지정 일상적인 경보 설정은 snmpalerts -sys custom:lo tio 형식의 값에 대한 파이프 분리 목록을 사용하여 지정되며, 여기서 사용자 지정값은 다음과 같습니다.</p> <ul style="list-style-type: none"> lo: 원격 로그인 성공 tio: 운영 체제 제한시간 ot: 기타 모든 정보 및 시스템 이벤트 po: 시스템 전원 켜기/끄기 bf: 운영 체제 부팅 실패 til: 운영 체제 로더 감시 장치 제한시간 pf: PFA(예측된 장애) el: 이벤트 로그 75 참 ne: 네트워크 변경 nl: 호스트 NIC 링크 다운/업 dh: 드라이브 핫플러그 oa: 기타 모든 감사 이벤트

sshcfg 명령

이 명령을 사용하여 SSH 매개 변수를 표시 및 구성합니다.

구문:
 sshcfg [-options]

표 44. sshcfg 옵션

옵션	설명	값
-cstatus	SSH CLI의 주	enabled, disabled
-hk	서버 키	gen, all <ul style="list-style-type: none"> • gen: SSH 서버 개인 키 생성 • all: 서버 공개 키 표시

예:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

sslcfg 명령

이 명령을 사용하여 IMM에 대한 SSL을 표시 및 구성하고 인증서를 관리합니다.

sslcfg는 새 암호화키 및 자체 서명된 인증서 또는 CSR(인증서 서명 요청)을 생성하는 데 사용됩니다.

구문:

```
sslcfg [-options]
```

표 45. sslcfg 옵션

옵션	설명	값
-server	HTTPS를 통한 웹 상태	enabled, disabled 참고: <ul style="list-style-type: none"> • HTTPS를 통한 웹은 인증서가 제 위치에 있는 경우에만 활성화할 수 있습니다. • 인증서를 완전히 비활성화하려면 -rm을 사용합니다.
-client	보안 LDAP 상태	enabled, disabled 참고: 올바른 인증서 또는 클라이언트 인증서가 제자리에 있는 경우에만 SSL 클라이언트를 활성화할 수 있습니다.
-cert	자체 서명된 인증서 생성	server, client, sysdir, storekey 참고: <ul style="list-style-type: none"> • 자체 서명된 인증서를 생성하는 경우에는 -c, -sp, -cl, -on 및 -hn 명령 옵션에 대한 값이 필요합니다. • 자체 서명된 인증서를 생성하는 경우에는 -cp, -ea, -ou, -s, -gn, -in 및 -dq 명령 옵션에 대한 값이 선택적입니다.
-csr	CSR 생성	server, client, sysdir, storekey 참고: <ul style="list-style-type: none"> • CSR을 생성하는 경우에는 -c, -sp, -cl, -on 및 -hn 명령 옵션에 대한 값이 필요합니다. • CSR을 생성하는 경우에는 -cp, -ea, -ou, -s, -gn, -in, -dq, -cpwd 및 -un 명령 옵션에 대한 값이 선택적입니다.
-form	내보낼 CSR 또는 인증서의 형식.	der, pem(기본값 pem)
-algo	CSR 알고리즘	p256, p384, rsa2048, rsa3072, rsa4096 참고: -algo 옵션이 없는 경우 기본값(p256)이 설정됩니다.

표 45. sslcfg 옵션 (계속)

옵션	설명	값
-rm	인증서 제거	server, storekey 참고: 기본 자체 서명된 인증서(서버)는 현재의 자체 서명된 인증서가 제거된 후 자동으로 생성됩니다.
-i	TFTP/SFTP의 IP 주소	유효한 IP 주소 참고: 인증서를 업로드하거나 인증서 또는 CSR을 다운로드하는 경우에는 TFTP 또는 SFTP 서버의 IP 주소를 지정해야 합니다.
-pn	TFTP/SFTP 서버의 포트 번호	유효한 포트 번호(기본값 69/22)
-u	SFTP 서버의 사용자 이름	유효한 사용자 이름
-pw	SFTP 서버의 암호	유효한 암호
-l	인증서 파일 이름	유효한 파일 이름 참고: 인증서 또는 CSR을 다운로드하거나 업로드하는 경우에는 파일 이름이 필요합니다. 다운로드를 위해 파일 이름을 지정하는 경우 파일의 기본 이름이 사용 및 표시됩니다.
-dnld	지정된 파일을 원격 호스트로 내보냅니다	이 옵션은 인수를 사용하지 않지만 -cert 또는 -csr과 -i 및 -l 명령 옵션으로 사용되어야 합니다.
-upld	인증서 파일 가져오기	이 옵션에서는 인수를 사용하지 않지만, -cert, -i 및 -l 명령 옵션의 값을 지정해야 합니다.
-tcx	SSL 클라이언트의 신뢰할 수 있는 인증서 x	가져오기, 다운로드, 제거 참고: 신뢰할 수 있는 인증서 번호 x는 명령 옵션에서 1~4의 정수로 지정됩니다.
자체 서명된 인증서 또는 CSR 생성에 필요한 옵션 참고: 자체 서명된 인증서 또는 CSR를 생성할 때 필요.		
-c	국가	국가 코드(2자리)
-sp	주 또는 도	따옴표로 구분된 문자열(최대 60자).
-cl	시 또는 군	따옴표로 구분된 문자열(최대 50자).
-on	조직 이름	따옴표로 구분된 문자열(최대 60자).
-hn	BMC 호스트 이름	문자열(최대 60자)
자체 서명된 인증서 또는 CSR 생성을 위한 선택적 옵션 참고: 자체 서명된 인증서 또는 CSR를 생성할 때 선택 사항.		
-cp	담당자	따옴표로 구분된 문자열(최대 60자).
-ea	담당자 이메일 주소	유효한 이메일 주소(최대 60자)
-ou	조직 단위	따옴표로 구분된 문자열(최대 60자).
-s	성	따옴표로 구분된 문자열(최대 60자).
-gn	이름	따옴표로 구분된 문자열(최대 60자).
-in	이니셜	따옴표로 구분된 문자열(최대 20자).
-dq	도메인 이름 식별자	따옴표로 구분된 문자열(최대 60자).
CSR 생성을 위한 선택적 옵션 참고: CSR을 생성할 때 옵션 사항.		
-cpwd	첼린지 암호	문자열(최소 6자~최대 30자)
-un	비구조화된 이름	따옴표로 구분된 문자열(최대 60자).

예:

```

system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
A self-signed certificate is installed
SSL Client Certificate status:
A self-signed certificate is installed
SSL Client Trusted Certificate status:
Trusted Certificate 1: Not available
Trusted Certificate 2: Not available
Trusted Certificate 3: Not available
Trusted Certificate 4: Not available

```

클라이언트 인증서 예:

- 스토리지 키의 CSR를 생성하려면 다음 명령을 입력하십시오.

```
system> sslcfg -csr storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou ""
```

ok
- 인증서를 IMM에서 다른 서버로 다운로드하려면 다음 명령을 입력하십시오.

```
system> sslcfg -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
```

ok
- CA(Certificate Authority)로 처리된 인증서를 업로드하려면 다음 명령을 입력하십시오.

```
system> sslcfg -cert storekey -upld -i 192.168.70.230 -l tklm.der
```
- 자체 서명된 인증서를 생성하려면 다음 명령을 입력하십시오.

```
system> sslcfg -cert storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou ""
```

ok

SKLM 서버 인증서 예:

- SKLM 서버 인증서를 가져오려면 다음 명령을 입력하십시오.

```
system> storekeycfg -add -ip 192.168.70.200 -f tklm-server.der
```

ok

syslock 명령

이 명령을 사용하여 시스템 잠금 설정을 표시 및 구성합니다.

구문:

syslock [-options]

표 46. syslock 옵션

옵션	설명	값
-en	시스템 구성 잠금 기능을 활성화 또는 비활성화합니다. 참고: -e 옵션을 통해 활성화하면 현재 인벤토리를 신뢰할 수 있는 스냅샷으로 승격할 수 있습니다.	enabled, disabled
-e	현재 인벤토리를 신뢰할 수 있는 스냅샷에 적용하거나 적용하지 않고 시스템 구성 잠금 설정을 활성화합니다.	enabled, disabled

표 46. syslock 옵션 (계속)

옵션	설명	값
	참고: -e 옵션이 없는 경우 기본값이 설정됩니다.	
-l [x]	색인 x에 있는 특정 스냅샷의 인벤토리를 나열합니다.	색인 번호 x는 명령 옵션에서 정수로 지정됩니다.
-m	수동 스냅샷을 만듭니다.	
-d	수동 스냅샷에 대한 설명입니다.	최대 32자의 문자열.
-c	신뢰할 수 있는 스냅샷과 인벤토리의 차이를 나열합니다.	
-po	잠금 정책을 설정합니다. 참고: 이 작업은 시스템 가드가 비준수 상태인 경우 서버가 부팅되지 않도록 합니다.	none, osboot, pperm
-cpu	CPU 잠금을 설정합니다.	on, off
-dimm	DIMM 잠금을 설정합니다.	on, off
-pci	PCI 잠금을 설정합니다.	on, off
-drive	드라이브 잠금을 설정합니다.	on, off
-riser	라이저 잠금을 설정합니다.	on, off
-bp	백플레인 잠금을 설정합니다.	on, off

thermal 명령

이 명령을 사용하여 호스트 시스템의 열전도 모드 정책을 표시 및 구성합니다.

옵션이 없이 thermal 명령을 실행하면 텔넷 모드 정책이 표시됩니다. 다음 표는 옵션의 인수를 보여줍니다.

구문:

thermal [-options]

표 47. thermal 옵션

옵션	설명	값
-mode	열전도 모드 정책 표시 및 호스트 시스템의 열전도 표 구성(읽기 전용)	<ul style="list-style-type: none"> • 일반 컴퓨팅 - 전력 효율 • 일반 컴퓨팅 - 피크 주파수 • 일반 컴퓨팅 - 최대 성능 • 가상화 - 전력 효율 • 가상화 - 최대 성능 • 데이터베이스 - 트랜잭션 처리 • 낮은 지연 시간 • 고성능 컴퓨팅 • 사용자 지정 • 알 수 없음
-table ta-	table_number는 사용할 대체 열전도 표를 지정합니다.	1 = 낮음: 팬 속도 약간 부스트

표 47. thermal 옵션 (계속)

옵션	설명	값
ble_num-ber		2 = 중간: 팬 속도 중간 수준 부스트 3 = 높음: 팬 속도 아주 빠르게 부스트 0 = 보통: 팬 속도 부스트 없음

예:
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>

tls 명령

이 명령을 사용하여 최소 TLS 수준을 설정합니다.

구문:
tls [-options]

표 48. tls 옵션

옵션	설명	값
-min	최소 TLS 수준을 선택하십시오.	1.2, 1.3 참고: 암호화 모드를 NIST-800-131A 준수 모드로 설정하는 경우 TLS 버전을 1.2로 설정해야 합니다.
-h	사용 및 옵션 열거	
참고: 1. 암호화 모드를 NIST-800-131A 준수 모드로 설정하는 경우 TLS 버전을 1.2로 설정해야 합니다.		

예:

tls 명령에 대한 사용을 가져오려면 다음 명령을 내립니다.
system> tls
-h
system>

현재 tls 버전을 가져오려면 다음 명령을 내립니다.
system> tls
-min 1.2
system>

현재의 tls 버전을 1.2로 변경하려면 다음 명령을 내립니다.
system> tls -min 1.2
ok
system>

trespass 명령

이 명령을 사용하여 침입 메시지를 구성하고 표시합니다.

trespass 명령은 침입 메시지를 구성하고 표시하는 데 사용할 수 있습니다. 침입 메시지는 WEB 또는 CLI 인터페이스를 통해 로그인하는 모든 사용자에게 표시됩니다.

구문:
trespass [-options]

표 49. trespass 옵션

옵션	설명
-s	침입 메시지 구성
-h	사용 및 옵션 열거

예:
system> trespass -s testingmessage
ok
system> trespass
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>

uefipw 명령

이 명령을 사용하여 UEFI 관리자 암호를 구성합니다. 암호는 쓰기 전용입니다.

uefipw 명령을 "-p" 옵션과 함께 사용하여 XCC에 대한 UEFI 관리자 암호를 구성하거나 LXCA에 대한 "-ep" 옵션과 함께 사용하여 CLI 인터페이스를 통해 UEFI 관리자 암호를 구성할 수 있습니다. 암호는 쓰기 전용입니다.

구문:
uefipw [-options]

표 50. uefipw 옵션

옵션	설명
-cp	현재 암호(20자로 제한)
-p	새 암호(20자로 제한)

usbeth 명령

이 명령을 사용하여 USB를 통한 대역 내 LAN 인터페이스를 활성화 또는 비활성화합니다.

참고:

- OS IP 구성 설정은 USB를 통한 이더넷 인터페이스의 OS IP 주소를 설정하는 데 사용되지 않지만 USB를 통한 이더넷의 OS IP 주소가 변경되었음을 BMC에 알리는 데 사용됩니다.
- USB를 통한 이더넷에 대한 세 가지 IP 설정을 구성하기 전에 로컬 운영 체제의 USB를 통한 이더넷 인터페이스의 OS IP 주소를 수동으로 구성해야 합니다.

구문:
usbeth [-options]

표 51. usbeth 옵션

옵션	설명	값
-en	대역 내(USB를 통한 이더넷) 인터페이스를 활성화 또는 비활성화합니다.	enabled, disabled
-am	주소 모드 IPv4 또는 IPv6 LLA를 선택합니다.	ipv4, ipv6lla
참고: -ip, -sn 및 -ipos 옵션은 -am ipv4 모드를 선택한 경우에만 유효합니다		
-ip	BMC용 USB를 통한 이더넷 인터페이스 IP 주소.	유효한 IP 주소
-sn	BMC용 USB를 통한 이더넷 인터페이스 서브넷 마스크.	유효한 IP 주소
-ipos	OS용 USB를 통한 이더넷 인터페이스 IP 주소.	유효한 IP 주소

```

예:
system> usbeth
-en : disabled
system> usbeth -en enabled
ok
system> usbeth
-en : disabled
system>
    
```

users 명령

이 명령을 사용하여 모든 사용자 계정 및 권한 수준에 액세스합니다.

users 명령은 또한 새 사용자 계정을 만들고 기존 계정을 수정하는 데 사용됩니다. 옵션이 없이 users 명령을 실행하면 사용자 목록 및 일부 기본 사용자 정보가 표시됩니다.

구문:
 users [-user_index][-options]

표 52. users 옵션

옵션	설명	값
-user_index	사용자 계정 색인 번호.	여기서 user_index는 1~12(포함) 또는 all(모든 사용자를 나타냄).
-l	암호 만료일 표시	
-n	사용자 계정 이름	번호, 숫자, 문자, 마침표 및 밑줄을 포함하는 고유 문자열. 최소 4자~최대 16자.
-p	사용자 계정 암호	최소 1개의 알파벳 문자와 1개의 비알파벳 포함. 최소 6자 및 최대 255자. Null는 사용자가 처음에 로그인할 때 설정해야 하는 암호가 없는 계정을 만듭니다.
-shp	해시 암호 설정	총 64자
-ssalt	salt 설정	64자로 제한
-ghp	hashpassword 가져오기	
-gsalt	salt 가져오기	
-ep	암호화 암호(백업/복구용)	유효한 암호

표 52. users 옵션 (계속)

옵션	설명	값
-esalt	암호화된 암호에 대한 salt	백업 또는 복원에만 해당
-r	역할 이름	Administrator, Operator, ReadOnly. "roles 명령" 112페이지 명령에 나열된 대로.
-clear	특정 사용자 계정을 지우십시오.	지울 사용자 계정 색인 번호를 다음의 형식에 따라 지정해야 합니다. users -clear -user_index 참고: 권한이 부여된 경우 사용자 계정 관리 권한이 있는 유일한 계정만 아니면 현재 로그인되어 있는 상태이더라도 자신의 계정 또는 다른 사용자의 계정을 제거할 수 있습니다. 사용자 계정을 삭제할 때 진행 중인 세션은 자동으로 종료되지 않습니다.
-curr	현재 로그인된 다른 사용자 표시	
-ai	사용자 액세스 가능 인터페이스	web, ssh, redfish, ipmi, snmp, all 참고: -ai 옵션이 없는 경우 기본값(web ssh redfish)이 설정됩니다.
-sauth	SNMPv3 인증 프로토콜	None, HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_SHA256, HMAC256_SHA384, HMAC384_SHA512
-spriv	SNMPv3 개인 정보 프로토콜	None, CBC_DES, CFB128_AES128, AES192, AES256, AES192C, AES256C
-spw	SNMPv3 개인 정보 암호	유효한 암호
-sepw	SNMPv3 개인 정보 암호 (암호화됨)	유효한 암호
-sacc	SNMPv3 액세스 유형	가져오기
-strap1	SNMPv3 트랩 호스트 이름 1	유효한 호스트 이름
-strap2	SNMPv3 트랩 호스트 이름 2	유효한 호스트 이름
-strap3	SNMPv3 트랩 호스트 이름 3	유효한 호스트 이름
-pk	사용자의 SSH 공개 키 표시	사용자 계정 색인 번호. 참고: <ul style="list-style-type: none"> • 식별하는 키 색인 번호와 함께 사용자에게 할당된 각 SSH 키가 표시됩니다. • SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인 (-userindex 옵션) 다음에 users -2 -pk의 형식으로 사용해야 합니다. • 모든 키는 OpenSSH 형식입니다.
다음 옵션은 -pk와 함께 사용됩니다		
-e	모든 SSH 키를 OpenSSH 형식으로 표시합니다. (SSH 공개 키 옵션)	이 옵션은 인수를 사용하지 않으며 다른 모든 users -pk 옵션을 제외하고 사용해야 합니다. 참고: SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인 (-userindex 옵션) 다음에 users -2 -pk -e의 형식으로 사용해야 합니다.

표 52. users 옵션 (계속)

옵션	설명	값
-remove	사용자에게서 SSH 공개 키 제거 (SSH 공개 키 옵션)	사용자에게 할당된 모든 키에 대해 제거할 공개 키 색인 번호를 특정 -key_index 또는 -all의 형식으로 부여해야 합니다. 참고: SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인 (-userindex 옵션) 다음에 users -2 -pk -remove -1의 형식으로 사용해야 합니다.
-add	사용자의 SSH 공개 키 추가 (SSH 공개 키 옵션)	OpenSSH 형식의 따옴표로 구분된 키 참고: <ul style="list-style-type: none"> 다른 모든 users -pk 명령 옵션을 제외하고 -add 옵션을 사용해야 합니다. SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인(-userindex 옵션) 다음에 다음 형식으로 사용해야 합니다. users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAvmfTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaNOy400ICEKcQjKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzCJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBL3SAtMucUsTkYjLXcqex10Qz4+N5OR6MbNcwlx+mTEAvvcpJhuga70UNP6hLJML6k7jeJiQ8Xd2p XboZQ=="
-upld	SSH 공개 키를 OpenSSH 또는 RFC4716 형식으로 업로드 (SSH 공개 키 옵션)	키 위치를 지정할 -i 및 -l 옵션이 필요합니다. 참고: <ul style="list-style-type: none"> 다른 모든 users -pk 명령 옵션을 제외하고 -upld 옵션을 사용해야 합니다(-i 및 -l 제외). 키를 새 키로 교체하려면 -key_index를 지정해야 합니다. 키를 현재 키의 목록 끝에 추가하려면 키 색인을 지정하지 마십시오. SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인 (-userindex 옵션) 다음에 users -2 -pk -upld -i tftp://9.72.216.40/-l file.key의 형식으로 사용해야 합니다.
-dnld	지정된 SSH 공개 키를 TFTP/SFTP 서버에 다운로드 (SSH 공개 키 옵션)	다운로드할 키를 지정하기 위해 -key_index가 필요하며 TFTP 서버를 실행하는 다른 컴퓨터에 다운로드 위치를 지정하기 위해 -i 및 -l 옵션이 필요합니다. 참고: <ul style="list-style-type: none"> 다른 모든 users -pk 명령 옵션을 제외하고 -dnld 옵션이 사용됩니다(-i, -l 및 -key_index 제외). SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인(-userindex 옵션) 다음에 users -2 -pk -dnld -1 -i tftp://9.72.216.40/-l file.key의 형식으로 사용해야 합니다.
-i	키 파일 업로드 및 다운로드를 위한 TFTP/SFTP 서버의 IP 주소 (SSH 공개 키 옵션)	유효한 IP 주소 참고: -i 옵션은 users -pk -upld 및 users -pk -dnld 옵션에 반드시 필요합니다.
-pn	TFTP/SFTP 서버의 포트 번호 (SSH 공개 키 옵션)	유효한 포트 번호(기본값 69/22) 참고: users -pk -upld 및 users -pk -dnld 명령 옵션에 대한 옵션 매개 변수.
-u	SFTP 서버의 사용자 이름 (SSH 공개 키 옵션)	유효한 사용자 이름 참고: users -pk -upld 및 users -pk -dnld 명령 옵션에 대한 옵션 매개 변수.

표 52. users 옵션 (계속)

옵션	설명	값
-pw	SFTP 서버의 암호 (SSH 공개 키 옵션)	유효한 암호 참고: users -pk -upld 및 users -pk -dnld 명령 옵션에 대한 옵션 매개 변수.
-l	TFTP 또는 SFTP를 통해 키 파일을 업로드 및 다운로드하기 위한 파일 이름 (SSH 공개 키 옵션)	유효한 파일 이름 참고: -l 옵션은 users -pk -upld 및 users -pk -dnld 옵션에 반드시 필요합니다.
-af	호스트의 연결 승인 (SSH 공개 키 옵션)	쉽표로 구분한 호스트 이름과 IP 주소 목록은 511자로 제한됨. 유효한 문자는 다음과 같습니다. 영숫자, 쉽표, 별표, 물음표, 감탄 부호, 마침표, 하이픈, 콜론 및 백분율 기호.
-cm	주석 (SSH 공개 키 옵션)	최대 255자의 따옴표로 구분된 문자열. 참고: SSH 공개 키 옵션을 사용하는 경우 -pk 옵션을 사용자 색인(-userindex 옵션) 다음에 users -2 -pk -cm "This is my comment."의 형식으로 사용해야 합니다.

예:

```

system> users
Login ID   Name      Advanced Attribute  Role          Password Expires
-----
1         USERID   Native              Administrator  89 day(s)
system> users -2 -n sptest -p PasswOrd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
Login ID   Name      Advanced Attribute  Role          Password Expires
-----
1         USERID   Native              Administrator  90 day(s)
2         sptest    Native              Administrator  Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r Administrator
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system>

```

IMM 제어 명령

이 항목에서는 IMM 제어 CLI 명령 목록을 알파벳순으로 제공합니다.

현재 다음과 같은 7가지 IMM 제어 명령이 있습니다.

batch 명령

이 명령을 사용하여 파일에 포함된 1개 이상의 CLI 명령을 실행합니다.

참고:

- 배치 파일의 주석 줄은 #로 시작됩니다.
- 배치 파일을 실행할 때 실패하는 명령은 실패 반환 코드와 함께 반환됩니다.
- 인식되지 않은 명령 옵션이 포함되어 있는 배치 파일 명령은 경고를 생성할 수 있습니다.

구문:

batch [-options]

표 53. batch 옵션

옵션	설명	값
-f	배치 파일 이름	유효한 파일 이름
-ip	TFTP/SFTP 서버의 IP 주소	유효한 IP 주소
-pn	TFTP/SFTP 서버의 포트 번호	유효한 포트 번호(기본값 69/22)
-u	SFTP 서버의 사용자 이름	유효한 사용자 이름
-pw	SFTP 서버의 암호	유효한 암호

예:
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>

clock 명령

이 명령을 사용하여 현재 날짜 및 시간을 표시합니다. UTC 오프셋 및 일광 절약 시간 설정을 지정할 수 있습니다.

구문:
clock [-options]

표 54. clock 옵션

옵션	설명	값
-u	UTC 오프셋	+2, -7, -6, -5, -4, -3 특수 일광 절약 시간 설정의 UTC 오프셋이 필요합니다. <ul style="list-style-type: none"> +2의 경우 일광 절약 시간 옵션은 다음과 같습니다. off, ee(동유럽), tky(터키), bei(베이루트), amm(암만), jem(예루살렘). -7의 경우 일광 절약 시간 설정은 다음과 같습니다. off, mtn(산지), maz(마사틀란). -6의 경우 일광 절약 시간 설정은 다음과 같습니다. off, mex(멕시코), cna(북아메리카 중부). -5의 경우 일광 절약 시간 설정은 다음과 같습니다. off, cub(쿠바), ena(북아메리카 동부). -4의 경우 일광 절약 시간 설정은 다음과 같습니다. off, asu(아순시온), cui(쿠이아바), san(산티아고), cat(캐나다-대서양). -3의 경우 일광 절약 시간 설정은 다음과 같습니다. off, gtb(고트호프), bre(브라질-동부).
-dst	일광 절약 시간	on, off, 특수 케이스
-host	호스트에서 가져온 시간 형식(기본값: utc)	local, utc 참고: Windows 시스템은 local 사용, Linux는 utc 사용

참고:

- BMC는 호스트 서버 또는 NTP 서버에서 시간을 가져옵니다.

- 호스트에서 가져온 시간은 로컬 시간이거나 UTC 시간일 수 있습니다. NTP가 사용되지 않고 호스트에서 UTC 형식을 사용하는 경우 호스트 옵션을 UTC로 설정해야 합니다.
- UTC 오프셋은 양의 오프셋인 경우 +0200, +2:00, +2 또는 2 형식이고 음의 오프셋인 경우 -0500, 5:00 또는 -5 형식일 수 있습니다.
- UTC 오프셋 및 일광 절약 시간은 NTP와 함께 사용되거나 호스트 모드가 UTC인 경우 사용됩니다.

예:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

info 명령

이 명령을 사용하여 BMC에 대한 정보를 표시하고 구성합니다.

구문:

```
info [-options]
```

표 55. info 옵션

옵션	설명	값
-name	BMC 이름	String
-contact	BMC 담당자의 이름	String
-location	BMC 위치	String
-postal	BMC의 전체 우편 주소	String
-room	BMC 룸 식별자	String
-rack	BMC 랙 식별자	String
-rup	랙에서 BMC의 위치	String

예:

```
system> info
-name: BMCName
-location: location
-contact: contact
-rack: rack
-room: room
-postal: postal
-rup: 1
system>
```

sreset 명령

이 명령을 사용하여 IMM을 다시 시작합니다.

이 명령을 실행하려면 최소한 고급 어댑터 구성 권한이 있어야 합니다.

구문:

```
sreset
```

Agent-less 명령

이 주제에서는 Agent-less 명령 목록을 알파벳순으로 제공합니다.

현재 3가지 Agent-less 명령이 있으며 다음과 같습니다.

storage 명령

이 명령을 사용하여 IMM에서 관리하는 서버의 스토리지 장치에 대한 정보를 표시하고 구성합니다 (플랫폼에서 지원하는 경우).

구문:
storage [-options]

표 56. 스토리지 옵션

옵션	설명	값
-list	IMM에서 관리하는 스토리지 대상을 나열합니다.	controllers pools volumes drives <ul style="list-style-type: none"> controllers: 지원되는 RAID 컨트롤러 나열¹ pools: RAID 컨트롤러와 관련된 스토리지 풀 나열¹ volumes: RAID 컨트롤러와 관련된 스토리지 볼륨 나열¹ drives: RAID 컨트롤러와 관련된 스토리지 드라이브 나열¹
-list storage targets -target target_id	target_id에 따라 IMM에서 관리하는 스토리지 대상을 나열합니다.	pools volumes drives 및 ctrl[x] pool[x] 여기서 storage targets 및 target_id는 다음과 같습니다. <ul style="list-style-type: none"> pools 및 ctrl[x]: target_id를 기준으로 RAID 컨트롤러와 관련된 스토리지 풀 나열¹ volumes 및 ctrl[x] pool[x]: target_id를 기준으로 RAID 컨트롤러와 관련된 스토리지 볼륨 나열¹ drives 및 ctrl[x] pool[x]: target_id를 기준으로 RAID 컨트롤러와 관련된 스토리지 드라이브 나열¹
-list devices	IMM에서 관리하는 모든 디스크의 상태를 표시합니다.	
-show target_id	IMM에서 관리하는 선택된 대상에 대한 정보를 표시합니다.	여기서 target_id는 ctrl[x] vol[x] disk[x] pool[x] ³
-show target_id info	IMM에서 관리하는 선택된 대상에 대한 자세한 정보를 표시합니다.	여기서 target_id는 ctrl[x] vol[x] disk[x] pool[x] ³
-show target_id firmware ³	IMM에서 관리하는 선택된 대상에 대한 펌웨어 정보를 표시합니다.	여기서 target_id는 ctrl[x] disk[x] ²
-showinfo nvme	Nvme 디스크의 펌웨어 정보를 표시합니다.	
-wthre show	위험 및 경고 SSD 마모 임계값을 표시합니다.	임계값(1~99)
-wthre -ct threshold value	SSD 마모 위험 임계값을 설정합니다.	임계값(1~99)
-wthre -wt threshold value	SSD 마모 경고 임계값을 설정합니다.	임계값(1~99) 참고: 경고 값은 위험 값보다 커야 합니다.

표 56. 스토리지 옵션 (계속)

옵션	설명	값
-config ctrl -scanforgn -target target_id ³	외부 RAID 구성을 감지합니다.	여기서 target_id는 ctrl[x] ⁵
-config ctrl -imptforgn -target target_id ³	외부 RAID 구성을 가져옵니다.	여기서 target_id는 ctrl[x] ⁵
-config ctrl -clrforgn -target target_id ³	외부 RAID 구성을 지웁니다.	여기서 target_id는 ctrl[x] ⁵
-config ctrl -clrcfg -target target_id ³	RAID 구성을 지웁니다.	여기서 target_id는 ctrl[x] ⁵
-config ctrl -bootdevice -vd volume -target target_id	볼륨별로 부팅 장치를 설정합니다.	여기서 target_id는 ctrl[x]이고 volume은 'list volumes' 출력의 첫 번째 열에 있는 값입니다.
-config ctrl -bootdevice -pd drive -target target_id	드라이브별로 부팅 장치를 설정합니다.	여기서 target_id는 ctrl[x]이고 drive는 'list drives' 출력의 첫 번째 열에 있는 값입니다.
-config ctrl -bootdevice -index index -target target_id	색인별로 부팅 장치를 설정합니다.	여기서 target_id는 ctrl[x]이고 index는 'display' 옵션의 출력인 "[]"의 값입니다.
-config ctrl -bootdevice -display -target target_id	부팅 가능한 장치를 표시합니다.	
-config drv -mkoffline -target target_id ³	드라이브 상태를 온라인에서 오프라인으로 변경합니다.	여기서 target_id는 disk[x] ⁵
-config drv -mkonline -target target_id ³	드라이브 상태를 오프라인에서 온라인으로 변경합니다.	여기서 target_id는 disk[x] ⁵
-config drv -mkmissing -target target_id ³	오프라인 드라이브를 구성되지 않은 정상 드라이브로 표시합니다.	여기서 target_id는 disk[x] ⁵
-config drv -prprm -target target_id ³	구성되지 않은 정상 드라이브를 제거할 준비를 합니다.	여기서 target_id는 disk[x] ⁵
-config drv -undoprprm -target target_id ³	구성되지 않은 정상 드라이브 제거 준비 동작을 취소합니다.	여기서 target_id는 disk[x] ⁵
-config drv -mkbad -target target_id ³	구성되지 않은 정상 드라이브를 구성되지 않은 잘못된 드라이브로 변경합니다.	여기서 target_id는 disk[x] ⁵
-config drv -mkgood -target target_id ³	구성되지 않은 잘못된 드라이브를 구성되지 않은 정상 드라이브로 변경합니다. 또는 디스크 묶음을 구성되지 않은 정상 드라이브로 변환합니다.	여기서 target_id는 disk[x] ⁵

표 56. 스토리지 옵션 (계속)

옵션	설명	값
-config drv -mkjbod -target target_id ³	구성되지 않은 양호 상태를 JBOD로 만듭니다.	여기서 target_id는 disk[x] ⁵
-config drv -rebuild -target target_id ³	드라이브 재구축을 시작합니다.	여기서 target_id는 disk[x] ⁵
-config drv -addhsp -target target_id ³	선택된 드라이브를 핫 스페어로 1개의 컨트롤러 또는 기존 스토리지 풀에 할당합니다.	여기서 target_id는 disk[x] ⁵
-config drv -dedicated pools -target target_id ³	드라이브를 선택한 스토리지 풀에 전용 핫 스페어로 할당합니다.	여기서 target_id는 disk[x] ⁵
-config drv -rmhsp -target target_id ³	핫 스페어를 제거합니다.	여기서 target_id는 disk[x] ⁵
-config vol -remove -targettarget_id ³	1개의 볼륨을 제거합니다.	여기서 target_id는 vol[x] ⁵
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target target_id ³	볼륨 1개의 속성을 수정합니다.	<ul style="list-style-type: none"> • [-N volume_name]은 볼륨의 이름입니다. • [-w <0 1 2 3>]은 캐시 쓰기 정책입니다. <ul style="list-style-type: none"> - 동시 쓰기 정책은 0 입력 - 보호된 나중 쓰기 정책은 1 입력 - 보호되지 않는 나중 쓰기 정책은 2 입력 - 정책 없음은 3 입력 • [-r <0 1>]은 캐시 읽기 정책입니다. <ul style="list-style-type: none"> - 미리 읽기 없음 정책은 0 입력 - 미리 읽기 정책은 1 입력 • [-i <0 1>]은 캐시 I/O 정책입니다. <ul style="list-style-type: none"> - 직접 I/O 정책은 0 입력 - 캐시된 I/O 정책은 1 입력 • [-r <0 2 3>]은 캐시 읽기 정책입니다. <ul style="list-style-type: none"> - 읽기 쓰기 정책은 0 입력 - 읽기 전용 정책은 2 입력 - 차단 정책은 3 입력 • [-d <0 1 2>]은 디스크 캐시 정책입니다. <ul style="list-style-type: none"> - 정책이 변경되지 않으면 0 입력 - 정책⁶을 사용하려면 1 입력 - 정책을 사용 안 함으로 설정하려면 2 입력 • [-b <0 1>]은 백그라운드 초기화입니다. <ul style="list-style-type: none"> - 초기화를 활성화하려면 0 입력 - 초기화를 비활성화하려면 1 입력 • -target_id는 vol[x]⁵입니다.

표 56. 스토리지 옵션 (계속)

옵션	설명	값
<p>-config vol -add [-R] [-D disk] [-H disk] [-l hole] [-N] [-w] [-r]^{3,7}</p>	<p>대상이 컨트롤러이면 새 스토리지 풀에 대해 1개의 볼륨을 작성하십시오.</p> <p>또는</p> <p>대상이 스토리지 풀이면 기존 스토리지 풀으로 1개의 볼륨을 작성하십시오.</p>	<ul style="list-style-type: none"> • [-R <0 1 5 1E 6 10 50 60 00>] 이 옵션은 RAID 수준을 정의하며 새 스토리지 풀에서만 사용됨 • [-D disk [id1]:disk[id2]:..disk[id21]:disk[id22]:..] 이 옵션은 드라이브 그룹(스팬 포함)을 정의하며 새 스토리지 풀에서만 사용됩니다. • [-H disk [id1]:disk[id2]:..] 이 옵션은 핫 스페어 그룹을 정의하며 새 스토리지 풀에서만 사용됨 • [-l hole] 이 옵션은 기존 스토리지 풀에 대한 여유 구멍 공간의 색인 번호를 정의합니다. • [-N volume_name]은 볼륨의 이름입니다. • [-w <0 1 2 3>]은 캐시 쓰기 정책입니다. <ul style="list-style-type: none"> - 동시 쓰기 정책은 0 입력 - 보호된 나중 쓰기 정책은 1 입력 - 보호되지 않는 나중 쓰기 정책은 2 입력 - 정책 없음은 3 입력 • [-r <0 1>]은 캐시 읽기 정책입니다. <ul style="list-style-type: none"> - 미리 읽기 없음 정책은 0 입력 - 미리 읽기 정책은 1 입력
<p>-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target target_id³</p>	<p>대상이 컨트롤러이면 새 스토리지 풀에 대해 1개의 볼륨을 작성하십시오.</p> <p>또는</p> <p>대상이 스토리지 풀이면 기존 스토리지 풀으로 1개의 볼륨을 작성하십시오.</p>	<ul style="list-style-type: none"> • [-i <0 1>]은 캐시 I/O 정책입니다. <ul style="list-style-type: none"> - 직접 I/O 정책은 0 입력 - 캐시된 I/O 정책은 1 입력 • [-r <0 2 3>]은 캐시 읽기 정책입니다. <ul style="list-style-type: none"> - 읽기 쓰기 정책은 0 입력 - 읽기 전용 정책은 2 입력 - 차단 정책은 3 입력 • [-d <0 1 2>]은 디스크 캐시 정책입니다. <ul style="list-style-type: none"> - 정책이 변경되지 않는 상태로 유지되면 0 입력 - 6 정책을 활성화하려면 1 입력 - 정책을 비활성화하려면 2 입력 • [-f <0 1 2>]은 초기화의 유형입니다. <ul style="list-style-type: none"> - 초기화 없음은 0 입력 - 빠른 초기화는 1 입력 - 전체 초기화는 2 입력 • [-S volume_size]은 MB의 새 볼륨 크기입니다. • [-P strip_size]는 볼륨 스트립 크기입니다(예: 512B, 4K, 128K, 1M 등) • -target target_id는 다음과 같습니다. <ul style="list-style-type: none"> - ctrl[x](새 스토리지 풀)⁵ - pool[x](기존 스토리지 풀)⁵

표 56. 스토리지 옵션 (계속)

옵션	설명	값
-config vol -getfreecap [-R] [-D disk] [-H disk] -target target_id ³	드라이브 그룹의 여유 용량을 가 져줍니다.	<ul style="list-style-type: none"> [-R <0 1 5 1E 6 10 50 60 00>] 이 옵션은 RAID 수준을 정의하며 새 스토리지 풀에서 만 사용됨 [-D disk [id1]:[id2]:..[id21]:[id22]:..] 이 옵션은 드라이브 그룹(스팬 포함)을 정의하며 새 스토리지 풀에서만 사용됩니다. [-H disk [id1]:[id2]:..] 이 옵션은 핫 스페어 를 정의하며 새 스토리지 풀에서만 사용됩니다. -target target_id는 ctrl[x]⁵
-fgi vol[idx]	지정된 볼륨 빠른 초기화	여기서 vol[idx]는 vol[id1],vol[id2]:..
-help	명령 사용 및 옵션 표시	
<p>참고:</p> <ol style="list-style-type: none"> 이 명령은 IMM가 RAID 컨트롤러에 액세스할 수 있는 서버에서만 지원됩니다. 관련 컨트롤러, 디스크 및 플래시 DIMM에 대해서만 펌웨어 정보가 표시됩니다. 관련 풀 및 볼륨에 대 한 펌웨어 정보는 표시되지 않습니다. 공간 제한으로 인해 정보가 여러 라인에 표시됩니다. 이 명령은 RAID 로그를 지원하는 서버에서만 지원됩니다. 이 명령은 RAID 구성을 지원하는 서버에서만 지원됩니다. 사용값은 RAID 수준 1 구성을 지원하지 않습니다. 사용 가능한 옵션의 부분적인 목록이 여기에 나열됩니다. storage -config vol -add 명령에 대한 나머지 옵션은 다음 행에 나열됩니다. 		

예:

```

system> storage -config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage -config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage -config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage -config drv -addhsp -target disk[0-0]
ok
system>
system> storage -config drv -mkbad -target disk[0-0]
ok
system>
system> storage -config drv -mkgood -target disk[0-0]
ok
system>
system> storage -config drv -mkmissing -target disk[0-0]
ok
system>
system> storage -config drv -mkoffline -target disk[0-0]
ok
system>
system> storage -config drv -mkonline -target disk[0-0]

```

```

ok
system>
system> storage -config drv -prprm -target disk[0-0]
ok
system>
system> storage -config drv -rmhsp -target disk[0-0]
ok
system>
system> storage -config drv -undoprprm -target disk[0-0]
ok
system>
system> storage -config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage -config vol -add -R 1 -D
disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage -config vol -getfreecap -R 1 -D
disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage -config vol -remove -target vol[0-1]
ok
system>
system> storage -config vol -set -N LD_volume
-w 0 -target vol[0-0]
ok
system>
system> storage -list controllers
ctrl[0] ServerRAID M5110e(Slot No. 0)
ctrl[1] ServerRAID M5110f(Slot No. 1)
system>
system> storage -list drives
disk[0-0] Drive 0
disk[0-1] Drive 1
disk[0-2] Drive 2
system>
system> storage -list pools
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
system>
system> storage -list volumes
vol[0-0] Volume 0
vol[0-1] Volume 1
Vol[0-2] Volume 2
system>
system> storage -list drives -target ctrl[0]
disk[0-0] Drive 0
disk[0-1] Drive 1
disk[0-2] Drive 2
system>
system> storage -list drives -target pool[0-0]
disk[0-0] Drive 0
disk[0-1] Drive 1
system>
system> storage -list pools -target ctrl[0]
pool[0-0] Storage Pool 0
system>
system> storage -list volumes -target ctrl[0]

```

```

vol[0-0] Volume 0
vol[0-1] Volume 1
system>
system> storage -list volumes -target pool[0-0]
vol[0-0] Volume 0
vol[0-1] Volume 1
system>
system> storage -show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manufacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage -show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
Drives: 3
disk[0-0] Drive 0
disk[0-1] Drive 1
disk[0-2] Drive 2
system>
system> storage -show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage -show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD

```

```

Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclosure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage -show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0] Drive 0
disk[0-1] Drive 1
Volumes: 2
vol[0-0] Volume 0
vol[0-1] Volume 1
system>
system> storage -show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1] Drive 1
disk[0-2] Drive 2

Volume: 1
vol[0-1] LD_volume
system>
system> storage -show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage -show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>

```

adapter 명령

이 명령은 PCIe 어댑터 인벤토리 정보를 표시하는 데 사용됩니다.

구문:
adapter [-options]

표 57. adapter 옵션

옵션	설명	값
-list	서버의 모든 PCIe 어댑터를 나열합니다.	
-show target_id	대상 PCIe 어댑터에 대한 자세한 정보를 표시합니다.	target_id [info firmware ports] 변수 설명: <ul style="list-style-type: none"> • info: 어댑터에 대한 하드웨어 정보를 표시합니다. • firmware: 어댑터에 대한 모든 펌웨어 정보를 표시합니다. • ports: 어댑터에 대한 모든 이더넷 정보를 표시합니다.

adapter 명령이 지원되지 않는 경우 서버는 명령이 실행되면 다음 메시지에 응답합니다.
Your platform does not support this command.

참고: 어댑터를 제거, 교체 또는 구성하는 경우 업데이트된 어댑터 정보를 표시하도록 서버를 최소한 한 번 이상 다시 시작해야 합니다.

예:

```
system> adapter -list
ob-1 Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2 GPU Card 1
slot-1 Raid Controller 1
slot-2 Adapter 01:02:03
system>
```

```
system> adapter -show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2
Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
```

```
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
system>
```

지원 명령

이 주제에서는 지원 명령의 목록을 알파벳 순서로 제공합니다.

1개의 지원 명령 (["dbgshbmc 명령" 140페이지](#))만 있습니다.

dbgshbmc 명령

이 명령을 사용하여 보안 디버그 셸에 대한 네트워크 액세스의 잠금을 해제합니다.

참고: 이 명령은 dbgshimm 명령이었습니다.

중요: 이 명령은 지원 담당자만 사용할 수 있습니다.

다음 표는 옵션의 인수를 보여줍니다.

구문:

```
dbgshbmc [subset_command]
```

표 58. dbgshbmc 서브세트 명령

옵션	설명
status	상태 표시
사용	디버그 액세스 사용(옵션이 지정되어 있지 않은 경우 기본값)
사용 안 함	디버그 액세스 사용 안 함

제 11 장 IPMI 인터페이스

이 장에서는 XClarity Controller에서 지원하는 IPMI 인터페이스에 대해 설명합니다.

표준 IPMI 명령에 대한 세부 정보는 IPMI(Intelligent Platform Management Interface) 사양 문서(버전 2.0 이상)를 참조하십시오. 이 문서는 XClarity Controller 펌웨어에서 지원하는 표준 IPMI 및 OEM IPMI 명령과 함께 사용되는 OEM 매개 변수에 대한 설명을 제공합니다.

IPMI로 XClarity Controller 관리

이 주제의 정보를 사용하여 IPMI(Intelligent Platform Management Interface)로 XClarity Controller를 관리합니다.

XClarity Controller는 처음에 사용자 이름 USERID 및 암호 PASSWORD(문자 O가 아니라 숫자 0 사용)로 설정된 사용자 ID가 제공됩니다. 이 사용자에게는 감독자 액세스 권한이 있습니다.

중요: 보안 강화를 위해 초기 구성 중에 이 사용자 이름과 암호를 변경하십시오.

Flex System에서는 사용자가 Flex System CMM을 구성하여 XClarity Controller IPMI 사용자 계정을 중앙에서 관리할 수 없습니다. 이런 상황에서는 CMM이 IPMI 사용자 ID의 구성을 완료할 때까지 IPMI를 사용하여 XClarity Controller에 액세스하지 못할 수 있습니다.

참고: CMM으로 구성된 사용자 ID 자격 증명은 위에 설명된 USERID/PASSWORD 조합과 다를 수 있습니다. CMM으로 IPMI 사용자 ID를 구성하지 않은 경우 IPMI 프로토콜과 연결된 네트워크 포트가 닫힙니다.

XClarity Controller는 다음의 IMM 원격 서버 관리 기능도 제공합니다.

IPMI 명령줄 인터페이스

IPMI 명령줄 인터페이스는 IPMI 2.0 프로토콜을 통해 서버 관리 기능에 대한 직접 액세스를 제공합니다. 서버 전원을 제어하고, 서버 정보를 보고, 서버를 식별하는 명령을 실행하려면 IPMITool을 사용하십시오. IPMITool에 관한 자세한 내용은 "[IPMITool 사용](#)" 143페이지의 내용을 참조하십시오.

Serial over LAN

원격 위치에서 서버를 관리하려면 IPMITool을 사용하여 SOL(Serial over LAN) 연결을 설정하십시오. IPMITool에 관한 자세한 내용은 "[IPMITool 사용](#)" 143페이지의 내용을 참조하십시오.

IPMITool 사용

이 주제의 정보를 사용하여 IPMITool에 대한 정보에 액세스합니다.

IPMITool에서는 IPMI 시스템을 관리 및 구성하는 데 사용할 수 있는 다양한 도구를 제공합니다. 대역 내 또는 대역 외 IPMITool을 사용하여 XClarity Controller를 관리 및 구성할 수 있습니다.

IPMITool에 대한 자세한 내용을 보거나 IPMITool을 다운로드하려면 <https://github.com/ipmitool/ipmitool>로 이동하십시오.

OEM 매개 변수가 있는 IPMI 명령

LAN 구성 매개 변수 가져오기/설정

일부 네트워크 설정에 대해 XCC가 제공하는 기능을 반영하기 위해 일부 매개 변수 데이터의 값은 다음과 같이 정의됩니다.

DHCP

IP 주소를 얻는 일반적인 방법 외에도 XCC는 일정 기간 동안 DHCP 서버에서 IP 주소를 가져오려고 시도하고 실패한 경우 고정 IP 주소를 사용하여 장애 조치하는 모드를 제공합니다.

다음 표는 옵션, 옵션 설명 및 옵션에 대한 관련 값으로 구성되어 있는 멀티 행 3열 표입니다.

매개 변수	#	매개 변수 데이터
IP 주소 소스	4	<u>data 1</u> [7:4] - 예약됨 [3:0] - 주소 소스 0h = 지정되지 않음 1h = 고정 주소(수동 구성) 2h = DHCP를 실행하여 XCC에서 얻은 주소 3h = BIOS 또는 시스템 소프트웨어에서 얻은 주소 4h = 다른 주소 할당 프로토콜을 실행하여 XCC에서 얻은 주소 XCC는 값 4h를 사용하여 고정으로 장애 조치하는 DHCP의 주소 모드를 나타냅니다.

이더넷 인터페이스 선택

XCC 하드웨어에는 RMII 인터페이스가 있는 듀얼 10/100 이더넷 MAC가 포함되어 있습니다. XCC 하드웨어에는 RGMII 인터페이스가 있는 듀얼 1Gbps 이더넷 MAC도 포함되어 있습니다. MAC 중 하나는 일반적으로 공유 서버 NIC에 연결되고 다른 MAC는 전용 시스템 관리 포트에 사용됩니다. 주어진 시간에 서버에서 하나의 이더넷 포트만 활성화됩니다. 두 포트가 동시에 활성화되지 않습니다.

일부 서버에서 시스템 설계자는 시스템 플래너에서 이 이더넷 인터페이스 중 하나만 연결하도록 선택할 수 있습니다. 이러한 시스템에서는 플래너에 연결된 이더넷 인터페이스만 XCC에서 지원됩니다. 연결되지 않은 포트를 사용하도록 요청하면 CCh 완료 코드가 리턴됩니다.

모든 옵션 네트워크 카드의 패키지 ID 번호는 다음과 같습니다.

- 옵션 카드 #1, 패키지 ID = 03h (eth2),
- 옵션 카드 #2, 패키지 ID = 04h (eth3),

다음 표는 옵션, 옵션 설명 및 옵션에 대한 관련 값으로 구성되어 있는 멀티 행 3열 표입니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>이 매개 변수 번호는 XCC에서 사용 가능한 이더넷 포트(논리 패키지)를 나타내는 데 사용됩니다.</p> <p>LAN 구성 매개 변수 가져오기 / 설정 명령에서 이 매개 변수는 세트 선택기 또는 필수 블록 선택기를 사용하지 않으므로 이 필드를 00h로 설정해야 합니다.</p> <p>응답 데이터는 장치가 NCSI 패키지에 있는 경우 3바이트 또는 선택적으로 4바이트를 리턴합니다.</p> <p> 바이트 1 = 완료 코드</p> <p> 바이트 2 = 개정</p> <p> 바이트 3 = eth0의 경우 00h, eth1의 경우 01h 등...</p> <p> 바이트 4 = (옵션) 채널 번호 (장치가 NCSI 패키지에 있는 경우)</p>	C0h	<p><u>data1</u></p> <p>00h = eth0</p> <p>01h = eth1</p> <p>02h = eth2</p> <p>기타...</p> <p>FFh = 모든 외부 네트워크 포트 비활성화</p> <p>XCC는 패키지에서 사용할 채널을 지정하기 위해 두 번째 옵션 데이터 바이트를 지원합니다.</p> <p><u>data2</u></p> <p>00h = 채널 0</p> <p>01h = 채널 1</p> <p>기타...</p> <p>요청에 data2를 지정하지 않으면 채널 0으로 가정합니다.</p>

data1 바이트는 논리 패키지를 지정하는 데 사용됩니다. 서버와 공유되는 NIC에 대한 전용 시스템 관리 NIC 또는 NCSI 인터페이스일 수 있습니다.

패키지가 NCSI 장치인 경우 data2 바이트는 논리 패키지의 채널을 지정하는 데 사용됩니다. 요청에 data2가 지정되지 않고 논리 패키지가 NCSI 장치인 경우 채널 0으로 가정합니다. 요청에 data2가 지정되었지만 논리 패키지가 NCSI 장치가 아닌 경우 채널 정보를 무시합니다.

예:

부록 A: 플래너에서 공유 NIC의 채널 2(패키지 ID = 0, eth0)를 관리 포트에 사용하는 경우 입력 데이터는 0xC0 0x00 0x02입니다.

부록 B: 첫 번째 네트워크 메자닌 카드의 첫 번째 채널을 사용하는 경우 입력은 0xC0 0x02 0x0입니다.

USB를 통한 이더넷 사용/사용 안 함

아래 매개 변수는 XCC 대역 내 인터페이스를 사용 또는 사용 안 함으로 설정하는 데 사용됩니다.

다음 표는 옵션, 옵션 설명 및 옵션에 대한 관련 값으로 구성되어 있는 멀티 행 3열 표입니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xcc에서 USB를 통한 이더넷 인터페이스를 사용 또는 사용 안 함으로 설정하는 데 사용됩니다.)</p> <p>LAN 구성 매개 변수 가져오기 명령에서 이 매개 변수는 세트 선택기 또는 필수 블록 선택기를 사용하지 않으므로 이 필드를 00h로 설정해야 합니다.</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p> 바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3 = 00h(사용 안 함) 또는 01h(사용)</p>	C1h	<p><u>data 1</u></p> <p>0x00 = 사용 안 함</p> <p>0x01 = 사용</p>

data1 바이트는 논리 패키지를 지정하는 데 사용됩니다. 서버와 공유되는 NIC에 대한 전용 시스템 관리 NIC 또는 NCSI 인터페이스일 수 있습니다.

패키지가 NCSI 장치인 경우 data2 바이트는 논리 패키지의 채널을 지정하는 데 사용됩니다. 요청에 data2가 지정되지 않고 논리 패키지가 NCSI 장치인 경우 채널 0으로 가정합니다. 요청에 data2가 지정되었지만 논리 패키지가 NCSI 장치가 아닌 경우 채널 정보를 무시합니다.

예:

부록 A: 플래너에서 공유 NIC의 채널 2(패키지 ID = 0, eth0)를 관리 포트에 사용하는 경우 입력 데이터는 0xC0 0x00 0x02입니다.

부록 B: 첫 번째 네트워크 메자닌 카드의 첫 번째 채널을 사용하는 경우 입력은 0xC0 0x02 0x0입니다.

DUID-LLT를 얻는 IPMI 옵션

IPMI를 통해 공개해야 하는 추가 읽기 전용 값은 DUID입니다. RFC3315에 따라 이 DUID 형식은 링크 레이어 주소와 시간을 기반으로 합니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xcc에서 USB를 통한 이더넷 인터페이스를 사용 또는 사용 안 함으로 설정하는 데 사용됩니다.)</p> <p>LAN 구성 매개 변수 가져오기 명령에서 이 매개 변수는 세트 선택기 또는 필수 블록 선택기를 사용하지 않으므로 이 필드를 00h로 설정해야 합니다.</p>	C2h	

매개 변수	#	매개 변수 데이터
<p>응답 데이터는 3바이트를 리턴합니다.</p> <p>바이트 1 = 완료 코드</p> <p>바이트 2 = 매개 변수 개정 (IPMI 사양에서와 같음)</p> <p>바이트 3 = 다음 데이터 바이트의 길이(현재 16바이트)</p> <p>바이트 4-n DUID_LL</p>		

이더넷 구성 매개 변수

아래 매개 변수는 특정 이더넷 설정을 구성하는 데 사용될 수 있습니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xCC에서 이더넷 인터페이스에 대한 자동 협상 설정을 사용 또는 사용 안 함으로 설정하는 데 사용됩니다.)</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p>바이트 1 = 완료 코드</p> <p>바이트 2 = 개정</p> <p>바이트 3 = 00h(사용 안 함) 또는 01h(사용)</p>	C3h	<p><u>data 1</u></p> <p>0x00 = 사용 안 함</p> <p>0x01 = 사용</p> <p>참고: Flex 및 ThinkSystem D2 엔클로저 (ThinkSystem SD530 컴퓨팅 노드) 시스템에서는 자동 교섭 설정을 변경할 수 없으며, 이는 CMM 및 SMM을 통해 네트워크 통신 경로를 중단시킬 수 있기 때문입니다.</p>
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xCC에서 이더넷 인터페이스의 데이터 속도를 가져오거나 설정하는 데 사용됩니다.)</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p>바이트 1 = 완료 코드</p> <p>바이트 2 = 개정</p> <p>바이트 3 = 00h(10Mb) 또는 01h(100Mb)</p>	C4h	<p><u>data 1</u></p> <p>0x00 = 10Mbit</p> <p>0x01 = 100Mbit</p>

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xCC에서 이더넷 인터페이스의 이중 (Duplex) 설정을 가져오거나 설정하는 데 사용됩니다.)</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p> 바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3 = 00h (반이중) 또는 01h(전이중)</p>	C5h	<p><u>data 1</u></p> <p>0x00 = 반이중 0x01 = 전이중</p>
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xCC에서 이더넷 인터페이스의 최대 전송 단위 (MTU) 를 가져오거나 설정하는 데 사용됩니다.)</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p> 바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3-4 = MTU 크기</p>	C6h	<p><u>data 1</u></p> <p>MTU 크기</p>
<p>OEM 매개 변수</p> <p>(이 매개 변수 번호는 xCC에서 로컬 관리 MAC 주소를 가져오거나 설정하는 데 사용됩니다.)</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p> 바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3-8 = Mac 주소</p>	C7h	<p><u>data 1-6</u></p> <p>Mac 주소</p>

링크 로컬 주소를 얻는 IPMI 옵션

IPV6 링크 로컬 주소를 검색하기 위한 읽기 전용 매개 변수입니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>이 매개 변수는 xCC의 링크 로컬 주소를 얻는 데 사용됩니다.</p> <p>응답 데이터는 다음을 리턴합니다.</p> <p> 바이트 1 = 완료 코드</p>	C8h	

매개 변수	#	매개 변수 데이터
바이트 2 = 매개 변수 개정 (IPMI 사양에서와 같음) 바이트 3 = IPV6 주소 접두 사 길이 바이트 4-19 = 2진 형식의 로 컬 링크 주소		

IPv6를 사용/사용 안 함으로 설정하는 IPMI 옵션

이는 XCC에서 IPV6를 사용/사용 안 함으로 설정하는 읽기/쓰기 매개 변수입니다.

매개 변수	#	매개 변수 데이터
OEM 매개 변수 이 매개 변수는 XCC에서 IPv6 을 사용/사용 안 함으로 설정하 는 데 사용됩니다. 응답 데이터는 다음을 리턴합니 다. 바이트 1 = 완료 코드 바이트 2 = 매개 변수 개정 (IPMI 사양에서와 같음) 바이트 3 = 00h(사용 안 함) 또는 01h(사용)	C9h	<u>data 1</u> 0x00 = 사용 안 함 0x01 = 사용

외부 네트워크에 대한 USB를 통한 이더넷 패스스루

아래 매개 변수는 외부 이더넷 패스스루에 대한 USB를 통한 이더넷을 구성하는 데 사용됩니다.

매개 변수	#	매개 변수 데이터
OEM 매개 변수 LAN 구성 매개 변수 가져오기/설정 명령에서 이 매개 변수는 세트 선택 기 또는 필수 블록 선택기를 사용하 지 않으므로 이 필드를 00h로 설정 해야 합니다. 가져오기 응답 데이터는 다음을 리 턴합니다. 바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3 = 예약됨(00h) 바이트 4:5 = USB를 통한 이더넷 포트 번호(LSByte 우선) 바이트 6:7 = 외부 이더넷 포트 번호 (LSByte 우선)	CAh	LAN 구성 매개 변수 설정: <u>data 1</u> 예약됨 (= 00h) <u>data 2:3</u> USB를 통한 이더넷 포트 번호, LSByte 우선 <u>data 4:5</u> 외부 이더넷 포트 번호, LSByte 우선 사용할 바이트 수는 주소 지정 모드에 따라 다를 수 있습니다 (1, 4 또는 16바이트). <u>data 6</u> 00h = 패스스루 사용 안 함

매개 변수	#	매개 변수 데이터
<p>사용할 바이트 수는 주소 지정 모드에 따라 다를 수 있습니다 (1, 4 또는 16바이트).</p> <ul style="list-style-type: none"> • 바이트 8 = 사전 정의된 모드: <ul style="list-style-type: none"> 00h = 패스스루를 사용하지 않음 01h = CMM의 IP 주소가 사용됨 • 바이트 8:11 = 2진 형식의 IPv4 외부 네트워크 IP 주소 • 바이트 8:23 = 2진 형식의 IPv6 외부 네트워크 IP 주소 <p>완료 코드:</p> <p>00h - 성공</p> <p>80h - 매개 변수가 지원되지 않음</p> <p>C1h - 명령이 지원되지 않음</p> <p>C7h - 요청 데이터 길이가 올바르지 않음</p>		<p>01h = CMM의 IP 주소 사용</p> <p><u>data 6:9</u></p> <p>2진 형식의 IPv4 외부 네트워크 IP 주소</p> <p><u>data 6:21</u></p> <p>2진 형식의 IPv6 외부 네트워크 IP 주소</p>
<p>OEM 매개 변수</p> <p>이 매개 변수는 XCC의 USB를 통한 LAN IP 주소 및 넷마스크를 설정하고 가져오는 데 사용됩니다.</p> <p>응답 데이터는 다음을 리턴합니다.</p> <ul style="list-style-type: none"> • 바이트 1 = 완료 코드 • 바이트 2 = 매개 변수 개정(IPMI 사양에서와 같음) <p>바이트 3:10 = IP 주소 및 넷마스크 값 (MS 바이트) 우선</p>	CBh	<p>Data 1:4</p> <p>XCC 측 USB를 통한 LAN 인터페이스의 IP 주소.</p> <p>Data 5:8</p> <p>XCC 측 USB를 통한 LAN 인터페이스의 넷마스크</p>
<p>OEM 매개 변수</p> <p>이 매개 변수는 호스트 OS의 USB를 통한 LAN IP 주소를 설정하고 가져오는 데 사용됩니다.</p> <p>응답 데이터는 다음을 리턴합니다.</p> <ul style="list-style-type: none"> • 바이트 1 = 완료 코드 • 바이트 2 = 매개 변수 개정(IPMI 사양에서와 같음) <p>바이트 3:6 = IP 주소 (MS 바이트) 우선</p>	CCh	<p>Data 1:4</p> <p>호스트 측 USB를 통한 LAN 인터페이스의 IP 주소.</p>

논리 패키지 인벤토리 쿼리

아래 매개 변수는 NCSI 패키지 인벤토리를 쿼리하는 데 사용됩니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>LAN 구성 매개 변수 가져오기 /설정 명령에서 이 매개 변수는 세트 선택기 또는 필수 블록 선택기를 사용하지 않으므로 이 필드를 00h로 설정해야 합니다.</p> <p>패키지 인벤토리 쿼리 작업</p> <p>패키지 정보 쿼리 작업은 D3h 매개 변수 번호 외에 두 개의 0x00 데이터 바이트로 요청을 발행하여 수행됩니다.</p> <p>패키지 인벤토리 쿼리:</p> <pre>--> 0x0C 0x02 0x00 0xD3 0x00 0x00</pre> <p>XCC 응답에는 존재하는 각 패키지에 대한 정보 바이트가 포함됩니다.</p> <p>비트 7:4 = 패키지의 NCSI 채널 수</p> <p>비트 3:0 = 논리 패키지 번호</p> <p>응답</p> <pre>--> 0x00 0x00 0x40 0x01 0x32</pre> <p>3개의 논리 패키지가 있음을 나타냅니다.</p> <p>패키지 0에는 4개의 NCSI 채널이 있음</p> <p>패키지 1은 NCSI NIC가 아니므로 NCSI 채널을 지원하지 않음</p> <p>패키지 2에는 3개의 NCSI 채널이 있음</p>	D3h	LAN 구성 매개 변수 가져오기/설정:

논리 패키지 데이터 가져오기/설정

아래 매개 변수는 각 패키지에 지정된 우선 순위를 읽고 설정하는 데 사용됩니다.

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>LAN 구성 매개 변수 가져오기 /설정 명령에서 이 매개 변수는 세트 선택기 또는 필수 블록 선택기를 사용하지 않으므로 이 필드를 00h로 설정해야 합니다.</p> <p>이 명령은 2개의 작업을 지원 합니다.</p> <ul style="list-style-type: none"> 패키지 우선 순위 읽기 패키지 우선 순위 설정 <p>패키지 우선 순위 읽기 작업</p> <p>패키지 우선 순위 읽기 작업은 D4h 매개 변수 번호 외에 두 개의 0x00 데이터 바이트로 요청을 발행하여 수행됩니다.</p> <p>패키지 우선 순위 읽기:</p> <pre>--> 0x0C 0x02 0x01 0xD4 0x00 0x00</pre> <p>응답</p> <pre>--> 0x00 0x00 0x00 0x12 0x23</pre> <p>논리 패키지 0 = 우선 순위 0 논리 패키지 2 = 우선 순위 1 논리 패키지 3 = 우선 순위 2</p> <p>패키지 우선 순위 설정 작업</p> <p>패키지 우선 순위 설정 작업은 D4h 매개 변수 번호 외에 하나 이상의 매개 변수로 요청을 발행하여 수행됩니다.</p> <p>패키지 우선 순위 설정:</p> <pre>--> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23</pre> <p>논리 패키지 0 설정 = 우선 순위 0 논리 패키지 2 설정 = 우선 순위 1 논리 패키지 3 설정 = 우선 순위 2</p> <p>응답:</p> <p>완료 코드만, 추가 데이터 없음</p>	D4	<p>LAN 구성 매개 변수 가져오기/설정:</p> <p>비트 [7-4] = 논리 패키지의 우선 순위 (1 = 최고, 15 = 최저)</p> <p>비트 [3-0] = 논리 패키지 번호</p>

XCC 네트워킹 동기화 상태 가져오기/설정

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>바이트는 전용 및 공유 NIC 모드 간의 네트워킹 설정을 동기화하도록 구성하는 데 사용됩니다.</p> <p>LAN 구성 매개 변수 가져오기 명령에서 이 매개 변수는 세트 선택기 또는 필수 블록 선택기를 사용하지 않으므로 이 필드를 00h로 설정해야 합니다.</p> <p>응답 데이터는 3바이트를 리턴합니다.</p> <p>바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3 = 00h(사용) 또는 01h(사용 안 함)</p>	D5h	<p><u>data 1</u></p> <p>0x00 = 동기화 0x01 = 독립</p>

이 바이트는 전용 및 공유 NIC 모드 간의 네트워킹 설정을 동기화하도록 구성하는 데 사용되며 기본값은 0h입니다. 즉, XCC는 모드 변경 간에 네트워킹 설정을 자동으로 업데이트하고 1h로 설정된 경우 공유 NIC(온보드)를 주요 참조로 사용합니다. 여기서, 각 네트워킹 설정은 독립적이므로 전용 NIC 모드에서 VLAN을 사용으로 설정하고 공유 NIC 모드에서 VLAN을 사용 안 함으로 설정하는 것과 같이 모드 간에 다른 네트워킹 설정을 구성할 수 있습니다.

XCC 네트워킹 모드 가져오기/설정

매개 변수	#	매개 변수 데이터
<p>OEM 매개 변수</p> <p>이 매개 변수는 XCC 관리 NIC의 네트워크 모드를 가져오거나 설정하는 데 사용됩니다.</p> <p>응답 데이터는 4바이트를 리턴합니다.</p> <p>바이트 1 = 완료 코드 바이트 2 = 개정 바이트 3 = 적용/지정된 네트워크 모드 바이트 4 = 적용된 네트워크 모드의 패키지 ID 바이트 5 = 적용된 네트워크 모드의 채널</p>	D6h	<p>LAN 구성 매개 변수 설정:</p> <p><u>data 1</u></p> <p>설정할 네트워크 모드</p> <p>LAN 구성 매개 변수 가져오기:</p> <p><u>data 1</u></p> <p>가져올 네트워크 모드. 이는 옵션 데이터로 현재 네트워크 모드를 쿼리하도록 기본 설정됩니다.</p>

OEM IPMI 명령

XCC에서는 다음 IPMI OEM 명령을 지원합니다. 각 명령에는 아래와 같이 서로 다른 권한 수준이 필요합니다.

코드	Netfn 0x2E 명령	권한
0xCC	XCC를 기본값으로 재설정	PRIV_USR

코드	Netfn 0x3A 명령	권한
0x00	펌웨어 버전 쿼리	PRIV_USR
0x0D	보드 정보	PRIV_USR
0x1E	새시 전력 복구 지연 옵션	PRIV_USR
0x38	NMI 및 재설정	PRIV_USR
0x49	데이터 수집 시작	PRIV_USR
0x4A	파일 푸시	PRIV_USR
0x4D	데이터 수집 상태	PRIV_USR
0x50	Build 정보 가져오기	PRIV_USR
0x55	호스트 이름 가져오기/설정	PRIV_USR
0x6B	FPGA 펌웨어 개정 수준 쿼리	PRIV_USR
0x6C	보드 하드웨어 개정 수준 쿼리	PRIV_USR
0x6D	PSoC 펌웨어 개정 수준 쿼리	PRIV_USR
0x98	FP USB 포트 제어	PRIV_USR
0xC7	기본 NM IPMI 스위치	PRIV_ADM

XCC를 기본값으로 재설정 명령

이 명령은 XCC 구성 설정을 기본값으로 재설정합니다.

망 함수 = 0x2E			
코드	명령	요청, 응답 데이터	설명
0xCC	XCC를 기본값으로 재설정	요청: 바이트 1 - 0x5E 바이트 2 - 0x2B 바이트 3 - 0x00 바이트 4 - 0x0A 바이트 5 - 0x01 바이트 6 - 0xFF 바이트 7 - 0x00 바이트 8 - 0x00 바이트 9 - 0x00	이 명령은 XCC 구성 설정을 기본값으로 재설정합니다.

망 함수 = 0x2E			
코드	명령	요청, 응답 데이터	설명
		응답: 바이트 1 - 완료 코드 바이트 2 - 0x5EByte 3 - 0x2B 바이트 4 - 0x00 바이트 5 - 0x0A 바이트 6 - 0x01 바이트 7 - 응답 데이터 0 = 성공 0 이외 = 실패	

보드/펌웨어 정보 명령

이 절에서는 보드 및 펌웨어 정보를 쿼리하는 명령을 나열합니다.

망 함수 = 0x3A			
코드	명령	요청, 응답 데이터	설명
0x00	펌웨어 버전 쿼리	요청: 요청에 데이터가 없음 응답: 바이트 1 - 완료 코드 바이트 2 - 주 버전 바이트 3 - 부 버전	이 명령은 펌웨어의 주 버전 번호와 부 버전 번호를 리턴합니다. 선택적 1바이트의 요청 데이터를 사용하여 명령을 수행하면 XCC 응답은 버전의 세 번째 필드(개정)도 리턴합니다. (주.부.개정)
0x0D	보드 정보 쿼리	요청: 해당 없음 응답: 바이트 1 - 시스템 ID 바이트 2 - 보드 개정	이 명령은 보드 ID 및 플래너 개정을 리턴합니다.
0x50	Build 정보 쿼리	요청: 해당 없음 응답: 바이트 1 - 완료 코드. 바이트 2:10 - ASCIIZ Build 이름 바이트 11:23 - ASCIIZ Build 날짜 바이트 24:31 - ASCII Build 시간	이 명령은 Build 이름, Build 날짜 및 Build 시간을 리턴합니다. Build 이름과 Build 날짜 문자열은 0으로 끝나지 않습니다. Build 날짜의 형식은 YYYY-MM-DD입니다. 예: "ZUBT99A" "2005-03-07" "23:59:59"

망 함수 = 0x3A			
코드	명령	요청, 응답 데이터	설명
0x6B	FPGA 펌웨어 개정 수준 쿼리	<p>요청:</p> <p>바이트 1 - FPGA 장치 유형*</p> <p>FPGA 장치 유형</p> <p>0 = 로컬 (활성 수준)</p> <p>1 = CPU 카드 1 (활성 수준)</p> <p>2 = CPU 카드 2 (활성 수준)</p> <p>3 = CPU 카드 3 (활성 수준)</p> <p>4 = CPU 카드 4 (활성 수준)</p> <p>5 = 로컬 기본 ROM</p> <p>6 = 로컬 복구 ROM</p> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2 - 주 개정 수준</p> <p>바이트 3 - 부 개정 수준</p> <p>바이트 4 - 하위 부 개정 수준</p> <p>(XCC 플랫폼의 테스트 바이트)</p>	<p>이 명령은 FPGA 펌웨어의 개정 수준을 리턴합니다.</p> <p>바이트 1을 생략하면 로컬 (활성 수준)이 선택됩니다.</p>
0x6C	보드 하드웨어 개정 수준 쿼리	<p>요청:</p> <p>데이터 없음.</p> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2 - 개정 수준</p>	<p>이 명령은 FPGA가 상주하는 보드 하드웨어의 개정 수준을 리턴합니다.</p>
0x6D	PSoC 펌웨어 개정 수준 쿼리	<p>요청:</p> <p>없음</p> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2 - bin#</p> <p>바이트 3 - APID</p> <p>바이트 4 - Rev</p> <p>바이트 5-6 - FRU ID</p>	<p>이 명령은 감지된 모든 PSoC 장치의 개정 수준을 리턴합니다.</p> <p>참고: bin#은 실제 위치를 나타냅니다. 세부 정보는 시스템 사양을 참조하십시오.</p>

망 함수 = 0x3A			
코드	명령	요청, 응답 데이터	설명
		바이트 6:N - 감지된 각 PSoC에 대해 바이트 2-6 반복	

시스템 제어 명령

IPMI 사양은 기본 전원 및 재설정 제어 기능을 제공합니다. Lenovo는 추가 제어 기능을 추가합니다.

망 함수 = 0x2E							
코드	명령	요청, 응답 데이터	설명				
0x1E	새시 전력 복구 지연 옵션	<p>요청:</p> <table border="1"> <tr> <td>바이트 1</td> <td> 요청 유형: 0x00 = 지연 옵션 설정 0x01 = 지연 옵션 쿼리 </td> </tr> <tr> <td>바이트 2</td> <td> (바이트 1 = 0x00인 경우) 0x00 = 사용 안 함 (기본 값) 0x01 = 무작위 0x02 - 0xFF 예약됨 </td> </tr> </table> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2 - 지연 옵션 (쿼리 요청의 경우만)</p>	바이트 1	요청 유형: 0x00 = 지연 옵션 설정 0x01 = 지연 옵션 쿼리	바이트 2	(바이트 1 = 0x00인 경우) 0x00 = 사용 안 함 (기본 값) 0x01 = 무작위 0x02 - 0xFF 예약됨	<p>이 설정은 AC를 적용/반환한 후 새시 전력 복구 정책이 항상 전원 켜기 또는 전원 켜기 복원(이전에 전원이 켜진 경우)으로 설정된 경우에 사용됩니다. 사용 안 함(기본 설정, 전원을 켤 때 지연 없음) 및 무작위의 두 가지 선택 사항이 있습니다. 무작위 지연 설정은 AC가 적용/리턴될 때부터 서버 전원이 자동으로 켜질 때까지 1~15초 사이의 무작위 지연 시간을 제공합니다.</p> <p>XCC는 이 명령을 랙 서버에서만 지원합니다.</p>
바이트 1	요청 유형: 0x00 = 지연 옵션 설정 0x01 = 지연 옵션 쿼리						
바이트 2	(바이트 1 = 0x00인 경우) 0x00 = 사용 안 함 (기본 값) 0x01 = 무작위 0x02 - 0xFF 예약됨						
0x38	NMI 및 재설정	<p>요청:</p> <p>바이트 1 - 초 수 0 = NMI만 해당</p> <p>바이트 2 - 재설정 유형 0 = 소프트 재설정 1 = 전원 주기</p> <p>응답:</p> <p>바이트 1 - 완료 코드</p>	<p>이 명령은 시스템 NMI를 수행하는 데 사용됩니다. 선택적으로 NMI 후에 시스템을 재설정(채부팅)하거나 전원을 껐다가 다시 켤 수 있습니다.</p> <p>"초 수" 필드가 0이 아닌 경우 시스템은 지정된 시간(초) 후에 재설정되거나 전원을 껐다가 다시 켵니다.</p> <p>요청의 바이트 2는 선택 사항입니다. 바이트 2가 제공되지 않거나 값이 0x00이면 소프트 재설정이 수행됩니다. 바이트 2</p>				

망 함수 = 0x2E			
코드	명령	요청, 응답 데이터	설명
			가 0x01이면 시스템 전원이 꺼졌다 다시 켜집니다.

기타 명령

이 절에서는 다른 절에 해당되지 않는 명령을 설명합니다.

망 함수 = 0x3A									
코드	명령	요청, 응답 데이터	설명						
0x55	호스트 이름 가져오기/설정	<p>요청 길이 = 0:</p> <p>비어 있는 요청 데이터</p> <p>응답:</p> <table border="1"> <tr> <td>바이트 1</td> <td>완료 코드</td> </tr> <tr> <td>바이트 2-65</td> <td>현재 호스트 이름. ASCIIZ, Null 종료 문자열.</td> </tr> </table> <p>요청 길이 1-64:</p> <table border="1"> <tr> <td>바이트 1-64</td> <td>DHCP 호스트 이름 ASCIIZ가 00h로 끝남</td> </tr> </table>	바이트 1	완료 코드	바이트 2-65	현재 호스트 이름. ASCIIZ, Null 종료 문자열.	바이트 1-64	DHCP 호스트 이름 ASCIIZ가 00h로 끝남	<p>이 명령을 사용하여 호스트 이름을 가져오거나 설정합니다.</p> <p>호스트 이름을 설정할 때 원하는 값이 00h로 끝나야 합니다. 호스트 이름은 63자+Null로 제한됩니다.</p>
바이트 1	완료 코드								
바이트 2-65	현재 호스트 이름. ASCIIZ, Null 종료 문자열.								
바이트 1-64	DHCP 호스트 이름 ASCIIZ가 00h로 끝남								
0x98	FP USB 포트 제어	<p>요청:</p> <p>바이트 1</p> <table border="1"> <tr> <td>01h:</td> <td>앞면 패널 USB 포트의 현재 소유자 가져오기</td> </tr> </table> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2</p> <table border="1"> <tr> <td>00h:</td> <td>호스트 소유</td> </tr> <tr> <td>01h:</td> <td>BMC 소유</td> </tr> </table> <p>요청:</p> <p>바이트 1</p>	01h:	앞면 패널 USB 포트의 현재 소유자 가져오기	00h:	호스트 소유	01h:	BMC 소유	<p>이 명령은 FP USB 포트의 상태/구성 쿼리, FP USB 포트의 모드/제한 시간 초과 구성 및 호스트와 BMC 간의 USB 포트 소유자 전환에 사용됩니다.</p> <p>구성에서 FP USB에는 세 가지 모드 (호스트 전용, BMC 단독 소유 또는 호스트와 BMC 간의 소유자 전환을 허용하는 공유 모드)가 있습니다.</p> <p>공유 모드를 사용하는 경우 서버 전원이 꺼지면 USB 포트가 BMC에 연결되고 서버 전원이 켜지면 서버에 연결됩니다.</p> <p>공유 모드를 사용하고 서버 전원이 켜진 경우 BMC는 구성에서 비활동 제한 시간 초과가 발생한 후 USB 포트를 다시 서버로 되돌려 놓습니다.</p>
01h:	앞면 패널 USB 포트의 현재 소유자 가져오기								
00h:	호스트 소유								
01h:	BMC 소유								

망 함수 = 0x3A

코드	명령	요청, 응답 데이터	설명																						
		<table border="1"> <tr> <td>02h:</td> <td>앞면 패널 USB 포트의 구성 가져오기</td> </tr> </table> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2</p> <table border="1"> <tr> <td>00h:</td> <td>호스트 전용</td> </tr> <tr> <td>01h:</td> <td>BMC 전용</td> </tr> <tr> <td>02h:</td> <td>공유 모드</td> </tr> </table> <p>바이트 3:4 - 비활성 제한 시간 초과 (분) (MSB 우선)</p> <p>바이트 5 - ID 버튼 사용</p> <table border="1"> <tr> <td>00h:</td> <td>사용 안 함</td> </tr> <tr> <td>01h:</td> <td>사용</td> </tr> </table> <p>바이트 6 - 이력 시간 (초) (옵션)</p> <p>요청:</p> <p>바이트 1</p> <p>03h: 앞면 패널 USB 포트의 구성 설정</p> <p>바이트 2</p> <table border="1"> <tr> <td>00h:</td> <td>호스트 전용</td> </tr> <tr> <td>01h:</td> <td>BMC 전용</td> </tr> <tr> <td>02h:</td> <td>공유 모드</td> </tr> </table> <p>바이트 3:4 - 비활성 제한 시간 초과 (분) (MSB 우선)</p> <p>바이트 5 - ID 버튼 사용</p> <table border="1"> <tr> <td>00h:</td> <td>사용 안 함</td> </tr> <tr> <td>01h:</td> <td>사용</td> </tr> </table> <p>바이트 6 - 이력 시간 (초) (옵션)</p> <p>응답:</p>	02h:	앞면 패널 USB 포트의 구성 가져오기	00h:	호스트 전용	01h:	BMC 전용	02h:	공유 모드	00h:	사용 안 함	01h:	사용	00h:	호스트 전용	01h:	BMC 전용	02h:	공유 모드	00h:	사용 안 함	01h:	사용	<p>서버에 ID 버튼이 있는 경우 사용자는 ID 버튼을 3초 이상 눌러 ID 버튼을 사용/사용 안 함으로 설정하여 FP USB 포트의 소유자를 전환할 수 있습니다.</p> <p>전원 사이클 중에 포트를 자동으로 전환하면 이력(초)이 설정됩니다. 이는 옵션 매개 변수입니다.</p> <p>SD530 서버</p> <p>SD530 플랫폼에서 포트는 옵션이며, 존재하는 경우 XCC에 직접 연결되며 XCC에만 연결됩니다. 포트를 호스트로 전환할 수 없습니다.</p> <ul style="list-style-type: none"> • 바이트 1 = 1로 명령이 실행되면 XCC는 항상 BMC에서 포트를 소유하고 있다고 응답합니다. • 바이트 1 = 2로 명령이 실행되면 XCC는 항상 포트가 BMC 전용이라고 응답합니다. • 바이트 1 = 3 또는 바이트 1 = 4로 명령이 실행되면 XCC는 완료 코드 D6h로 응답합니다. <p>비 SD530 서버</p> <p>비 SD530 플랫폼에서는 "호스트 전용" 모드로 전환하여 XCC의 앞면 패널 USB 포트 사용을 사용 안 함으로 설정할 수 있습니다.</p> <p>바이트 1 = 5 또는 바이트 1 = 6으로 명령이 실행되면 XCC는 완료 코드 D6h로 응답합니다.</p>
02h:	앞면 패널 USB 포트의 구성 가져오기																								
00h:	호스트 전용																								
01h:	BMC 전용																								
02h:	공유 모드																								
00h:	사용 안 함																								
01h:	사용																								
00h:	호스트 전용																								
01h:	BMC 전용																								
02h:	공유 모드																								
00h:	사용 안 함																								
01h:	사용																								

망 함수 = 0x3A

코드	명령	요청, 응답 데이터	설명												
		<p>바이트 1 - 완료 코드 바이트 2</p> <table border="1"> <tr> <td>00h:</td> <td>호스트로 전환</td> </tr> <tr> <td>01h:</td> <td>BMC로 전환</td> </tr> </table> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 1</p> <table border="1"> <tr> <td>05h:</td> <td>앞면 패널 USB 포트 사 용/사용 안 함</td> </tr> </table> <p>바이트 2</p> <table border="1"> <tr> <td>00h:</td> <td>사용 안 함</td> </tr> <tr> <td>01h:</td> <td>사용</td> </tr> </table> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>요청:</p> <p>바이트 1</p> <table border="1"> <tr> <td>06h:</td> <td>앞면 패널 USB 포트의 사용/사용 안 함 상태 읽기</td> </tr> </table> <p>응답:</p> <p>바이트 1 - 완료 코드</p> <p>바이트 2</p>	00h:	호스트로 전환	01h:	BMC로 전환	05h:	앞면 패널 USB 포트 사 용/사용 안 함	00h:	사용 안 함	01h:	사용	06h:	앞면 패널 USB 포트의 사용/사용 안 함 상태 읽기	
00h:	호스트로 전환														
01h:	BMC로 전환														
05h:	앞면 패널 USB 포트 사 용/사용 안 함														
00h:	사용 안 함														
01h:	사용														
06h:	앞면 패널 USB 포트의 사용/사용 안 함 상태 읽기														
0xC7	기본 NM IPMI 스위치	<p>요청 길이 = 0:</p> <p>비어 있는 요청 데이터</p> <p>응답:</p> <table border="1"> <tr> <td>바이트 1</td> <td>완료 코드</td> </tr> <tr> <td>바이트 2</td> <td>현재 사용/사 용 안 함 상 태</td> </tr> </table>	바이트 1	완료 코드	바이트 2	현재 사용/사 용 안 함 상 태	이 명령은 기본 Intel IPMI 명령에 대한 XCC의 브리징 기능을 사용/사용 안 함으로 설정하는 데 사용됩니다.								
바이트 1	완료 코드														
바이트 2	현재 사용/사 용 안 함 상 태														

망 함수 = 0x3A							
코드	명령	요청, 응답 데이터	설명				
		요청 길이 = 1: <table border="1" data-bbox="683 348 1057 653"> <tr> <td>바이트 1</td> <td> 기본 NM IPMI 인터페이스 사용/사용 안 함 속성 00h - 사용 안 함 01h - 사용 </td> </tr> </table> 응답: <table border="1" data-bbox="683 737 1057 789"> <tr> <td>바이트 1</td> <td>완료 코드</td> </tr> </table>	바이트 1	기본 NM IPMI 인터페이스 사용/사용 안 함 속성 00h - 사용 안 함 01h - 사용	바이트 1	완료 코드	
바이트 1	기본 NM IPMI 인터페이스 사용/사용 안 함 속성 00h - 사용 안 함 01h - 사용						
바이트 1	완료 코드						

부록 A. 도움말 및 기술 지원 얻기

도움말, 서비스 또는 기술 지원이 필요하거나 Lenovo 제품에 대한 자세한 정보를 원하는 경우 도움이 되는 다양한 정보를 Lenovo에서 구할 수 있습니다.

World Wide Web에서 Lenovo 시스템, 옵션 장치, 서비스 및 지원에 관한 최신 정보를 얻을 수 있는 웹 사이트:

<http://datacentersupport.lenovo.com>

참고: 다음은 IBM 웹 사이트에 대한 참조 및 서비스 확보에 관한 정보를 제공합니다. IBM은 ThinkSystem에 대해 Lenovo가 선호하는 서비스 공급자입니다.

문의하기 전에

문의하기 전에 직접 문제를 시도 및 해결하도록 시도할 수 있는 몇 가지 단계가 있습니다. 도움을 요청해야 한다고 결정하는 경우 서비스 기술자가 보다 신속하게 문제를 해결하는 데 필요한 정보를 수집하십시오.

직접 문제를 해결하기 위한 시도

온라인 도움말 또는 Lenovo 제품 문서에서 Lenovo가 제공하는 문제 해결 절차에 따라 외부 지원 없이 많은 문제를 해결할 수 있습니다. Lenovo 제품 문서는 사용자가 수행할 수 있는 진단 테스트에 대해서도 설명합니다. 대부분의 시스템, 운영 체제 및 프로그램에는 문제 해결 절차와 오류 메시지 및 오류 코드에 대한 설명이 포함되어 있습니다. 소프트웨어 문제가 의심되면 운영 체제 또는 프로그램에 대한 설명서를 참조하십시오.

ThinkSystem 제품에 대한 제품 설명서는 다음 위치에서 제공됩니다.

<https://pubs.lenovo.com/>

다음 단계를 수행하여 직접 문제를 해결하도록 시도할 수 있습니다.

- 케이블이 모두 연결되어 있는지 확인하십시오.
- 전원 스위치를 검사하여 시스템과 옵션 장치가 켜져 있는지 확인하십시오.
- Lenovo 제품에 대한 업데이트된 소프트웨어, 펌웨어 및 운영 체제 장치 드라이버를 확인하십시오. Lenovo Warranty 사용 약관에 따르면 추가 유지보수 계약이 적용되지 않는 한 제품의 모든 소프트웨어 및 펌웨어를 유지하고 업데이트할 책임은 제품의 소유자에게 있습니다. 서비스 기술자는 소프트웨어 업그레이드에 문제에 대한 솔루션이 문서화되어 있을 경우 소프트웨어 및 펌웨어를 업그레이드하도록 요청할 것입니다.
- 사용자 환경에 새 하드웨어 또는 소프트웨어를 설치한 경우 <http://www.lenovo.com/serverproven/>의 내용을 확인하여 제품에 해당 하드웨어 및 소프트웨어가 지원되는지 확인하십시오.
- <http://datacentersupport.lenovo.com>의 내용을 참조하여 문제 해결에 도움이 되는 정보를 확인하십시오.
 - 다른 사람이 유사한 문제를 겪었는지 확인하려면 https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg에서 Lenovo 포럼을 확인하십시오.

온라인 도움말 또는 Lenovo 제품 문서에서 Lenovo가 제공하는 문제 해결 절차에 따라 외부 지원 없이 많은 문제를 해결할 수 있습니다. Lenovo 제품 문서는 사용자가 수행할 수 있는 진단 테스트에 대해서도 설명합니다. 대부분의 시스템, 운영 체제 및 프로그램에는 문제 해결 절차와 오류 메시지 및 오류 코드에 대한 설명이 포함되어 있습니다. 소프트웨어 문제가 의심되면 운영 체제 또는 프로그램에 대한 설명서를 참조하십시오.

지원 담당자를 호출하는 데 필요한 정보 수집

본인의 Lenovo 제품에 대한 보증 서비스가 필요하다고 판단되는 경우, 전화하기 전에 준비하면 서비스 기술자로부터 보다 효율적으로 도움을 받을 수 있습니다. 제품 보증에 관한 자세한 정보는 <http://datacentersupport.lenovo.com/warrantylookup>의 내용을 참조할 수도 있습니다.

서비스 기술자에게 제공할 다음 정보를 수집하십시오. 이 데이터는 서비스 기술자가 문제에 대한 솔루션을 신속하게 제공하며 사용자가 계약한 수준의 서비스를 받는 데 도움이 됩니다.

- 하드웨어 및 소프트웨어 유지보수 계약 번호(해당되는 경우)
- 시스템 유형 번호(Lenovo 4자리 시스템 ID)
- 모델 번호
- 일련 번호
- 현재 시스템 UEFI 및 펌웨어 수준
- 오류 메시지 및 로그와 같은 기타 관련 정보

Lenovo 지원팀 호출에 대한 대체 방법으로 <https://www-947.ibm.com/support/servicerequest/Home.action>로 이동하여 전자 서비스 요청을 제출할 수 있습니다. 전자 서비스 요청을 제출하면 서비스 기술자에게 관련 정보를 제공하여 이 문제에 대한 솔루션을 결정하는 프로세스가 시작됩니다. Lenovo 서비스 기술자는 전자 서비스 요청을 작성하여 제출하면 바로 솔루션에 대한 작업을 시작할 수 있습니다.

서비스 데이터 수집

서버 문제의 근본 원인을 분명하게 식별하려고 하는 경우 또는 Lenovo 지원팀의 요청이 있을 때, 추가 분석에 사용해야 할 수 있는 서비스 데이터를 수집해야 할 수 있습니다. 서비스 데이터에는 이벤트 로그 및 하드웨어 인벤토리 같은 정보가 포함됩니다.

서비스 데이터는 다음 도구를 통해 수집할 수 있습니다.

- **Lenovo XClarity Controller**

Lenovo XClarity Controller 웹 인터페이스 또는 CLI를 사용해 서버에 대한 서비스 데이터를 수집할 수 있습니다. 파일을 저장하여 Lenovo 지원팀에 보낼 수 있습니다.

- 웹 인터페이스를 사용한 서비스 데이터 수집에 대한 자세한 정보는 https://pubs.lenovo.com/xcc3/nnlia_c_servicesandsupport.html의 내용을 참조하십시오.
- CLI를 사용한 서비스 데이터 수집에 대한 자세한 정보는 https://pubs.lenovo.com/xcc3/nnlia_r_ffdcommand.html의 내용을 참조하십시오.

- **Lenovo XClarity Administrator**

서비스 가능한 특정 이벤트가 Lenovo XClarity Administrator 및 관리되는 엔드포인트에서 발생하는 경우 진단 파일을 수집하고 자동으로 Lenovo 지원팀에 보내도록 Lenovo XClarity Administrator를 설정할 수 있습니다. 진단 파일을 Call Home을 사용하는 Lenovo 지원이나 SFTP를 사용하는 다른 서비스 제공업체로 보내는 방법을 선택할 수 있습니다. 진단 파일을 수동으로 수집하고 문제 레코드를 열고 진단 파일을 Lenovo 지원 센터에 보낼 수 있습니다.

Lenovo XClarity Administrator 에서 자동 문제 알림을 설정하는 방법에 대한 자세한 내용은 https://pubs.lenovo.com/lxca/admin_setupcallhome.html에서 확인할 수 있습니다.

- **Lenovo XClarity Provisioning Manager**

Lenovo XClarity Provisioning Manager의 서비스 데이터 수집 기능을 사용하여 시스템 서비스 데이터를 수집할 수 있습니다. 기존 시스템 로그 데이터를 수집하거나 새 진단을 실행하여 새 데이터를 수집할 수 있습니다.

- **Lenovo XClarity Essentials**

Lenovo XClarity Essentials를 운영 체제에서 대역 내로 실행할 수 있습니다. 하드웨어 서비스 데이터 외에 Lenovo XClarity Essentials가 운영 체제 이벤트 로그 같은 운영 체제에 대한 정보를 수집할 수 있습니다.

getinfor 명령을 실행하여 서비스 데이터를 얻을 수 있습니다. getinfor 실행에 대한 자세한 정보는 https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html의 내용을 참조하십시오.

지원팀에 문의

지원팀에 문의하여 문제에 대한 도움을 받을 수 있습니다.

Lenovo 공인 서비스 공급자를 통해 하드웨어 서비스를 받을 수 있습니다. 보증 서비스를 제공하는 Lenovo 공인 서비스 공급자를 찾으려면 <https://datacentersupport.lenovo.com/us/en/serviceprovider> 사이트로 이동하여 필터링으로 여러 나라를 검색해 보십시오. Lenovo 지원 전화 번호는 <https://datacentersupport.lenovo.com/us/en/supportphonenumber>에서 거주 지역의 지원 세부 정보를 참조하십시오.

부록 B. 주의사항

Lenovo가 모든 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하는 것은 아닙니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 Lenovo 담당자에게 문의하십시오.

이 책에서 Lenovo 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 Lenovo 제품, 프로그램 또는 서비스만 사용할 수 있다는 것은 아닙니다. Lenovo의 지적 재산을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 기타 제품, 프로그램 또는 서비스의 운영에 대한 평가와 검증은 사용자의 책임입니다.

Lenovo는 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공하는 것은 오픈링이 아니며 이 책을 제공한다고 해서 특허 또는 특허 응용 프로그램에 대한 라이선스까지 부여하는 것은 아닙니다. 의문사항은 다음으로 문의하십시오.

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO는 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현재 상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. Lenovo는 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 책에서 설명한 제품은 오작동으로 인해 인체 상해 또는 사망이 발생할 수 있는 이식 또는 기타 생명 유지 응용 프로그램에서 사용하도록 고안되지 않았습니다. 이 책에 포함된 정보는 Lenovo 제품 사양 또는 보증에 영향을 미치거나 그 내용을 변경하지 않습니다. 이 책의 어떠한 내용도 Lenovo 또는 타사의 지적 재산권 하에서 묵시적 또는 명시적 라이선스 또는 면책 사유가 될 수 없습니다. 이 책에 포함된 모든 정보는 특정 환경에서 얻은 것이며 설명 목적으로만 제공됩니다. 운영 환경이 다르면 결과가 다를 수 있습니다.

Lenovo는 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

이 책에서 언급되는 Lenovo 이외 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 Lenovo 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

본 책에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 운영 환경이 다르면 결과가 현저히 다를 수 있습니다. 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

상표

Lenovo, Lenovo 로고, ThinkSystem, Flex System, System x, NeXtScale System 및 x Architecture는 미국 또는 기타 국가에서 사용되는 Lenovo의 상표입니다.

Intel 및 Intel Xeon은 미국 또는 기타 국가에서 사용되는 Intel Corporation의 상표입니다.

Internet Explorer, Microsoft 및 Windows는 Microsoft 그룹의 상표입니다.

Linux는 Linus Torvalds의 등록 상표입니다.

기타 회사, 제품 및 서비스 이름은 해당 회사의 상표 또는 서비스 표시입니다.

중요 참고사항

프로세서 속도는 마이크로프로세서의 내부 클럭 속도를 나타냅니다. 다른 요소 또한 응용 프로그램 성능에 영향을 줍니다.

CD 또는 DVD 드라이브 속도는 읽기 속도가 가변적입니다. 실제 속도는 표시된 속도와는 다르며 일반적으로 가능한 최대값보다 작습니다.

프로세서 스토리지, 실제 및 가상 스토리지 또는 채널 볼륨을 언급할 때, KB는 1,024바이트, MB는 1,048,576바이트, GB는 1,073,741,824바이트를 나타냅니다.

하드 디스크 드라이브 용량 또는 통신 볼륨을 언급할 때 MB는 1,000,000바이트, GB는 1,000,000,000바이트를 나타냅니다. 사용자가 액세스할 수 있는 총량은 운영 환경에 따라 다를 수 있습니다.

최대 내장 하드 디스크 드라이브 용량은 모든 하드 디스크 드라이브 베이에서 표준 하드 디스크 드라이브를 현재 Lenovo에서 지원되는 가장 큰 드라이브로 교체한 상태에서의 용량을 나타냅니다.

최대 메모리를 사용하려면 표준 메모리를 옵션 메모리 모듈로 교체해야 할 수도 있습니다.

각 솔리드 스테이트 메모리 셀에는 셀에서 발생할 수 있는 고유한 한정된 수의 쓰기 주기가 들어 있습니다. 따라서 솔리드 스테이트 장치는 TBW(total bytes written)로 표시될 수 있는 최대 쓰기 주기 수를 갖습니다. 이 한도를 초과한 장치는 시스템에서 생성된 명령에 응답하지 못하거나 기록할 수 없을 수도 있습니다. Lenovo는 장치에 대한 공식 발행 사양에 설명된 대로 최대 프로그램 보장 횟수/삭제 주기를 초과한 장치의 교체에 대해 책임을 지지 않습니다.

Lenovo는 Lenovo 이외 제품에 대해서는 어떠한 진술 또는 보증도 하지 않습니다. Lenovo 이외 제품에 대한 지원은 Lenovo가 아닌 타사에서 제공됩니다.

일부 소프트웨어는 일반 정품 버전과 차이가 있을 수 있으며, 사용 설명서나 일부 프로그램 기능이 포함되지 않을 수도 있습니다.

미립자 오염

주의: 대기중 미립자(금속 조각 또는 입자) 및 단독으로 혹은 습도나 온도와 같은 다른 환경 요인과 결합하여 작용하는 반응성 기체는 본 문서에서 기술하는 장치에 위험을 초래할 수도 있습니다.

과도하게 미세한 입자가 있거나 유독 가스의 응축으로 인해 제기되는 위험 중에는 장치에 고장을 일으키거나 완전히 작동을 중단시킬 수도 있는 피해도 있습니다. 본 사양은 이와 같은 피해를 예방하고자 미립자와 가스에 대한 제한을 제시합니다. 공기의 온도나 수분 함량과 같은 수많은 다른 요인이 미립자나 주변의 부식 물질 및 가스 오염물질 전파에 영향을 줄 수 있으므로 이러한 제한이 한정된 값으로 표시되거나 사용되어서는 안 됩니다. 이 문서에 제시되어 있는 특정 제한이 없을 경우 사용자는 인체의 건강 및 안전과 직결되는 미립자 및 가스 수준을 유지하는 관행을 실천에 옮겨야 합니다. 사용자 측 환경에서 미립자 또는 가스 수준으로 인해 장치가 손상되었다고 Lenovo에서 판단한 경우 Lenovo는 이러한 환경 오염 상태를 완화하기 위해 적절한 선후책을 마련하는 차원에서 장치 또는 부품의 수리나 교체에 관한 조항을 규정할 수 있습니다. 이러한 구제 조치의 이행 책임은 고객에게 있습니다.

표 59. 미립자 및 가스의 제한

오염물질	제한
미립자	<ul style="list-style-type: none"> 실내 공기는 ASHRAE 표준 52.2¹에 따라 40%의 대기 변색 도법 효율(MERV 9)로 끊임없이 필터링되어야 합니다. 데이터 센터에 들어오는 공기는 MIL-STD-282 기준을 충족하는 HEPA(High Efficiency Particulate Air) 필터를 사용하여 99.97% 이상의 효율로 필터링되어야 합니다. 미립자 오염물질의 조해성 상대 습도는 60%²를 초과해야 합니다. 실내에 아연 결정과 같은 전도성 오염물질이 있으면 절대로 안 됩니다.
가스	<ul style="list-style-type: none"> 구리: Class G1, ANSI/ISA 71.04-1985³ 기준 은: 30일 후 300Å 미만의 부식도

¹ ASHRAE 52.2-2008 - 일반 환기 공기정화 장치의 입자 크기별 제거 효율 테스트 방법. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

² 미립자 오염물질의 조해성 상대 습도는 물기가 생겨 이온 전도가 촉진되기에 충분한 상태가 될 정도로 미립자가 수분을 흡수하는 상대 습도입니다.

³ ANSI/ISA-71.04-1985. 프로세스 측정 및 제어 시스템의 환경 조건: 대기중 오염물질. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

통신 규제 취급방침

이 제품은 공공 통신 네트워크의 인터페이스에 어떤 방식으로든 연결을 위해 해당 국가에서 인증할 수 없습니다. 또한 이러한 연결을 만들기 전에 법률에 의해 인증 받아야 할 수 있습니다. 의문사항은 Lenovo 담당자 또는 대리점에 문의하십시오.

전자 방출 주의사항

모니터를 장비에 연결할 경우 지정된 모니터 케이블과 모니터와 함께 제공되는 간섭 억제 장치를 사용해야 합니다.

추가 전자 방출 주의사항은 다음에서 제공됩니다.

<https://pubs.lenovo.com/>

대만 BSMI RoHS 준수 선언

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁶⁺)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組零件	-	○	○	○	○	○
空氣傳動設備	-	○	○	○	○	○
冷卻組零件	-	○	○	○	○	○
內存模塊	-	○	○	○	○	○
處理器模塊	-	○	○	○	○	○
鍵盤	-	○	○	○	○	○
調製解調器	-	○	○	○	○	○
監視器	-	○	○	○	○	○
滑鼠	-	○	○	○	○	○
電纜組零件	-	○	○	○	○	○
電源	-	○	○	○	○	○
儲備設備	-	○	○	○	○	○
電池匣組零件	-	○	○	○	○	○
有mech的電路卡	-	○	○	○	○	○
無mech的電路卡	-	○	○	○	○	○
雷射器	-	○	○	○	○	○
<p>備考1. “超出0.1 wt %” 及 “超出0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值。 Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.</p> <p>備考2. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。 Note2 : “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.</p> <p>備考3. “-” 係指該項限用物質為排除項目。 Note3 : The “-” indicates that the restricted substance corresponds to the exemption.</p>						

대만 수입 및 수출 연락처 정보

대만 수입 및 수출 정보를 문의할 수 있는 연락처가 제공됩니다.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

색인

- BMC
 - 구성 재설정 113
 - 기본값 구성 113
- IMM
 - sreset 130
 - 재설정 130
- IMM 제어 명령 128
- 1회
 - 설정 54

- a**
 - accseccfg 명령 96
 - Active Directory 사용자
 - LDAP 125
 - adapter 명령 139
 - Agent-less 명령 131
 - asu 명령 97

- b**
 - backup 명령 100
 - batch 명령 128
 - BIOS(기본 입/출력 시스템) 1
 - BMC 관리
 - BMC 구성
 - BMC 구성 백업 및 복원 44
 - BMC 구성 복원 44
 - 공장 출하 기본값으로 복원 44
 - 백업 BMC 구성 44

- c**
 - clearlog 명령 86
 - CLI(명령줄 인터페이스)
 - 기능 및 제한사항 82
 - 로그인 81
 - 명령 구문 82
 - 설명 81
 - 액세스 81
 - clock 명령 129
 - create
 - 사용자 계정 125

- d**
 - D3 V2 채시, XClarity Controller
 - 설정 61
 - dbgshbmc 명령 140
 - dcmi
 - 기능 및 명령 58
 - 전원 관리 58
 - DDNS
 - DHCP 서버 지정 도메인 이름 101
 - 관리 101
 - 구성 101
 - 도메인 이름 원본 101
 - 사용자 지정 도메인 이름 101
 - dhcpinfo 명령 100
 - DNS
 - IPv4 주소 101
 - IPv6 주소 101
 - LDAP 서버 107
 - 구성 101
 - 서버 주소 101
 - dns 명령 101

- e**
 - encaps 명령 102
 - ethtousb 명령 102
 - exit 명령 85

- f**
 - fans 명령 86
 - Features on Demand
 - 관리 107
 - 설치 기능 107
 - 원격 기능 107
 - firewall 명령 103
 - Flex server 1
 - Flex System 1
 - FoD
 - 관리 107
 - 설치 기능 107
 - 원격 기능 107
 - fuelg 명령 95

- h**
 - hashpw 명령 104
 - help 명령 85
 - history 명령 85
 - HTTP 포트
 - set 110
 - HTTPS 서버
 - 보안 119
 - 인증서 관리 119
 - HTTPS 포트
 - set 110
 - HTTPS를 통한 CIM
 - 보안 119
 - 인증서 관리 119
 - HTTPS를 통한 CIM 포트
 - set 110
 - HTTP를 통한 CIM 포트

설정 110

i

ifconfig 명령 105

IMM

구성 복원 112

info 명령 130

IP 주소

IPv4 9

IPv6 9

LDAP 서버 107

구성 9

IP 주소, 기본 고정 10

IPMI

구성 32

원격 서버 관리 143

ipmi 명령

전원 소모량 57

IPMI 명령을 사용하여

전원 모니터링 57

ipmi 브리징

XClarity Controller를 통해 57

전원 관리 57

IPMI 인터페이스

설명 143

IPMItool 143

IPv4

구성 105

IPv4 주소

DNS 101

IPv6 9

구성 105

IPv6 주소

DNS 101

k

KCS를 통한 IPMI 액세스

구성 41

keycfg 명령 107

l

LDAP

Active Directory 사용자 125

구성 107

그룹 검색 속성 107

그룹 필터 107

로그인 권한 속성 107

보안 119

서버 대상 이름 107

역할 기반 보안, 향상된 125

인증서 관리 119

향상된 역할 기반 보안 125

LDAP

구성 17

ldap 명령 107

LDAP 서버

DNS 107

IP 주소 107

UID 검색 속성 107

구성 107

도메인 검색 107

루트 고유 이름 107

미리 구성됨 107

바인딩 방법 107

암호 107

클라이언트 고유 이름 107

포트 번호 107

호스트 이름 107

LDAP 서버 포트

설정 107

led 명령 87

m

MAC 주소

관리 105

mhlog 명령 86

MIB 소개 7

MTU

설정 105

n

ntp 명령 109

o

OEM IPMI 명령 153

OneCLI 1

p

portcontrol 명령 109

ports 명령 110

power 명령 94

pxeboot 명령 96

r

RAID 설정

서버 구성 71

rdmount 명령 111

readlog 명령 89

remove

정품 인증 키 79, 107

reset 명령 95

restore 명령 112

restoredefaults 명령 113

roles 명령 112

s

seccfg 명령 113

security password manager

구성 42

- security password manager 42
- securityinfo 명령 114
- securitymode 명령 114
- Serial over LAN 143
- servicelog 명령 90
- set
 - HTTP 포트 110
 - HTTPS 포트 110
 - HTTPS를 통한 CIM 포트 110
 - SNMP 에이전트 포트 110
 - SNMP 트랩 포트 110
 - SSH CLI 포트 110
 - 원격 콘솔 포트 110
- set 명령 114
- SKM
 - 옵션 42
- snmp 명령 115
- SNMP 에이전트 포트
 - set 110
- SNMP 트랩 수신인 52
- SNMP 트랩 포트
 - set 110
- snmpalerts 명령 117
- SNMPv1
 - 구성 115
- SNMPv1 TRAP
 - 구성 115
- SNMPv1 연락처
 - 설정 115
- SNMPv1 커뮤니티
 - 관리 115
- SNMPv3 사용자 계정
 - 구성 125
- SNMPv3 설정
 - 사용자 125
- SNMPv3 연락처
 - 설정 115
- sreset 명령 130
- SSH CLI 포트
 - set 110
- SSH 서버
 - 보안 118
 - 인증서 관리 118
- SSH 키
 - 사용자 125
- sshcfg 명령 118
- SSL
 - 인증서 관리 40
 - 인증서 취급 40
- sslcfg 명령 119
- storage 명령 131
 - 스토리지 장치 131
- syshealth 명령 91
- syslock 명령 121

t

- temps 명령 92
- thermal 명령 122
- ThinkSystem 서버 펌웨어

- 설명 1
- TLS
 - 최소 수준 123
- TLS 명령 123
- TLS 버전 지원
 - TLS 버전 지원 43
- trespass 명령 124

u

- uefipw 명령 124
- UID 검색 속성
 - LDAP 서버 107
- USB
 - 구성 102
- usbeth 명령 124
- USB를 통한 이더넷
 - 구성 102
 - 포트 전달 102
- users 명령 125

v

- volts 명령 92
- vpd 명령 93

x

- XClarity Controller
 - ipmi 브리징 57
 - 구성 옵션 17
 - 기능 1
 - 네트워크 연결 10
 - 네트워크 프로토콜 구성 28
 - 새 기능 1
 - 설명 1
 - 웹 인터페이스 9
 - 직렬 방향 재지정 81
- XClarity Controller
 - XClarity Controller Standard 수준 1
 - XClarity Controller 플래티넘 수준 1
- XClarity Controller 관리
 - LDAP 구성 17
 - XClarity Controller 속성
 - D3 V2 세시 61
 - 날짜 및 시간 61
 - 보안 설정 35
 - 사용자 계정 구성 17
 - 사용자 계정 삭제 21
 - 새 로컬 사용자 작성 19
 - 새 역할 만들기 18
- XClarity Controller 구성
 - 구성할 옵션
 - XClarity Controller 17
- XClarity Controller 기능
 - 웹 인터페이스 13
 - 표준 수준 2
- XClarity Controller 기능 플래티넘 수준 기능
 - 플래티넘 수준 4

- XClarity Controller 다시 시작 45
- XClarity Controller에 로그인 12
- XClarity Controller의 기능 1
- XClarity 프로비저닝 관리자 Setup Utility 10

ㄱ

- 가상 드라이브 보기 및 구성 71
- 가스 오염 168
- 감사 로그 52
- 개요 47
 - ssl 39
 - 보안 대시보드 35
 - 보안 모드 35
 - 시스템 가드 43
- 개인별 지원 웹 페이지 만들기 163
- 고급 관리 모듈 1
- 고급 이더넷
 - 설정 28, 144
- 고유 이름, 루트
 - LDAP 서버 107
- 고유 이름, 클라이언트
 - LDAP 서버 107
- 고정 IP 주소, 기본 10
- 관련 작업
 - 감사 로그의 이벤트 52
 - 이벤트 로그의 이벤트 51
- 관리
 - DDNS 101
 - Features on Demand 107
 - FoD 107
 - MAC 주소 105
 - SNMPv1 커뮤니티 115
 - 사용자 125
 - 정품 인증 키 107
- 구성
 - DDNS 101
 - DDNS 설정 30
 - DNS 101
 - DNS 설정 30
 - IPMI 32
 - IPv4 105
 - IPv6 105
 - KCS를 통한 IPMI 액세스 41
 - LDAP 107
 - LDAP 서버 107
 - LDAP 설정 24
 - security password manager 42
 - SNMPv1 115
 - SNMPv1 TRAP 115
 - SNMPv3 경보 설정 32
 - SNMPv3 사용자 계정 125
 - SSH 서버 41
 - USB 102
 - USB를 통한 이더넷 102
 - USB를 통한 이더넷 설정 31
 - 네트워크 서비스 포트 109
 - 네트워크 프로토콜 28

- 보안 설정 35
- 사용자 계정 보안 수준 96
- 사용자 계정당 동시 로그인 제한 42
- 시스템 가드 43
- 시스템 펌웨어 하위 수준 방지 42
- 앞면 패널 USB 관리 포트 35
- 이더넷 105
- 이더넷 설정 28, 144
- 전역 로그인 설정 23
- 직렬을 SSH로 방향 재지정 81
- 차단 목록 및 시간 제한 33
- 포트 110
- 포트 할당 33
- 구성 명령 96
- 구성 복원
 - IMM 112
- 구성 재설정
 - BMC 113
- 그룹 검색 속성
 - LDAP 107
- 그룹 필터
 - LDAP 107
- 기능 및 명령
 - dcmi 58
 - 노드 관리자 57
- 기본 고정 IP 주소 10
- 기본값 구성
 - BMC 113

ㄴ

- 날짜
 - 설정 129
- 날짜 및 시간, XClarity Controller
 - 설정 61
- 내보내기
 - 정품 인증 키 80
- 네트워크 서비스 포트
 - 구성 109
- 네트워크 설정
 - IPMI 명령 33
- 네트워크 연결 10
 - IP 주소, 기본 고정 10
 - 고정 IP 주소, 기본 10
 - 기본 고정 IP 주소 10
- 네트워크 프로토콜 속성
 - DDNS 30
 - DNS 30
 - IPMI 32
 - KCS를 통한 IPMI 액세스 41
 - SNMP 경고 설정 32
 - USB를 통한 이더넷 31
 - 시스템 펌웨어 하위 수준 방지 42
 - 이더넷 설정 28, 144
 - 차단 목록 및 시간 제한 33
 - 포트 할당 33
- 노드 관리자
 - 기능 및 명령 57

ㄷ

- 다국어 지원 7
- 다국어의 지원 7
- 대만 BSMI RoHS 준수 선언 170
- 대만 수입 및 수출 연락처 정보 171
- 대상 이름, 서버
 - LDAP 107
- 도구
 - IPMItool 143
- 도메인 검색
 - LDAP 서버 107
- 도메인 이름 원본
 - DDNS 101
- 도메인 이름, DHCP 서버 지정
 - DDNS 101
- 도메인 이름, 사용자 지정
 - DDNS 101
- 도움 받기 163
- 도움말 163
- 드라이브 액세스 탭
 - 보안 옵션 42

ㄹ

- 라이선스 관리 79
- 로그인 권한 속성
 - LDAP 107
- 로그인 시도 인증 17
- 루트 고유 이름
 - LDAP 서버 107

ㄴ

- 명령
 - accsecfg 96
 - asu 97
 - clearlog 86
 - dbgshbmc 140
 - dhcinfo 100
 - dns 101
 - encaps 102
 - ethusb 102
 - firewall 103
 - fuelg 95
 - hashpw 104
 - ifconfig 105
 - info 130
 - keycfg 107
 - ldap 107
 - led 87
 - mhlog 86
 - ntp 109
 - portcontrol 109
 - pxeboot 96
 - rdmount 111
 - readlog 89
 - restoredefaults 113
 - roles 112
 - secfg 113

- securityinfo 114
- securitymode 114
- servicelog 90
- snmp 115
- snmpalerts 117
- sreset 130
- sshcfg 118
- sslcfg 119
- syshealth 91
- syslock 121
- temps 92
- TLS 123
- trespass 124
- uefipw 124
- usbeth 124
- volts 92
- vpd 93
- 내역 85
- 도움말 85
- 래치 128
- 백업 100
- 복원 112
- 사용자 125
- 설정 114
- 스토리지 131
- 시계 129
- 어댑터 139
- 열전도 122
- 재설정 95
- 전원 94
- 종료 85
- 팬 86
- 포트 110
- 명령, 알파벳 목록 83
- 명령, 유형
 - IMM 제어 128
 - Agent-less 131
 - 구성 96
 - 모니터 85
 - 서버 전원 및 다시 시작 93
 - 유틸리티 85
 - 지원 140
- 모니터 명령 85
- 미디어 탑재 방법 65
- 미디어 탑재 오류 문제 69
- 미리 구성됨
 - LDAP 서버 107
- 미립자 오염 168

ㄷ

- 바인딩 방법
 - LDAP 서버 107
- 베이스보드 관리 컨트롤러(BMC) 1
- 보안
 - HTTPS 서버 119
 - HTTPS를 통한 CIM 119
 - LDAP 119
 - SSH 서버 41, 118
 - ssl 개요 39

- SSL 인증서 관리 40
- ssl 인증서 취급 40
- 보안 대시보드 개요 35
- 보안 모드 개요 35
- 보안 모드 전환 39
- 시스템 가드 개요 43
- 보안 옵션
 - 드라이브 액세스 탭 42
- 브라우저 요구사항 6
- 블루 스크린 캡처 64
- 비디오 뷰어
 - 비디오 컬러 모드 64
 - 전원 및 다시 시작 명령 64
 - 화면 캡처 64

入

- 사용
 - 원격 콘솔 기능 63
- 사용자
 - SNMPv3 설정 125
 - SSH 키 125
 - 관리 125
 - 삭제 125
 - 암호 125
 - 현재 보기 125
- 사용자 계정
 - 삭제 21
- 사용자 계정
 - create 125
- 사용자 계정 보안 수준
 - 구성 96
- 사용자 계정당 동시 로그인 제한
 - 구성 42
 - 사용자 계정당 동시 로그인 제한 42
- 사용자 인증 방법 17
 - 설정 96
- 사용자 정의 지원 웹 페이지 163
- 삭제
 - 사용자 125
- 상표 168
- 새 로컬 계정
 - 만들기 19
- 새 역할
 - 만들기 18
- 서버
 - 구성 옵션 53
- 서버 관리
 - 1회 54
 - 서버 제한시간, 설정 60
 - 서버 펌웨어 75-76
 - 시스템 부팅 모드 53
 - 시스템 부팅 순서 53
- 서버 관리 탭
 - 전원 관리 옵션 54
- 서버 구성
 - RAID 설정 71
 - 구성할 옵션
 - 서버 53
 - 서버 속성 59

- 스토리지 세부 정보 71
- 어댑터 정보 53
- 서버 대상 이름
 - LDAP 107
- 서버 상태
 - 모니터링 47
- 서버 상태 모니터링 47
- 서버 속성
 - 위치 및 담당자 설정 59
- 서버 속성
 - 서버 구성 59
- 서버 시간제한
 - 선택사항 60
- 서버 전원 및 다시 시작
 - 명령 93
- 서버 제한시간 설정 60
- 서버 주소
 - DNS 101
- 서버 펌웨어
 - 업데이트 75-76
- 서비스 데이터 164
- 서비스 데이터 로그
 - 다운로드 59
 - 수집 59
- 서비스 데이터 로그 수집 59
- 서비스 데이터 수집 164
- 서비스 및 지원
 - 문의하기 전에 163
 - 소프트웨어 165
 - 하드웨어 165
- 설정
 - DDNS 30
 - DNS 30
 - HTTP를 통한 CIM 포트 110
 - LDAP 24
 - LDAP 서버 포트 107
 - MTU 105
 - SNMP 경고 32
 - SNMPv1 연락처 115
 - SNMPv3 연락처 115
 - SSH 서버 41
 - USB를 통한 이더넷 31
 - XClarity Controller 날짜 및 시간 61
 - 고급 28, 43, 144
 - 날짜 129
 - 보안 35
 - 사용자 인증 방법 96
 - 시간 129
 - 시스템 가드 43
 - 웹 비활성 제한시간 96
 - 이더넷 28, 144
 - 자동 협상 105
 - 전역 로그인 23
 - 계정 보안 정책 설정 23
 - 차단 목록 및 시간 제한 33
 - 최대 전송 단위 105
 - 포트 할당 33
 - 호스트 이름 105
- 설치
 - 정품 인증 키 79, 107

- 설치 기능
 - Features on Demand 107
 - FoD 107
- 소프트웨어 서비스 및 지원 전화 번호 165
- 솔루션 서비스 60
- 스위치
 - 보안 모드 39
- 스토리지
 - 구성 옵션 71
- 스토리지 구성
 - 구성할 옵션
 - 스토리지 71
- 스토리지 세부 정보
 - 서버 구성 71
- 스토리지 인벤토리 72
- 스토리지 장치
 - storage 명령 131
- 시간
 - 설정 129
- 시스템 가드
 - 설정 43
 - 시스템 가드 43
- 시스템 사용자 50
- 시스템 사용자
 - 보기 50
- 시스템 정보 48
- 시스템 정보
 - 보기 48
- 시스템 펌웨어 하위 수준 방지
 - 구성 42

○

- 알파벳 명령 목록 83
- 암호
 - LDAP 서버 107
 - 사용자 125
- 암호화 키
 - 중앙 관리 42
- 어댑터 정보
 - 서버 구성 53
- 역할 기반 보안, 향상된
 - LDAP 125
- 열린 항목 보기 110
- 오염, 미립자 및 가스 168
- 온라인 문서
 - 설명서 업데이트 정보 1
 - 오류 코드 정보 1
 - 펌웨어 업데이트 정보 1
- 옵션
 - SKM 42
- 요구사항
 - 운영 체제 6
 - 웹 브라우저 6
- 운영 체제 블루 스크린 64
- 운영 체제 요구사항 6
- 원격 기능
 - Features on Demand 107
 - FoD 107
- 원격 액세스 1

- 원격 전원 제어 64
- 원격 콘솔
 - 가상 미디어 세션 63
 - 비디오 뷰어 63
 - 전원 및 다시 시작 명령 64
 - 키보드 지원 64
 - 화면 캡처 64
- 원격 콘솔 기능 63
 - 사용 가능 64
- 원격 콘솔 세션 종료 70
- 원격 콘솔 포트
 - set 110
- 원격 콘솔 화면 모드 65
- 원격 콘솔의 키보드 지원 64
- 웹 브라우저 요구사항 6
- 웹 비활성 세션 제한시간 23
- 웹 비활성 제한시간
 - 설정 96
- 웹 인터페이스
 - 웹 인터페이스에 로그인 12
- 웹 인터페이스, 열기 및 사용 9
- 웹 페이지 지원, 사용자 지정 163
- 위치 및 담당자 설정 59
- 유지보수 내역 52
- 유틸리티 명령 85
- 이더넷
 - 구성 105
- 이메일 및 syslog 알람 52
- 이벤트 로그 51
- 이벤트 창
 - 로그 51-52
- 인증서 관리
 - HTTPS 서버 119
 - HTTPS를 통한 CIM 119
 - LDAP 119
 - SSH 서버 118

ㄱ

- 자동 협상
 - 설정 105
- 재설정
 - IMM 130
- 전역 로그인
 - 설정 23
- 전역 로그인 설정
 - 계정 보안 정책 설정 23
- 전원
 - IPMI 명령을 사용한 관리 57
 - IPMI 명령을 사용한 모니터링 57
- 전원 관리
 - dcmi 58
 - ipmi 브리징 57
- 전원 관리 옵션
 - 서버 관리 탭 54
 - 전력 복구 정책 56
 - 전원 작업 56
 - 전원 중복성 54
 - 전원 최대 가용량 사용 정책 55
- 전원 소모량

- ipmi 명령 57
- 전화 번호 165
- 정품 인증 키
 - remove 79, 107
 - 관리 107
 - 내보내기 80
 - 설치 79, 107
- 주의사항 167
- 주의사항 및 경고문 8
- 중앙 관리
 - 암호화 키 42
- 중요 주의사항 168
- 지원 명령 140
- 직렬을 SSH로 방향 재지정 81

ㄸ

- 차단 목록 및 시간 제한
 - 설정 33
- 참고사항, 중요 168
- 최대 전송 단위
 - 설정 105
- 최소, 수준
 - TLS 123
- 침입 메시지 옵션 60

ㄷ

- 클라이언트 고유 이름
 - LDAP 서버 107

ㄹ

- 통신 규제 취급방침 169

ㅍ

- 펌웨어
 - 서버 보기 93

- 펌웨어 정보 보기
 - 서버 93
- 펌웨어, 서버
 - 업데이트 75-76
- 포트
 - 구성 110
 - 번호 설정 110
 - 열린 항목 보기 110
- 포트 번호
 - LDAP 서버 107
 - 설정 110
- 포트 번호 설정 110
- 포트 전달
 - USB를 통한 이더넷 102
- 포트 할당
 - 구성 33
 - 설정 33
- 표준 수준 기능 2

ㅎ

- 하드웨어 상태 47
- 하드웨어 서비스 및 지원 전화 번호 165
- 해시 암호 21
- 향상된 역할 기반 보안
 - LDAP 125
- 현재 보기
 - 사용자 125
- 호스트 이름
 - LDAP 서버 107
 - 설정 105
- 확장된 감사 로그
 - 확장된 감사 로그 42
- 활성 시스템 이벤트
 - 개요 47

Lenovo