# Docker 환경 Lenovo XClarity Administrator 계획 및 설치 안내서

버전 4.0.0

## 주의

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, XClarity Administrator 온라인 설명서의 일반 및 법적 주의사항을 읽으십시오.

초판 (2023년 2월)

# 목차


목차 . . . . . i

그림 . . . . . iii

표 . . . . . v

변경사항 요약 . . . . . vii

제 1 장. Lenovo XClarity Administrator 개요 . . . . . 1

제 2 장. XClarity Administrator 계획 . . . . . 7

라이센스 및 무료 90일 평가판 . . . . . 7

하드웨어 및 소프트웨어 전제조건 . . . . . 8

방화벽 및 프록시 서버 . . . . . 10

포트 사용 가능성 . . . . . 12

관리 고려사항 . . . . . 16

네트워크 고려사항 . . . . . 17

IP 구성 제한 . . . . . 17

네트워크 유형 . . . . . 17

네트워크 구성 . . . . . 17

보안 고려사항 . . . . . 27

encapsulation 관리 . . . . . 27

암호화 관리 . . . . . 28

보안 인증서 . . . . . 30

인증 . . . . . 30

사용자 계정 및 역할 그룹 . . . . . 33

사용자 계정 보안 . . . . . 33

고가용성 고려사항 . . . . . 33

Features on Demand . . . . . 34

제 3 장. 에서 Lenovo XClarity Administrator 설치 . . . . . 37

단일 데이터 및 관리 네트워크 . . . . . 37

1단계: 섀시, 랙 서버 및 Lenovo XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결 . . . . . 39

2단계: ToR(top-of-rack) 스위치 구성 . . 40

3단계: CMM(Chassis Management Module) 구성 . . . . . 40

4단계: Flex 스위치 구성 . . . . . 42

5단계: 호스트 설치 및 구성 . . . . . 43

6단계. XClarity Administrator 설치 및 구성 . . . . . 43

물리적으로 분리된 데이터 및 관리 네트워크 . . 46

1단계: 섀시, 랙 서버 및 Lenovo XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결 . . . . . 48

2단계: ToR(top-of-rack) 스위치 구성 . . 49

3단계: CMM(Chassis Management Module) 구성 . . . . . 49

4단계: Flex 스위치 구성 . . . . . 51

5단계: 호스트 설치 및 구성 . . . . . 52

6단계. XClarity Administrator 설치 및 구성 . . . . . 52

가상으로 분리된 데이터 및 관리 네트워크 토폴로지 . . . . . 56

1단계: ToR(top-of-rack) 스위치에 섀시 및 랙 서버의 케이블 연결 . . . . . 59

2단계: ToR(top-of-rack) 스위치 구성 . . 59

3단계: CMM(Chassis Management Module) 구성 . . . . . 60

4단계: Flex 스위치 구성 . . . . . 62

5단계: 호스트 설치 및 구성 . . . . . 63

6단계. XClarity Administrator 설치 및 구성 . . . . . 64

관리 전용 네트워크 토폴로지 . . . . . 67

1단계: 섀시, 랙 서버 및 Lenovo XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결 . . . . . 69

2단계: ToR(top-of-rack) 스위치 구성 . . 70

3단계: CMM(Chassis Management Module) 구성 . . . . . 70

4단계: Flex 스위치 구성 . . . . . 72

5단계: 호스트 설치 및 구성 . . . . . 73

6단계. XClarity Administrator 설치 및 구성 . . . . . 73

고가용성 구현 . . . . . 76

제 4 장. Lenovo XClarity Administrator 구성 . . . . . 77

Lenovo XClarity Administrator 웹 인터페이스에 처음 액세스 . . . . . 77

사용자 계정 만들기 . . . . . 80

네트워크 액세스 구성 . . . . . 81

날짜 및 시간 구성 . . . . . 86

서비스 및 지원 구성 . . . . . 88

보안 구성 . . . . . 90

장치 관리 . . . . . 91

제 5 장. XClarity Administrator 등록 . . . . . 103

제 6 장. 전체 기능 사용 라이센스 설치 . . . . . 105

XClarity Administrator 웹 인터페이스를 사용하여 전체 기능 사용 라이센스 설치 . . . . . 106
Features on Demand 웹 포털에서 전체 기능 사용 라이센스 설치 . . . . . 110

**제 7 장. XClarity Administrator를 로 업데이트 . . . . . 113**

**제 8 장. XClarity Administrator 제거 . . . . . 117**

# 그림


1. 관리, 데이터 및 운영 체제 배포를 위한 단일 네트워크의 예제 구현 . . . . . 21
2. 데이터 네트워크의 일부로 운영 체제 네트워크가 포함된 물리적으로 분리된 데이터 및 관리 네트워크의 예제 구현. . . . . 22
3. 관리 네트워크의 일부로 운영 체제 네트워크가 포함된 물리적으로 분리된 데이터 및 관리 네트워크의 예제 구현 . . . . . 23
4. 데이터 네트워크의 일부로 운영 체제 네트워크가 포함된 가상으로 분리된 데이터 및 관리 네트워크의 예제 구현 . . . . . 24
5. 관리 네트워크의 일부로 운영 체제 네트워크가 포함된 가상으로 분리된 관리 및 데이터 네트워크의 예제 구현 . . . . . 25
6. 운영 체제 배포가 지원되지 않는 관리 전용 네트워크의 예제 구현 . . . . . 26
7. 운영 체제 배포가 지원되는 관리 전용 네트워크의 예제 구현 . . . . . 27
8. 가상 어플라이언스의 단일 데이터 및 관리 네트워크 토폴로지 샘플 . . . . . 38
9. 컨테이너의 단일 데이터 및 관리 네트워크 토폴로지 샘플 . . . . . 38
10. 단일 데이터 및 관리 네트워크의 케이블 연결 예. . . . . 40
11. 섀시의 Flex 스위치 위치 . . . . . 43
12. 가상 어플라이언스의 물리적으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플 . . 47
13. 컨테이너의 물리적으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플 . . . . . 48
14. 물리적으로 분리된 데이터 및 관리 네트워크의 케이블 연결 예. . . . . 49
15. 섀시의 Flex 스위치 위치 . . . . . 52
16. 가상 어플라이언스의 가상으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플 . . . 57
17. 컨테이너의 가상으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플 . . . . . 58
18. 가상으로 분리된 데이터 및 관리 네트워크의 케이블 연결 예. . . . . 59
19. 관리 네트워크에서 VLAN 태그 지정이 사용으로 설정된 가상으로 분리된 데이터 및 관리 네트워크(VMware ESXi)의 Flex 스위치 구성 예 . . . . . 60
20. 관리 네트워크에서 VLAN 태그 지정이 사용으로 설정된 가상으로 분리된 데이터 및 관리 네트워크(VMware ESXi)의 Flex 스위치 구성 예 . . . . . 63
21. 가상 어플라이언스의 샘플 관리 전용 네트워크 토폴로지 . . . . . 68
22. 컨테이너의 샘플 관리 전용 네트워크 토폴로지 . . . . . 69
23. 관리 전용 네트워크 케이블 연결 예 . . . 70
24. 섀시의 Flex 스위치 위치 . . . . . 73

# 표

1. 인터넷 연결 필요 . . . . . 10
2. 네트워크 토폴로지 기준 각 네트워크 인터페이스 역할 . . . . . 19
3. 네트워크 토폴로지 기준 각 네트워크 인터페이스 역할 . . . . . 82

# 변경사항 요약

Lenovo XClarity Administrator 관리 소프트웨어의 후속 릴리스는 새로운 하드웨어, 소프트웨어, 향상 기능 및 수정 지원을 지원합니다.

수정에 대한 정보는 업데이트 패키지에 제공된 변경 이력 파일(*.chg)을 참조하십시오.

지원되는 모든 하드웨어(서버, 섀시 및 Flex 스위치 등)에 대한 정보는 하드웨어 및 소프트웨어 전제조건의 내용을 참조하십시오.

이전 릴리스의 변경 사항에 대한 정보는 XClarity Administrator 온라인 설명서에서 새로운 기능의 내용을 참조하십시오.

이번 릴리스에서는 다음 하드웨어가 지원됩니다.

- **서버 및 어플라이언스**
  - ThinkAgile HX630 V3(7D6M)
  - ThinkAgile HX645 V3(7D9M)
  - ThinkAgile HX650 V3(7D6N)
  - ThinkAgile HX665 V3(7D9N)
  - ThinkAgile MX630 V3(7D6U)
  - ThinkAgile MX650 V3(7D6S)
  - ThinkAgile VX630 V3(7D6X, 7Z63)
  - ThinkAgile VX635 V3(7D9V)
  - ThinkAgile VX645 V3(7D9K)
  - ThinkAgile VX650 V2-DPU(7Z63)
  - ThinkAgile VX650 V3(7D6W)
  - ThinkAgile VX650 V3-DPU(7D6W)
  - ThinkAgile VX655 V3(7D9W)
  - ThinkAgile VX665 V3(7D9L)
  - ThinkAgile VX850 V3(7DDK)
  - ThinkEdge SE350 V2(7DA9)
  - ThinkEdge SE455 V3(7DBY)
  - ThinkEdge SE360 V2(7DAM)
  - ThinkSystem SD555 V3(7DDP, 7DDQ)
  - ThinkSystem SD650 V3(7D7M)
  - ThinkSystem SD650-I V3(7D7L)
  - ThinkSystem SD650-N V3(7D7L)
  - ThinkSystem SD665 V3(7D9P)
  - ThinkSystem SD665-N V3(7DAZ)
  - ThinkSystem SR630 V3(7D72, 7D73, 7D74)
  - ThinkSystem SR635 V3(7D9G, 7D9H)
  - ThinkSystem SR645 V3(7D9C, 7D9D)
  - ThinkSystem SR650 V3(7D75, 7D76, 7D77)
  - ThinkSystem SR655 V3(7D9E, 7D9F)
  - ThinkSystem SR665 V3(7D9B, 7D9A)
  - ThinkSystem SR675 V3(7D9Q, 7D9R)
  - ThinkSystem SR850 V3(7D96, 7D97, 7D98)
  - ThinkSystem SR860 V3(7D93, 7D94, 7D95)
  - ThinkSystem SR950 V3(7DC4, 7DC5, 7DC6)
  - ThinkSystem ST650 V3(7D7A, 7D7B)
- **스토리지 장치**
  - ThinkSystem DE6400F All Flash Array(7DB6)

  - ThinkSystem DE6400H Hybrid Flash Array(7DB6)
  - ThinkSystem DE6600F All Flash Array(7DB7)
  - ThinkSystem DE6600H Hybrid Flash Array(7DB7)
- **스위치**
  - ThinkSystem DB730S FC SAN Switch(7D9J)
  - ThinkSystem DB400D FC SAN 디렉터(6684)
  - ThinkSystem DB800D FC SAN 디렉터(6682)

이 버전에서는 다음과 같은 관리 소프트웨어 계획 또는 설치 개선 사항을 지원합니다.

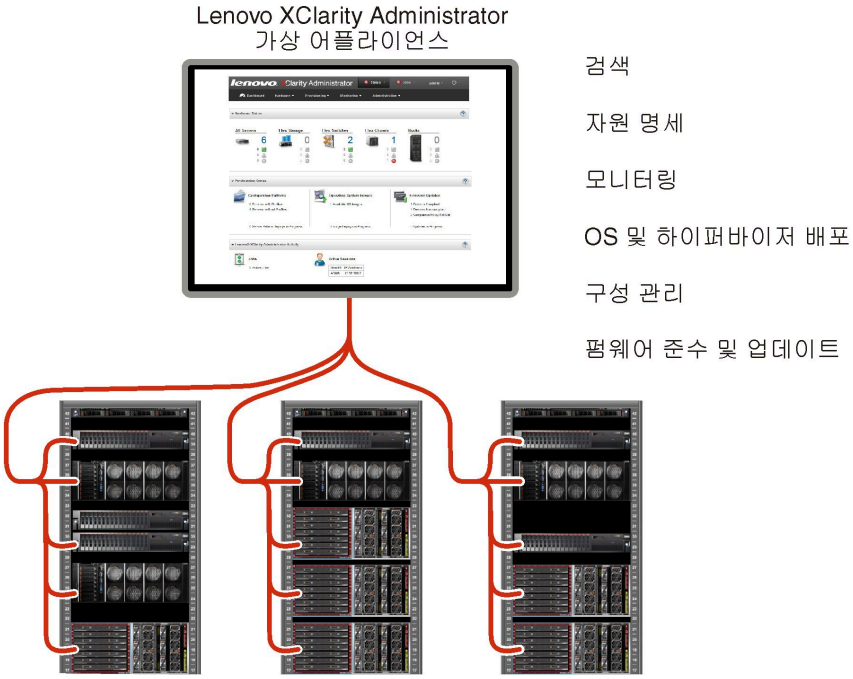
| 기능 | 설명 |
| --- | --- |
| 계획 및 설치 | ssh-rsa를 제거하고 ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 및 ecdsa-sha2-nistp521을 지원되는 호스트 키 알고리즘 목록에 추가했습니다(암호화 관리 참조). |

# 제 1 장 Lenovo XClarity Administrator 개요

Lenovo XClarity Administrator는 인프라 관리를 간소화하고, 응답 속도를 높이고, Lenovo® 서버 시스템 및 솔루션의 사용 가능성을 향상시키는 중앙 집중식 리소스 관리 솔루션입니다. 안전한 환경에서 서버, 네트워크 및 스토리지 하드웨어에 대한 검색, 목록 작성, 추적, 모니터링 및 프로비저닝을 자동화하는 가상 기기로 실행됩니다.

**자세히 알아보기:**

- XClarity Administrator: 소프트웨어 같은 하드웨어 관리
- XClarity Administrator: 개요




XClarity Administrator는 모든 관리 장치에 대한 다음 기능을 수행하기 위한 중앙 인터페이스를 제공합니다.

**하드웨어 관리**

XClarity Administrator는 에이전트가 없는 하드웨어 관리를 제공합니다. 서버, 네트워크 및 스토리지 하드웨어 등 관리 가능한 장치를 자동으로 검색할 수 있습니다. 관리 장치에 대해 인벤토리 데이터가 수집되므로 하드웨어 인벤토리 및 상태를 한 눈에 파악할 수 있습니다.

상태 및 속성 보기 및 시스템 및 네트워크 설정 구성, 관리 인터페이스 실행, 전원 켜기 및 끄기 및 원격 제어 등 지원되는 각 장치에 대한 다양한 관리 작업이 있습니다. 장치 관리에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 섀시 관리, 서버 관리 및 스위치 관리의 내용을 참조하십시오.

**팁:** XClarity Administrator가 관리할 수 있는 서버, 네트워크 및 스토리지 하드웨어를 *장치*라고 합니다. XClarity Administrator 관리 중인 하드웨어를 *관리 장치*라고 합니다.

XClarity Administrator에 있는 랙 보기를 사용하여 데이터 센터의 물리적 랙 설정을 반영하도록 관리 장치를 그룹화할 수 있습니다. 랙에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 랙 관리의 내용을 참조하십시오.

**자세히 알아보기:**

- XClarity Administrator: 검색
- XClarity Administrator: 인벤토리
- XClarity Administrator: 원격 제어

**하드웨어 모니터링**

XClarity Administrator는 관리 장치에서 발생하는 모든 이벤트 및 경고에 대한 중앙 집중식 보기를 제공합니다. 이벤트 또는 경고는 XClarity Administrator에 전달되고 이벤트 또는 경고 로그에 표시됩니다. 모든 이벤트 및 경고에 대한 요약이 대시보드와 상태 표시줄에 표시됩니다. 특정 장치의 이벤트 및 경고는 해당 장치의 경고 및 이벤트 세부사항 페이지에서 확인할 수 있습니다.

하드웨어 관리에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 이벤트 작업 및 경고 작업의 내용을 참조하십시오.

**자세히 알아보기:** XClarity Administrator: 모니터링

**구성 관리**

일관된 구성을 사용하여 모든 서버를 빠르게 프로비전 및 사전 프로비전할 수 있습니다. 구성 설정(예, 로컬 스토리지, I/O 어댑터, 부팅 설정, 펌웨어, 포트, 관리 컨트롤러 및 UEFI 설정)이 하나 이상의 관리 서버에 적용될 수 있는 서버 패턴으로 저장됩니다. 서버 패턴이 업데이트되면 변경 내용이 적용되는 서버에 자동으로 배포됩니다.

또한 서버 패턴은 I/O 주소 가상화를 위한 지원을 통합하기 때문에 패브릭을 중단하지 않고 Flex System 패브릭 연결을 가상화하거나 서버의 용도를 변경할 수 있습니다.

서버 구성에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 XClarity Administrator를 사용하여 서버 구성의 내용을 참조하십시오.

**자세히 알아보기:**

- XClarity Administrator: 베어메탈에서 클러스터로
- XClarity Administrator: 구성 패턴

**펌웨어 준수 및 업데이트**

펌웨어 준수 정책을 관리 장치에 할당하여 펌웨어 관리가 간소화됩니다. 준수 정책을 만들어 관리 장치에 할당하는 경우 XClarity Administrator는 해당 장치에 대한 인벤토리 변경 사항을 모니터링하고 준수하지 않는 장치를 플래그합니다.

장치가 준수하지 않는 경우 XClarity Administrator를 사용하여 관리하는 펌웨어 업데이트의 리포지토리에서 해당 장치의 모든 장치에 대해 펌웨어 업데이트를 적용 및 활성화할 수 있습니다.

**참고:** 리포지토리를 새로 고치고 펌웨어 업데이트를 다운로드하려면 인터넷 연결이 필요합니다. XClarity Administrator가 인터넷에 연결되지 않은 경우 리포지토리에 펌웨어 업데이트를 수동으로 가져올 수 있습니다.

펌웨어 업데이트에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 관리 장치에서 펌웨어 업데이트의 내용을 참조하십시오.

**자세히 알아보기:**

- XClarity Administrator: 베어메탈에서 클러스터로
- XClarity Administrator: 펌웨어 업데이트
- XClarity Administrator: 펌웨어 보안 업데이트 프로비저닝

**운영 체제 배포**

XClarity Administrator를 사용하여 운영 체제 이미지 레포지토리를 관리하고 운영 체제 이미지를 동시에 관리 서버 최대 28개 서버에 배포할 수 있습니다.

운영 체제 배포에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 운영 체제 이미지 배포의 내용을 참조하십시오.

**자세히 알아보기:**

- XClarity Administrator: 베어메탈에서 클러스터로
- XClarity Administrator: 운영 체제 배포

### 사용자 관리

XClarity Administrator는 사용자 계정을 만들고 관리하며 사용자 자격 증명을 관리하고 인증하기 위한 중앙 인증 서버를 제공합니다. 인증 서버는 관리 서버를 처음 시작할 때 자동으로 만들어집니다. XClarity Administrator를 위해 만든 사용자 계정을 사용하여 관리되는 인증 모드로 관리되는 섀시와 서버에 로그인할 수도 있습니다. 사용자에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 사용자 계정 관리의 내용을 참조하십시오.

XClarity Administrator는 다음 세 가지 유형의 인증 서버를 지원합니다.

- **로컬 인증 서버**. 기본적으로 XClarity Administrator는 관리 노드에 상주하는 로컬 인증 서버를 사용하도록 구성되었습니다.
- **외부 LDAP 서버**. 현재 Microsoft Active Directory만 지원됩니다. 이 서버는 관리 네트워크에 연결된 아웃보드 Microsoft Windows 서버에 상주해야 합니다.외부 LDAP 서버가 사용되는 경우 로컬 인증 서버가 사용 불가능합니다.
- **외부 SAML 2.0 ID 공급자**. 현재 Microsoft Active Directory Federation Services(AD FS)만 지원됩니다. 사용자 이름 및 암호를 입력하는 것 외에 다중 인증을 설정하여 PIN 코드를 요구하고 스마트 카드와 클라이언트 인증서를 판독하여 추가 보안을 지원할 수 있습니다.

인증 유형에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 인증 서버 관리의 내용을 참조하십시오.

사용자 계정을 만들 때 사용자 계정에 사전 정의 또는 사용자 지정된 역할 그룹을 할당하여 해당 사용자의 액세스 레벨을 제어합니다. 역할 그룹에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 역할 그룹 만들기의 내용을 참조하십시오.

XClarity Administrator에는 로그인, 새로운 사용자 만들기 또는 사용자 암호 변경 등 사용자 작업의 기록 레코드를 제공하는 감사 로그가 포함됩니다. 감사 로그에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 이벤트 작업의 내용을 참조하십시오.

### 장치 인증

XClarity Administrator는 다음 방법을 사용하여 관리되는 섀시와 서버를 인증합니다.

- **관리되는 인증**. 관리되는 인증을 사용하면 XClarity Administrator에서 작성한 사용자 계정을 사용하여 관리되는 섀시와 서버를 인증합니다.

  사용자에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 사용자 계정 관리의 내용을 참조하십시오.

- **로컬 인증**. 관리되는 인증을 사용하지 않으면 XClarity Administrator에서 정의한 저장된 자격 증명을 사용하여 관리되는 서버를 인증합니다. 저장된 자격 증명은 장치 또는 Active Directory의 활성 사용자 계정과 일치해야 합니다.

  저장된 자격 증명에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 저장된 자격 증명 관리의 내용을 참조하십시오.

### 보안

사용자 환경이 NIST SP 800-131A 표준을 준수해야 하는 경우 XClarity Administrator가 완벽하게 준수하는 환경을 갖도록 도울 수 있습니다.

XClarity Administrator는 자체 서명된 SSL 인증서(내부 인증 기관에서 발행함) 및 외부 SSL 인증서(개인 또는 상업용 CA에서 발행함)를 지원합니다.

수신 요청을 XClarity Administrator에서만 수락하도록 섀시 및 서버의 방화벽을 구성할 수 있습니다.

보안에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 보안 환경 구현의 내용을 참조하십시오.

**서비스 및 지원**

서비스 가능한 특정 이벤트가 XClarity Administrator 및 관리 장치에서 발생하는 경우 진단 파일을 수집하고 선호하는 서비스 제공업체에 자동으로 보내도록 XClarity Administrator를 설정할 수 있습니다. 콜 홈을 사용하여 Lenovo 지원에 진단 파일을 보내거나 SFTP를 통해 다른 서비스 제공업체 보내도록 선택할 수 있습니다. 진단 파일을 수동으로 수집하고 문제 레코드를 열고 진단 파일을 Lenovo 지원 센터에 보낼 수 있습니다.

**자세히 알아보기:** XClarity Administrator: 서비스 및 지원

**스크립트를 사용한 작업 자동화**

공개 REST API(Application Programming Interface)를 통해 XClarity Administrator를 더 높은 수준의 외부 관리 및 자동화 플랫폼으로 통합할 수 있습니다. REST API를 사용하여 XClarity Administrator는 기존 관리 인프라와 손쉽게 통합할 수 있습니다.

PowerShell 툴킷은 Microsoft PowerShell 세션에서 리소스 관리와 프로비저닝을 자동화하는 cmdlet 라이브러리를 제공합니다. Python 툴킷은 Python 기반의 명령 및 API 라이브러리를 제공하여 Ansible 또는 Puppet 등 OpenStack 환경에서 프로비저닝 및 리소스 관리를 자동화합니다. 이러한 모든 툴킷은 다음과 같은 기능을 자동화하기 위한 XClarity Administrator REST API 인터페이스를 제공합니다.

- XClarity Administrator에 로그인
- 섀시, 서버, 스토리지 장치 및 TOR(top-of-rack) 스위치(장치) 관리 및 관리 해제
- 장치와 구성 요소에 대한 인벤토리 데이터 수집 및 보기
- 하나 이상의 서버에 운영 체제 이미지 배포
- 구성 패턴을 사용하여 서버 구성
- 장치에 펌웨어 업데이트 적용

**다른 관리 소프트웨어와 통합**

XClarity Administrator 모듈은 XClarity Administrator를 타사의 관리 소프트웨어와 통합하여 지원되는 장치에 대한 일상적인 시스템 관리의 비용과 복잡성을 줄이는 검색, 모니터링, 구성 및 관리 기능을 제공합니다.

XClarity Administrator에 대한 자세한 정보는 다음 설명서를 참조하십시오.
- Microsoft System Center용 Lenovo XClarity Integrator
- VMware vCenter용 Lenovo XClarity Integrator

추가 고려사항에 대해서는 관리 고려사항의 내용을 참조하십시오.

**자세히 알아보기:**
- Microsoft System Center용 Lenovo XClarity Integrator 개요
- VMware vCenter용 Lenovo XClarity Integrator

**문서**

XClarity Administrator 설명서(영어)는 온라인에서 정기적으로 업데이트됩니다. 최신 정보와 절차에 대해서는 XClarity Administrator 온라인 설명서의 내용을 참조하십시오.

온라인 설명서는 다음 언어로 제공됩니다.
- 독일어(de)
- 영어(en)
- 스페인어(es)

- 프랑스어(fr)
- 이탈리아어(it)
- 일본어(ja)
- 한국어(ko)
- 브라질 포르투갈어(pt_BR)
- 러시아어(ru)
- 태국어(th)
- 중국어 간체(zh_CN)
- 중국어 번체(zh_TW)

다음과 같은 방법으로 온라인 설명서의 언어를 변경할 수 있습니다.

- 웹 브라우저에서 언어 설정 변경
- 예를 들어 중국어 간체로 된 온라인 설명서를 표시하려면 URL의 끝에 ?lang=*<language_code>*를 추가하십시오.
  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html?lang=zh_CN

# 제 2 장 XClarity Administrator 계획

Lenovo XClarity Administrator를 설치하기 전에 설치 및 일상 관리 계획에 도움이 되도록 다음 고려 사항을 검토하십시오.

## 라이센스 및 무료 90일 평가판

Lenovo XClarity Administrator는 제한된 시간 동안 사용 가능한 모든 기능을 사용할 수 있는 90일 무료 평가판 라이센스를 제공합니다.

XClarity Administrator 제목 표시줄에서 사용자 작업 메뉴( 

)를 클릭한 후 **정보**를 클릭하여 평가판 라이센스에 남아 있는 기간(일) 등의 라이센스 상태를 판별할 수 있습니다.

XClarity Administrator는 다음 라이센스를 지원합니다.

- **Lenovo XClarity Pro**. 각 라이센스는 단일 장치에 대해 다음과 같은 권한을 제공합니다.
  - Lenovo XClarity Integrator에 대한 서비스 및 지원
  - XClarity Administrator에 대한 서비스 및 지원
  - XClarity Administrator 내 고급 기능
    - 구성 패턴을 사용하여 서버 구성
    - 운영 체제 배포
    - 콜 홈을 사용하여 XClarity Administrator 문제 보고(하드웨어 경고에 대한 콜 홈은 해당되지 않음)

고급 기능을 지원하는 각 관리 장치에 대해 라이센스를 구입해야 합니다. 라이센스는 특정 장치에 묶여 있지 않습니다.

라이센스 준수는 고급 기능을 지원하는 관리되는 장치의 수에 따라 결정됩니다. 관리되는 장치의 수는 모든 활성 라이센스 키의 총 라이센스 수를 초과해서는 안 됩니다. XClarity Administrator가 설치된 라이센스 수를 준수하지 않는 경우(예: 라이센스가 만료되거나 관리 중인 추가 장치가 총 활성 라이센스 수를 초과하는 경우), 적절한 라이센스를 설치할 수 있는 유예 기간은 90일입니다. XClarity Administrator이(가) 비준수 상태가 될 때마다 유예 기간이 90일로 재설정됩니다. 라이센스를 준수하기 전에 유예 기간(무료 평가판 포함)이 종료되면 모든 장치에서 고급 기능이 사용 중지됩니다.

**참고:**

- 유예 기간이 만료되면 서버 구성 및 운영 체제 배포 기능이 비활성화됩니다.
- XClarity Administrator 문제를 위한 콜 홈(소프트웨어 콜 홈 기능)은 라이센스를 준수하지 않는 경우 사용 중지됩니다. 이 기능에 대한 유예 기간은 없습니다. 하지만 하드웨어 경고에 대한 콜 홈은 영향을 받지 않습니다.

라이센스를 이미 설치한 경우 XClarity Administrator의 새 릴리스로 업그레이드할 때 새 라이센스가 필요하지 *않습니다*.

Lenovo XClarity Pro 라이센스 구입에 대한 정보는 Lenovo 담당자 또는 공인 비즈니스 파트너에게 문의하십시오.

라이센스 설치에 대한 정보는 XClarity Administrator 온라인 설명서에서 전체 기능 사용 라이센스 설치의 내용을 참조하십시오.

# 하드웨어 및 소프트웨어 전제조건

Lenovo XClarity Administrator 관리 어플라이언스는 호스트 시스템의 가상 컴퓨터에서 실행됩니다.

### 하이퍼바이저 요구사항

#### 컨테이너 환경

다음 컨테이너 환경에서는 XClarity Administrator을(를) 컨테이너로 실행할 수 있습니다.

- Docker v20.10.9
- Docker-compose v1.29.2

#### 하이퍼바이저

다음 하이퍼바이저에서는 XClarity Administrator를 가상 어플라이언스로 실행할 수 있습니다.

- Citrix 하이퍼바이저 v8.2
- Citrix XenServer v7.6
- CentOS 7 및 8[1]
- Hyper-V가 설치된 Microsoft Windows Server 2022
- Hyper-V가 설치된 Microsoft Windows Server 2019
- Hyper-V가 설치된 Microsoft Windows Server 2016
- Hyper-V가 설치된 Microsoft Windows Server 2012 R2
- Hyper-V가 설치된 Microsoft Windows Server 2012
- Nutanix Acropolis Hypervisor(AHV)
- 커널 기반 가상 컴퓨터(KVM) v2.12.0이 설치된 Red Hat v8.x
- KVM v1.2.17이 설치된 Red Hat v7.x
- KVM v4.2.3이 설치된 Ubuntu 20.04.2 LTS
- VMware ESXi 7.0, U1, U2 및 U3
- VMware ESXi 6.7, U1, U2[2] 및 U3

**참고:**

1. CentOS Linux는 더 이상 Red Hat에 의해 업데이트되지 않습니다. 대신 Red Hat Enterprise Linux로 마이그레이션하는 것이 좋습니다(Red Hat: CentOS 또는 Oracle Linux에서 RHEL 웹 페이지로 변환하는 방법 참조).
2. VMware ESXi 6.7 U2의 경우, ISO 이미지 VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso 이상을 사용해야 합니다.

VMware 및 Citrix의 경우 가상 컴퓨터를 OVF 템플릿으로 사용할 수 있습니다. Hyper-V 및 Nutanix AHV의 경우 가상 컴퓨터는 가상 디스크 이미지(VHD)입니다. CentOS 및 KVM의 경우 가상 컴퓨터는 qcow2 형식으로 사용 가능합니다.

**중요:** 2.6 커널 기반의 Linux 게스트에서 실행되고 가상 어플라이언스에 대량의 메모리를 사용하는 Hyper-V 환경의 경우 Hyper-V Manager의 Hyper-V 설정 패널에서 비균등 메모리 액세스(NUMA) 사용을 사용 안 함으로 설정해야 합니다. 이 설정을 변경하려면 Hyper-V 서비스를 다시 시작해야 합니다. 그러면 실행 중인 모든 가상 컴퓨터도 다시 시작됩니다. 이 설정을 사용 안 함으로 설정하지 않은 경우 초기 시작 중에 XClarity Administrator 가상 어플라이언스에 문제가 발생할 수 있습니다.

### 하드웨어 요구사항

XClarity Administrator에 대한 다음 *최소 요구사항*을 충족해야 합니다. 환경의 규모와 구성 패턴 사용에 따라 최적의 성능을 위해서는 추가 리소스가 필요할 수 있습니다.

- 가상 마이크로프로세서 2개
- 8GB 메모리
- XClarity Administrator 가상 어플라이언스가 사용할 수 있는 스토리지의 192GB.
- 너비의 최소 해상도가 1024픽셀인 디스플레이(XGA)

다음 테이블에는 지정된 수의 장치에 대한 최소 권장 구성이 나열되어 있습니다. 최소 구성을 실행하는 경우에는 관리 작업의 예상 완료 시간보다 오래 걸릴 수 있습니다. 운영 체제 배포, 펌웨어 업데이트 및 서버 구성과 같은 프로비저닝 작업의 경우 리소스를 일시적으로 늘려야 할 수 있습니다.

| 관리 장치의 수 | 가상 CPU/메모리 구성 |
|---|---|
| 0~100개의 장치 | 2개의 vCPU, 8GB RAM |
| 100~200개의 장치 | 4개의 vCPU, 10GB RAM |
| 200~400개의 장치 | 6개의 vCPU, 12GB RAM |
| 400~600개의 장치 | 8개의 vCPU, 16GB RAM |
| 600~800개의 장치 | 10개의 vCPU, 20GB RAM |
| 800~1,000개의 장치 | 12개의 vCPU, 24GB RAM |

**참고:**

- 단일 XClarity Administrator 인스턴스는 최대 1,000개의 장치를 지원할 수 있습니다.
- 최신 권장 사항 및 추가 성능 고려 사항은 XClarity Administrator: 성능 가이드( 백서)를 참조하십시오.
- 관리 환경의 크기와 설치의 설치 패턴을 사용하면, 수용 가능한 성능을 유지하기 위해 자원을 추가해야 할 수 있습니다. 시스템 리소스 대시 보드에서 높은 값 또는 매우 높은 값을 표시하는 프로세서 사용량이 자주 나타나는 경우, 1~2개의 가상 프로세서 코어 추가를 고려하십시오. 유휴 상태에서 메모리 사용량이 80%를 초과하는 경우, 1~2GB RAM 추가를 고려하십시오. 시스템이 표에 정의된 구성에서 응답하는 경우, 시스템 성능을 평가하기 위해 더 오랜 기간에 VM을 실행하는 것을 고려하십시오.
- 더 이상 필요하지 않은 XClarity Administrator 리소스를 삭제하여 디스크 공간을 비우는 방법에 대한 정보는 XClarity Administrator 온라인 설명서에서 디스크 공간 관리의 내용을 참조하십시오.

### 소프트웨어 요구사항

- **Orchestrator 서버**

  여러 XClarity Administrator 인스턴스를 사용하여 많은 수의 장치를 관리하는 경우 Lenovo XClarity Orchestrator를 사용하여 모니터링, 관리, 프로비저닝 및 분석을 중앙 집중화할 수 있습니다. XClarity Orchestrator는 최대 10,000대의 비 ThinkEdge-Client 장치를 총체적으로 관리하는 XClarity Administrator 인스턴스를 무제한으로 지원 가능합니다.

  Lenovo XClarity Orchestrator를 사용하여 XClarity Administrator v4.0 이상의 인스턴스를 관리하려면 XClarity Orchestrator v2.0 이상이 필요합니다.

- **인증 서버**

  외부 인증 서버를 사용하는 경우 Windows Server 2008 이상에서 실행 중인 Microsoft Active Directory만 지원됩니다.

  SAML ID 공급자를 사용하는 경우 Windows Server 2012에서 실행 중인 Microsoft Active Directory Federation Services(AD FS) 버전 2.0 이상만 지원됩니다.

- **NTP 서버**

  관리 장치에서 수신되는 모든 이벤트 및 경고에 대한 타임 스탬프가 XClarity Administrator와 동기화되도록 하려면 NPT(Network Time Protocol) 서버가 필요합니다. NTP 서버는 관리 네트워크(일반적으로 Eth0 인터페이스)로 액세스 가능해야 합니다.

  **팁:** XClarity Administrator가 NTP 서버로 설치된 호스트 시스템 사용을 고려하십시오. 그런 경우 호스트 시스템은 관리 네트워크로 액세스 가능해야 합니다.

## 관리 가능 리소스

단일 XClarity Administrator 인스턴스가 최대 1,000대의 물리적 장치를 관리, 모니터링 및 프로비저닝할 수 있습니다.

지원되는 장치 및 옵션(예: I/O, DIMM 및 스토리지 어댑터)의 전체 목록, 필요한 최소 펌웨어 수준, XClarity Administrator 지원 – 호환성 웹 페이지의 제한 및 고려사항은 **호환성** 탭을 클릭한 다음 해당 장치 유형의 링크를 클릭하여 확인할 수 있습니다.

특정 장치의 하드웨어 구성 및 옵션에 대한 일반 정보는 Lenovo Server Proven 웹 페이지의 내용을 참조하십시오.

**제한:** XClarity Administrator가 설치된 호스트 시스템이 관리되는 랙 서버 또는 컴퓨팅 노드인 경우 XClarity Administrator를 사용하여 해당 호스트 시스템에 또는 한 번에 전체 섀시에 펌웨어 업데이트를 적용할 수 없습니다. 펌웨어 업데이트가 호스트 시스템에 적용되면 호스트 시스템을 다시 시작해야 합니다. 호스트 시스템을 다시 시작하면 XClarity Administrator도 다시 시작되어 호스트 시스템에서 업데이트를 완료하는 데 XClarity Administrator를 사용할 수 없게 됩니다.

### 지원되는 웹 브라우저

XClarity Administrator 웹 인터페이스는 다음과 같은 웹 브라우저에서 작동합니다.
- Chrome™ 48.0 이상(원격 콘솔의 경우 55.0 이상)
- Firefox® ESR 38.6.0 이상
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 이상(IOS7 이상 및 OS X)

## 방화벽 및 프록시 서버

관리 서버 업데이트, 펌웨어 업데이트, 서비스 및 지원을 포함한 Lenovo XClarity Administrator의 일부 기능은 인터넷에 대한 액세스가 필요합니다. 네트워크에 방화벽이 있는 경우 XClarity Administrator 관리 서버가 이러한 작업을 수행하도록 방화벽을 구성하십시오. 관리 서버가 인터넷에 직접 액세스할 수 없는 경우 프록시 서버를 사용하도록 XClarity Administrator를 구성하십시오.

### 방화벽

다음 DNS 이름 및 경로가 방화벽에 열려 있는지 확인하십시오.

**참고:** IP 주소는 변경할 수 있습니다. 가능한 경우 DNS 이름을 사용하십시오.

***표 1. 인터넷 연결 필요***

| DNS 이름 | IPv4 주소 | IPv6 주소 | 포트 | 프로토콜 |
|---|---|---|---|---|
| **라이센스 활성화 키 다운로드** | | | | |
| fod.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 | https |
| **서비스 게시판 다운로드** | | | | |
| download.lenovo.com/servers/LXCA_Bulletin_Service.json | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |
| **업데이트 다운로드(관리 서버 업데이트, 펌웨어 업데이트, UpdateXpress System Packs(OS 장치 드라이버) 및 리포지토리 팩)** | | | | |
| datacentersupport.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |
| download.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |
| filedownload.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |
| support.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https 및 http |
| supportapi.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |

*표 1. 인터넷 연결 필요 (계속)*

| DNS 이름 | IPv4 주소 | IPv6 주소 | 포트 | 프로토콜 |
|---|---|---|---|---|
| **펌웨어 다운로드(Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, 일부 Flex 스위치 및 1세대 CMM만 해당)** | | | | |
| www.ibm.com | 129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.197 | 해당사항 없음 | 443 및 80 | https 및 http |
| www-03.ibm.com | 204.146.30.17 | 해당사항 없음 | 443 및 80 | https 및 http |
| download3.boulder.ibm.com | 170.225.126.24 | 해당사항 없음 | 443 | https |
| download4.boulder.ibm.com | 170.225.126.43 | 해당사항 없음 | 443 및 80 | https 및 http |
| delivery04-bld.dhe.ibm.com | 170.225.126.45 | 해당사항 없음 | 443 및 80 | https 및 http |
| delivery04-mul.dhe.ibm.com | 170.225.126.46 | 해당사항 없음 | 443 및 80 | https 및 http |
| delivery04.dhe.ibm.com | 170.225.126.44 | 해당사항 없음 | 443 및 80 | https 및 http |
| **Lenovo 지원에 서비스 데이터 업로드(콜 홈)** | | | | |
| soaus.lenovo.com | 3.222.8.29, 52.6.14.20 | 해당사항 없음 | 443 | https |
| logupload.lenovo.com/BLL/Logupload.ashx | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |
| **Lenovo 업데이트 기능에 서비스 데이터 업로드** | | | | |
| logupload.lenovo.com/BLL/Logupload.ashx | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https |
| **보증 정보 다운로드** | | | | |
| ibase.lenovo.com(전세계) | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https 및 http |
| service.lenovo.com.cn(중국 전용) | 114.247.140.212(중국 전용) | 해당사항 없음 | 83 | http |
| supportapi.lenovo.com | 해당사항 없음 | 해당사항 없음 | 443 및 80 | https 및 http |

**주의:** 중국 사용자의 경우 XClarity Administrator을 사용하여 관리되는 장치에 대한 보증 정보를 검색하려면 XClarity Administrator v1.3.1 이상으로 업그레이드해야 합니다.

### 프록시 서버

관리 서버가 인터넷에 직접 액세스할 수 없는 경우 관리 서버가 HTTP 프록시 서버를 사용하도록 구성되었는지 확인하십시오(네트워크 액세스 구성 참조).

- 프록시 서버가 기본 인증을 사용하도록 설정되었는지 확인하십시오.

- 프록시 서버가 비종결 프록시(non-terminating proxy)로 설정되었는지 확인하십시오.
- 프록시 서버가 전달 프록시로 설정되었는지 확인하십시오.
- 로드 밸런서가 한 프록시 서버와의 세션을 유지하고 세션 간을 전환하지 않도록 구성되었는지 확인하십시오.

## 포트 사용 가능성

환경에서 방화벽이 구현되는 방법에 따라 여러 개의 포트를 사용할 수 있어야 합니다. 필요한 포트가 차단되었거나 다른 프로세스에서 사용하는 경우 일부 Lenovo XClarity Administrator 기능이 작동하지 않을 수 있습니다.

환경에 따라 열려 있어야 하는 포트를 판별하려면 다음 섹션을 검토하십시오. 이 섹션의 표에는 각 포트가 XClarity Administrator에서 사용되는 방법, 영향을 받는 관리되는 장치, 프로토콜(TCP 또는 UDP) 및 트래픽 흐름 방향에 대한 정보가 있습니다. *인바운드* 트래픽은 관리되는 장치 또는 외부 시스템에서 XClarity Administrator(으)로의 흐름을 식별하므로 XClarity Administrator 어플라이언스에서 포트를 열어야 합니다. *아웃바운드* 트래픽은 XClarity Administrator에서 관리되는 장치로 흐릅니다.

- XClarity Administrator 서버 액세스
- XClarity Administrator와 관리 장치 간의 액세스
- OS 배포 및 장치 드라이버 업데이트를 위한 XClarity Administrator과(와) 데이터 네트워크 간의 액세스

### XClarity Administrator 서버 액세스

XClarity Administrator 서버 및 모든 관리 장치가 방화벽 안에 있고 방화벽 밖에 있는 브라우저에서 그러한 장치에 액세스하려는 경우 XClarity Administrator 포트가 열려 있어야 합니다. 이벤트 관리에 SNMP 및 SMTP를 사용하는 경우 XClarity Administrator 서버가 이벤트 전달에 사용하는 포트도 열려 있어야 합니다.

XClarity Administrator 서버는 대기하다가 다음 테이블에 나열된 포트를 통해 응답합니다.

**참고:**

- XClarity Administrator은(는) 포트 443에서 TCP를 통해 안전하게 통신하는 RESTful 응용 프로그램입니다.
- LDAP, SMTP 또는 syslog와 같은 외부 서비스로의 아웃바운드 연결을 위해 XClarity Administrator을(를) 선택적으로 구성할 수 있습니다. 이러한 연결에는 일반적으로 사용자가 구성할 수 있으며 이 목록에 포함되지 않은 추가 포트가 필요할 수 있습니다. 이러한 연결은 외부 서버 이름을 해석하기 위해 TCP 또는 UDP 포트 53에서 도메인 이름 서비스(DNS) 서버에 액세스해야 할 수도 있습니다.

| 통신 | XClarity Administrator 어플라이언스 | 외부 인증 서버 | 이벤트 전달 서비스 | Lenovo Services(콜 홈 포함) |
|---|---|---|---|---|
| **아웃바운드**(외부 시스템에서 열리는 포트) | • DNS – 포트 53의 TCP/UDP | • LDAP– 포트 389[1]의 TCP<br>• LDAPS – 포트 636의 TCP<br>• SAML 인증 – 포트 3268, 3269의 TCP | • FTP 서버 – 포트 21[1]의 TCP<br>• 이메일 서버(SMTP) – 포트 25[1]의 UDP<br>• REST 웹 서비스(HTTP) – 포트 80[1]의 UDP<br>• SNMP 관리자 – 포트 161[2], 162[1]의 UDP<br>• MS Azure – 포트 443[1]의 UDP | • 보증(중국만 해당) – 포트 83[5]의 TCP<br>• HTTPS(콜 홈) – 포트 443의 TCP |

| 통신 | XClarity Administrator 어플라이언스 | 외부 인증 서버 | 이벤트 전달 서비스 | Lenovo Services(콜 홈 포함) |
|---|---|---|---|---|
| | | | • Syslog – 포트 514[1]의 UDP<br>• Apple 푸시[3] – 포트 443, 2195, 5223의 TCP<br>• Google 푸시[4] – 포트 443, 5288, 5299, 5230의 TCP | |
| **인바운드**(XClarity Administrator 어플라이언스에서 열리는 포트) | • HTTPS – 포트 443의 TCP | 해당사항 없음 | • SNMP – 포트 161의 UDP | 해당사항 없음 |

1. 기본 포트입니다. 사용자 인터페이스에서 이 포트를 구성할 수 있습니다.
2. 이 포트는 사용자 인증으로 SNMP 이벤트 전달이 구성되면 사용됩니다.
3. Wi-Fi가 방화벽 또는 셀룰러 데이터용 APN(Access Point Name) 안에 있는 경우 이 포트를 엽니다. 이 포트에서는 APN 서버에 대한 직접 프록시 미설정 연결이 필요합니다. 이 포트는 장치가 포트 5223에서 Apple 푸시 알림 서비스에 연결할 수 없는 경우 Wi-Fi에서만 장애 복구 처리로 사용됩니다. IP 주소 범위는 17.0.0.0/8입니다.
4. IP 주소 범위는 Google ASN 15169에서 확인하십시오. 도메인은 android.googleapis.com입니다.
5. 중국 외 지역에는 필요하지 않지만 XClarity Administrator가 다른 국가에서 이 서비스에 연결하려고 할 수 있습니다.

### XClarity Administrator와 관리 장치 간의 액세스

관리 장치(예, 컴퓨팅 노드 또는 랙 서버)가 방화벽 안에 있고 해당 방화벽 밖에 있는 XClarity Administrator 서버에서 그러한 장치를 관리하려고 하는 경우 XClarity Administrator와 각 관리 장치의 베이스보드 관리 컨트롤러 간의 통신이 열려 있는 상태에서 모든 포트가 통신에 연결되어야 합니다.

XClarity Administrator를 사용하여 관리되는 장치에 운영 체제를 설치하려는 경우 OS 배포 및 장치 드라이버 업데이트를 위한 XClarity Administrator과(와) 데이터 네트워크 간의 액세스의 포트 목록을 검토해야 합니다.

- Flex Chassis CMM

| 통신 | Flex Chassis CMM |
|---|---|
| **아웃바운드**(외부 시스템에서 열리는 포트) | – SLP – 포트 427의 UDP/TCP<br>– CIM HTTP – 포트 5988[2]의 TCP<br>– CIM HTTPS – 포트 5989의 TCP<br>– TCP 명령 – 포트 6090[2]의 TCP<br>– 보안 TCP 명령 – 포트 6091의 TCP |
| **인바운드**(XClarity Administrator 어플라이언스에서 열리는 포트) | – SFTP – 포트 22[1]의 TCP<br>– CIM 표시 HTTPS – TCP 9090<br>– LDAPS – 포트 50637의 TCP |

1. 이 포트는 SFTP를 사용하여 펌웨어 업데이트를 전송하는 데 사용됩니다.
2. 기본적으로 보안 포트를 통해 관리가 수행됩니다. 비보안 포트는 선택 사항입니다.

- **서버 및 컴퓨팅 노드**

| 통신 | ThinkSystem 및 ThinkAgile | System x | Flex System | ThinkServer |
|---|---|---|---|---|
| **아웃바운드**(외부 시스템에서 열리는 포트) | – SFTP – 포트 115의 TCP<br>– SLP – 포트 427의 UDP/TCP<br>– HTTPS – 포트 443의 TCP<br>– SSDP 검색 – 포트 1900의 UDP<br>– 원격 제어 – 포트 3888[4]의 TCP<br>– 원격 KVM – 포트 3889[4]의 TCP<br>– CIM HTTPS – 포트 5989의 TCP<br>– 펌웨어 업데이트 – 포트 6990[5]의 TCP | – SLP – 포트 427의 UDP/TCP<br>– HTTPS – 포트 443의 TCP<br>– IPMI – 포트 623의 TCP<br>– 원격 제어 – 포트 3888[4]의 TCP<br>– 원격 KVM – 포트 3889[4]의 TCP<br>– CIM HTTP – 포트 5988[3]의 TCP<br>– CIM HTTPS – 포트 5989[3]의 TCP<br>– 펌웨어 업데이트 – 포트 6990[5]의 TCP | – SLP – 포트 427의 UDP/TCP<br>– 원격 제어 – 포트 3888[4]의 TCP<br>– 원격 KVM – 포트 3889[1, 4]의 TCP<br>– CIM HTTP – 포트 5988[3]의 TCP<br>– CIM HTTPS – 포트 5989[3]의 TCP<br>– 펌웨어 업데이트 – 포트 6990[5]의 TCP | – SNMP 트랩 – 포트 162의 UDP<br>– IPMI – 포트 623의 UDP |
| **인바운드**(XClarity Administrator 어플라이언스에서 열리는 포트) | – SFTP – 포트 22[2]의 TCP<br>– HTTPS – 포트 443의 TCP<br>– SSDP 검색 – 포트 1900의 UDP<br>– 펌웨어 업데이트 – 포트 6990[5]의 TCP<br>– CIM 표시 HTTPS – TCP 9090<br>– LDAPS – 포트 50636[6], 50637의 TCP | – SFTP – 포트 22[2]의 TCP<br>– HTTPS – 포트 443의 TCP<br>– 펌웨어 업데이트 – 포트 6990[5]의 TCP<br>– CIM 표시 HTTPS – TCP 9090<br>– LDAPS – 포트 50636[6], 50637의 TCP | – SFTP – 포트 22[2]의 TCP<br>– HTTPS – 포트 443의 TCP<br>– 펌웨어 업데이트 – 포트 6990[5]의 TCP<br>– CIM 표시 HTTPS – TCP 9090<br>– LDAPS – 포트 50636[6], 50637의 TCP | – SNMP 트랩 – 포트 162의 UDP |

1. 이 포트는 IMM2를 사용하는 서버에서만 열어야 합니다.
2. 이 포트는 SFTP를 사용하여 펌웨어 업데이트를 전송하는 데 사용됩니다.
3. 기본적으로 보안 포트를 통해 관리가 수행됩니다. 비보안 포트는 선택 사항입니다.
4. 원격 제어 및 원격 KVM은 XClarity Administrator 서버가 아닌 웹 브라우저에서 실행됩니다.
5. 이 포트는 BMU OS에 연결하여 파일을 전송하고 업데이트 명령을 실행하는 데 사용됩니다.
6. 이 포트는 구성 패턴을 사용하여 서버를 구성하는 데 필요합니다.

- **랙 및 Flex 스위치**

| 통신 | 랙 스위치 | Flex 스위치 |
|---|---|---|
| **아웃바운드**(외부 시스템에서 열리는 포트) | – SSH – 포트 22[1, 3]의 TCP<br>– SNMP – 포트 161[2]의 UDP<br>– SLP – 포트 427[6]의 UDP/TCP<br>– HTTPS – 포트 443[7]의 TCP | – SSH – 포트 22[3]의 TCP<br>– SNMP – 포트 161[5]의 UDP |
| **인바운드**(XClarity Administrator 어플라이언스에서 열리는 포트) | – SFTP – 포트 22[4]의 TCP<br>– SNMP 트랩 – 포트 162[2]의 TCP | – SFTP – 포트 22[4]의 TCP<br>– SNMP 트랩 – 포트 162[2]의 TCP |

1. ENOS 랙 스위치의 경우 SFTP 파일 전송 작업 전에 CMM과 Flex 스위치 간에 사용되는 스택 헤드(HoS) 자격 증명을 구성하고, 펌웨어 슬롯을 활성화하고, SSH 호스트 키를 지우는 데 이 포트가 사용됩니다.
2. 이 포트는 스위치가 XClarity Administrator과(와) 다른 네트워크에 있을 때 XClarity Administrator 어플라이언스(인바운드)에서 열어야 XClarity Administrator이(가) 해당 장치에 대한 이벤트를 수신할 수 있습니다.
3. 이 포트는 관리(SSH)에 사용됩니다.
4. 이 포트는 SFTP를 사용하여 펌웨어 업데이트를 전송하는 데 사용됩니다.
5. ENOS 랙 스위치의 경우 인벤토리 데이터를 전송하는 데 이 포트가 사용됩니다.
6. 이 포트는 검색에 사용됩니다.
7. 이 포트는 펌웨어 업데이트를 적용하는 데 사용됩니다.

- **스토리지 장치**

| 통신 | 스토리지 장치 |
|---|---|
| **아웃바운드**(외부 시스템에서 열리는 포트) | – FTP – 포트 21의 TCP<br>– SFTP – 포트 22[2]의 TCP<br>– SLP – 포트 427의 UDP/TCP<br>– HTTPS – 포트 443[1]의 TCP |
| **인바운드**(XClarity Administrator 어플라이언스에서 열리는 포트) | – HTTPS – 포트 443[2]의 TCP<br>– SNMP 트랩 – 포트 115의 UDP |

1. 이 포트는 펌웨어 업데이트를 전송하는 데 사용됩니다.
2. 이 포트는 펌웨어 업데이트를 전송하고 적용하는 데 사용됩니다.

### OS 배포 및 장치 드라이버 업데이트를 위한 XClarity Administrator과(와) 데이터 네트워크 간의 액세스

| 통신 | OS 배포[1, 2, 3] | OS 장치 드라이버 업데이트[2] |
|---|---|---|
| **아웃바운드**(외부 시스템에서 열리는 포트) | | • HTTP를 통한 WinRM – 포트 5985[5]의 TCP<br>• HTTPS를 통한 WinRM – 포트 5986[6]의 TCP |
| **인바운드**(XClarity Administrator 어플라이언스에서 열리는 포트) | • SMB 통신 – 포트 445의 TCP[4]<br>• HTTPS(ThinkServer 제외) – 포트 8443[6]의 TCP | • SMB 통신 – 포트 445의 TCP[4] |

1. 운영 체제 배포 네트워크를 사용하도록 XClarity Administrator을(를) 구성했다면 해당 네트워크에서 포트를 열어야 합니다.

2. 운영 체제를 배포하는 데 사용 가능해야 하는 포트 목록은 XClarity Administrator 온라인 설명서에서 배포된 운영 체제에 대한 포트 가용성의 내용을 참조하십시오. 예를 들어 데이터 네트워크(eth1)를 사용하도록 운영 체제 배포를 구성했다면 해당 네트워크에서 포트를 열어야 합니다.
3. 각 XClarity Administrator 인스턴스에는 OS 배포에만 사용되는 고유한 인증 기관(CA)이 있습니다. 해당 CA는 포트 8443에서 대상 서버에 사용되는 인증서에 서명합니다. OS 배포가 시작되면 대상 서버에 푸시된 OS 이미지에 CA 인증서가 포함됩니다. 배포 프로세스의 일부로 해당 서버는 포트 8443에 다시 연결하고 CA 인증서가 있기 때문에 핸드셰이크 중에 포트 8443이 제공하는 인증서를 확인합니다.
4. 이 포트는 Windows 드라이버 파일을 전송하는 데 사용됩니다.
5. 이 포트는 대상 서버 WinRM에 연결하는 데 사용됩니다.
6. 이 포트는 OS 이미지와 상태를 포함하여 대상 OS와XClarity Administrator 간에 데이터를 교환하는 데 사용됩니다.

## 관리 고려사항

장치를 관리할 때 선택할 수 있는 다양한 대안이 있습니다. 관리 중인 장치에 따라 여러 개의 관리 솔루션을 동시에 실행해야 할 수 있습니다.

하나의 장치는 하나의 Lenovo XClarity Administrator 인스턴스로만 관리할 수 있습니다. 그러나 다른 관리 소프트웨어(예: VMware vRealize Operations Manager)를 Lenovo XClarity Administrator과(와) 함께 사용하여 XClarity Administrator이(가) 관리하는 장치를 *모니터링*할 수 있습니다.

**주의:** 여러 관리 도구를 사용하여 장치를 관리하는 경우에는 예기치 않은 충돌을 방지하기 위해 별도의 주의가 필요합니다. 예를 들어 다른 도구를 사용하여 전원 상태 변경을 제출하는 경우 XClarity Administrator에서 실행 중인 구성 또는 업데이트 작업과 충돌이 발생할 수 있습니다.

### ThinkSystem, ThinkServer 및 System x 장치

다른 관리 소프트웨어를 사용하여 관리되는 장치를 모니터링하려는 경우 IMM 인터페이스에서 올바른 SNMP 또는 IPMI 설정을 가진 새 로컬 사용자를 만드십시오. 사용자 요구에 따라 SNMP 또는 IPMI 권한이 부여되어야 합니다.

### Flex System 장치

다른 관리 소프트웨어를 사용하여 관리되는 장치를 모니터링하려는 경우 및 해당 관리 소프트웨어가 SNMPv3 또는 IPMI 통신을 사용하는 경우 각 관리되는 CMM에 대해 다음 단계를 수행하여 환경을 준비해야 합니다.

1. RECOVERY_ID 사용자 이름 및 암호를 사용하여 섀시에 대한 관리 컨트롤러 웹 인터페이스에 로그인하십시오.
2. 보안 정책이 **보안**으로 설정되는 경우 사용자 인증 방법을 변경하십시오.
   a. **관리 모듈 관리 → 사용자 계정**을 클릭하십시오.
   b. **계정** 탭을 클릭하십시오.
   c. **전역 로그인 설정**을 클릭하십시오.
   d. General 탭을 클릭하십시오.
   e. 사용자 인증 방법으로 **외부 먼저, 로컬 인증 다음**을 선택하십시오.
   f. **확인**을 누르십시오.
3. 관리 컨트롤러 웹 인터페이스에서 올바른 SNMP 또는 IPMI 설정을 가진 새 로컬 사용자를 만드십시오.
4. 보안 정책이 **보안**으로 설정된 경우 로그아웃한 다음 새 사용자 이름 및 암호를 사용하여 관리 컨트롤러 웹 인터페이스에 로그인하십시오. 메시지가 표시되면 새 사용자의 암호를 변경하십시오.

이제 새 사용자를 활성 SNMP 또는 IPMI 사용자로 사용할 수 있습니다.

**참고:** 섀시를 관리 해제했다가 관리하는 경우 이 새 사용자 계정이 잠기고 사용할 수 없게 됩니다. 이 경우 이러한 단계를 반복하여 새 사용자 계정을 만드십시오.

## 네트워크 고려사항

Lenovo XClarity Administrator 설치를 준비하는 경우 환경에 구현된 네트워크 토폴로지와 XClarity Administrator가 해당 토폴로지에 장착되는 방식을 고려하십시오.

**중요:** IP 주소 변경을 최소화하는 방식으로 장치 및 구성 요소를 구성하십시오. DHCP(Dynamic Host Configuration Protocol) 대신에 고정 IP 주소 사용을 고려하십시오. DHCP를 사용하는 경우 IP 주소 변경이 최소화되어야 합니다.

## IP 구성 제한

다음 기능 및 관리되는 장치의 경우 네트워크 인터페이스를 IPv4 주소로 구성해야 합니다. IPv6 주소는 지원되지 않습니다.

- Lenovo Storage 장치의 펌웨어 업데이트
- ThinkServer 서버
- Lenovo Storage 장치

데이터 포트 또는 관리 포트를 통해 IPv6 링크 로컬을 사용하는 RackSwitch 장치 관리는 지원되지 않습니다.

한 IP 주소 공간을 다른 공간으로 재맵핑하는 네트워크 주소 변환(NAT)은 지원되지 않습니다.

## 네트워크 유형

일반적으로 대부분의 환경은 다음과 같은 유형의 네트워크를 구현합니다. 요구사항에 따라 이러한 네트워크 중 하나만 구현하거나 세 가지 모두 구현할 수 있습니다.

- **관리 네트워크**

  관리 네트워크는 일반적으로 Lenovo XClarity Administrator와 관리 장치의 관리 프로세서 간의 통신을 위해 예약됩니다. 예를 들어 관리 네트워크는 XClarity Administrator, 각 관리 섀시의 CMM 및 XClarity Administrator가 관리하는 각 서버의 베이스보드 관리 컨트롤러가 포함되도록 구성될 수 있습니다.

- **데이터 네트워크**

  데이터 네트워크는 일반적으로 서버에 설치된 운영 체제와 회사 인트라넷, 인터넷 또는 두 가지 모두 간의 통신에 사용됩니다.

- **운영 체제 배포 네트워크**

  경우에 따라서는 운영 체제 배포 네트워크가 서버에 운영 체제를 배포하는 데 필요한 통신을 분리하도록 설정됩니다. 구현된 경우 이 네트워크에는 일반적으로 XClarity Administrator 및 모든 서버 호스트가 포함됩니다.

  분리된 운영 체제 배포 네트워크를 구현하는 대신 관리 네트워크 또는 데이터 네트워크에서 이 기능을 결합할 수 있습니다.

## 네트워크 구성

하나 또는 두 개의 네트워크 인터페이스를 사용하도록 Lenovo XClarity Administrator를 구성할 수 있습니다.

**주의:**

- 장치를 관리 설정한 후 XClarity Administrator IP 주소를 변경하면 XClarity Administrator에서 장치가 오프라인 상태가 될 수 있습니다. IP 주소를 변경하기 전에 모든 장치가 관리 해제되었는지 확인하십시오.
- **중복 IP 주소 검사** 토글을 클릭하여 동일한 서브넷에서 중복 IP 주소 검사를 사용 또는 사용 안 함으로 설정할 수 있습니다. 기본적으로 사용 안 함으로 설정됩니다. 이를 사용하는 경우 XClarity

Administrator의 IP 주소를 변경하거나 관리 중인 다른 장치 또는 동일한 서브넷에서 찾은 다른 장치와 동일한 IP 주소를 가진 장치를 관리하려고 하면 XClarity Administrator에서 경고를 표시합니다.

**참고:** 사용으로 설정하면 XClarity Administrator가 ARP 스캔을 실행하여 동일한 서브넷의 활성 IPv4 장치를 찾습니다. ARP 스캔을 방지하려면 **중복 IP 주소 검사**를 사용 안 함으로 설정하십시오.

- XClarity Administrator을(를) 가상 어플라이언스로 실행할 때 관리 네트워크의 네트워크 인터페이스가 DHCP(Dynamic Host Configuration Protocol)를 사용하도록 구성된 경우 관리 인터페이스 IP 주소는 DHCP 임대가 만료될 때 변경될 수 있습니다. IP 주소가 변경되는 경우 섀시, 랙 및 타워 서버를 관리 해제한 다음 다시 관리해야 합니다. 이러한 문제를 방지하려면 관리 인터페이스를 고정 IP 주소로 변경하거나 DHCP 서버 구성이 DHCP 주소가 MAC 주소를 기준으로 하거나 DHCP 임대가 만료되지 않도록 설정되어야 합니다.
- 운영 체제를 배포하거나 OS 장치 드라이버를 업데이트하는 데 XClarity Administrator를 사용하지 *않을* 경우, **하드웨어만 검색 및 관리** 옵션을 사용하도록 네트워크 인터페이스를 변경하여 Samba 및 Apache 서버를 사용 안 함으로 설정할 수 있습니다. 네트워크 인터페이스를 변경하면 관리 서버가 다시 시작됩니다.
- XClarity Administrator을(를) 컨테이너로 실행하는 경우.
  - 중복 IP 주소 검사를 사용 또는 사용 중지하고, 네트워크 인터페이스 역할을 수정하고, 프록시 설정을 수정하는 것만 가능합니다. 다른 모든 네트워크 설정(IP 주소, 게이트웨이 및 DNS 포함)은 컨테이너 설정에서 정의됩니다.
  - 호스트 시스템에 macvlan 네트워크가 설정되어 있어야 합니다.

XClarity Administrator에는 구현하는 네트워크 토폴로지에 따라 환경에 대해 정의할 수 있는 두 개의 분리된 네트워크 인터페이스가 있습니다. 가상 어플라이언스에서 이러한 네트워크의 이름은 eth0 및 eth1입니다. 컨테이너의 경우 이름을 직접 지정할 수 있습니다.

- 네트워크 인터페이스(Eth0)가 하나만 있는 경우:
  - 인터페이스는 장치 검색 및 관리(예, 서버 구성 및 펌웨어 업데이트)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 베이스보드 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
  - XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
  - 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
  - 운영 체제 이미지를 배포하고 OS 장치 드라이버를 업데이트 하려는 경우, 네트워크 인터페이스는 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 IP 네트워크 연결을 해야 합니다.

    **참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.
- 2개의 네트워크 인터페이스(Eth0 및 Eth1)가 있는 경우:
  - 첫 번째 네트워크 인터페이스(일반적으로 Eth0 인터페이스)는 관리 네트워크에 연결해야 하며 장치 검색 및 관리(서버 구성 및 펌웨어 업데이트 포함)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
  - 두 번째 네트워크 인터페이스(일반적으로 Eth1 인터페이스)는 내부 데이터 네트워크, 공개 데이터 네트워크 또는 둘 다와 통신하도록 구성할 수 있습니다.

- XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
- 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
- 운영 체제 이미지를 배포하고 장치 드라이버를 업데이트하려는 경우, eth1 또는 eth0 인터페이스를 사용하도록 선택할 수 있습니다. 그러나 사용하는 인터페이스에 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결이 있어야 합니다.

  **참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.

다음 테이블은 사용자 환경에 구현된 네트워크 토폴로지 유형을 기반으로 하여 XClarity Administrator 네트워크 인터페이스에 가능한 구성을 표시합니다. 이 테이블을 사용하여 각 네트워크 인터페이스를 정의하는 방법을 판별하십시오.

***표 2. 네트워크 토폴로지 기준 각 네트워크 인터페이스 역할***

| 네트워크 토폴로지 | 인터페이스 1(eth0)의 역할 | 인터페이스 2(eth1)의 역할 |
|---|---|---|
| 컨버지드 네트워크(OS 배포 및 OS 장치 드라이버 업데이트를 지원하는 관리 및 데이터 네트워크) | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색<br>• OS 배포<br>• OS 장치 드라이버 업데이트 | 없음 |
| 분리형 관리 네트워크(OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원 포함) | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색<br>• OS 배포<br>• OS 장치 드라이버 업데이트 | 데이터 네트워크<br>• 없음 |
| OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원을 포함하는 분리형 관리 네트워크 및 데이터 네트워크 | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색 | 데이터 네트워크<br>• OS 배포<br>• OS 장치 드라이버 업데이트 |

*표 2. 네트워크 토폴로지 기준 각 네트워크 인터페이스 역할 (계속)*

| 네트워크 토폴로지 | 인터페이스 1(eth0)의 역할 | 인터페이스 2(eth1)의 역할 |
|---|---|---|
| OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원을 포함하지 않는 분리형 관리 네트워크 및 데이터 네트워크 | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색 | 데이터 네트워크<br>• 없음 |
| 관리 네트워크만(OS 배포 및 OS 장치 드라이버 업데이트는 지원되지 않음) | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색 | 없음 |

## 단일 데이터 및 관리 네트워크

이 네트워크에서는 토폴로지, 관리 통신, 데이터 통신 및 운영 체제 배포가 동일한 네트워크를 통해 이루어집니다. 이 토폴로지는 ***통합*** 네트워크라고 합니다.

**중요:** 공유 데이터 및 관리 네트워크를 구현하면 네트워크 구성에 따라(예, 서버의 트래픽의 우선 순위가 높거나 관리 컨트롤러 트래픽의 우선순위가 낮은 경우) 패킷이 중지되거나 관리 네트워크 연결 문제와 같은 트래픽 중단이 발생할 수 있습니다. 관리 네트워크는 추가 TCP에 UDP 트래픽을 사용합니다. 네트워크 트래픽이 높은 경우 UDP 트래픽의 우선 순위가 더 낮을 수 있습니다.

Lenovo XClarity Administrator를 설치하는 경우 다음 고려사항을 사용하여 eth0 네트워크 인터페이스를 정의하십시오.

- 인터페이스는 장치 검색 및 관리(예, 서버 구성 및 펌웨어 업데이트)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 베이스보드 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
- XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
- 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
- 운영 체제 이미지를 배포하고 OS 장치 드라이버를 업데이트 하려는 경우, 네트워크 인터페이스는 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 IP 네트워크 연결을 해야 합니다.

  **참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.
- 단일 데이터 및 관리 네트워크 토폴로지 또는 가상으로 분리된 데이터 및 관리 네트워크 토폴로지를 구현하는 경우에만 관리 서버 등 XClarity Administrator에 대한 요구사항을 충족하는 모든 시스템에서 XClarity Administrator를 설정할 수 있습니다. 그러나 XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 그런 경우에도 일부 펌웨어만 즉시 활성화가 적용되고 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.

또한 XClarity Administrator에서 동일한 네트워크에 연결하여 중복을 지원하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다.

다음 그림에는 통합 네트워크 토폴로지 예제 구현이 표시되어 있습니다.

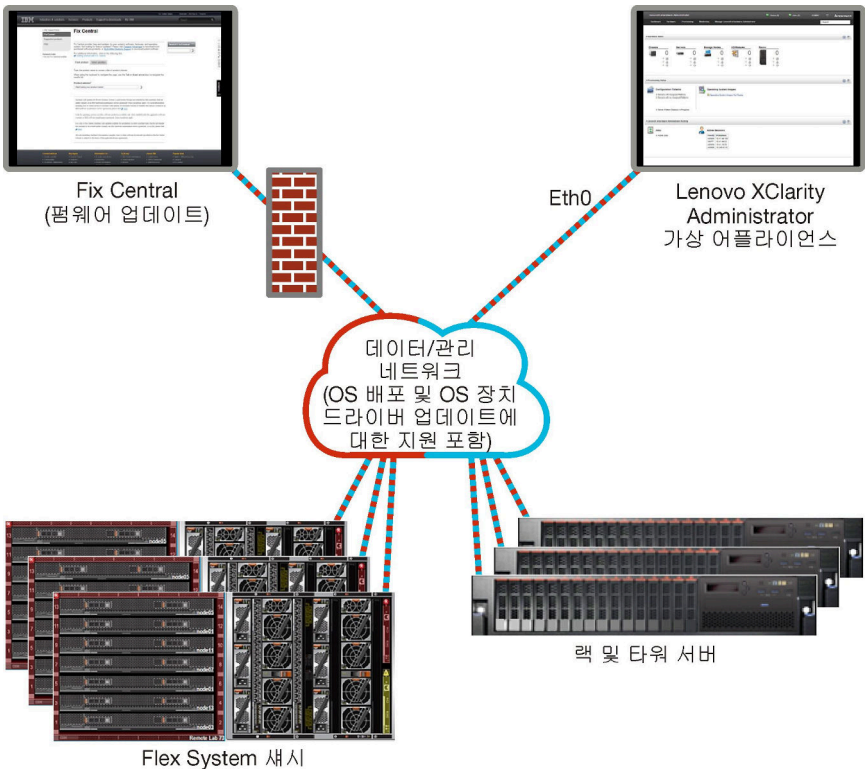



*그림 1. 관리, 데이터 및 운영 체제 배포를 위한 단일 네트워크의 예제 구현*

## 물리적으로 분리된 데이터 및 관리 네트워크

이 네트워크 토폴로지에서는 관리 네트워크 및 데이터 네트워크는 물리적으로 분리된 네트워크이며 운영 체제 배포 네트워크는 관리 네트워크 또는 데이터 네트워크의 일부로 구성됩니다.

Lenovo XClarity Administrator를 설치하는 경우 다음 고려사항을 사용하여 네트워크 설정을 정의하십시오.

- 첫 번째 네트워크 인터페이스(일반적으로 Eth0 인터페이스)는 관리 네트워크에 연결해야 하며 장치 검색 및 관리(서버 구성 및 펌웨어 업데이트 포함)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
- 두 번째 네트워크 인터페이스(일반적으로 Eth1 인터페이스)는 내부 데이터 네트워크, 공개 데이터 네트워크 또는 둘 다와 통신하도록 구성할 수 있습니다.
- XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
- 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
- 운영 체제 이미지를 배포하고 장치 드라이버를 업데이트하려는 경우, eth1 또는 eth0 인터페이스를 사용하도록 선택할 수 있습니다. 그러나 사용하는 인터페이스에 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결이 있어야 합니다.

**참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.

그림 2 "데이터 네트워크의 일부로 운영 체제 네트워크가 포함된 물리적으로 분리된 데이터 및 관리 네트워크의 예제 구현" 22페이지에는 운영 체제 배포 네트워크가 데이터 네트워크의 일부로 구성된 분리된 관리 및 데이터 네트워크의 예제 구현이 표시됩니다.

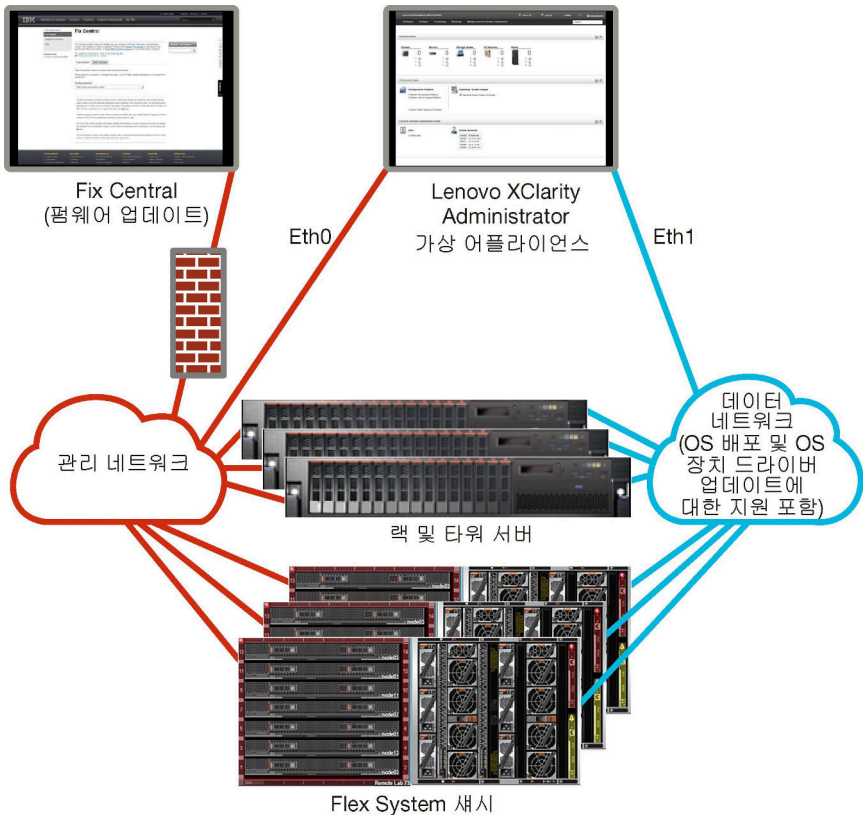



***그림 2. 데이터 네트워크의 일부로 운영 체제 네트워크가 포함된 물리적으로 분리된 데이터 및 관리 네트워크의 예제 구현***

그림 3 "관리 네트워크의 일부로 운영 체제 네트워크가 포함된 물리적으로 분리된 데이터 및 관리 네트워크의 예제 구현" 23페이지에는 운영 체제 배포 네트워크가 관리 네트워크의 일부로 구성된 분리된 관리 및 데이터 네트워크의 다른 예제 구현이 표시됩니다. 이 구현에서는 XClarity Administrator가 데이터 네트워크에 연결할 필요가 없습니다.

**참고:** 운영 체제 배포 네트워크가 데이터 네트워크에 액세스할 수 없는 경우 서버의 추가 인터페이스를 필요 시 서버의 호스트 운영 체제에서 데이터 네트워크로 연결되게 구성하십시오.

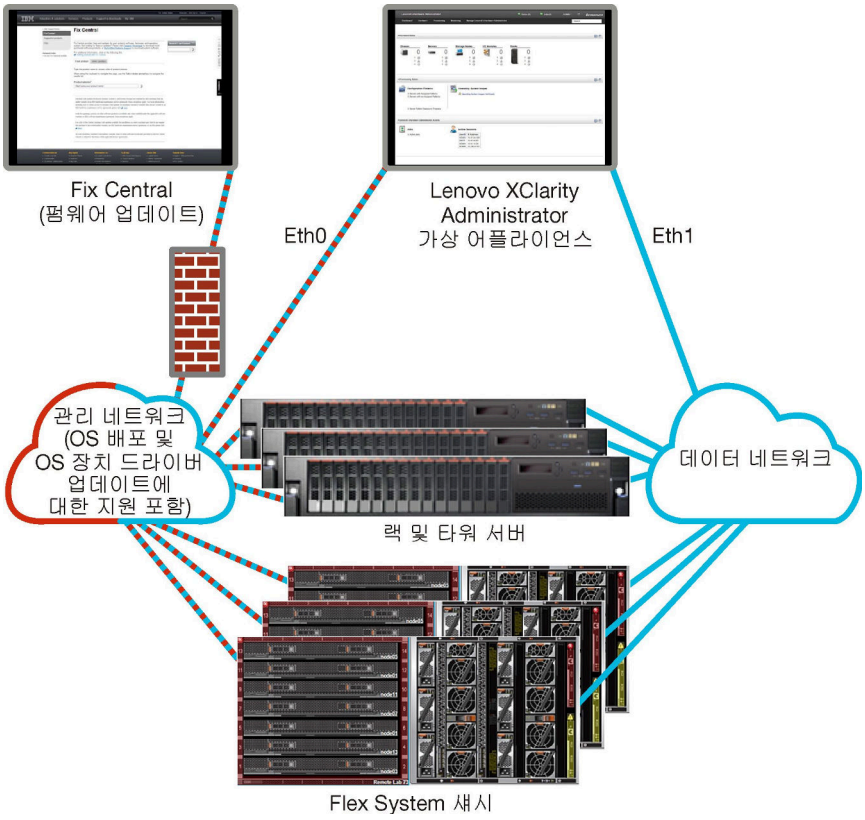



*그림 3. 관리 네트워크의 일부로 운영 체제 네트워크가 포함된 물리적으로 분리된 데이터 및 관리 네트워크의 예제 구현*

## 가상 분리된 데이터 및 관리 네트워크

이 토폴로지에서 데이터 네트워크와 관리 네트워크는 가상 분리되어 있습니다. 데이터 네트워크의 패킷 및 관리 네트워크의 패킷은 동일한 물리적 연결을 통해 전송됩니다. 모든 관리 네트워크 데이터 패킷의 VLAN 태그 지정을 사용하여 두 네트워크 간의 트래픽을 별도로 유지합니다.

**참고:** Lenovo XClarity Administrator가 섀시의 관리되는 서버에서 실행 중인 호스트에 설치된 경우 XClarity Administrator를 사용하여 한 번에 전체 섀시에 펌웨어 업데이트를 적용할 수 없습니다. 펌웨어 업데이트가 적용되면 호스트 시스템을 다시 시작해야 합니다.

XClarity Administrator를 설치하는 경우 다음 고려사항을 사용하여 네트워크 설정을 정의하십시오.

- 첫 번째 네트워크 인터페이스(일반적으로 Eth0 인터페이스)는 관리 네트워크에 연결해야 하며 장치 검색 및 관리(서버 구성 및 펌웨어 업데이트 포함)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
- 두 번째 네트워크 인터페이스(일반적으로 Eth1 인터페이스)는 내부 데이터 네트워크, 공개 데이터 네트워크 또는 둘 다와 통신하도록 구성할 수 있습니다.
- XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
- 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
- 운영 체제 이미지를 배포하고 장치 드라이버를 업데이트하려는 경우, eth1 또는 eth0 인터페이스를 사용하도록 선택할 수 있습니다. 그러나 사용하는 인터페이스에 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결이 있어야 합니다.

**참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.

- 단일 데이터 및 관리 네트워크 토폴로지 또는 가상으로 분리된 데이터 및 관리 네트워크 토폴로지를 구현하는 경우에만 관리 서버 등 XClarity Administrator에 대한 요구사항을 충족하는 모든 시스템에서 XClarity Administrator를 설정할 수 있습니다. 그러나 XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 그런 경우에도 일부 펌웨어만 즉시 활성화가 적용되고 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.

그림 4 "데이터 네트워크의 일부로 운영 체제 네트워크가 포함된 가상으로 분리된 데이터 및 관리 네트워크의 예제 구현" 24페이지 에는 운영 체제 배포 네트워크가 데이터 네트워크의 일부로 구성된 가상으로 분리된 관리 및 데이터 네트워크의 예제 구현이 표시됩니다. 이 예제에서는 XClarity Administrator가 섀시의 관리되는 서버에 설치됩니다.

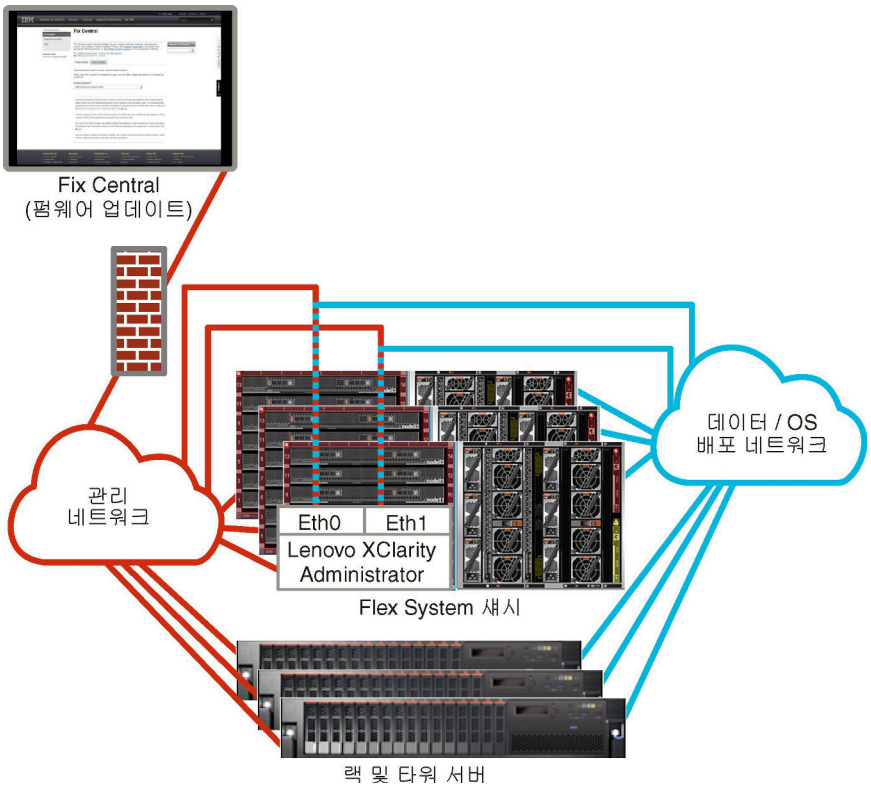



***그림 4. 데이터 네트워크의 일부로 운영 체제 네트워크가 포함된 가상으로 분리된 데이터 및 관리 네트워크의 예제 구현***

그림 5 "관리 네트워크의 일부로 운영 체제 네트워크가 포함된 가상으로 분리된 관리 및 데이터 네트워크의 예제 구현" 25페이지 에는 운영 체제 배포 네트워크가 관리 네트워크의 일부로 구성된 가상으로 분리된 관리 및 데이터 네트워크의 예제 구현이 표시되고, XClarity Administrator은 섀시의 관리 서버에 설치됩니다. 이 구현에서는 XClarity Administrator가 데이터 네트워크에 연결할 필요가 없습니다.

**참고:** 운영 체제 배포 네트워크가 데이터 네트워크에 액세스할 수 없는 경우 서버의 추가 인터페이스를 필요 시 서버의 호스트 운영 체제에서 데이터 네트워크로 연결되게 구성하십시오.

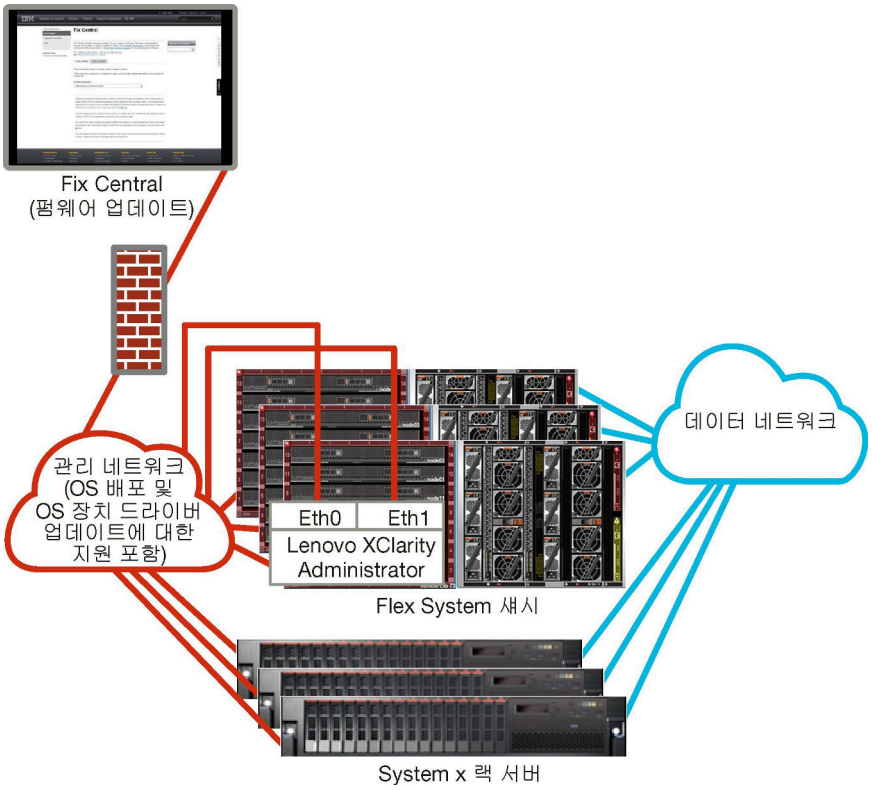



*그림 5. 관리 네트워크의 일부로 운영 체제 네트워크가 포함된 가상으로 분리된 관리 및 데이터 네트워크의 예제 구현*

## 관리 전용 네트워크

이 토폴로지에서 Lenovo XClarity Administrator는 관리 네트워크에만 액세스할 수 있습니다. 데이터 네트워크에 액세스할 수 없습니다. 그러나 XClarity Administrator는 운영 체제 이미지를 XClarity Administrator에서 관리 서버에 배포하려는 경우 운영 체제 배포 네트워크에 액세스할 수 있어야 합니다.

XClarity Administrator를 설치하고 네트워크 설정을 정의하는 경우 eth0 네트워크 인터페이스를 구성하여 다음과 같이 해야 합니다.

- 인터페이스는 장치 검색 및 관리(예, 서버 구성 및 펌웨어 업데이트)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 베이스보드 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
- XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
- 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
- 운영 체제 이미지를 배포하고 OS 장치 드라이버를 업데이트 하려는 경우, 네트워크 인터페이스는 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 IP 네트워크 연결을 해야 합니다.

  **참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.

또한 XClarity Administrator에서 동일한 네트워크에 연결하여 중복을 지원하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다.

그림 6 "운영 체제 배포가 지원되지 않는 관리 전용 네트워크의 예제 구현" 26페이지에는 XClarity Administrator의 운영 체제 배포가 지원되지 않는 관리 전용 네트워크에 대한 예제 구현이 표시됩니다.

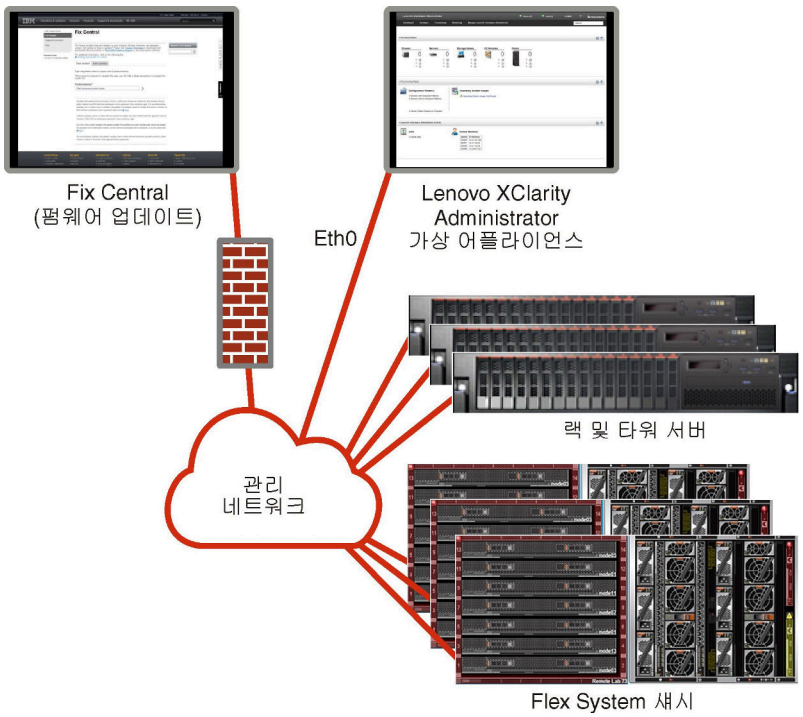



***그림 6. 운영 체제 배포가 지원되지 않는 관리 전용 네트워크의 예제 구현***

그림 6 "운영 체제 배포가 지원되지 않는 관리 전용 네트워크의 예제 구현" 26페이지에는 XClarity Administrator의 운영 체제 배포가 지원되는 관리 전용 네트워크에 대한 예제 구현이 표시됩니다.

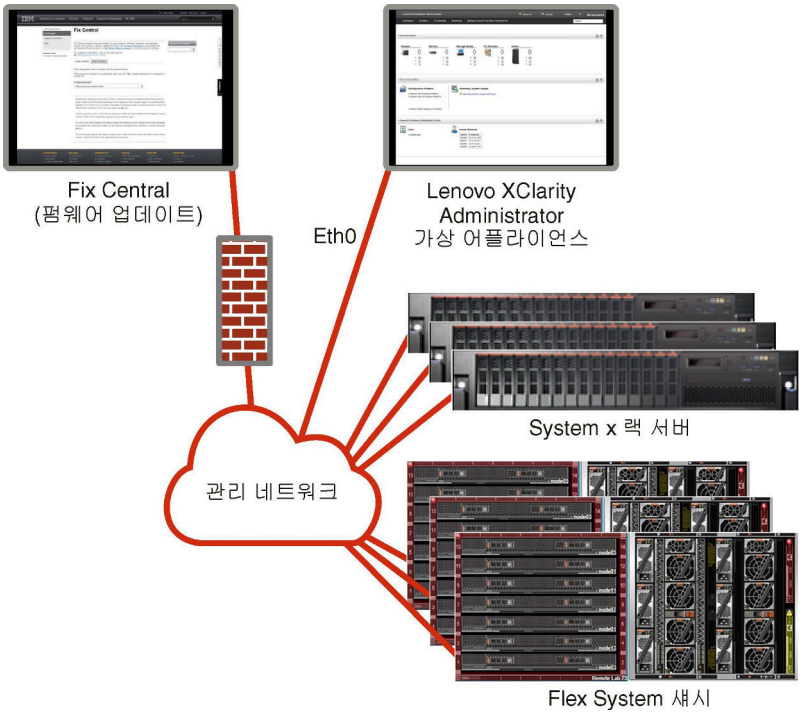



*그림 7. 운영 체제 배포가 지원되는 관리 전용 네트워크의 예제 구현*

## 보안 고려사항

Lenovo XClarity Administrator 및 모든 관리 장치의 보안을 계획하십시오.

## encapsulation 관리

Lenovo XClarity Administrator에서 Lenovo 섀시 및 서버를 관리하는 경우 Lenovo XClarity Administrator를 구성하여 Lenovo XClarity Administrator의 수신 요청만 승인하도록 장치 방화벽 규칙을 변경할 수 있습니다. 이것을 *encapsulation*이라 합니다. 또한 Lenovo XClarity Administrator에서 이미 관리되고 있는 섀시 및 서버에서 encapsulation을 사용 또는 사용 안 함으로 설정할 수 있습니다.

Encapsulation을 지원하는 장치에서 사용으로 설정된 경우 Lenovo XClarity Administrator는 장치 encapsulation 모드를 "encapsulationLite"로 변경하고 장치의 방화벽 규칙을 변경하여 이 Lenovo XClarity Administrator의 수신 요청으로만 제한합니다.

사용 안 함으로 설정된 경우 encapsulation 모드는 "일반"으로 설정됩니다. Encapsulation이 이전에 장치에서 사용으로 설정된 경우 encapsulation 방화벽 규칙이 제거됩니다.

**주의:** Encapsulation을 사용하고 장치를 관리 해제하기 전에 XClarity Administrator를 사용할 수 없게 되는 경우 encapsulation을 사용하지 않도록 필요한 단계를 취해 장치와의 통신을 설정해야 합니다. 복구 절차는 XClarity Administrator 온라인 설명서에서 관리 서버 오류 후 CMM으로 섀시 관리 복구 및 관리 서버 오류 후 랙 또는 타워 서버 관리 복구의 내용을 참조하십시오.

**참고:**

- Encapsulation은 스위치, 스토리지 장치 및 Lenovo 이외 섀시 및 서버에에서 지원되지 않습니다.
- 관리 네트워크 인터페이스가 DHCP(Dynamic Host Configuration Protocol)를 사용하도록 구성되어 있고 encapsulation이 사용으로 설정된 경우 랙 서버를 관리하는 데 오랜 시간이 걸릴 수 있습니다.

Encapsulation에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 Encapsulation 사용의 내용을 참조하십시오.

# 암호화 관리

암호 관리는 Lenovo XClarity Administrator와 관리 장치(예, 섀시, 서버 및 Flex 스위치) 간에 보안 통신이 처리되는 방식을 제어하는 통신 모드와 프로토콜로 구성됩니다.

### 암호화 알고리즘

XClarity Administrator는 안전한 네트워크 연결을 위해 TLS 1.2 및 강력한 암호화 알고리즘을 지원합니다.

보안 강화를 위해 고강도 암호만 지원됩니다. 클라이언트 운영 체제와 웹 브라우저가 다음 암호 세트 중 하나를 지원해야 합니다.

- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

### 관리 서버의 암호화 모드

이 설정은 관리 서버에서 보안 통신에 사용할 모드를 결정합니다.

- **호환성**. 이 모드는 기본값입니다. NIST SP 800-131A 준수에 필요한 엄격한 보안 표준을 구현하지 않는 이전 펌웨어 버전, 브라우저 및 기타 네트워크 클라이언트와 호환됩니다.
- NIST SP 800-131A. 이 모드는 NIST SP 800-131A 표준을 준수하도록 설계되어 있습니다. XClarity Administrator는 항상 내부적으로 강력한 암호를 사용하고 사용 가능한 경우 강력한 암호 네트워크 연결을 사용하도록 설계되어 있습니다. 그러나 이 모드에서는 SHA-1 또는 이보다 약한 해시로 서명된 TLS(Transport Layer Security) 인증서 거부 등 NIST SP 800-131A가 승인하지 않는 암호를 사용하는 네트워크 연결은 허용되지 않습니다.

  이 모드를 선택하는 경우:

  - 포트 8443을 제외한 모든 포트의 경우 모든 TLS CBC 암호 및 Perfect Forward Secrecy를 지원하지 않는 모든 암호가 비활성화됩니다.
  - 이벤트 알림은 일부 모바일 장치 구독에는 성공적으로 푸시되지 않을 수 있습니다(XClarity Administrator 온라인 설명서에서 모바일 장치에 이벤트 전달 참조). Android 및 iOS와 같은 외부 서비스는 NIST SP 800-131A 모드의 더 엄격한 요구사항을 준수하지 않는 알고리즘인 SHA-1로 서명된 인증서를 제공합니다. 결과적으로 이러한 서비스에 대한 연결은 인증서 예외 또는 핸드셰이크 오류로 실패할 수 있습니다.

  NIST SP 800-131A 준수에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 NIST 800-131A 준수 구현의 내용을 참조하십시오.

관리 서버의 보안 모드 설정에 대한 자세한 정보는 XClarity Administrator 온라인 설명서의 암호 모드 및 통신 프로토콜 설정 내용을 참조하십시오.

### 관리되는 서버의 보안 모드

이 설정은 관리되는 서버에서 보안 통신에 사용할 모드를 결정합니다.

- **호환성 보안**. 서비스 및 클라이언트에 CNSA/FIPS와 호환되지 않는 암호가 필요한 경우 이 모드를 선택하십시오. 이 모드는 광범위한 암호화 알고리즘을 지원하며 모든 서비스를 활성화할 수 있습니다.
- NIST SP 800-131A. NIST SP 800-131A 표준을 준수하도록 하려면 이 모드를 선택하십시오. 여기에는 RSA 키를 2048비트 이상으로 제한하고, 디지털 서명에 사용되는 해시를 SHA-256 이상으로 제한하며, NIST 승인 대칭적 암호화 알고리즘만 사용되도록 하는 것 등이 포함됩니다. 이 모드에서는 SSL/TLS 모드를 TLS 1.2 **서버 클라이언트**로 설정해야 합니다.

  이 모드는 XCC2가 있는 서버에 지원되지 *않습니다*.
- **표준 보안**. (XCC2가 있는 서버만 해당) XCC2가 있는 서버의 기본 보안 모드입니다. FIPS 140-3 표준을 준수하도록 하려면 이 모드를 선택하십시오. XCC가 FIPS 140-3 검증 모드에서 작동하려면 FIPS 140-3 수준 암호화를 지원하는 서비스만 활성화할 수 있습니다. FIPS 140-2/140-3 수준 암호화를 지원하지 않는 서비스는 기본적으로 비활성화되지만 필요한 경우 활성화할 수 있습니다. 비 FIPS 140-3 수준 암호화를 사용하는 서비스가 활성화된 경우 XCC는 FIPS 140-3 검증 모드에서 작동 불가합니다. 이 모드에는 FIPS 수준 인증서가 필요합니다.
- Enterprise Strict **보안**. (XCC2가 있는 서버만 해당) 가장 안전한 모드입니다. CNSA 표준을 준수하도록 하려면 이 모드를 선택하십시오. CNSA 수준 암호화를 지원하는 서비스만 허용됩니다. 비보안 서비스는 기본적으로 비활성화되며 활성화할 수 없습니다. 이 모드에는 CNSA 수준 인증서가 필요합니다.

  Enterprise Strict **보안** 모드에서 XClarity Administrator는 서버에 RSA-3072/SHA-384 인증서 서명을 사용합니다.

  **중요:**

  - XCC2 Feature On Demand 키를 선택한 각 XCC2가 있는 서버에 설치하여 이 모드를 사용해야 합니다.
  - 이 모드에서 XClarity Administrator가 자체 서명된 인증서를 사용하는 경우 XClarity Administrator는 RSA3072/SHA384 기반 루트 인증서와 서버 인증서를 사용해야 합니다. XClarity Administrator가 외부 서명 인증서를 사용하는 경우 XClarity Administrator는 RSA3072/SHA384 기반 CSR을 생성하고 외부 CA에 연결하여 RSA3072/SHA384 기반의 새 서버 인증서에 서명해야 합니다.
  - XClarity Administrator가 RSA3072/SHA384 기반 인증서를 사용하는 경우 XClarity Administrator는 Flex System 섀시(CMMS) 및 서버, ThinkSystem 서버, ThinkServer 서버, System x M4 및 M5 서버, Lenovo ThinkSystem DB 시리즈 스위치, Lenovo RackSwitch, Flex System 스위치, Mellanox 스위치, ThinkSystem DE/DM 스토리지 장치, IBM 테이프 라이브러리 및 22C 이전의 펌웨어로 플래시된 ThinkSystem SR635/SR655 서버 이외의 장치 연결을 끊을 수도 있습니다. 연결이 끊긴 장치를 계속 관리하려면 RSA2048/SHA384 기반 인증서로 다른 XClarity Administrator 인스턴스를 설정하십시오.

다음과 같은 암호화 모드 변경의 영향을 고려하십시오.

- **호환성 보안** 모드 또는 **표준 보안** 모드에서 Enterprise Strict **보안** 모드로 변경하는 것은 지원되지 않습니다.
- **호환성 보안** 모드에서 **표준 보안** 모드로 업그레이드하는 경우 가져온 인증서 또는 SSH 공개 키가 호환되지 않으면 경고가 표시되지만 **표준 보안** 모드로 업그레이드할 수는 있습니다.
- Enterprise Strict **보안**에서 **호환성 보안** 또는 **표준 보안** 모드로 다운그레이드하는 경우.
  - 해당 보안 모드를 적용하기 위해 서버가 자동으로 다시 시작됩니다.
  - XCC2에서 strict 모드 FoD 키가 없거나 만료된 경우 및 XCC2가 자체 서명된 TLS 인증서를 사용하는 경우에는 XCC2가 Standard Strict 호환 알고리즘을 기반으로 자체 서명된 TLS 인증서를 다시 생성합니다. XClarity Administrator에서는 인증서 오류로 인한 연결 실패를 표시합니다. 신뢰할 수 없는 인증서 오류를 해결하려면 XClarity Administrator 온라인 설명서의 신뢰할 수 없는 서버 인증서 해결 내용을 참조하십시오. XCC2가 사용자 지정 TLS 인증서를 사용하는 경우 XCC2는 다운그레이드를 허용하며 **표준 보안** 모드 암호를 기반으로 하는 서버 인증서를 가져와야 한다고 경고가 표시됩니다.
- NIST SP 800-131A 모드는 XCC2가 있는 서버에 지원되지 않습니다.

- XClarity Administrator의 암호화 모드가 TLS v1.2로 설정된 경우 및 관리되는 인증을 사용하는 관리되는 서버에 보안 모드가 TLS v1.2로 설정된 경우, XClarity Administrator 또는 XCC를 사용하여 서버 보안 모드를 TLS v1.3로 변경하면 서버가 영구적으로 오프라인 상태가 됩니다.
- XClarity Administrator의 암호화 모드가 TLS v1.2로 설정되어 있고 보안 모드가 TLS v1.3으로 설정된 XCC가 있는 서버를 관리하려고 하면 관리되는 인증을 사용하여 서버를 관리할 수 없습니다.

다음 장치의 보안 설정을 변경할 수 있습니다.
- Intel 또는 AMD 프로세서가 탑재된 Lenovo ThinkSystem 서버(SR635/SR655 제외)
- Lenovo ThinkSystem V2 서버
- Intel 또는 AMD 프로세서가 탑재된 Lenovo ThinkSystem V3 서버
- Lenovo ThinkEdge SE350/SE450 서버
- Lenovo System x 서버

관리되는 서버의 보안 모드 설정에 대한 자세한 정보는 XClarity Administrator 온라인 설명서의 서버의 보안 설정 구성 내용을 참조하십시오.

# 보안 인증서

Lenovo XClarity Administrator은(는) XClarity Administrator 및 관리되는 장치(예: System x 서버의 섀시와 서비스 프로세서) 간의 안전하고 신뢰할 수 있는 통신뿐만 아니라 사용자의 XClarity Administrator 또는 다른 서비스와의 통신을 위해 SSL 인증서를 사용합니다. 기본적으로 XClarity Administrator, CMM 및 베이스보드 관리 컨트롤러는 내부 인증 기관에서 자체 서명하고 발행한 XClarity Administrator가 생성한 인증서를 사용합니다.

XClarity Administrator의 모든 인스턴스에서 고유 생성되는 기본 자체 서명 서버 인증서는 여러 환경에서 충분한 보안을 제공합니다. XClarity Administrator가 대신 인증서를 관리하게 하거나 더 적극적인 역할을 하여 서버 인증서를 사용자 지정 또는 교체할 수 있습니다. XClarity Administrator는 환경에 맞게 인증서를 사용자 지정하는 옵션을 제공합니다. 예를 들어 다음 사항을 선택할 수 있습니다.

- 조직에 고유한 값을 사용하는 내부 인증 기관 또는 최종 서버 인증서를 재생성하여 새로운 키 쌍을 생성합니다.
- 선택한 인증 기관에 보내 사용자 지정 인증서에 서명할 수 있는 CSR(인증서 서명 요청)을 생성합니다. 이 인증서는 XClarity Administrator에 업로드하여 호스팅되는 모든 서비스에 대한 최종 서버 인증서로 사용할 수 있습니다.
- 웹 브라우저의 신뢰할 수 있는 인증서 목록으로 해당 인증서를 가져올 수 있도록 로컬 시스템에 서버 인증서를 다운로드합니다.

인증서에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 보안 인증서 작업의 내용을 참조하십시오.

# 인증

### 지원되는 인증 서버

*인증 서버*는 사용자 자격 증명을 인증하는 데 사용되는 사용자 레지스트리입니다. Lenovo XClarity Administrator은(는) 다음 인증 서버 유형을 지원합니다.

- **로컬 인증 서버**. 기본적으로 XClarity Administrator는 관리 서버에 있는 내장 LDAP(Lightweight Directory Access Protocol) 서버를 사용하도록 구성됩니다.
- **외부 LDAP 서버**. 현재 Microsoft Active Directory 및 OpenLDAP만 지원됩니다. 이 서버는 관리 네트워크에 연결된 아웃보드 Microsoft Windows 서버에 상주해야 합니다. 외부 LDAP 서버가 사용되는 경우 로컬 인증 서버가 사용 불가능합니다.

  **주의:** Active Directory 바인딩 방법을 로그인 자격 증명을 사용하도록 구성하려면 각 관리되는 서버에 대한 베이스보드 관리 컨트롤러는 2016년 9월 이후의 펌웨어를 실행해야 합니다.

- **외부 ID 관리 시스템**. 현재 CyberArk만 지원됩니다.

  ThinkSystem 또는 ThinkAgile 서버의 사용자 계정이 CyberArk에 온보딩된 경우, 관리되는 인증 또는 로컬 인증을 사용하여 관리하도록 서버를 처음 설정하면 XClarity Administrator이(가) 서버에 로그인하기 위해 CyberArk에서 자격 증명을 검색하도록 선택할 수 있습니다. CyberArk에서 자격 증명을 검색하려면 먼저 CyberArk 경로가 XClarity Administrator에 정의되어 있어야 하며 클라이언트 인증서를 통한 TLS 상호 인증을 사용하여 CyberArk와 XClarity Administrator 간에 상호 신뢰가 만들어져야 합니다.
- **외부 SAML ID 공급자**. 현재 Microsoft Active Directory Federation Services(AD FS)만 지원됩니다. 사용자 이름 및 암호를 입력하는 것 외에 다중 인증을 설정하여 PIN 코드를 요구하고 스마트 카드와 클라이언트 인증서를 판독하여 추가 보안을 지원할 수 있습니다. SAML ID 공급자를 사용하는 경우 로컬 인증 서버가 사용 안 함으로 설정되지 않습니다. 로컬 사용자 계정은 PowerShell 및 REST API 인증 및 외부 인증을 사용할 수 있는 경우 복구를 위해서는 관리 섀시 또는 서버에 직접 로그인해야 합니다(Encapsulation을 사용할 수 없는 경우).

  외부 LDAP 서버 및 외부 ID 공급자를 둘 다 사용할 수 있습니다. 둘 다 사용할 수 있는 경우 외부 LDAP 서버를 사용하여 관리 장치에 직접 로그인하고 ID 공급자를 사용하여 관리 서버에 로그인합니다.

인증 서버에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 인증 서버 관리의 내용을 참조하십시오.

### 장치 인증

기본적으로 장치는 XClarity Administrator 관리되는 인증을 사용하여 장치에 로그인하도록 관리됩니다. 랙 서버 및 Lenovo 섀시를 관리할 때 로컬 인증 또는 관리 인증을 사용하여 장치에 로그인하도록 선택할 수 있습니다.

- 랙 서버, Lenovo 섀시 및 Lenovo 랙 스위치에 *로컬 인증*을 사용하는 경우, XClarity Administrator는 저장된 자격 증명을 사용하여 장치를 인증합니다. *저장된 자격 증명*은 장치의 활성 사용자 계정 또는 Active Directory 서버의 사용자 계정입니다.

  로컬 인증을 사용하여 장치를 관리하기 전에 장치의 활성 사용자 계정 또는 Active Directory 서버의 사용자 계정과 일치하는 XClarity Administrator다음 위치에 저장된 자격 증명을 만들어야 합니다(XClarity Administrator온라인 설명서의 저장된 자격 증명 관리 참조).

  **참고:**

  – RackSwitch 장치는 인증을 위해 저장된 자격 증명만 지원합니다. XClarity Administrator 사용자 자격 증명은 지원되지 않습니다.
- *관리되는 인증*을 사용하면 로컬 자격 증명 대신 XClarity Administrator 인증 서버의 자격 증명을 사용하여 여러 장치를 관리하고 모니터링할 수 있습니다. 장치(ThinkServer 서버, System x M4 서버 및 스위치 이외의 장치)에 관리되는 인증을 사용하는 경우 XClarity Administrator는 중앙 집중식 관리를 위해 XClarity Administrator 인증 서버를 사용하도록 장치 및 설치된 구성 요소를 구성합니다.

  – 관리되는 인증을 사용으로 설정하면 수동으로 입력되거나 저장된 자격 증명을 사용하여 장치를 관리할 수 있습니다(XClarity Administrator 온라인 설명서에서 사용자 계정 관리 및 저장된 자격 증명 관리 참조).

    저장된 자격 증명은 XClarity Administrator가 장치에 LDAP 설정을 구성할 때까지만 사용됩니다. 그 후에는 저장된 자격 증명을 변경해도 장치를 관리하거나 모니터링하는 데 아무런 영향을 주지 않습니다.

    **참고:** 장치에 대해 관리되는 인증을 사용하는 경우 XClarity Administrator를 사용하여 해당 장치에 대한 저장된 자격 증명을 편집할 수 없습니다.

  – 로컬 또는 외부 LDAP 서버를 XClarity Administrator 인증 서버로 사용하는 경우 인증 서버에 정의된 사용자 계정은 XClarity Administrator 도메인에서 XClarity Administrator, CMM 및 베이스보드 관리 컨트롤러에 로그인하는 데 사용됩니다. 로컬 CMM 및 관리 컨트롤러 사용자 계정은 사용하지 않습니다.

- SAML 2.0 ID 공급자를 XClarity Administrator 인증 서버로 사용하는 경우 SAML 계정은 관리되는 장치에 액세스할 수 없습니다. 하지만 SAML ID 공급자와 LDAP 서버를 함께 사용할 때 ID 공급자가 LDAP 서버에 존재하는 계정을 사용하는 경우 LDAP 사용자 계정을 사용하여 관리되는 장치에 로그인할 수 있고 SAML 2.0이 제공하는 고급 인증 방식(예, 다중 인증 및 SSO(Single sign-on))을 사용하여 XClarity Administrator에 로그인할 수 있습니다.
- SSO(Single sign-on)를 사용하면 XClarity Administrator에 이미 로그인한 사용자가 베이스보드 관리 컨트롤에 자동으로 로그인할 수 있습니다. ThinkSystem 또는 ThinkAgile 서버가 XClarity Administrator에 의해 관리되는 경우 서버가 CyberArk 암호로 관리되지 않는 한 SSO(Single sign-on)는 기본적으로 사용됩니다. 관리되는 모든 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용 또는 사용하지 않도록 전역 설정을 구성할 수 있습니다. 특정 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용하면 모든 ThinkSystem 및 ThinkAgile 서버에 대한 전역 설정이 재정의됩니다(XClarity Administrator 온라인 설명서의 서버 관리 참조).

  **참고:** 인증에 CyberArk ID 관리 시스템을 사용하면 SSO(Single sign-on)가 자동으로 비활성화됩니다.
- ThinkSystem SR635 및 SR655 서버에 관리되는 인증이 사용되는 경우:
  - 베이스보드 관리 컨트롤러 펌웨어는 최대 5개의 LDAP 사용자 역할을 지원하고 XClarity Administrator는 관리하는 동안 다음 LDAP 사용자 역할을 서버에 추가합니다. **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** 및 **lxc-os-admin**.

    ThinkSystem SR635 및 SR655 서버와 통신하려면 사용자가 지정된 LDAP 사용자 역할 중 하나 이상으로 지정되어야 합니다.
  - 관리 컨트롤러 펌웨어는 서버의 로컬 사용자와 동일한 사용자 이름을 가진 LDAP 사용자를 지원하지 않습니다.
- ThinkServer 및 System x M4 서버의 경우, XClarity Administrator 인증 서버가 사용되지 않습니다. 대신 장치에 접두사가 "LXCA_"이고 무작위 문자열이 따르는 IPMI 계정이 만들어집니다. (기존 로컬 IPMI 사용자 계정은 사용 안 함으로 설정되지 않습니다.) ThinkServer 서버를 관리 해제하는 경우 "LXCA_" 사용자 계정을 사용할 수 없는 경우 접두사 "LXCA_"가 접두사 "DISABLED_"로 교체됩니다. ThinkServer 서버가 다른 인스턴스로 관리되는지 판별하기 위해 XClarity Administrator는 접두사 "LXCA_"가 있는 IPMI 계정이 있는지 확인합니다. 관리 ThinkServer 서버를 강제 관리하는 경우 "LXCA_" 접두사가 포함된 장치의 모든 IPMI 계정을 사용할 수 없고 이름이 변경됩니다. 더 이상 사용되지 않는 IPMI 계정을 지울 것을 고려해 보십시오.

  수동으로 입력한 자격 증명을 사용하는 경우 XClarity Administrator는 저장된 자격 증명을 자동으로 만들고 이 저장된 자격 증명을 사용하여 장치를 관리합니다.

  **참고:** 장치에 대해 관리되는 인증을 사용하는 경우 XClarity Administrator를 사용하여 해당 장치에 대한 저장된 자격 증명을 편집할 수 없습니다.
  - 수동으로 입력한 자격 증명을 사용하여 장치를 관리할 때마다 이전 관리 프로세스 중에 해당 장치에 대해 다른 저장된 자격 증명이 만들어진 경우에도 새로운 저장된 자격 증명이 만들어집니다.
  - 장치를 관리 해제할 때 XClarity Administrator는 관리 프로세스 중에 해당 장치에 대해 자동으로 만들어진 저장된 자격 증명은 삭제하지 않습니다.

### 복구 사용자 계정

복구 암호를 지정하면 XClarity Administrator가 로컬 CMM 또는 관리 컨트롤러 사용자 계정을 사용 안 함으로 설정하고 이후의 인증을 위해 장치에 새 복구 사용자 계정(RECOVERY_ID)을 만듭니다. 관리 서버에 오류가 발생하는 경우 RECOVERY_ID 계정을 사용하여 장치에 로그인하고 복구 작업을 수행하여 관리 노드가 복원 또는 교체될 때까지 장치 계정 관리 기능을 복원할 수 있습니다.

RECOVERY_ID 사용자 계정이 있는 장치를 관리 해제하면 모든 로컬 사용자 계정이 사용이 사용 설정되고 RECOVERY_ID 계정이 삭제됩니다.

- 사용 안 함으로 설정된 로컬 사용자 계정을 변경하는 경우(예, 암호를 변경하는 경우) 이 변경은 RECOVERY_ID 계정에 영향을 주지 않습니다. 관리되는 인증 모드에서 RECOVERY_ID 계정은 활성화되고 작동 가능한 유일한 사용자 계정입니다.
- RECOVERY_ID 계정은 예를 들어 관리 서버에 오류가 발생하거나 네트워크 문제로 장치가 XClarity Administrator와 통신하여 사용자를 인증하지 못하는 경우와 같은 비상 시에만 사용하십시오.
- 장치를 발견하면 RECOVERY_ID 암호가 지정됩니다. 나중에 사용하도록 암호를 기록해야 합니다.

장치 관리 복구에 대한 정보는 XClarity Administrator 온라인 설명서에서 관리 서버 오류 후 CMM으로 섀시 관리 복구 및 관리 서버 오류 후 랙 또는 타워 서버 관리 복구의 내용을 참조하십시오.

## 사용자 계정 및 역할 그룹

*사용자 계정*은 로그인하고 Lenovo XClarity Administrator 및 모든 관리 섀시 및 서버를 관리하는 데 사용됩니다. XClarity Administrator 사용자 계정은 인증과 승인이라는 두 개의 상호 의존적인 프로세스를 거칩니다.

*인증*은 사용자의 자격 증명을 확인하는 보안 메커니즘입니다. 인증 프로세스는 구성된 인증 서버에 저장된 사용자 자격 증명을 사용합니다. 또한 승인되지 않은 관리 서버 또는 비인증 관리 시스템 응용 프로그램이 리소스에 액세스하지 못하도록 방지합니다. 인증 후 사용자는 XClarity Administrator에 액세스할 수 있습니다. 그러나 특정 리소스에 액세스하거나 특정 작업을 수행하려면 사용자는 적절한 승인이 필요합니다.

*승인*은 인증된 사용자의 권한을 검사하고 역할 그룹의 사용자 멤버십에 따라 리소스에 대한 액세스 권한을 제어합니다. *역할 그룹*은 인증 서버에서 정의 및 관리되는 사용자 계정 세트에 특정 역할을 할당하는 데 사용됩니다. 예를 들어 사용자가 감독자 권한이 있는 역할 그룹 멤버인 경우 해당 사용자는 XClarity Administrator에서 사용자 계정을 만들고 편집하고 삭제할 수 있습니다. 사용자가 오퍼레이터 권한이 있는 경우 사용자는 사용자 계정 정보만 볼 수 있습니다.

사용자 계정 및 역할 그룹에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 사용자 계정 관리의 내용을 참조하십시오.

## 사용자 계정 보안

사용자 계정 설정은 암호 복잡도, 계정 잠금 및 웹 세션 비활성 제한시간을 제어합니다. 계정 보안 설정 값을 변경할 수 있습니다.

계정 보안 설정에 대한 자세한 정보는 Lenovo XClarity Administrator 온라인 설명서에서 사용자 계정 보안 설정 변경의 내용을 참조하십시오.

---

# 고가용성 고려사항

Lenovo XClarity Administrator에 대해 고가용성을 설정하려면 호스트 운영 체제 또는 컨테이너 환경의 일부인 고가용성 기능을 사용하십시오.

### Docker

Docker Datacenter를 사용하여 Docker Engine에서 실행 중인 XClarity Administrator 컨테이너를 위한 고가용성 환경을 설정할 수 있습니다. Docker Datacenter 고가용성에 대한 자세한 정보는 Docker Datacenter 웹 페이지의 고가용성 아키텍처 및 앱의 내용을 참고하십시오.

### Citrix

Citrix 환경에 제공되는 고가용성 기능을 사용하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 고가용성 구현(Citrix)의 내용을 참조하십시오.

### KVM(CentOS, RedHat 및 Ubuntu)

OpenStack을 사용할 수 있습니다. 또는 고가용성 환경이 이미 있는 경우 계속해서 내부 프로세스를 사용할 수 있습니다. OpenStack 고가용성에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 고가용성 구현(KVM)의 내용을 참조하십시오.

### Microsoft Hyper-V

ESXi 환경에 제공되는 고가용성 기능을 사용하십시오. 정보는 XClarity Administrator 온라인 설명서에서 고가용성 구현(Microsoft Hyper-V)의 내용을 참조하십시오.

### Nutanix AHV

Nutanix AHV 환경에 제공되는 가상 컴퓨터 고가용성 기능을 사용하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 고가용성 구현(Nutanix)의 내용을 참조하십시오.

### VMware ESXi

VMware 고가용성 환경에서는 여러 호스트가 클러스터로 구성됩니다. 공유 스토리지는 클러스터의 호스트에 가상 컴퓨터(VM)의 디스크 이미지를 제공하는 데 사용됩니다. VM은 한 번에 하나의 호스트에서만 실행됩니다. VM에 문제가 있는 경우 해당 VM의 다른 인스턴스가 백업 호스트에서 시작됩니다.

VMware High Availability에는 다음 구성 요소가 필요합니다.

- ESXi가 설치된 최소 2개의 호스트. 이러한 호스트는 VMware 클러스터의 일부분이 됩니다.
- VMware vCenter가 설치된 세 번째 호스트.

  **팁:** 클러스터에서 사용할 호스트에 설치된 ESXi 버전과 호환되는 VMware vCenter 버전을 설치해야 합니다.

  VMware vCenter는 클러스터에 사용되는 호스트 중 하나에 설치할 수 있습니다. 그러나 해당 호스트의 전원이 꺼져 있거나 사용할 수 없는 경우 VMware vCenter 인터페이스에 대한 액세스 권한도 손실됩니다.
- 클러스터의 모든 호스트가 액세스할 수 있는 공유 스토리지(데이터스토어). VMware가 지원하는 모든 유형의 공유 스토리지를 사용할 수 있습니다. VMware는 데이터스토어를 사용하여 VM이 다른 호스트로 장애 조치되는지(하트비트) 판별합니다.

VMware 고가용성 클러스터 설정에 대한 세부 정보는 XClarity Administrator 온라인 설명서에서 고가용성 구현(VMware ESXi)의 내용을 참조하십시오.

## Features on Demand

Features on Demand는 하드웨어를 설치하거나 새 장비를 구매하지 않아도 기능을 활성화합니다. 이 활성화는 해당 Features on Demand 키를 획득하고 설치하여 이루어집니다.

Lenovo XClarity Administrator에서 원격 제어 및 운영 체제 배포 작업을 사용하려면, 이미 기본적으로 활성화된 이러한 기능과 함께 제공되지 않는 서버에 대한 XClarity Controller Enterprise 수준 또는 MM 고급 업그레이드를 사용으로 설정해야 합니다. 이러한 작업을 하려면 원격 관리를 위한 Features on Demand 키가 ThinkSystem, Converged 및 System x 서버에 설치되어야 합니다. 원격 관리 상태가 서버 페이지에서 사용, 사용 안 함 또는 서버에 설치되어 있지 않은지 여부를 판별할 수 있습니다(XClarity Administrator 온라인 설명서에서 관리 서버의 상태 보기 참조).

일부 고급 서버 기능은 Features on Demand 키를 사용하여 활성화됩니다. 기능에 UEFI 설정 중에 노출되는 구성 가능 설정이 있는 경우 구성 패턴을 사용하여 설정을 구성할 수 있습니다. 그러나 결과 구성은 해당 Features on Demand 키가 설치될 때까지 활성화되지 않습니다.

**참고:** XClarity Administrator에서 Features on Demand 키를 설치 또는 관리할 수 없습니다. 그러나 현재 관리 서버에 설치된 Features on Demand 키의 목록을 볼 수 있습니다. 설치된 Features

on Demand 키 보기에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 Feature on Demand 키 보기의 내용을 참조하십시오.

Features on Demand 키를 획득하고 설치하려면 다음과 같이 하십시오.

1. 적절한 부품 번호를 사용하여 Features on Demand 업그레이드를 구매합니다.

   Features on Demand 웹 포털에서 키를 구매할 수 있습니다. 구매가 완료되면 이메일로 승인 코드가 수신됩니다.
2. Features on Demand 웹 포털에 수신한 승인 코드와 업그레이드할 서버의 고유 시스템 식별자와 함께 입력하십시오.
3. 활성화 키를 .KEY 키의 양식으로 다운로드하십시오.
4. 서버에 대한 관리 컨트롤러에 활성화 키를 업로드하십시오.
5. 서버를 다시 시작하십시오. 구성이 완료되면 시스템을 다시 시작해야 합니다.

Features on Demand 키에 대한 자세한 정보는 Lenovo Features on Demand 사용의 내용을 참조하십시오.

# 제 3 장  에서 Lenovo XClarity Administrator 설치

관리 가능한 장치를 네트워크에 연결하고 해당 장치를 관리하도록 Lenovo XClarity Administrator 가상 어플라이언스를 설정하는 몇 가지 방법이 있습니다. 이 섹션의 정보를 사용하여 관리 가능한 장치를 설정하고 XClarity Administrator을(를) 설치하십시오.

이 섹션에서는 몇 가지 공통 토폴로지를 설정하는 방법에 대해 설명합니다. 이 섹션은 가능한 모든 네트워크 토폴로지를 다루지 않습니다.

**주의:** 장치를 관리하려면 XClarity Administrator가 관리 네트워크에 대한 액세스 권한을 가지고 있어야 합니다.

**자세히 알아보기:**
- VMware vCenter에 Lenovo XClarity Administrator 설치
- VMware vSphere에 Lenovo XClarity Administrator 설치
- Windows Hyper-V에 Lenovo XClarity Administrator 설치
- Red Hat KVM에 Lenovo XClarity Administrator 설치

## 단일 데이터 및 관리 네트워크

이 네트워크 토폴로지에서 데이터 네트워크와 관리 네트워크는 동일한 네트워크입니다.

### 시작하기 전에

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

XClarity Administrator를 사용하여 관리하려는 각 장치에 최소 요구 펌웨어가 설치되어 있어야 합니다. 필요한 최소 펌웨어 수준은 XClarity Administrator 지원 – 호환성 웹 페이지에서 **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하여 확인할 수 있습니다.

**중요:** IP 주소 변경을 최소화하는 방식으로 장치 및 구성 요소를 구성하십시오. DHCP(Dynamic Host Configuration Protocol) 대신에 고정 IP 주소 사용을 고려하십시오. DHCP를 사용하는 경우 IP 주소 변경이 최소화되어야 합니다.

### 이 작업 정보

가상 어플라이언스의 경우 XClarity Administrator 및 네트워크 간의 모든 통신은 호스트의 eth0 네트워크 인터페이스를 통해 발생합니다. 컨테이너의 경우 사용자 지정 이름을 사용할 수 있지만, 이 시나리오에서는 eth0을 사용합니다.

**중요:** 공유 데이터 및 관리 네트워크를 구현하면 네트워크 구성에 따라(예, 서버의 트래픽의 우선 순위가 높거나 관리 컨트롤러 트래픽의 우선순위가 낮은 경우) 패킷이 중지되거나 관리 네트워크 연결 문제와 같은 트래픽 중단이 발생할 수 있습니다. 관리 네트워크는 추가 TCP에 UDP 트래픽을 사용합니다. 네트워크 트래픽이 높은 경우 UDP 트래픽의 우선 순위가 더 낮을 수 있습니다.

다음 그림은 데이터 네트워크와 관리 네트워크가 동일한 네트워크인 경우 사용자 환경을 설정하는 한 방법에 대해 설명합니다. 그림의 숫자는 다음 섹션에서 숫자 지정된 단계에 해당합니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 단일 데이터/관리 네트워크 설정과 관련된 랙 서버, 랙 스위치, Flex 스위치 및 CMM의 케이블 연결 옵션 요구사항만 표시합니다.

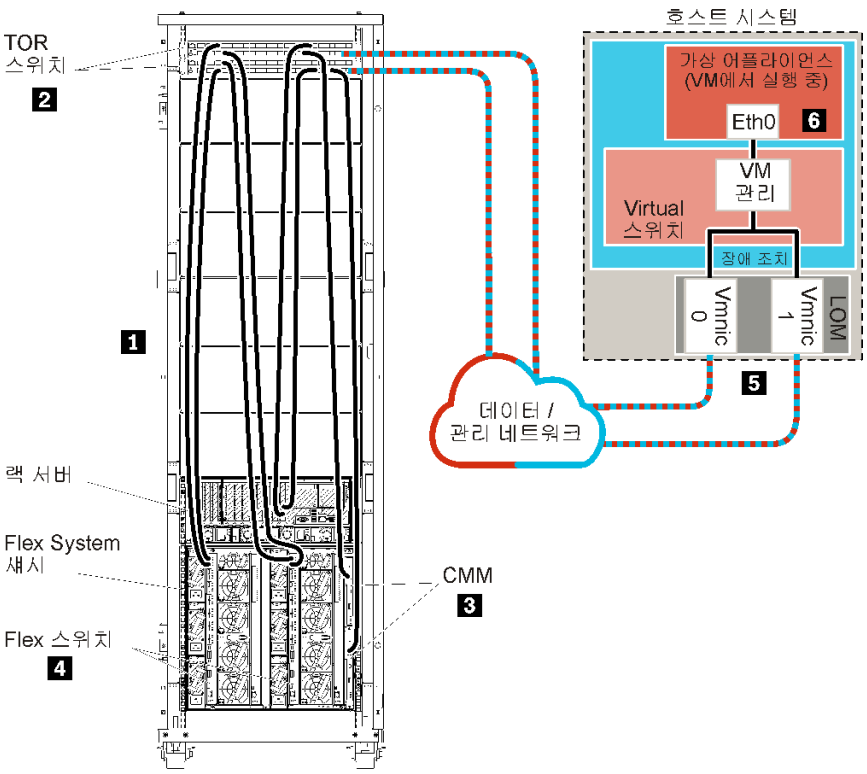



*그림 8. 가상 어플라이언스의 단일 데이터 및 관리 네트워크 토폴로지 샘플*

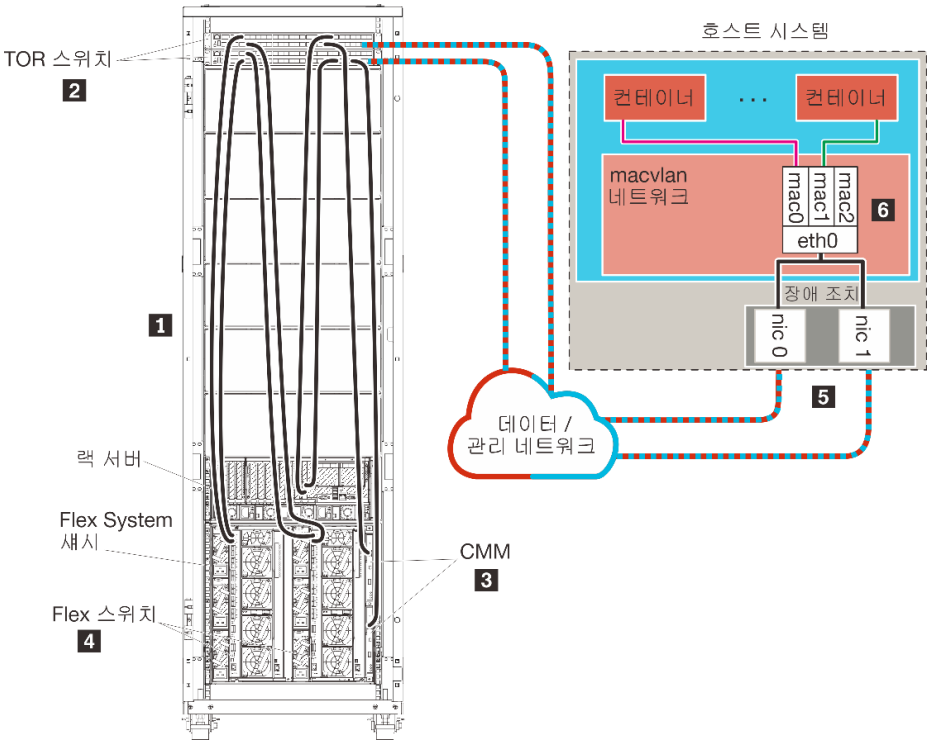



*그림 9. 컨테이너의 단일 데이터 및 관리 네트워크 토폴로지 샘플*

**중요:** 관리되는 서버를 포함하여 XClarity Administrator의 요구사항을 충족하는 시스템에 XClarity Administrator를 설정할 수 있습니다. XClarity Administrator 호스트의 관리되는 서버를 사용하는 경우:

- 가상으로 분리된 데이터 및 관리 네트워크 토폴로지나 단일 데이터 및 관리 네트워크 토폴로지를 구현해야 합니다.
- XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 일부 펌웨어만 즉시 활성화가 적용되는 경우에도 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.
- Flex System 섀시의 서버를 사용하는 경우 서버가 자동으로 전원이 켜지도록 설정되어야 합니다. **섀시 관리 → 컴퓨팅 노드**를 클릭한 후 서버를 선택하고 **자동 전원 켜기 모드**에 **자동 전원**을 선택하여 CMM 웹 인터페이스에서 이 옵션을 설정할 수 있습니다.

XClarity Administrator를 설치하여 이미 구성된 기존 섀시와 랙 서버를 관리하려는 경우 계속해서 5단계: 호스트 설치 및 구성을(를) 진행하십시오.

네트워크 설정과 Eth1 및 Eth0 구성에 대한 정보를 포함하여 이 토폴로지 계획에 대한 추가 정보는 단일 데이터 및 관리 네트워크의 내용을 참조하십시오.

## 1단계: 섀시, 랙 서버 및 Lenovo XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결

섀시, 랙 서버 및 XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결하여 장치와 네트워크 간에 통신을 사용 가능하게 합니다.

### 절차

각 섀시, 각 랙 서버 및 XClarity Administrator 호스트에 있는 각 Flex 스위치와 CMM을 두 ToR(top-of-rack) 스위치에 케이블 연결하십시오. ToR(top-of-rack) 스위치에서 포트를 선택할 수 있습니다.

다음 그림은 섀시(Flex 스위치 및 CMM), 랙 서버 및 XClarity Administrator 호스트에서 ToR(top-of-rack) 스위치로 케이블을 연결하는 예시입니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 단일 데이터/관리 네트워크 설정과 관련된 랙 서버, 랙 스위치, Flex 스위치 및 CMM의 케이블 연결 옵션 요구사항만 표시합니다.

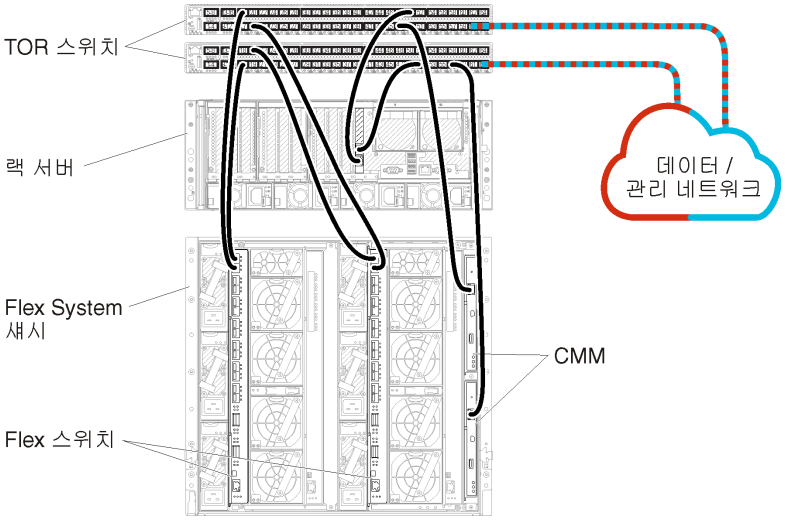



*그림 10. 단일 데이터 및 관리 네트워크의 케이블 연결 예*

## 2단계: ToR(top-of-rack) 스위치 구성

ToR(top-of-rack) 스위치를 구성합니다.

### 시작하기 전에

ToR(top-of-rack) 스위치의 일반적인 구성 요구사항에 추가로 Flex 스위치, 랙 서버 및 네트워크의 외부 포트와 CMM, 랙 서버 및 네트워크의 내부 포트를 포함하여 적합한 모든 포트가 사용 설정되어 있는지 확인하십시오.

### 절차

구성 단계는 설치되는 랙 스위치 유형에 따라 다를 수 있습니다.

Lenovo ToR(top-of-rack) 스위치 구성에 대한 정보는 System x 온라인 설명서의 랙 스위치의 내용을 참조하십시오. 다른 ToR(top-of-rack) 스위치가 설치되는 경우 해당 스위치와 함께 제공된 설명서를 참조하십시오.

## 3단계: CMM(Chassis Management Module) 구성

섀시의 모든 장치를 관리하도록 섀시에서 기본 CMM(Chassis Management Module)을 구성합니다.

### 이 작업 정보

CMM 구성에 대한 자세한 정보는 Flex System 온라인 설명서의 섀시 구성 요소 구성의 내용을 참조하십시오.

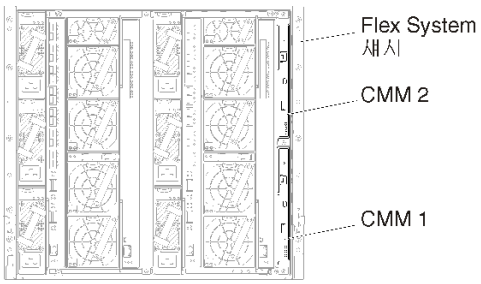
또한 섀시와 함께 제공된 안내 포스터에서 4.1 - 4.5단계를 참조하십시오.

### 절차

CMM을 구성하려면 다음 단계를 완료하십시오.

두 개의 CMM이 설치된 경우 구성을 대기 CMM과 자동으로 동기화하는 *기본* CMM만 구성하십시오.

단계 1. 베이 1의 CMM에서 클라이언트 워크스테이션으로 이더넷 케이블을 연결하여 직접 연결을 작성하십시오.




처음으로 CMM에 연결하려면 클라이언트 워크스테이션의 인터넷 프로토콜 속성을 변경해야 할 수 있습니다.

**중요:** 클라이언트 워크스테이션 서브넷이 CMM 서브넷과 같아야 합니다. 기본 CMM 서브넷은 255.255.255.0입니다. 클라이언트 워크스테이션에 선택된 IP 주소는 CMM과 동일한 네트워크에 있어야 합니다(예, 192.168.70.0 - 192.168.70.24).

단계 2. CMM 관리 인터페이스를 실행하려면 클라이언트 워크스테이션에서 웹 브라우저를 열고 CMM IP 주소로 지정하십시오.

**참고:**

- 보안 연결을 사용하고 URL에 **https**가 포함되어야 합니다(예, https://192.168.70.100). https를 포함하지 않는 경우 페이지를 찾을 수 없음 오류가 발생합니다.
- 기본 IP 주소 192.168.70.100을 사용하는 경우 CMM 관리 인터페이스가 사용 가능하게 되기까지 몇 분이 걸릴 수 있습니다. CMM이 기본 고정 주소로 다시 돌아가기 전에 2분 동안 DHCP 주소를 얻으려고 시도하기 때문에 이러한 지연이 발생합니다.

단계 3. 기본 사용자 ID USERID와 암호 PASSWORD를 사용하여 CMM 관리 인터페이스에 로그인하십시오. 로그인한 후 기본 암호를 변경해야 합니다.

단계 4. CMM 초기 설치 마법사를 완료하여 사용자 환경의 세부 정보를 지정하십시오. 초기 설치 마법사에는 다음 옵션이 포함되어 있습니다.

- 섀시 인벤토리 및 상태 보기.
- 기존 구성 파일에서 구성 가져오기.
- 일반 CMM 설정 구성.
- CMM 날짜 및 시간 구성.

  **팁:** XClarity Administrator을 설치하는 경우 NTP 서버를 사용하도록 XClarity Administrator 및 XClarity Administrator에서 관리되는 모든 섀시를 구성합니다.
- CMM IP 정보 구성.
- CMM 보안 정책 구성.
- DNS(Domain Name System) 구성.
- 이벤트 전달자 구성.

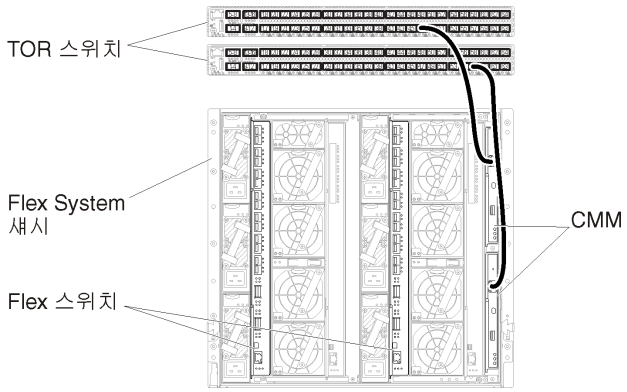
단계 5. 설정 마법사 설정을 저장하고 변경사항을 적용한 후 섀시에 있는 모든 구성 요소의 IP 주소를 구성하십시오.

섀시와 함께 제공된 안내 포스트에서 4.6단계를 참조하십시오.

**참고:** 새 IP 주소를 표시하려면 각 컴퓨팅 노드의 시스템 관리 프로세서를 재설정하고 Flex 스위치를 다시 시작해야 합니다.

단계 6. CMM 관리 인터페이스를 사용하여 CMM을 다시 시작하십시오.

단계 7. CMM이 다시 시작되면 CMM의 이더넷 포트에서 네트워크로 케이블을 연결하십시오.




단계 8. 새 IP 주소를 사용하여 CMM 관리 인터페이스에 로그인하십시오.

### 완료한 후에

중복을 지원하도록 CMM을 구성할 수도 있습니다. CMM 도움말 시스템을 사용하여 다음 각 페이지에서 사용 가능한 필드에 대한 자세한 정보를 얻을 수 있습니다.

- 기본 CMM에 하드웨어 오류가 있는 경우 CMM에 대한 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 속성 → 고급 장애 조치**를 클릭하십시오.
- 네트워크 문제(업링크)로 인해 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 네트워크**를 클릭하고 **이더넷** 탭을 클릭한 다음 **고급 이더넷**을 클릭하십시오. 최소한 **물리적 네트워크 링크 손실 시 장애 조치**가 선택되어야 합니다.

## 4단계: Flex 스위치 구성

각 섀시에서 Flex 스위치(I/O 모듈)를 구성합니다.

### 시작하기 전에

Flex 스위치에서 ToR(top-of-rack) 스위치로의 외부 포트와 CMM의 내부 포트를 포함하여 적합한 모든 포트가 사용으로 설정되어야 합니다.

DHCP를 통해 동적 네트워크 설정(IP 주소, 넷마스크, 게이트웨이 및 DNS 주소)을 가져오도록 Flex 스위치가 설정된 경우 Flex 스위치에 일관된 설정이 있어야 합니다(예, IP 주소가 CMM과 동일한 서브넷에 있어야 함).

**중요:** 각 Flex System 섀시에 대해 섀시의 각 서버에 있는 확장 카드의 패브릭 유형이 동일한 섀시에 있는 모든 Flex 스위치의 패브릭 유형과 호환 가능해야 합니다. 예를 들어 섀시에 이더넷 스위치가 설치된 경우 해당 섀시의 모든 서버가 LAN-on-motherboard 커넥터 또는 이더넷 확장 카드를 통해 이더넷과 연결되어 있어야 합니다. Flex 스위치 구성에 대한 자세한 정보는 Flex Systems 온라인 설명서의 I/O 모듈 구성의 내용을 참조하십시오.

### 절차

설치된 Flex 스위치 유형에 따라 구성 단계가 다를 수 있습니다. 지원되는 각 Flex 스위치에 대한 자세한 정보는 Flex Systems 온라인 설명서의 Flex System 네트워크 스위치의 내용을 참조하십시오.

일반적으로 Flex 스위치 베이 1과 2에서 Flex 스위치를 구성해야 합니다.

**팁:** Flex 스위치 베이 2는 섀시 뒷면에서 볼 때 세 번째 모듈 베이입니다.

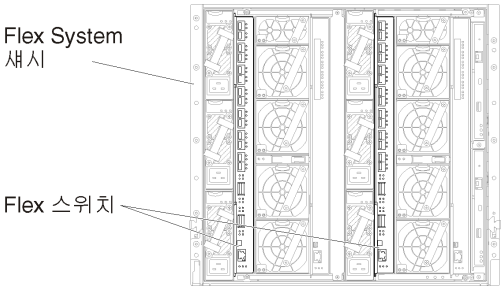



*그림 11. 섀시의 Flex 스위치 위치*

# 5단계: 호스트 설치 및 구성

Lenovo XClarity Administrator의 요구사항을 충족하는 서버에 Docker를 설치할 수 있습니다.

## 시작하기 전에

Docker Datacenter를 사용하여 Docker Engine에서 실행 중인 XClarity Administrator 컨테이너를 위한 고가용성 환경을 설정할 수 있습니다. Docker Datacenter 고가용성에 대한 자세한 정보는 Docker Datacenter 웹 페이지의 고가용성 아키텍처 및 앱의 내용을 참고하십시오.

호스트가 하드웨어 및 소프트웨어 전제조건에 정의된 전제조건을 충족하는지 확인하십시오.

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

**중요:** 관리되는 서버를 포함하여 XClarity Administrator의 요구사항을 충족하는 시스템에 XClarity Administrator를 설정할 수 있습니다. XClarity Administrator 호스트의 관리되는 서버를 사용하는 경우:

- 가상으로 분리된 데이터 및 관리 네트워크 토폴로지나 단일 데이터 및 관리 네트워크 토폴로지를 구현해야 합니다.
- XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 일부 펌웨어만 즉시 활성화가 적용되는 경우에도 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.
- Flex System 섀시의 서버를 사용하는 경우 서버가 자동으로 전원이 켜지도록 설정되어야 합니다. **섀시 관리 → 컴퓨팅 노드**를 클릭한 후 서버를 선택하고 **자동 전원 켜기 모드**에 **자동 전원**을 선택하여 CMM 웹 인터페이스에서 이 옵션을 설정할 수 있습니다.

## 절차

Docker 배포와 함께 제공된 지시 사항에 따라 호스트에 Docker를 설치 및 구성하십시오.

# 6단계. XClarity Administrator 설치 및 구성

설치한 Docker 호스트에 Lenovo XClarity Administrator 컨테이너를 설치하고 구성합니다.

## 시작하기 전에

호스트 시스템이 최소 하드웨어 및 소프트웨어 요구사항을 충족하는지 확인하십시오(하드웨어 및 소프트웨어 전제조건 참고).

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

호스트 OS와 XClarity Administrator이(가) 동일한 NTP 서버를 사용하는지 확인하십시오.

XClarity Administrator에서는 네트워크의 사용자 지정 이름을 데이터 및 하드웨어 관리와 OS 배포에 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 eth0을 사용합니다.

호스트 시스템의 커널에 macvlan 네트워크가 로드되어야 합니다. 로드되었는지 확인하려면 **lsmod | grep macvlan** 명령을 사용하십시오. macvlan을 커널에 로드하려면 **modprobe macvlan** 명령을 실행하십시오.

동일한 호스트에서 여러 XClarity Administrator 컨테이너를 실행하는 경우 각 컨테이너에 대해 고유한 이름과 IP 주소를 사용해야 합니다.

ThinkServer 및 기타 레거시 장치를 관리하려는 경우 Docker가 IPv6을 지원하도록 사용 설정되어 있는지 확인하십시오.

1. /etc/docker/daemon.json 파일을 편집하고 **ipv6** 키를 'true'로 설정하고 **fixed-cidr-v6** 키를 IPv6 서브넷으로 설정하십시오. 다음은 daemon 파일의 예입니다.
```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```
2. 다음 명령을 실행하여 Docker 설정 파일을 다시 로드하십시오.
```
systemctl reload docker
```

**참고:** XClarity Administrator는 권한이 있는 컨테이너로 실행되지 *않습니다*.

## 절차

Docker compose를 사용하여 XClarity Administrator 컨테이너를 설치하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 다운로드 웹 페이지에서 클라이언트 워크스테이션으로 XClarity Administrator 가상 어플라이언스 이미지, 환경 파일 및 YAML 파일을 다운로드하십시오. 웹 사이트에 로그온한 후 제공된 액세스 키를 사용하여 이미지를 다운로드하십시오.

단계 2. 다음 명령을 실행하여 XClarity Administrator 컨테이너 이미지를 Docker 호스트로 가져오십시오.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

단계 3. docker_compose.env 파일을 편집하고 다음 환경 변수를 업데이트하십시오.

- CONTAINER_NAME. 각 XClarity Administrator 인스턴스에 대한 Docker 볼륨을 만드는 데 사용되는 고유 컨테이너 이름(예: CONTAINER_NAME=LXCA-203)
- ADDRESS. 컨테이너의 고정 IPv4 주소(예: ADDRESS=192.0.2.0)
- BACKUP_MOUNT. (선택 사항) XClarity Administrator 백업을 저장하는 데 사용할 수 있는 원격 공유의 경로. /mnt/backup_share여야 합니다.
- FIRMWARE_MOUNT. (선택 사항) 펌웨어 업데이트를 위한 원격 리포지토리로 사용할 수 있는 원격 공유의 경로. /mnt/fw_share여야 합니다.

다음은 환경 파일의 예입니다.
```
CONTAINER_NAME="LXCA-203"
```

```
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

단계 4. docker_compose.yml을 편집하고 다음 속성을 업데이트합니다.

- **이미지** 속성을 2단계에서 사용한 설치 이미지 파일의 이름으로 설정합니다.

  **참고:** `docker tag` 명령을 사용하여 이미지 파일 이름을 변경할 수 있습니다(예: '최신'으로 변경).
- 원격 공유를 원격 펌웨어 리포지토리로 사용하고 XClarity Administrator 백업을 저장하려면 **볼륨** 속성에서 각 원격 공유에 대한 호스트 탑재 지점을 설정합니다.
- dns 속성을 DNS 서버의 IP 주소로 설정합니다.
- 컨테이너는 호스트에 사용할 수 있는 프로세서 및 메모리 리소스 풀을 공유합니다. 선택적으로 **CPU** 및 **메모리** 속성을 설정하여 리소스 사용량에 대한 제한사항을 정의합니다.
- 컨테이너에서 macvlan 인터페이스의 상위 인터페이스로 사용할 호스트 시스템의 네트워크 인터페이스 이름에 **상위** 속성을 설정합니다. 이 인터페이스는 컨테이너에 할당된 서브넷에 직접 액세스할 수 있어야 합니다.
- 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이**를 설정합니다. 일반적으로 서브넷과 게이트웨이는 ${ADDRESS}이(가) 속하는 관리 네트워크에 해당합니다.
- IPv6을 지원하려면 enable_ipv6 속성을 'true'로 설정하고, ipv6_address 속성을 IPv6 주소로 설정하고, 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이** 속성 세트를 추가하십시오(일반적으로 IPv6 주소가 속하는 관리 네트워크에 해당).

**참고:** XClarity Administrator는 macvlan을 사용하여 컨테이너 네트워크를 구성합니다. 자세한 정보는 macvlan 네트워크 웹 페이지 사용의 내용을 참조하십시오

다음은 IPv6가 사용 설정된 YML 파일의 예입니다.

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   #docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
   - ssh:/etc/ssh
   - xcat:/etc/xcat
  networks:
   lan:
    ipv4_address: ${ADDRESS}
    ipv6_address: "2001:8003:7d51:2003::2"
```

```
    dns:
     - 192.0.2.10
     - 192.0.2.11
    deploy:
     resources:
      limits:
       cpus: "2.0"
       memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
 lan:
  name: lan
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eth0
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
```

단계 5. 다음 명령을 실행하여 이미지를 Docker에 배포합니다. 여기에서 *<ENV_FILENAME>*은(는) 2단계에서 만든 환경 변수 파일의 이름입니다.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME}
--env-file <ENV_FILENAME> up -d
```

### 완료한 후에

XClarity Administrator에 로그인하여 구성하십시오(Lenovo XClarity Administrator 웹 인터페이스에 처음 액세스 및 Lenovo XClarity Administrator 구성 참조).

## 물리적으로 분리된 데이터 및 관리 네트워크

이 토폴로지에서 데이터 네트워크와 관리 네트워크는 물리적으로 분리된 네트워크입니다. Lenovo XClarity Administrator와 네트워크 간의 관리 통신은 호스트의 Eth0 네트워크 인터페이스를 통해 발생합니다. 데이터 통신은 Eth1 네트워크 인터페이스를 통해 발생합니다.

## 시작하기 전에

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

XClarity Administrator를 사용하여 관리하려는 각 장치에 최소 요구 펌웨어가 설치되어 있어야 합니다. 필요한 최소 펌웨어 수준은 XClarity Administrator 지원 – 호환성 웹 페이지에서 **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하여 확인할 수 있습니다.

**중요:** IP 주소 변경을 최소화하는 방식으로 장치 및 구성 요소를 구성하십시오. DHCP(Dynamic Host Configuration Protocol) 대신에 고정 IP 주소 사용을 고려하십시오. DHCP를 사용하는 경우 IP 주소 변경이 최소화되어야 합니다.

## 이 작업 정보

다음 그림은 데이터와 관리 네트워크가 물리적으로 다른 네트워크에 있는 경우 사용자 환경을 설정하는 한 방법을 설명합니다. 그림의 숫자는 다음 섹션에서 숫자 지정된 단계에 해당합니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 물리적으로 분리된 데이터 및 관리 네트워크 설정과 관련된 Flex 스위치, CMM 및 랙 서버의 케이블 연결 옵션 요구사항만 표시합니다.

**팁:** 중복을 위해 각 네트워크에 연결되는 두 개의 물리적인 스위치를 설정(총 네 개의 스위치)하는 대신 각 네트워크에 연결되는 하나의 물리적인 스위치(총 두 개의 스위치)를 설정할 수 있습니다. 이 경우 각 스위치는 두 네트워크에 연결되고 두 개의 VLAN을 구현합니다. 하나는 데이터 네트워크용이고 하나는 관리 네트워크용으로서 데이터 트래픽이 구분됩니다.

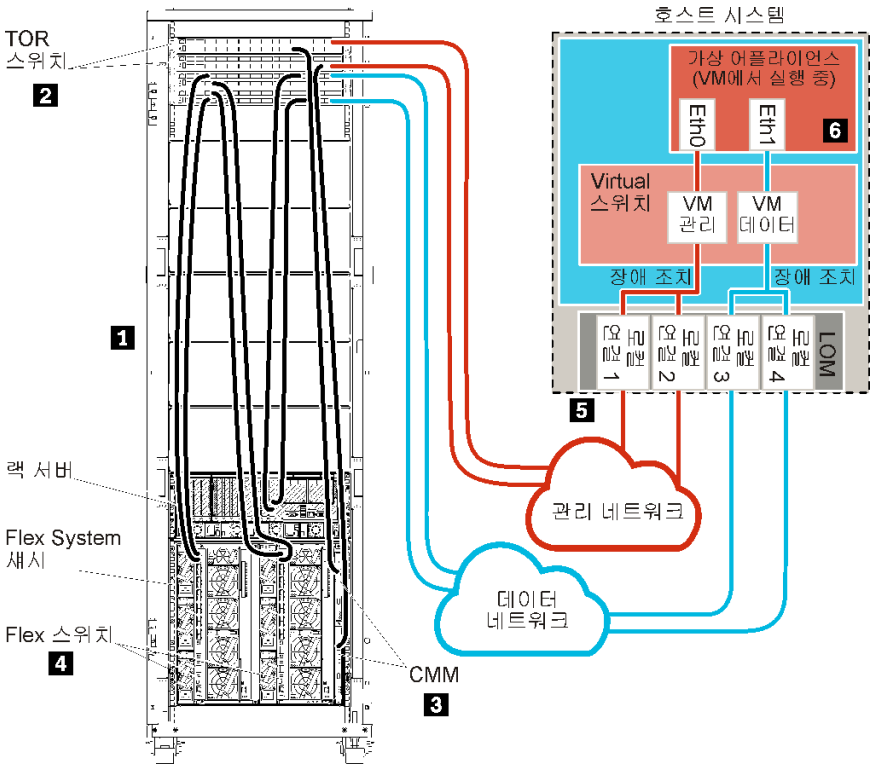



*그림 12. 가상 어플라이언스의 물리적으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플*

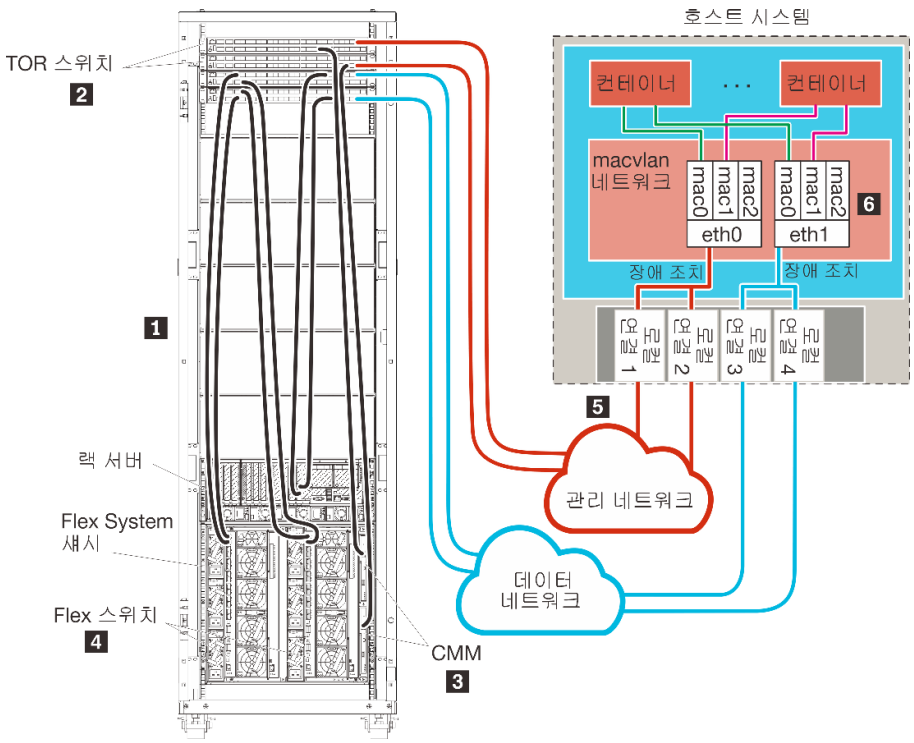



*그림 13. 컨테이너의 물리적으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플*

XClarity Administrator를 설치하여 이미 구성된 기존 섀시와 랙 서버를 관리하려는 경우 계속해서 5단계: 호스트 설치 및 구성을(를) 진행하십시오.

네트워크 설정과 Eth1 및 Eth0 구성에 대한 정보를 포함하여 이 토폴로지 계획에 대한 추가 정보는 물리적으로 분리된 데이터 및 관리 네트워크의 내용을 참조하십시오.

# 1단계: 섀시, 랙 서버 및 Lenovo XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결

섀시, 랙 서버 및 XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결하여 장치와 네트워크 간에 통신을 사용 가능하게 합니다.

## 절차

각 섀시, 각 랙 서버 및 XClarity Administrator 호스트에 있는 각 Flex 스위치와 CMM을 두 ToR(top-of-rack) 스위치에 케이블 연결하십시오. ToR(top-of-rack) 스위치에서 포트를 선택할 수 있습니다.

다음 그림은 섀시(Flex 스위치 및 CMM), 랙 서버 및 XClarity Administrator 호스트에서 ToR(top-of-rack) 스위치로 케이블을 연결하는 예시입니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 물리적으로 분리된 데이터 및 관리 네트워크 설정과 관련된 Flex 스위치, CMM 및 랙 서버의 케이블 연결 옵션 요구사항만 표시합니다.

**팁:** 중복을 위해 각 네트워크에 연결되는 두 개의 물리적인 스위치를 설정(총 네 개의 스위치)하는 대신 각 네트워크에 연결되는 하나의 물리적인 스위치(총 두 개의 스위치)를 설정할 수 있습니다. 이 경우 각 스위

치는 두 네트워크에 연결되고 두 개의 VLAN을 구현합니다. 하나는 데이터 네트워크용이고 하나는 관리 네트워크용으로서 데이터 트래픽이 구분됩니다.

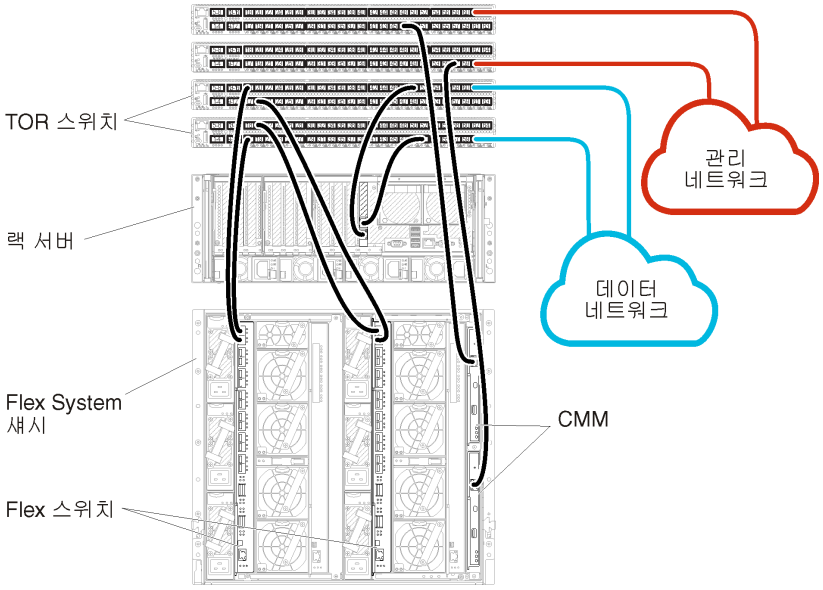



*그림 14. 물리적으로 분리된 데이터 및 관리 네트워크의 케이블 연결 예*

## 2단계: ToR(top-of-rack) 스위치 구성

ToR(top-of-rack) 스위치를 구성합니다.

### 시작하기 전에

ToR(top-of-rack) 스위치의 일반적인 구성 요구사항에 추가로 Flex 스위치, 랙 서버 및 네트워크의 외부 포트와 CMM, 랙 서버 및 네트워크의 내부 포트를 포함하여 적합한 모든 포트가 사용 설정되어 있는지 확인하십시오.

### 절차

구성 단계는 설치되는 랙 스위치 유형에 따라 다를 수 있습니다.

Lenovo ToR(top-of-rack) 스위치 구성에 대한 정보는 System x 온라인 설명서의 랙 스위치의 내용을 참조하십시오. 다른 ToR(top-of-rack) 스위치가 설치되는 경우 해당 스위치와 함께 제공된 설명서를 참조하십시오.

## 3단계: CMM(Chassis Management Module) 구성

섀시의 모든 장치를 관리하도록 섀시에서 기본 CMM(Chassis Management Module)을 구성합니다.

### 이 작업 정보

CMM 구성에 대한 자세한 정보는 Flex System 온라인 설명서의 섀시 구성 요소 구성의 내용을 참조하십시오.

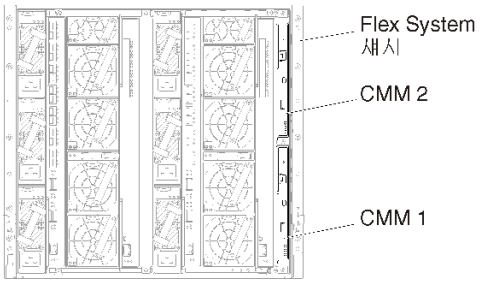
또한 섀시와 함께 제공된 안내 포스터에서 4.1 - 4.5단계를 참조하십시오.

### 절차

CMM을 구성하려면 다음 단계를 완료하십시오.

두 개의 CMM이 설치된 경우 구성을 대기 CMM과 자동으로 동기화하는 *기본* CMM만 구성하십시오.

단계 1. 베이 1의 CMM에서 클라이언트 워크스테이션으로 이더넷 케이블을 연결하여 직접 연결을 작성하십시오.




처음으로 CMM에 연결하려면 클라이언트 워크스테이션의 인터넷 프로토콜 속성을 변경해야 할 수 있습니다.

**중요:** 클라이언트 워크스테이션 서브넷이 CMM 서브넷과 같아야 합니다. 기본 CMM 서브넷은 255.255.255.0입니다. 클라이언트 워크스테이션에 선택된 IP 주소는 CMM과 동일한 네트워크에 있어야 합니다(예, 192.168.70.0 – 192.168.70.24).

단계 2. CMM 관리 인터페이스를 실행하려면 클라이언트 워크스테이션에서 웹 브라우저를 열고 CMM IP 주소로 지정하십시오.

**참고:**

- 보안 연결을 사용하고 URL에 **https**가 포함되어야 합니다(예, https://192.168.70.100). https를 포함하지 않는 경우 페이지를 찾을 수 없음 오류가 발생합니다.
- 기본 IP 주소 192.168.70.100을 사용하는 경우 CMM 관리 인터페이스가 사용 가능하게 되기까지 몇 분이 걸릴 수 있습니다. CMM이 기본 고정 주소로 다시 돌아가기 전에 2분 동안 DHCP 주소를 얻으려고 시도하기 때문에 이러한 지연이 발생합니다.

단계 3. 기본 사용자 ID `USERID`와 암호 `PASSWORD`를 사용하여 CMM 관리 인터페이스에 로그인하십시오. 로그인한 후 기본 암호를 변경해야 합니다.

단계 4. CMM 초기 설치 마법사를 완료하여 사용자 환경의 세부 정보를 지정하십시오. 초기 설치 마법사에는 다음 옵션이 포함되어 있습니다.

- 섀시 인벤토리 및 상태 보기.
- 기존 구성 파일에서 구성 가져오기.
- 일반 CMM 설정 구성.
- CMM 날짜 및 시간 구성.

  **팁:** XClarity Administrator을 설치하는 경우 NTP 서버를 사용하도록 XClarity Administrator 및 XClarity Administrator에서 관리되는 모든 섀시를 구성합니다.
- CMM IP 정보 구성.
- CMM 보안 정책 구성.
- DNS(Domain Name System) 구성.
- 이벤트 전달자 구성.

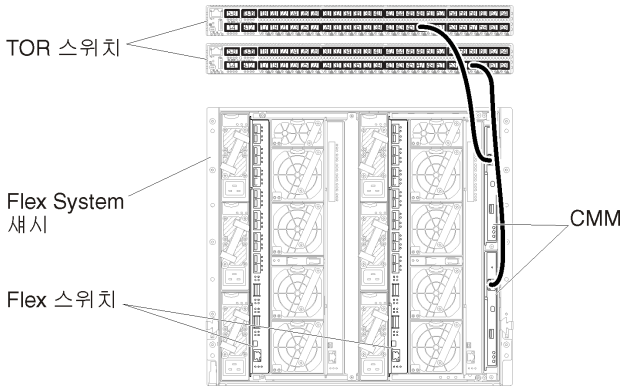
단계 5. 설정 마법사 설정을 저장하고 변경사항을 적용한 후 섀시에 있는 모든 구성 요소의 IP 주소를 구성하십시오.

섀시와 함께 제공된 안내 포스트에서 4.6단계를 참조하십시오.

**참고:** 새 IP 주소를 표시하려면 각 컴퓨팅 노드의 시스템 관리 프로세서를 재설정하고 Flex 스위치를 다시 시작해야 합니다.

단계 6. CMM 관리 인터페이스를 사용하여 CMM을 다시 시작하십시오.

단계 7. CMM이 다시 시작되면 CMM의 이더넷 포트에서 네트워크로 케이블을 연결하십시오.




단계 8. 새 IP 주소를 사용하여 CMM 관리 인터페이스에 로그인하십시오.

### 완료한 후에

중복을 지원하도록 CMM을 구성할 수도 있습니다. CMM 도움말 시스템을 사용하여 다음 각 페이지에서 사용 가능한 필드에 대한 자세한 정보를 얻을 수 있습니다.

- 기본 CMM에 하드웨어 오류가 있는 경우 CMM에 대한 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 속성 → 고급 장애 조치**를 클릭하십시오.
- 네트워크 문제(업링크)로 인해 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 네트워크**를 클릭하고 **이더넷** 탭을 클릭한 다음 **고급 이더넷**을 클릭하십시오. 최소한 **물리적 네트워크 링크 손실 시 장애 조치**가 선택되어야 합니다.

## 4단계: Flex 스위치 구성

각 섀시에서 Flex 스위치를 구성합니다.

### 시작하기 전에

Flex 스위치에서 ToR(top-of-rack) 스위치로의 외부 포트와 CMM의 내부 포트를 포함하여 적합한 모든 포트가 사용으로 설정되어야 합니다.

DHCP를 통해 동적 네트워크 설정(IP 주소, 넷마스크, 게이트웨이 및 DNS 주소)을 가져오도록 Flex 스위치가 설정된 경우 Flex 스위치에 일관된 설정이 있어야 합니다(예, IP 주소가 CMM과 동일한 서브넷에 있어야 함).

**중요:** 각 Flex System 섀시에 대해 섀시의 각 서버에 있는 확장 카드의 패브릭 유형이 동일한 섀시에 있는 모든 Flex 스위치의 패브릭 유형과 호환 가능해야 합니다. 예를 들어 섀시에 이더넷 스위치가 설치된 경우 해당 섀시의 모든 서버가 LAN-on-motherboard 커넥터 또는 이더넷 확장 카드를 통해 이더넷과 연결되어 있어야 합니다. Flex 스위치 구성에 대한 자세한 정보는 Flex Systems 온라인 설명서의 I/O 모듈 구성의 내용을 참조하십시오.

### 절차

설치된 Flex 스위치 유형에 따라 구성 단계가 다를 수 있습니다. 지원되는 각 Flex 스위치에 대한 자세한 정보는 Flex Systems 온라인 설명서의 Flex System 네트워크 스위치의 내용을 참조하십시오.

일반적으로 Flex 스위치 베이 1과 2에서 Flex 스위치를 구성해야 합니다.

**팁:** Flex 스위치 베이 2는 섀시 뒷면에서 볼 때 세 번째 모듈 베이입니다.

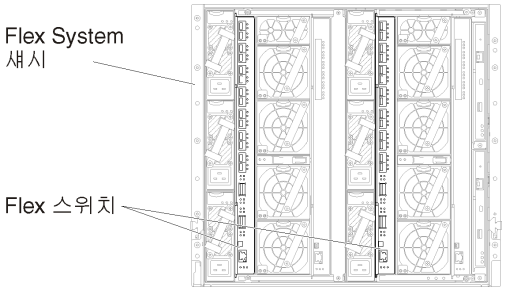



***그림 15. 섀시의 Flex 스위치 위치***

# 5단계: 호스트 설치 및 구성

Lenovo XClarity Administrator의 요구사항을 충족하는 서버에 Docker를 설치할 수 있습니다.

## 시작하기 전에

Docker Datacenter를 사용하여 Docker Engine에서 실행 중인 XClarity Administrator 컨테이너를 위한 고가용성 환경을 설정할 수 있습니다. Docker Datacenter 고가용성에 대한 자세한 정보는 Docker Datacenter 웹 페이지의 고가용성 아키텍처 및 앱의 내용을 참고하십시오.

호스트가 하드웨어 및 소프트웨어 전제조건에 정의된 전제조건을 충족하는지 확인하십시오.

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

**중요:** 관리되는 서버를 포함하여 XClarity Administrator의 요구사항을 충족하는 시스템에 XClarity Administrator를 설정할 수 있습니다. XClarity Administrator 호스트의 관리되는 서버를 사용하는 경우:

- 가상으로 분리된 데이터 및 관리 네트워크 토폴로지나 단일 데이터 및 관리 네트워크 토폴로지를 구현해야 합니다.
- XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 일부 펌웨어만 즉시 활성화가 적용되는 경우에도 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.
- Flex System 섀시의 서버를 사용하는 경우 서버가 자동으로 전원이 켜지도록 설정되어야 합니다. **섀시 관리 → 컴퓨팅 노드**를 클릭한 후 서버를 선택하고 **자동 전원 켜기 모드**에 **자동 전원**을 선택하여 CMM 웹 인터페이스에서 이 옵션을 설정할 수 있습니다.

## 절차

Docker 배포와 함께 제공된 지시 사항에 따라 호스트에 Docker를 설치 및 구성하십시오.

# 6단계. XClarity Administrator 설치 및 구성

설치한 Docker 호스트에 Lenovo XClarity Administrator 컨테이너를 설치하고 구성합니다.

## 시작하기 전에

호스트 시스템이 최소 하드웨어 및 소프트웨어 요구사항을 충족하는지 확인하십시오(하드웨어 및 소프트웨어 전제조건 참고).

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

호스트 OS와 XClarity Administrator이(가) 동일한 NTP 서버를 사용하는지 확인하십시오.

XClarity Administrator에서는 네트워크의 사용자 지정 이름을 데이터 및 하드웨어 관리와 OS 배포에 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 eth0을 사용합니다.

XClarity Administrator에서는 데이터 및 하드웨어 관리에 사용되는 네트워크와 OS 배포에 사용되는 네트워크에 대해 네트워크의 사용자 지정 이름을 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 각각 eth0 및 eth1을 사용합니다.

호스트 시스템의 커널에 macvlan 네트워크가 로드되어야 합니다. 로드되었는지 확인하려면 **lsmod | grep macvlan** 명령을 사용하십시오. macvlan을 커널에 로드하려면 **modprobe macvlan** 명령을 실행하십시오.

동일한 호스트에서 여러 XClarity Administrator 컨테이너를 실행하는 경우 각 컨테이너에 대해 고유한 이름과 IP 주소를 사용해야 합니다.

ThinkServer 및 기타 레거시 장치를 관리하려는 경우 Docker가 IPv6을 지원하도록 사용 설정되어 있는지 확인하십시오.

1. /etc/docker/daemon.json 파일을 편집하고 **ipv6** 키를 'true'로 설정하고 **fixed-cidr-v6** 키를 IPv6 서브넷으로 설정하십시오. 다음은 daemon 파일의 예입니다.
   ```
   {
     "ipv6": true,
     "fixed-cidr-v6": "2001:db8:1::/64",
     "experimental": true,
     "ip6tables": true
   }
   ```
2. 다음 명령을 실행하여 Docker 설정 파일을 다시 로드하십시오.
   ```
   systemctl reload docker
   ```

**참고:** XClarity Administrator는 권한이 있는 컨테이너로 실행되지 *않습니다*.

## 절차

Docker compose를 사용하여 XClarity Administrator 컨테이너를 설치하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 다운로드 웹 페이지에서 클라이언트 워크스테이션으로 XClarity Administrator 가상 어플라이언스 이미지, 환경 파일 및 YAML 파일을 다운로드하십시오. 웹 사이트에 로그온한 후 제공된 액세스 키를 사용하여 이미지를 다운로드하십시오.

단계 2. 다음 명령을 실행하여 XClarity Administrator 컨테이너 이미지를 Docker 호스트로 가져오십시오.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

단계 3. docker_compose.env 파일을 편집하고 다음 환경 변수를 업데이트하십시오.

- CONTAINER_NAME. 각 XClarity Administrator 인스턴스에 대한 Docker 볼륨을 만드는 데 사용되는 고유 컨테이너 이름(예: CONTAINER_NAME=LXCA-203)
- ADDRESS. 컨테이너의 고정 IPv4 주소(예: ADDRESS=192.0.2.0)

- BACKUP_MOUNT. (선택 사항) XClarity Administrator 백업을 저장하는 데 사용할 수 있는 원격 공유의 경로. /mnt/backup_share여야 합니다.
- FIRMWARE_MOUNT. (선택 사항) 펌웨어 업데이트를 위한 원격 리포지토리로 사용할 수 있는 원격 공유의 경로. /mnt/fw_share여야 합니다.

다음은 환경 파일의 예입니다.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

단계 4. docker_compose.yml을 편집하고 다음 속성을 업데이트합니다.

- **이미지** 속성을 2단계에서 사용한 설치 이미지 파일의 이름으로 설정합니다.

  **참고:** `docker tag` 명령을 사용하여 이미지 파일 이름을 변경할 수 있습니다(예: '최신'으로 변경).
- 원격 공유를 원격 펌웨어 리포지토리로 사용하고 XClarity Administrator 백업을 저장하려면 **볼륨** 속성에서 각 원격 공유에 대한 호스트 탑재 지점을 설정합니다.
- dns 속성을 DNS 서버의 IP 주소로 설정합니다.
- 컨테이너는 호스트에 사용할 수 있는 프로세서 및 메모리 리소스 풀을 공유합니다. 선택적으로 CPU 및 **메모리** 속성을 설정하여 리소스 사용량에 대한 제한사항을 정의합니다.
- 컨테이너에서 macvlan 인터페이스의 상위 인터페이스로 사용할 호스트 시스템의 네트워크 인터페이스 이름에 **상위** 속성을 설정합니다. 이 인터페이스는 컨테이너에 할당된 서브넷에 직접 액세스할 수 있어야 합니다.
- 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이**를 설정합니다. 일반적으로 서브넷과 게이트웨이는 ${ADDRESS}이(가) 속하는 관리 네트워크에 해당합니다.
- IPv6을 지원하려면 enable_ipv6 속성을 'true'로 설정하고, ipv6_address 속성을 IPv6 주소로 설정하고, 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이** 속성 세트를 추가하십시오(일반적으로 IPv6 주소가 속하는 관리 네트워크에 해당).

다음은 IPv6가 사용 설정된 YML 파일의 예입니다.

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   #docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
   - ssh:/etc/ssh
   - xcat:/etc/xcat
```

```
    networks:
     lan1:
      ipv4_address: ${ADDRESS}
      ipv6_address: "2001:8003:7d51:2000::2"
     lan2:
      ipv4_address: 192.0.1.3
      ipv6_address: "2001:8003:7d51:2003::2"
    dns:
     - 192.0.40.10
     - 192.0.50.11
    deploy:
     resources:
      limits:
       cpus: "2.0"
       memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
 lan1:
  name: lan1
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eno1
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
 lan2:
  name: lan2
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: virbr0
  ipam:
   config:
    - subnet: 192.0.122.0/24
    - subnet: "2001:8003:7d51:2005::/80"
```

단계 5. 다음 명령을 실행하여 이미지를 Docker에 배포합니다. 여기에서 *<ENV_FILENAME>*은(는) 2단계에서 만든 환경 변수 파일의 이름입니다.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME}
--env-file <ENV_FILENAME> up -d
```

### 완료한 후에

XClarity Administrator에 로그인하여 구성하십시오(Lenovo XClarity Administrator 웹 인터페이스에 처음 액세스 및 Lenovo XClarity Administrator 구성 참조).

## 가상으로 분리된 데이터 및 관리 네트워크 토폴로지

이 토폴로지에서 데이터 네트워크와 관리 네트워크는 가상 분리되어 있습니다. 데이터 네트워크의 패킷 및 관리 네트워크의 패킷은 동일한 물리적 연결을 통해 전송됩니다. 모든 관리 네트워크 데이터 패킷의 VLAN 태그 지정을 사용하여 두 네트워크 간의 트래픽을 별도로 유지합니다.

### 시작하기 전에

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

XClarity Administrator를 사용하여 관리하려는 각 장치에 최소 요구 펌웨어가 설치되어 있어야 합니다. 필요한 최소 펌웨어 수준은 XClarity Administrator 지원 – 호환성 웹 페이지에서 **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하여 확인할 수 있습니다.

데이터 네트워크 및 관리 네트워크에 대해 VLAN ID가 설정되어야 합니다. Flex 스위치에서 태그 지정을 구현하는 경우 Flex 스위치에서 VLAN 태그 지정을 사용으로 설정하고 ToR(top-of-rack) 스위치에서 태그 지정을 구현하는 경우 ToR(top-of-rack) 스위치에서 사용으로 설정하십시오(선택사항).

CMM이 연결되는 포트를 관리 VLAN에 속하도록 정의해야 합니다.

**중요:** IP 주소 변경을 최소화하는 방식으로 장치 및 구성 요소를 구성하십시오. DHCP(Dynamic Host Configuration Protocol) 대신에 고정 IP 주소 사용을 고려하십시오. DHCP를 사용하는 경우 IP 주소 변경이 최소화되어야 합니다.

### 이 작업 정보

다음 그림은 관리 네트워크가 가상 네트워크와 분리되도록 사용자 환경을 설정하는 한 방법을 설명합니다. 그림의 숫자는 다음 섹션에서 숫자 지정된 단계에 해당합니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 가상으로 분리된 데이터 및 관리 네트워크 설정과 관련된 Flex 스위치, CMM 및 랙 서버의 케이블 연결 옵션 요구사항만 표시합니다.

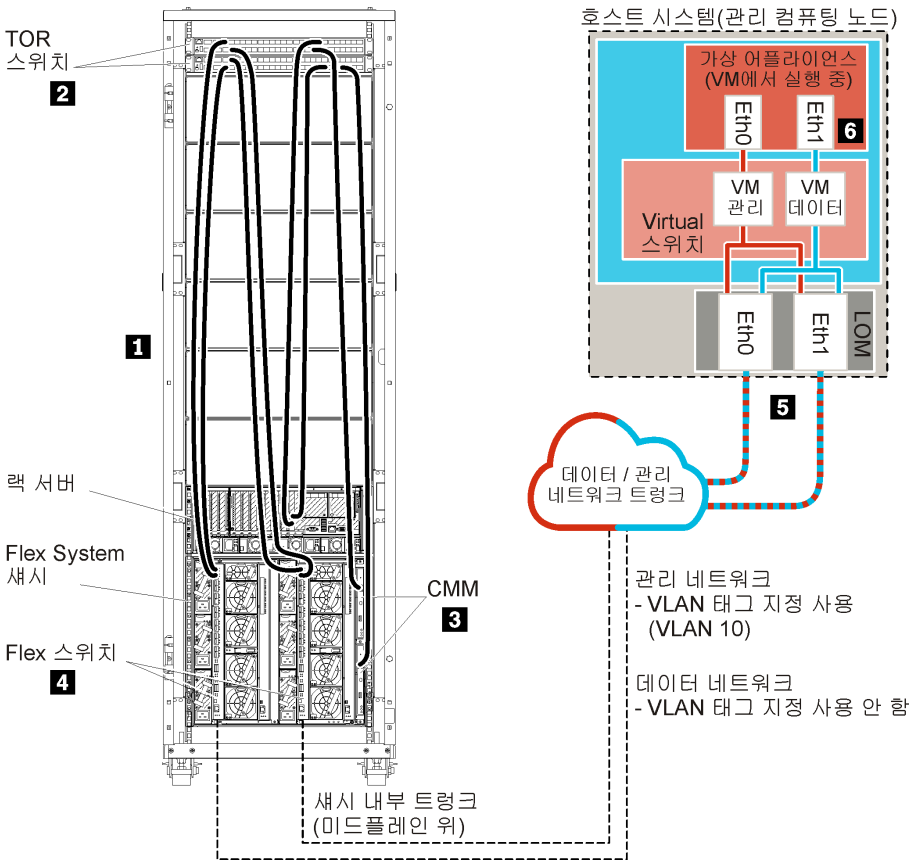



*그림 16. 가상 어플라이언스의 가상으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플*

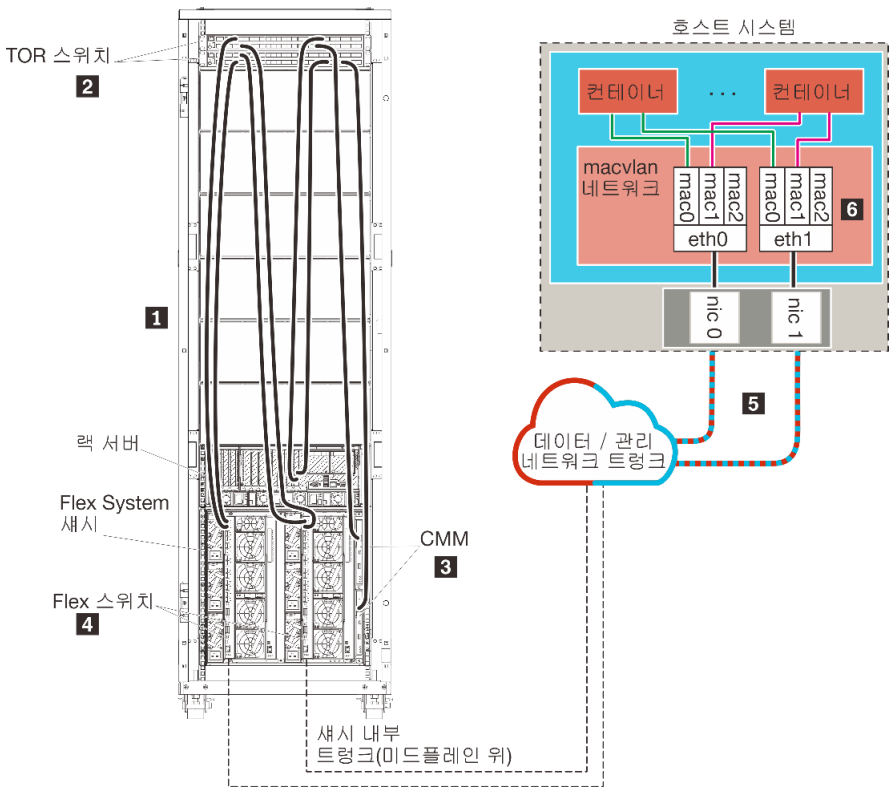



***그림 17. 컨테이너의 가상으로 분리된 데이터 및 관리 네트워크 토폴로지 샘플***

이 시나리오에서는 XClarity Administrator가 XClarity Administrator에서 관리되는 Flex System 섀시의 서버에 설치됩니다.

**중요:** 관리되는 서버를 포함하여 XClarity Administrator의 요구사항을 충족하는 시스템에 XClarity Administrator를 설정할 수 있습니다. XClarity Administrator 호스트의 관리되는 서버를 사용하는 경우:

- 가상으로 분리된 데이터 및 관리 네트워크 토폴로지나 단일 데이터 및 관리 네트워크 토폴로지를 구현해야 합니다.
- XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 일부 펌웨어만 즉시 활성화가 적용되는 경우에도 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.
- Flex System 섀시의 서버를 사용하는 경우 서버가 자동으로 전원이 켜지도록 설정되어야 합니다. **섀시 관리 → 컴퓨팅 노드**를 클릭한 후 서버를 선택하고 **자동 전원 켜기 모드**에 **자동 전원**을 선택하여 CMM 웹 인터페이스에서 이 옵션을 설정할 수 있습니다.

또한 모든 데이터가 동일한 물리적 연결을 통해 전송됩니다. 데이터 네트워크와 관리 네트워크의 분리는 VLAN 태그 지정을 통해 구축됩니다. 이 태그 지정에서는 관리 네트워크에 해당하는 특정 태그가 수신 데이터 패킷에 추가되어 적합한 인터페이스로 라우팅되도록 합니다. 이 태그는 발신 데이터 패킷에서 제거됩니다.

VLAN 태그 지정은 다음 장치 중 하나에서 사용할 수 있습니다.

- **ToR(Top-of-rack) 스위치**. 관리 네트워크에 해당하는 VLAN 태그는 ToR(top-of-rack) 스위치에 들어가 Flex 스위치를 통해 Flex System 섀시의 서버로 전달될 때 패킷에 추가됩니다. 리턴 경로에서 VLAN 태그는 ToR(top-of-rack) 스위치에서 관리 컨트롤러로 전송될 때 제거됩니다.

- **Flex 스위치**. 관리 네트워크에 해당하는 VLAN 태그는 Flex 스위치에 들어가 Flex System 섀시의 서버로 전달될 때 패킷에 추가됩니다. 리턴 경로에서 VLAN 태그는 서버에 의해 추가되고 Flex 스위치로 전달됩니다. 이 태그는 관리 컨트롤러로 전달할 때 제거됩니다.

VLAN 태그 지정을 구현할지에 대한 선택은 사용자 환경의 복잡도와 요구사항을 기반으로 합니다.

XClarity Administrator를 설치하여 이미 구성된 기존 섀시와 랙 서버를 관리하려는 경우 계속해서 5단계: 호스트 설치 및 구성을(를) 진행하십시오.

네트워크 설정과 Eth1 및 Eth0 구성에 대한 정보를 포함하여 이 토폴로지 계획에 대한 추가 정보는 가상 분리된 데이터 및 관리 네트워크의 내용을 참조하십시오.

# 1단계: ToR(top-of-rack) 스위치에 섀시 및 랙 서버의 케이블 연결

섀시 및 랙 서버를 동일한 ToR(top-of-rack) 스위치에 케이블 연결하여 장치 간에 통신을 사용 가능하게 합니다.

## 절차

섀시 및 랙 서버 각각에 있는 각 Flex 스위치와 CMM을 두 ToR(top-of-rack) 스위치에 케이블 연결하십시오. 해당 ToR(top-of-rack) 스위치에서 포트를 선택할 수 있습니다.

다음 그림은 Lenovo XClarity Administrator가 XClarity Administrator에서 관리되는 섀시의 서버에 설치된 경우 섀시(Flex 스위치 및 CMM) 및 랙 서버에서 ToR(top-of-rack) 스위치로 케이블을 연결하는 예시입니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 가상으로 분리된 데이터 및 관리 네트워크 설정과 관련된 Flex 스위치, CMM 및 랙 서버의 케이블 연결 옵션 요구사항만 표시합니다.

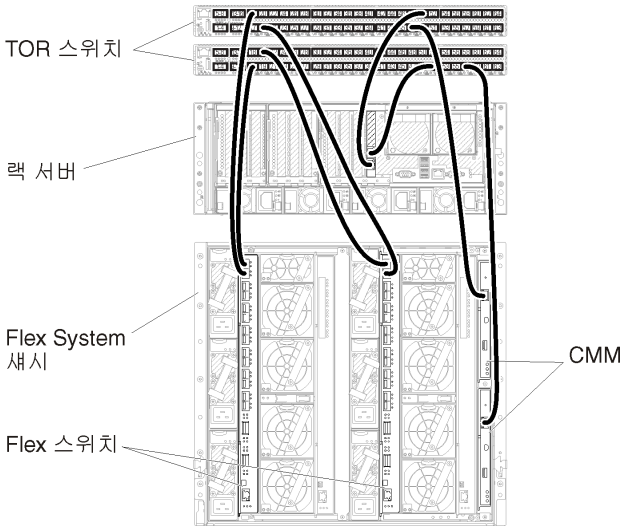



*그림 18. 가상으로 분리된 데이터 및 관리 네트워크의 케이블 연결 예*

# 2단계: ToR(top-of-rack) 스위치 구성

ToR(top-of-rack) 스위치를 구성합니다.

## 시작하기 전에

ToR(top-of-rack) 스위치의 일반적인 구성 요구사항에 추가로 Flex 스위치, 랙 서버 및 네트워크의 외부 포트와 CMM, 랙 서버 및 네트워크의 내부 포트를 포함하여 적합한 모든 포트가 사용 설정되어 있는지 확인하십시오.

사용자 환경의 복잡도와 요구사항에 따라 Flex 스위치 또는 ToR(top-of-rack) 스위치에서 VLAN 태그 지정을 구현할 수 있습니다. ToR(top-of-rack) 스위치에서 태그 지정을 구현하는 경우 ToR(top-of-rack) 스위치에서 VLAN 태그 지정을 사용으로 설정하십시오.

관리 및 데이터 네트워크에 대해 VLAN ID가 설정되어야 합니다.

### 절차

구성 단계는 설치되는 랙 스위치 유형에 따라 다를 수 있습니다.

다음 그림은 ToR(top-of-rack) 스위치에서 구현되고 관리 네트워크에서만 사용 설정된 VLAN 태그 지정을 설명하는 예제 시나리오입니다. 관리 VLAN이 VLAN 10으로 설정됩니다.

이 시나리오에서는 CMM이 연결되는 포트를 관리 VLAN에 속하도록 정의해야 합니다.

**참고:** 또한 데이터 네트워크에서 VLAN 태그 지정을 사용으로 설정하여 데이터 VLAN을 구성할 수도 있습니다.

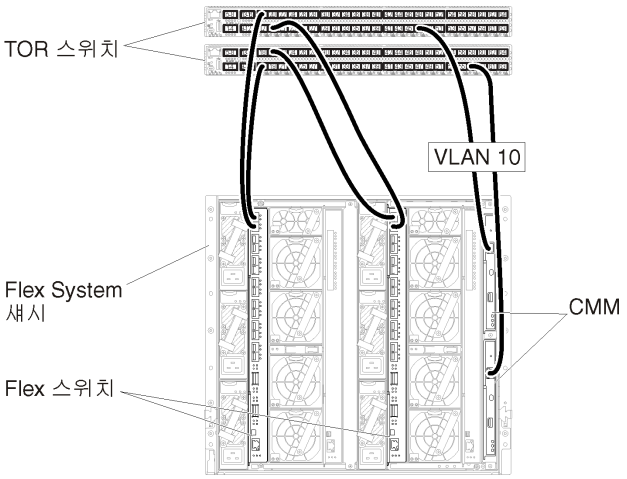



***그림 19. 관리 네트워크에서 VLAN 태그 지정이 사용으로 설정된 가상으로 분리된 데이터 및 관리 네트워크(VMware ESXi)의 Flex 스위치 구성 예***

Lenovo ToR(top-of-rack) 스위치 구성에 대한 정보는 System x 온라인 설명서의 랙 스위치의 내용을 참조하십시오. 다른 ToR(top-of-rack) 스위치가 설치되는 경우 해당 스위치와 함께 제공된 설명서를 참조하십시오.

## 3단계: CMM(Chassis Management Module) 구성

섀시의 모든 장치를 관리하도록 섀시에서 기본 CMM(Chassis Management Module)을 구성합니다.

### 이 작업 정보

CMM 구성에 대한 자세한 정보는 Flex System 온라인 설명서의 섀시 구성 요소 구성의 내용을 참조하십시오.

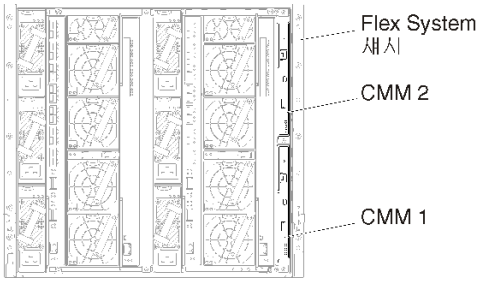
또한 섀시와 함께 제공된 안내 포스터에서 4.1 - 4.5단계를 참조하십시오.

## 절차

CMM을 구성하려면 다음 단계를 완료하십시오.

두 개의 CMM이 설치된 경우 구성을 대기 CMM과 자동으로 동기화하는 *기본* CMM만 구성하십시오.

단계 1. 베이 1의 CMM에서 클라이언트 워크스테이션으로 이더넷 케이블을 연결하여 직접 연결을 작성하십시오.




처음으로 CMM에 연결하려면 클라이언트 워크스테이션의 인터넷 프로토콜 속성을 변경해야 할 수 있습니다.

**중요:** 클라이언트 워크스테이션 서브넷이 CMM 서브넷과 같아야 합니다. 기본 CMM 서브넷은 255.255.255.0입니다. 클라이언트 워크스테이션에 선택된 IP 주소는 CMM과 동일한 네트워크에 있어야 합니다(예, 192.168.70.0 - 192.168.70.24).

단계 2. CMM 관리 인터페이스를 실행하려면 클라이언트 워크스테이션에서 웹 브라우저를 열고 CMM IP 주소로 지정하십시오.

**참고:**

- 보안 연결을 사용하고 URL에 **https**가 포함되어야 합니다(예, https://192.168.70.100). https를 포함하지 않는 경우 페이지를 찾을 수 없음 오류가 발생합니다.
- 기본 IP 주소 192.168.70.100을 사용하는 경우 CMM 관리 인터페이스가 사용 가능하게 되기까지 몇 분이 걸릴 수 있습니다. CMM이 기본 고정 주소로 다시 돌아가기 전에 2분 동안 DHCP 주소를 얻으려고 시도하기 때문에 이러한 지연이 발생합니다.

단계 3. 기본 사용자 ID USERID와 암호 PASSWORD를 사용하여 CMM 관리 인터페이스에 로그인하십시오. 로그인한 후 기본 암호를 변경해야 합니다.

단계 4. CMM 초기 설치 마법사를 완료하여 사용자 환경의 세부 정보를 지정하십시오. 초기 설치 마법사에는 다음 옵션이 포함되어 있습니다.

- 섀시 인벤토리 및 상태 보기.
- 기존 구성 파일에서 구성 가져오기.
- 일반 CMM 설정 구성.
- CMM 날짜 및 시간 구성.

  **팁:** XClarity Administrator을 설치하는 경우 NTP 서버를 사용하도록 XClarity Administrator 및 XClarity Administrator에서 관리되는 모든 섀시를 구성합니다.
- CMM IP 정보 구성.
- CMM 보안 정책 구성.
- DNS(Domain Name System) 구성.
- 이벤트 전달자 구성.

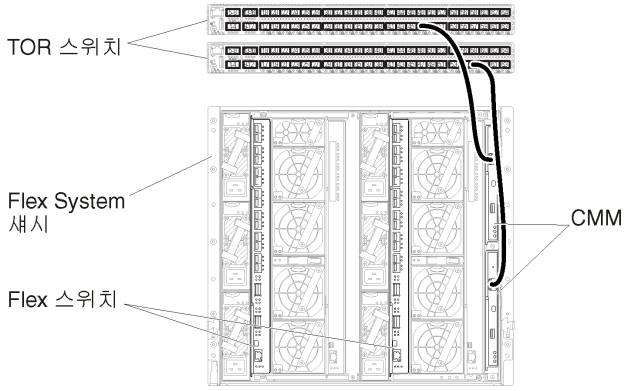
단계 5. 설정 마법사 설정을 저장하고 변경사항을 적용한 후 섀시에 있는 모든 구성 요소의 IP 주소를 구성하십시오.

섀시와 함께 제공된 안내 포스트에서 4.6단계를 참조하십시오.

**참고:** 새 IP 주소를 표시하려면 각 컴퓨팅 노드의 시스템 관리 프로세서를 재설정하고 Flex 스위치를 다시 시작해야 합니다.

단계 6. CMM 관리 인터페이스를 사용하여 CMM을 다시 시작하십시오.

단계 7. CMM이 다시 시작되면 CMM의 이더넷 포트에서 네트워크로 케이블을 연결하십시오.




단계 8. 새 IP 주소를 사용하여 CMM 관리 인터페이스에 로그인하십시오.

### 완료한 후에

중복을 지원하도록 CMM을 구성할 수도 있습니다. CMM 도움말 시스템을 사용하여 다음 각 페이지에서 사용 가능한 필드에 대한 자세한 정보를 얻을 수 있습니다.

- 기본 CMM에 하드웨어 오류가 있는 경우 CMM에 대한 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 속성 → 고급 장애 조치**를 클릭하십시오.
- 네트워크 문제(업링크)로 인해 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 네트워크**를 클릭하고 **이더넷** 탭을 클릭한 다음 **고급 이더넷**을 클릭하십시오. 최소한 **물리적 네트워크 링크 손실 시 장애 조치**가 선택되어야 합니다.

## 4단계: Flex 스위치 구성

각 섀시에서 Flex 스위치를 구성합니다.

### 시작하기 전에

Flex 스위치에서 ToR(top-of-rack) 스위치로의 외부 포트와 CMM의 내부 포트를 포함하여 적합한 모든 포트가 사용으로 설정되어야 합니다.

사용자 환경의 복잡도와 요구사항에 따라 Flex 스위치 또는 ToR(top-of-rack) 스위치에서 VLAN 태그 지정을 구현할 수 있습니다. Flex 스위치에서 태그 지정을 구현하는 경우 Flex 스위치에서 VLAN 태그 지정을 사용으로 설정하십시오.

관리 및 데이터 네트워크에 대해 VLAN ID가 설정되어야 합니다.

**중요:** 각 Flex System 섀시에 대해 섀시의 각 서버에 있는 확장 카드의 패브릭 유형이 동일한 섀시에 있는 모든 Flex 스위치의 패브릭 유형과 호환 가능해야 합니다. 예를 들어 섀시에 이더넷 스위치가 설치된 경우 해당 섀시의 모든 서버가 LAN-on-motherboard 커넥터 또는 이더넷 확장 카드를 통해 이더넷과 연결되어 있어야 합니다. Flex 스위치 구성에 대한 자세한 정보는 Flex Systems 온라인 설명서의 I/O 모듈 구성의 내용을 참조하십시오.

### 절차

설치된 Flex 스위치 유형에 따라 구성 단계가 다를 수 있습니다. 지원되는 각 Flex 스위치에 대한 자세한 정보는 Flex Systems 온라인 설명서의 Flex System 네트워크 스위치의 내용을 참조하십시오.

다음 그림은 Flex 스위치에서 구현되고 관리 네트워크에서만 사용 설정된 VLAN 태그 지정을 설명하는 예제 시나리오입니다. 관리 VLAN이 VLAN 10으로 설정됩니다.

**참고:** 데이터 네트워크에서 VLAN 태그 지정을 사용으로 설정하여 데이터 VLAN을 구성할 수 있습니다.

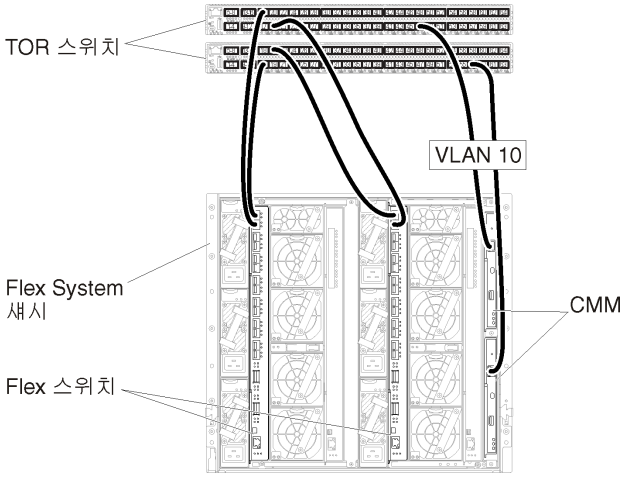



***그림 20. 관리 네트워크에서 VLAN 태그 지정이 사용으로 설정된 가상으로 분리된 데이터 및 관리 네트워크(VMware ESXi)의 Flex 스위치 구성 예***

이 시나리오를 위해 Flex 스위치를 구성하려면 다음 단계를 완료하십시오.

단계 1. 다음과 같이 Flex 스위치 베이 1에서 Flex 스위치를 구성하십시오.

a. 케이블이 ToR(top-of-rack) 관리 스위치로 라우팅되는 외부 포트(Ext1)를 포함하도록 관리 VLAN을 정의하십시오(이 예에서는 VLAN 10 선택).

b. 내부 포트를 VLAN 10(관리 VLAN)의 일부가 되도록 정의하십시오. 해당 포트에서 VLAN 트렁크가 사용으로 설정되어야 합니다.

단계 2. 다음과 같이 Flex 스위치 베이 2에서 Flex 스위치를 구성하십시오.

**팁:** Flex 스위치 베이 2는 섀시 뒷면에서 볼 때 실제로 세 번째 모듈 베이입니다.

a. 케이블이 ToR(top-of-rack) 관리 스위치로 라우팅되는 외부 포트를 포함하도록 관리 VLAN을 정의하십시오(이 예에서는 VLAN 10 선택).

b. 내부 포트를 VLAN 10(관리 VLAN)의 일부가 되도록 정의하십시오. 해당 포트에서 VLAN 트렁크가 사용으로 설정되어야 합니다.

## 5단계: 호스트 설치 및 구성

Lenovo XClarity Administrator의 요구사항을 충족하는 시스템에 Docker를 설치할 수 있습니다.

### 시작하기 전에

Docker Datacenter를 사용하여 Docker Engine에서 실행 중인 XClarity Administrator 컨테이너를 위한 고가용성 환경을 설정할 수 있습니다. Docker Datacenter 고가용성에 대한 자세한 정보는 Docker Datacenter 웹 페이지의 고가용성 아키텍처 및 앱의 내용을 참고하십시오.

호스트가 하드웨어 및 소프트웨어 전제조건에 정의된 전제조건을 충족하는지 확인하십시오.

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

**중요:** 관리되는 서버를 포함하여 XClarity Administrator의 요구사항을 충족하는 시스템에 XClarity Administrator를 설정할 수 있습니다. XClarity Administrator 호스트의 관리되는 서버를 사용하는 경우:

- 가상으로 분리된 데이터 및 관리 네트워크 토폴로지나 단일 데이터 및 관리 네트워크 토폴로지를 구현해야 합니다.
- XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 일부 펌웨어만 즉시 활성화가 적용되는 경우에도 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.
- Flex System 섀시의 서버를 사용하는 경우 서버가 자동으로 전원이 켜지도록 설정되어야 합니다. **섀시 관리 → 컴퓨팅 노드**를 클릭한 후 서버를 선택하고 **자동 전원 켜기 모드**에 **자동 전원**을 선택하여 CMM 웹 인터페이스에서 이 옵션을 설정할 수 있습니다.

### 절차

Docker 배포와 함께 제공된 지시 사항에 따라 호스트에 Docker를 설치 및 구성하십시오.

## 6단계. XClarity Administrator 설치 및 구성

설치한 Docker 호스트에 Lenovo XClarity Administrator 컨테이너를 설치하고 구성합니다.

### 시작하기 전에

호스트 시스템이 최소 하드웨어 및 소프트웨어 요구사항을 충족하는지 확인하십시오(하드웨어 및 소프트웨어 전제조건 참고).

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

호스트 OS와 XClarity Administrator이(가) 동일한 NTP 서버를 사용하는지 확인하십시오.

XClarity Administrator에서는 네트워크의 사용자 지정 이름을 데이터 및 하드웨어 관리와 OS 배포에 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 eth0을 사용합니다.

XClarity Administrator에서는 데이터 및 하드웨어 관리에 사용되는 네트워크와 OS 배포에 사용되는 네트워크에 대해 네트워크의 사용자 지정 이름을 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 각각 eth0 및 eth1을 사용합니다.

호스트 시스템의 커널에 macvlan 네트워크가 로드되어야 합니다. 로드되었는지 확인하려면 **lsmod | grep macvlan** 명령을 사용하십시오. macvlan을 커널에 로드하려면 **modprobe macvlan** 명령을 실행하십시오.

동일한 호스트에서 여러 XClarity Administrator 컨테이너를 실행하는 경우 각 컨테이너에 대해 고유한 이름과 IP 주소를 사용해야 합니다.

ThinkServer 및 기타 레거시 장치를 관리하려는 경우 Docker가 IPv6을 지원하도록 사용 설정되어 있는지 확인하십시오.

1. /etc/docker/daemon.json 파일을 편집하고 **ipv6** 키를 'true'로 설정하고 **fixed-cidr-v6** 키를 IPv6 서브넷으로 설정하십시오. 다음은 daemon 파일의 예입니다.
   {

```
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. 다음 명령을 실행하여 Docker 설정 파일을 다시 로드하십시오.
   `systemctl reload docker`

**참고:** XClarity Administrator는 권한이 있는 컨테이너로 실행되지 *않습니다*.

## 절차

Docker compose를 사용하여 XClarity Administrator 컨테이너를 설치하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 다운로드 웹 페이지에서 클라이언트 워크스테이션으로 XClarity Administrator 가상 어플라이언스 이미지, 환경 파일 및 YAML 파일을 다운로드하십시오. 웹 사이트에 로그온한 후 제공된 액세스 키를 사용하여 이미지를 다운로드하십시오.

단계 2. 다음 명령을 실행하여 XClarity Administrator 컨테이너 이미지를 Docker 호스트로 가져오십시오.
`docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz`

단계 3. `docker_compose.env` 파일을 편집하고 다음 환경 변수를 업데이트하십시오.

- CONTAINER_NAME. 각 XClarity Administrator 인스턴스에 대한 Docker 볼륨을 만드는 데 사용되는 고유 컨테이너 이름(예: `CONTAINER_NAME=LXCA-203`)
- ADDRESS. 컨테이너의 고정 IPv4 주소(예: `ADDRESS=192.0.2.0`)
- BACKUP_MOUNT. (선택 사항) XClarity Administrator 백업을 저장하는 데 사용할 수 있는 원격 공유의 경로. `/mnt/backup_share`여야 합니다.
- FIRMWARE_MOUNT. (선택 사항) 펌웨어 업데이트를 위한 원격 리포지토리로 사용할 수 있는 원격 공유의 경로. `/mnt/fw_share`여야 합니다.

다음은 환경 파일의 예입니다.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

단계 4. `docker_compose.yml`을 편집하고 다음 속성을 업데이트합니다.

- **이미지** 속성을 2단계에서 사용한 설치 이미지 파일의 이름으로 설정합니다.

  **참고:** `docker tag` 명령을 사용하여 이미지 파일 이름을 변경할 수 있습니다(예: '최신'으로 변경).
- 원격 공유를 원격 펌웨어 리포지토리로 사용하고 XClarity Administrator 백업을 저장하려면 **볼륨** 속성에서 각 원격 공유에 대한 호스트 탑재 지점을 설정합니다.
- dns 속성을 DNS 서버의 IP 주소로 설정합니다.
- 컨테이너는 호스트에 사용할 수 있는 프로세서 및 메모리 리소스 풀을 공유합니다. 선택적으로 CPU 및 **메모리** 속성을 설정하여 리소스 사용량에 대한 제한사항을 정의합니다.
- 컨테이너에서 macvlan 인터페이스의 상위 인터페이스로 사용할 호스트 시스템의 네트워크 인터페이스 이름에 **상위** 속성을 설정합니다. 이 인터페이스는 컨테이너에 할당된 서브넷에 직접 액세스할 수 있어야 합니다.
- 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이**를 설정합니다. 일반적으로 서브넷과 게이트웨이는 ${ADDRESS}이(가) 속하는 관리 네트워크에 해당합니다.

- IPv6을 지원하려면 enable_ipv6 속성을 'true'로 설정하고, ipv6_address 속성을 IPv6 주소로 설정하고, 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이** 속성 세트를 추가하십시오 (일반적으로 IPv6 주소가 속하는 관리 네트워크에 해당).

다음은 IPv6가 사용 설정된 YML 파일의 예입니다.

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   #docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
   - ssh:/etc/ssh
   - xcat:/etc/xcat
  networks:
   lan1:
    ipv4_address: ${ADDRESS}
    ipv6_address: "2001:8003:7d51:2000::2"
   lan2:
    ipv4_address: 192.0.1.3
    ipv6_address: "2001:8003:7d51:2003::2"
  dns:
   - 192.0.40.10
   - 192.0.50.11
  deploy:
   resources:
    limits:
     cpus: "2.0"
     memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
```

```
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"
```

단계 5. 다음 명령을 실행하여 이미지를 Docker에 배포합니다. 여기에서 *<ENV_FILENAME>*은(는) 2단계에서 만든 환경 변수 파일의 이름입니다.
```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME}
--env-file <ENV_FILENAME> up -d
```

### 완료한 후에

XClarity Administrator에 로그인하여 구성하십시오(Lenovo XClarity Administrator 웹 인터페이스에 처음 액세스 및 Lenovo XClarity Administrator 구성 참조).

## 관리 전용 네트워크 토폴로지

이 토폴로지에서 Lenovo XClarity Administrator는 관리 네트워크만 가집니다. 데이터 네트워크는 없습니다.

### 시작하기 전에

다음을 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오.
- XClarity Administrator에서 필요한 포트(포트 사용 가능성 참조)
- 네트워크의 외부 포트
- CMM의 내부 포트

XClarity Administrator를 사용하여 관리하려는 각 장치에 최소 요구 펌웨어가 설치되어 있어야 합니다. 필요한 최소 펌웨어 수준은 XClarity Administrator 지원 – 호환성 웹 페이지에서 **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하여 확인할 수 있습니다.

**중요:** IP 주소 변경을 최소화하는 방식으로 장치 및 구성 요소를 구성하십시오. DHCP(Dynamic Host Configuration Protocol) 대신에 고정 IP 주소 사용을 고려하십시오. DHCP를 사용하는 경우 IP 주소 변경이 최소화되어야 합니다.

## 이 작업 정보

다음 그림은 Lenovo XClarity Administrator에 관리 네트워크만 있는 경우(데이터 네트워크는 없음) 사용자 환경을 설정하는 한 방법에 대해 설명합니다. 그림의 숫자는 다음 섹션에서 숫자 지정된 단계에 해당합니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 관리 전용 네트워크 설정과 관련된 Flex 스위치, CMM 및 랙 서버의 케이블 연결 옵션 요구사항만 표시합니다.

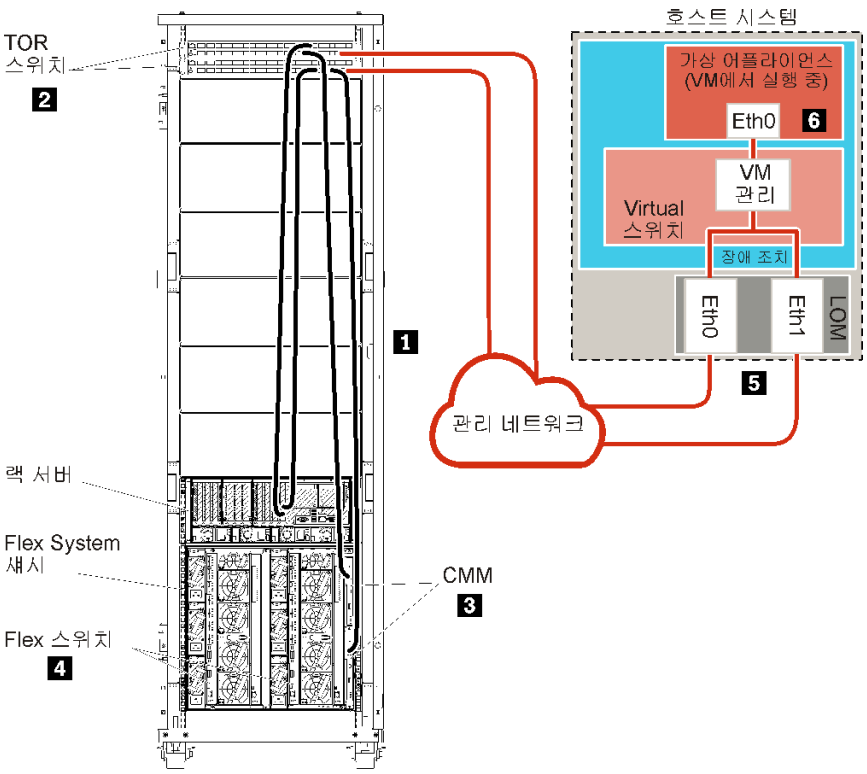



*그림 21. 가상 어플라이언스의 샘플 관리 전용 네트워크 토폴로지*

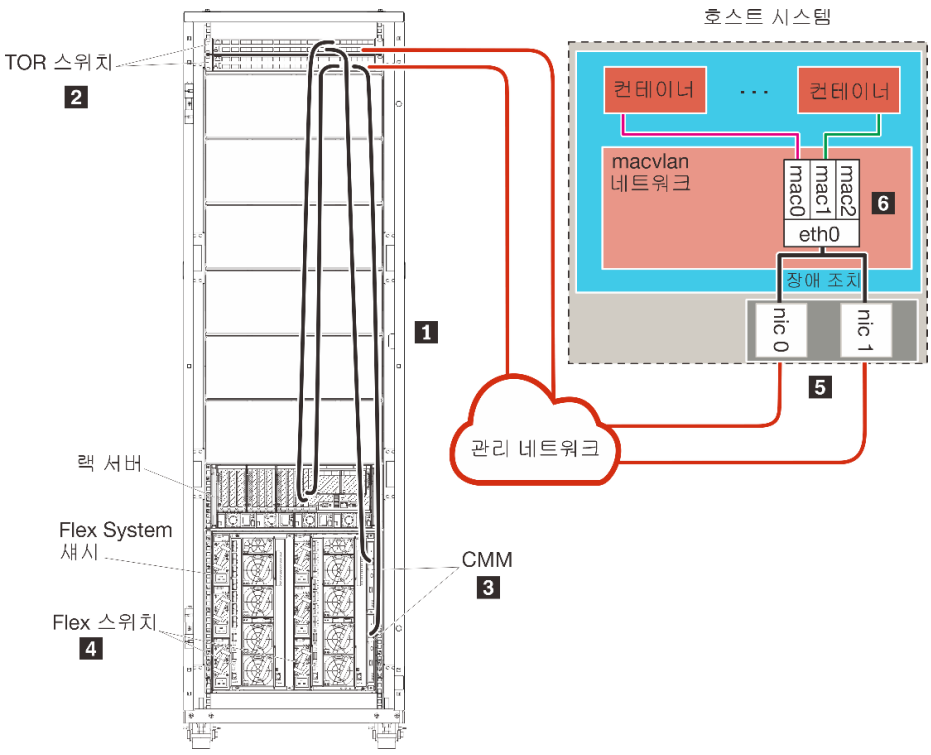



*그림 22. 컨테이너의 샘플 관리 전용 네트워크 토폴로지*

XClarity Administrator를 설치하여 이미 구성된 기존 섀시와 랙 서버를 관리하려는 경우 계속해서 5단계: 호스트 설치 및 구성을(를) 진행하십시오.

네트워크 설정과 Eth1 및 Eth0 구성에 대한 정보를 포함하여 이 토폴로지 계획에 대한 추가 정보는 관리 전용 네트워크의 내용을 참조하십시오.

# 1단계: 섀시, 랙 서버 및 Lenovo XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결

섀시, 랙 서버 및 XClarity Administrator 호스트를 ToR(top-of-rack) 스위치에 케이블 연결하여 장치와 네트워크 간에 통신을 사용 가능하게 합니다.

## 절차

각 섀시, 각 랙 서버 및 XClarity Administrator 호스트에 있는 각 Flex 스위치와 CMM을 두 ToR(top-of-rack) 스위치에 케이블 연결하십시오. ToR(top-of-rack) 스위치에서 포트를 선택할 수 있습니다.

다음 그림은 섀시(Flex 스위치 및 CMM), 랙 서버 및 XClarity Administrator 호스트에서 ToR(top-of-rack) 스위치로 케이블을 연결하는 예시입니다.

**참고:** 이 그림은 사용자 환경에 필요할 수 있는 모든 케이블 연결 옵션을 나타내지는 않습니다. 대신 이 그림은 관리 전용 네트워크 설정과 관련된 Flex 스위치, CMM 및 랙 서버의 케이블 연결 옵션 요구사항만 표시합니다.

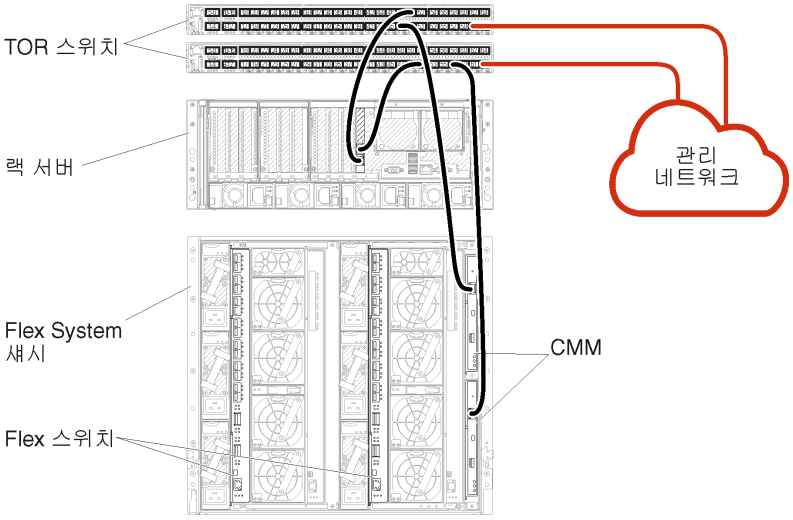



*그림 23. 관리 전용 네트워크 케이블 연결 예*

# 2단계: ToR(top-of-rack) 스위치 구성

ToR(top-of-rack) 스위치를 구성합니다.

## 시작하기 전에

ToR(top-of-rack) 스위치의 일반적인 구성 요구사항에 추가로 Flex 스위치, 랙 서버 및 네트워크의 외부 포트와 CMM, 랙 서버 및 네트워크의 내부 포트를 포함하여 적합한 모든 포트가 사용 설정되어 있는지 확인하십시오.

## 절차

구성 단계는 설치되는 랙 스위치 유형에 따라 다를 수 있습니다.

Lenovo ToR(top-of-rack) 스위치 구성에 대한 정보는 System x 온라인 설명서의 랙 스위치의 내용을 참조하십시오. 다른 ToR(top-of-rack) 스위치가 설치되는 경우 해당 스위치와 함께 제공된 설명서를 참조하십시오.

# 3단계: CMM(Chassis Management Module) 구성

섀시의 모든 장치를 관리하도록 섀시에서 기본 CMM(Chassis Management Module)을 구성합니다.

## 이 작업 정보

CMM 구성에 대한 자세한 정보는 Flex System 온라인 설명서의 섀시 구성 요소 구성의 내용을 참조하십시오.

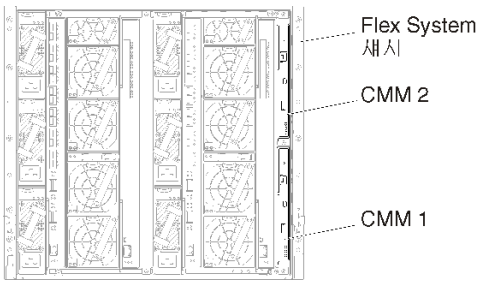
또한 섀시와 함께 제공된 안내 포스터에서 4.1 - 4.5단계를 참조하십시오.

## 절차

CMM을 구성하려면 다음 단계를 완료하십시오.

두 개의 CMM이 설치된 경우 구성을 대기 CMM과 자동으로 동기화하는 *기본* CMM만 구성하십시오.

단계 1. 베이 1의 CMM에서 클라이언트 워크스테이션으로 이더넷 케이블을 연결하여 직접 연결을 작성하십시오.




처음으로 CMM에 연결하려면 클라이언트 워크스테이션의 인터넷 프로토콜 속성을 변경해야 할 수 있습니다.

**중요:** 클라이언트 워크스테이션 서브넷이 CMM 서브넷과 같아야 합니다. 기본 CMM 서브넷은 255.255.255.0입니다. 클라이언트 워크스테이션에 선택된 IP 주소는 CMM과 동일한 네트워크에 있어야 합니다(예, 192.168.70.0 - 192.168.70.24).

단계 2. CMM 관리 인터페이스를 실행하려면 클라이언트 워크스테이션에서 웹 브라우저를 열고 CMM IP 주소로 지정하십시오.

**참고:**

- 보안 연결을 사용하고 URL에 **https**가 포함되어야 합니다(예, https://192.168.70.100). https를 포함하지 않는 경우 페이지를 찾을 수 없음 오류가 발생합니다.
- 기본 IP 주소 192.168.70.100을 사용하는 경우 CMM 관리 인터페이스가 사용 가능하게 되기까지 몇 분이 걸릴 수 있습니다. CMM이 기본 고정 주소로 다시 돌아가기 전에 2분 동안 DHCP 주소를 얻으려고 시도하기 때문에 이러한 지연이 발생합니다.

단계 3. 기본 사용자 ID USERID와 암호 PASSWORD를 사용하여 CMM 관리 인터페이스에 로그인하십시오. 로그인한 후 기본 암호를 변경해야 합니다.

단계 4. CMM 초기 설치 마법사를 완료하여 사용자 환경의 세부 정보를 지정하십시오. 초기 설치 마법사에는 다음 옵션이 포함되어 있습니다.

- 섀시 인벤토리 및 상태 보기.
- 기존 구성 파일에서 구성 가져오기.
- 일반 CMM 설정 구성.
- CMM 날짜 및 시간 구성.

  **팁:** XClarity Administrator을 설치하는 경우 NTP 서버를 사용하도록 XClarity Administrator 및 XClarity Administrator에서 관리되는 모든 섀시를 구성합니다.
- CMM IP 정보 구성.
- CMM 보안 정책 구성.
- DNS(Domain Name System) 구성.
- 이벤트 전달자 구성.

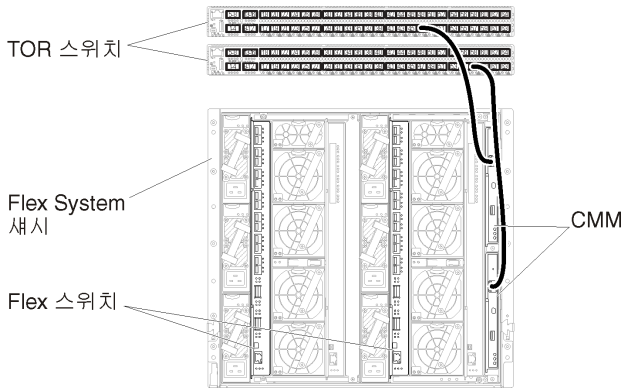
단계 5. 설정 마법사 설정을 저장하고 변경사항을 적용한 후 섀시에 있는 모든 구성 요소의 IP 주소를 구성하십시오.

섀시와 함께 제공된 안내 포스트에서 4.6단계를 참조하십시오.

**참고:** 새 IP 주소를 표시하려면 각 컴퓨팅 노드의 시스템 관리 프로세서를 재설정하고 Flex 스위치를 다시 시작해야 합니다.

단계 6. CMM 관리 인터페이스를 사용하여 CMM을 다시 시작하십시오.

단계 7. CMM이 다시 시작되면 CMM의 이더넷 포트에서 네트워크로 케이블을 연결하십시오.




단계 8. 새 IP 주소를 사용하여 CMM 관리 인터페이스에 로그인하십시오.

### 완료한 후에

중복을 지원하도록 CMM을 구성할 수도 있습니다. CMM 도움말 시스템을 사용하여 다음 각 페이지에서 사용 가능한 필드에 대한 자세한 정보를 얻을 수 있습니다.

- 기본 CMM에 하드웨어 오류가 있는 경우 CMM에 대한 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 속성 → 고급 장애 조치**를 클릭하십시오.
- 네트워크 문제(업링크)로 인해 장애 조치를 구성합니다. CMM 관리 인터페이스에서 **관리 모듈 관리 → 네트워크**를 클릭하고 **이더넷** 탭을 클릭한 다음 **고급 이더넷**을 클릭하십시오. 최소한 **물리적 네트워크 링크 손실 시 장애 조치**가 선택되어야 합니다.

## 4단계: Flex 스위치 구성

각 섀시에서 Flex 스위치를 구성합니다.

### 시작하기 전에

Flex 스위치에서 ToR(top-of-rack) 스위치로의 외부 포트와 CMM의 내부 포트를 포함하여 적합한 모든 포트가 사용으로 설정되어야 합니다.

DHCP를 통해 동적 네트워크 설정(IP 주소, 넷마스크, 게이트웨이 및 DNS 주소)을 가져오도록 Flex 스위치가 설정된 경우 Flex 스위치에 일관된 설정이 있어야 합니다(예, IP 주소가 CMM과 동일한 서브넷에 있어야 함).

**중요:** 각 Flex System 섀시에 대해 섀시의 각 서버에 있는 확장 카드의 패브릭 유형이 동일한 섀시에 있는 모든 Flex 스위치의 패브릭 유형과 호환 가능해야 합니다. 예를 들어 섀시에 이더넷 스위치가 설치된 경우 해당 섀시의 모든 서버가 LAN-on-motherboard 커넥터 또는 이더넷 확장 카드를 통해 이더넷과 연결되어 있어야 합니다. Flex 스위치 구성에 대한 자세한 정보는 Flex Systems 온라인 설명서의 I/O 모듈 구성의 내용을 참조하십시오.

### 절차

설치된 Flex 스위치 유형에 따라 구성 단계가 다를 수 있습니다. 지원되는 각 Flex 스위치에 대한 자세한 정보는 Flex Systems 온라인 설명서의 Flex System 네트워크 스위치의 내용을 참조하십시오.

일반적으로 Flex 스위치 베이 1과 2에서 Flex 스위치를 구성해야 합니다.

**팁:** Flex 스위치 베이 2는 섀시 뒷면에서 볼 때 세 번째 모듈 베이입니다.

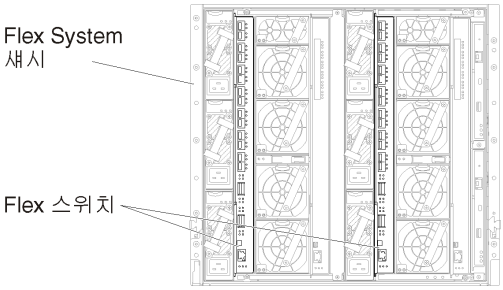



*그림 24. 섀시의 Flex 스위치 위치*

# 5단계: 호스트 설치 및 구성

Lenovo XClarity Administrator의 요구사항을 충족하는 시스템에 Docker를 설치할 수 있습니다.

## 시작하기 전에

Docker Datacenter를 사용하여 Docker Engine에서 실행 중인 XClarity Administrator 컨테이너를 위한 고가용성 환경을 설정할 수 있습니다. Docker Datacenter 고가용성에 대한 자세한 정보는 Docker Datacenter 웹 페이지의 고가용성 아키텍처 및 앱의 내용을 참고하십시오.

호스트가 하드웨어 및 소프트웨어 전제조건에 정의된 전제조건을 충족하는지 확인하십시오.

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

**중요:** 관리되는 서버를 포함하여 XClarity Administrator의 요구사항을 충족하는 시스템에 XClarity Administrator를 설정할 수 있습니다. XClarity Administrator 호스트의 관리되는 서버를 사용하는 경우:

- 가상으로 분리된 데이터 및 관리 네트워크 토폴로지나 단일 데이터 및 관리 네트워크 토폴로지를 구현해야 합니다.
- XClarity Administrator를 사용하여 해당 관리 서버에 펌웨어 업데이트를 적용할 수 없습니다. 일부 펌웨어만 즉시 활성화가 적용되는 경우에도 XClarity Administrator는 대상 서버를 강제로 다시 시작합니다. 이로 인해 XClarity Administrator도 다시 시작됩니다. 지연된 활성화가 적용되는 경우에는 XClarity Administrator 호스트가 다시 시작될 때 일부 펌웨어만 적용됩니다.
- Flex System 섀시의 서버를 사용하는 경우 서버가 자동으로 전원이 켜지도록 설정되어야 합니다. **섀시 관리 → 컴퓨팅 노드**를 클릭한 후 서버를 선택하고 **자동 전원 켜기 모드**에 **자동 전원**을 선택하여 CMM 웹 인터페이스에서 이 옵션을 설정할 수 있습니다.

## 절차

Docker 배포와 함께 제공된 지시 사항에 따라 호스트에 Docker를 설치 및 구성하십시오.

# 6단계. XClarity Administrator 설치 및 구성

설치한 Docker 호스트에 Lenovo XClarity Administrator 컨테이너를 설치하고 구성합니다.

## 시작하기 전에

호스트 시스템이 최소 하드웨어 및 소프트웨어 요구사항을 충족하는지 확인하십시오(하드웨어 및 소프트웨어 전제조건 참고).

XClarity Administrator에서 필요한 포트를 포함하여 모든 적합한 포트가 사용 설정되어 있는지 확인하십시오(포트 사용 가능성 참조).

호스트 시스템이 관리하려는 장치와 동일한 네트워크에 있어야 합니다.

호스트 OS와 XClarity Administrator이(가) 동일한 NTP 서버를 사용하는지 확인하십시오.

XClarity Administrator에서는 네트워크의 사용자 지정 이름을 데이터 및 하드웨어 관리와 OS 배포에 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 eth0을 사용합니다.

XClarity Administrator에서는 네트워크의 사용자 지정 이름을 데이터 및 하드웨어 관리에 사용할 수 있습니다(네트워크 구성 참고). 이 예는 다음 절차에서 eth0을 사용합니다.

호스트 시스템의 커널에 macvlan 네트워크가 로드되어야 합니다. 로드되었는지 확인하려면 **lsmod | grep macvlan** 명령을 사용하십시오. macvlan을 커널에 로드하려면 **modprobe macvlan** 명령을 실행하십시오.

동일한 호스트에서 여러 XClarity Administrator 컨테이너를 실행하는 경우 각 컨테이너에 대해 고유한 이름과 IP 주소를 사용해야 합니다.

ThinkServer 및 기타 레거시 장치를 관리하려는 경우 Docker가 IPv6을 지원하도록 사용 설정되어 있는지 확인하십시오.

1. /etc/docker/daemon.json 파일을 편집하고 **ipv6** 키를 'true'로 설정하고 **fixed-cidr-v6** 키를 IPv6 서브넷으로 설정하십시오. 다음은 daemon 파일의 예입니다.
   ```
   {
     "ipv6": true,
     "fixed-cidr-v6": "2001:db8:1::/64",
     "experimental": true,
     "ip6tables": true
   }
   ```
2. 다음 명령을 실행하여 Docker 설정 파일을 다시 로드하십시오.
   ```
   systemctl reload docker
   ```

**참고:** XClarity Administrator는 권한이 있는 컨테이너로 실행되지 *않습니다*.

## 절차

Docker compose를 사용하여 XClarity Administrator 컨테이너를 설치하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 다운로드 웹 페이지에서 클라이언트 워크스테이션으로 XClarity Administrator 가상 어플라이언스 이미지, 환경 파일 및 YAML 파일을 다운로드하십시오. 웹 사이트에 로그온한 후 제공된 액세스 키를 사용하여 이미지를 다운로드하십시오.

단계 2. 다음 명령을 실행하여 XClarity Administrator 컨테이너 이미지를 Docker 호스트로 가져오십시오.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

단계 3. docker_compose.env 파일을 편집하고 다음 환경 변수를 업데이트하십시오.

- CONTAINER_NAME. 각 XClarity Administrator 인스턴스에 대한 Docker 볼륨을 만드는 데 사용되는 고유 컨테이너 이름(예: CONTAINER_NAME=LXCA-203)
- ADDRESS. 컨테이너의 고정 IPv4 주소(예: ADDRESS=192.0.2.0)
- BACKUP_MOUNT. (선택 사항) XClarity Administrator 백업을 저장하는 데 사용할 수 있는 원격 공유의 경로. /mnt/backup_share여야 합니다.
- FIRMWARE_MOUNT. (선택 사항) 펌웨어 업데이트를 위한 원격 리포지토리로 사용할 수 있는 원격 공유의 경로. /mnt/fw_share여야 합니다.

다음은 환경 파일의 예입니다.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

단계 4. docker_compose.yml을 편집하고 다음 속성을 업데이트합니다.

- **이미지** 속성을 2단계에서 사용한 설치 이미지 파일의 이름으로 설정합니다.

  **참고:** `docker tag` 명령을 사용하여 이미지 파일 이름을 변경할 수 있습니다(예: '최신'으로 변경).
- 원격 공유를 원격 펌웨어 리포지토리로 사용하고 XClarity Administrator 백업을 저장하려면 **볼륨** 속성에서 각 원격 공유에 대한 호스트 탑재 지점을 설정합니다.
- dns 속성을 DNS 서버의 IP 주소로 설정합니다.
- 컨테이너는 호스트에 사용할 수 있는 프로세서 및 메모리 리소스 풀을 공유합니다. 선택적으로 **CPU** 및 **메모리** 속성을 설정하여 리소스 사용량에 대한 제한사항을 정의합니다.
- 컨테이너에서 macvlan 인터페이스의 상위 인터페이스로 사용할 호스트 시스템의 네트워크 인터페이스 이름에 **상위** 속성을 설정합니다. 이 인터페이스는 컨테이너에 할당된 서브넷에 직접 액세스할 수 있어야 합니다.
- 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이**를 설정합니다. 일반적으로 서브넷과 게이트웨이는 ${ADDRESS}이(가) 속하는 관리 네트워크에 해당합니다.
- IPv6을 지원하려면 enable_ipv6 속성을 'true'로 설정하고, ipv6_address 속성을 IPv6 주소로 설정하고, 네트워크 토폴로지에 따라 **서브넷** 및 **게이트웨이** 속성 세트를 추가하십시오(일반적으로 IPv6 주소가 속하는 관리 네트워크에 해당).

다음은 IPv6가 사용 설정된 YML 파일의 예입니다.

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   #docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
   - ssh:/etc/ssh
   - xcat:/etc/xcat
  networks:
   lan:
    ipv4_address: ${ADDRESS}
    ipv6_address: "2001:8003:7d51:2003::2"
  dns:
   - 192.0.2.10
```

```
    - 192.0.2.11
   deploy:
    resources:
     limits:
      cpus: "2.0"
      memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
 lan:
  name: lan
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eth0
  ipam:
   config:
    - subnet: 192.0.0.0/19
     gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
     gateway: "2001:8003:7d51:2000::1"
```

단계 5. 다음 명령을 실행하여 이미지를 Docker에 배포합니다. 여기에서 *<ENV_FILENAME>*은(는) 2단계에서 만든 환경 변수 파일의 이름입니다.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME}
--env-file <ENV_FILENAME> up -d
```

### 완료한 후에

XClarity Administrator에 로그인하여 구성하십시오(Lenovo XClarity Administrator 웹 인터페이스에 처음 액세스 및 Lenovo XClarity Administrator 구성 참조).

## 고가용성 구현

Docker Datacenter를 사용하여 Docker Engine에서 실행 중인 Lenovo XClarity Administrator 컨테이너를 위한 고가용성 환경을 설정할 수 있습니다.

Docker Datacenter 고가용성에 대한 자세한 정보는 Docker Datacenter 웹 페이지의 고가용성 아키텍처 및 앱의 내용을 참고하십시오.

# 제 4 장 Lenovo XClarity Administrator 구성

Lenovo XClarity Administrator에 처음 액세스하는 경우 처음으로 XClarity Administrator를 설정하려면 몇 가지 단계를 완료해야 합니다.

**자세히 알아보기:** XClarity Administrator, 첫 번째 구성

### 절차

XClarity Administrator를 처음 설정하려면 다음 단계를 완료하십시오.


단계 1. XClarity Administrator 웹 인터페이스에 액세스하십시오.

단계 2. 라이센스 계약을 읽고 동의하십시오.

단계 3. 감독자 권한을 가진 사용자 계정을 작성하십시오.

**팁:** 필요한 경우 백업을 위해 감독자 권한을 가진 두 개 이상의 사용자 계정을 작성할 것을 고려하십시오.

단계 4. 데이터 및 관리 네트워크의 IP 주소를 포함하여 네트워크 액세스를 구성하십시오.

단계 5. 날짜 및 시간을 구성하십시오.

단계 6. 개인정보 보호 정책, 사용 및 하드웨어 데이터, Lenovo 지원(콜 홈), Lenovo 업로드 기능 및 제품 보증 등 서비스 및 지원 설정을 구성하십시오.

단계 7. 인증 서버, 사용자 그룹, 서버 인증서 및 암호 모드를 포함하여 보안 설정을 구성하십시오.

단계 8. 섀시, 서버, 스위치 및 스토리지 장치를 관리하십시오.

## Lenovo XClarity Administrator 웹 인터페이스에 처음 액세스

XClarity Administrator 가상 컴퓨터와 네트워크 연결된 컴퓨터에서 XClarity Administrator 웹 인터페이스를 실행할 수 있습니다.

### 시작하기 전에

다음 지원되는 웹 브라우저 중 하나를 사용하십시오.
- Chrome™ 48.0 이상(원격 콘솔의 경우 55.0 이상)
- Firefox® ESR 38.6.0 이상
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 이상(IOS7 이상 및 OS X)

**참고:** Safari 웹 브라우저를 사용하여 XClarity Administrator에서 관리-컨트롤러 인터페이스를 실행하는 것은 지원되지 않습니다.

XClarity Administrator 관리 노드에 네트워크 연결된 시스템으로부터 XClarity Administrator 웹 인터페이스에 로그인하십시오.

## 절차

XClarity Administrator 웹 인터페이스에 처음으로 액세스하려면 다음 단계를 완료하십시오.

단계 1. 브라우저에서 XClarity Administrator의 IP 주소를 가리키십시오.

**팁:** 웹 인터페이스는 보안 연결을 통해 액세스합니다. https를 사용하십시오.

- **컨테이너의 경우**. 다음 URL을 사용하여 XClarity Administrator에 액세스하기 위해 ${ADDRESS} 변수에 지정된 IPv4 주소를 사용합니다.
  `https://<IPv4_address>/ui/login.html`

  예를 들어, 다음과 같습니다.
  `https://192.0.2.10/ui/login.html`

- **가상 어플라이언스의 경우**. 사용하는 IP 주소는 환경이 설정된 방식에 따라 다릅니다.

  분리된 서브넷에 Eth0 및 Eth1 네트워크가 있고 두 서브넷 모두에 DHCP를 사용하는 경우 초기 설정 시 웹 인터페이스에 액세스할 때 *Eth1* IP 주소를 사용하십시오. XClarity Administrator가 처음 시작되면 Eth0 및 Eth1은 DHCP 할당 IP 주소를 가져오고 XClarity Administrator 기본 게이트웨이는 *Eth1*의 DHCP 할당 게이트웨이로 설정됩니다.

  **고정 IPv4 주소 사용**

  eth0_config에서 IPv4를 지정한 경우 이 IPv4 주소를 사용하여 다음 URL로 XClarity Administrator에 액세스하십시오.
  `https://<IPv4_address>/ui/login.html`

  예를 들어, 다음과 같습니다.
  `https://192.0.2.10/ui/login.html`

  **XClarity Administrator와 동일한 브로드캐스트 도메인에서 DHCP 서버 사용**

  DHCP 서버가 XClarity Administrator와 동일한 브로드캐스트 도메인에서 설정되는 경우 XClarity Administrator 가상 컴퓨터 콘솔에 표시된 IPv4 주소를 사용하여 다음 URL로 XClarity Administrator에 액세스하십시오.
  `https://<IPv4_address>/ui/login.html`

  예를 들어, 다음과 같습니다.
  `https://192.0.2.10/ui/login.html`

  **XClarity Administrator와 다른 브로드캐스트 도메인에서 DHCP 서버 사용**

  DHCP 서버가 동일한 브로드캐스트 도메인에 설정되지 ***않은*** 경우 XClarity Administrator 가상 컴퓨터 콘솔에서 eEth0(관리 네트워크)에 대해 표시된 IPv6 LLA(링크 로컬 주소)를 사용하여 XClarity Administrator에 액세스하십시오. 예를 들면 다음과 같습니다.

```
---------------
Lenovo XClarity Administrator  Version x.x.x
---------------

eth0  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
      inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
      inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>
      ether 00:15:5d:0c:d1:92   txqueuelen 1000 (Ethernet)
      RX errors 0  dropped 0  overruns 0  frame 0

eth1  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
      inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
      inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
 1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
 2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
 x. To continue without changing IP settings
```

... ...

**팁:** IPv6 LLA(링크 로컬 주소)는 인터페이스의 MAC 주소에서 가져옵니다.

**주의:** XClarity Administrator를 원격으로 구성하는 경우 동일한 레이어 2 네트워크에 연결할 수 있어야 합니다. 초기 설정이 완료될 때까지 라우팅되지 않은 주소에서 액세스해야 합니다. 따라서 XClarity Administrator에 연결된 다른 VM에서 XClarity Administrator에 액세스하는 것을 고려하십시오. 예를 들어 XClarity Administrator가 설치된 호스트의 다른 VM에서 XClarity Administrator에 액세스할 수 있습니다.

- **Firefox:**

  Firefox 브라우저에서 XClarity Administrator 웹 인터페이스에 액세스하려면 다음 URL을 사용하여 로그인하십시오. IPv6 주소를 입력할 때 브래킷이 필요합니다.

  `https://[<IPv6_LLA>/ui/login.html]`

  예를 들어 Eth0에 대해 표시된 이전 예에 따라 웹 브라우저에 다음 URL을 입력하십시오.

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

- **Internet Explorer:**

  Internet Explorer 브라우저에서 XClarity Administrator 웹 인터페이스에 액세스하려면 다음 URL을 사용하여 로그인하십시오. IPv6 주소를 입력할 때 브래킷이 필요합니다.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  여기서 *<zone_index>*는 웹 브라우저를 실행한 컴퓨터에서 관리 네트워크에 연결된 이더넷 어댑터의 ID입니다. Windows에서 브라우저를 사용하는 경우 `ipconfig` 명령을 사용하여 영역 인덱스를 찾으십시오. 영역 인덱스는 어댑터의 **링크 로컬 IPv6 주소** 필드에서 백분율 기호(%) 다음에 나옵니다. 다음 예에서는 영역 인덱스는 "30"입니다.

  ```
  PS C:> ipconfig
  Windows IP 구성

  이더넷 어댑터 vEthernet(teamVirtualSwitch):

    연결 특정 DNS 접미사 . :
    링크 로컬 IPv6 주소 . . . . . : 2001:db8:56ff:fe80:bea3%30
    자동 구성 IPv4 주소. . : 192.0.2.30
    기본 게이트웨이 . . . . . :
  ```

  Linux에서 브라우저를 사용하는 경우 `ifconfig` 명령을 사용하여 영역 인덱스를 찾으십시오. 또한 어댑터 이름(일반적으로 Eth0)을 영역 인덱스로 사용할 수 있습니다.

  예를 들어 Eth0에 대해 표시된 예와 영역 인덱스에 따라 웹 브라우저에 다음 URL을 입력하십시오.

  `https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html`

단계 2. Lenovo XClarity Administrator에 처음 액세스하면 보안 또는 인증서 경고를 받을 수 있습니다. 이 경고는 무시할 수 있습니다.

## 결과

초기 설치 페이지가 표시됩니다.


### 완료한 후에

초기 설치 단계를 완료하여 XClarity Administrator를 구성하십시오(Lenovo XClarity Administrator 구성 참조).

## 사용자 계정 만들기

사용자 계정은 Lenovo XClarity Administrator 및 관리되는 인증 하에 있는 장치에 대한 권한 및 액세스 권한을 관리하는 데 사용됩니다.

### 이 작업 정보

작성하는 첫 번째 사용자 계정은 감독자 역할을 가지고 활성화(사용)되어야 합니다.

보안 강화를 위해 **감독자** 역할을 가진 둘 이상의 사용자 계정을 작성하십시오. Lenovo XClarity Administrator를 복원해야 하는 경우를 대비해 이러한 사용자 계정의 암호를 기록하여 이를 보안 위치에 저장하십시오.

### 절차

사용자 계정을 작성하려면 다음 단계를 완료하십시오.

단계 1. 새 감독자 사용자 만들기 대화 상자에서 다음 정보를 입력하십시오.

- 사용자의 사용자 이름과 설명을 입력하십시오.
- 새 암호와 새 암호 확인을 입력하십시오. 암호 규칙은 현재 계정 보안 설정을 기반으로 합니다.

- 사용자에게 적합한 작업을 수행할 권한을 부여할 역할 그룹을 하나 이상 선택하십시오.

  역할 그룹에 대한 정보 및 사용자 지정 역할 그룹 작성 방법에 대해서는 XClarity Administrator 온라인 설명서에서 역할 그룹 만들기의 내용을 참조하십시오.
- (옵션) 사용자가 XClarity Administrator에 처음 로그인할 때 암호를 강제로 변경하도록 하려면 **처음 액세스할 때 암호 변경**을 Yes로 설정하십시오.

단계 2. **만들기**를 클릭하십시오.

단계 3. 추가 사용자를 만들려면 **만들기** 아이콘( )을 클릭하고 이전 단계를 반복하십시오.

단계 4. **초기 설정으로 돌아가기**를 클릭하십시오.

# 네트워크 액세스 구성

네트워크 액세스를 구성하기 위해 최대 두 개의 네트워크 인터페이스, Lenovo XClarity Administrator의 호스트 이름 및 사용할 DNS 서버를 구성할 수 있습니다.

## 이 작업 정보

XClarity Administrator에는 구현하는 네트워크 토폴로지에 따라 환경에 대해 정의할 수 있는 두 개의 분리된 네트워크 인터페이스가 있습니다. 가상 어플라이언스에서 이러한 네트워크의 이름은 eth0 및 eth1입니다. 컨테이너의 경우 이름을 직접 지정할 수 있습니다.

- 네트워크 인터페이스(Eth0)가 하나만 있는 경우:
  - 인터페이스는 장치 검색 및 관리(예, 서버 구성 및 펌웨어 업데이트)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 베이스보드 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
  - XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
  - 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.
  - 운영 체제 이미지를 배포하고 OS 장치 드라이버를 업데이트 하려는 경우, 네트워크 인터페이스는 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 IP 네트워크 연결을 해야 합니다.

    **참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.
- 2개의 네트워크 인터페이스(Eth0 및 Eth1)가 있는 경우:
  - 첫 번째 네트워크 인터페이스(일반적으로 Eth0 인터페이스)는 관리 네트워크에 연결해야 하며 장치 검색 및 관리(서버 구성 및 펌웨어 업데이트 포함)를 지원하도록 구성해야 합니다. 각 관리 섀시의 CMM 및 Flex 스위치, 각 관리 서버의 관리 컨트롤러 및 각 RackSwitch 스위치와 통신할 수 있어야 합니다.
  - 두 번째 네트워크 인터페이스(일반적으로 Eth1 인터페이스)는 내부 데이터 네트워크, 공개 데이터 네트워크 또는 둘 다와 통신하도록 구성할 수 있습니다.
  - XClarity Administrator를 사용하여 펌웨어 및 OS 장치 드라이버 업데이트를 확보하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다. 그렇지 않으면 업데이트를 리포지토리로 가져와야 합니다.
  - 서비스 데이터를 수집하거나 자동 문제 알림(콜 홈 및 Lenovo 업로드 기능 포함)을 사용하려는 경우, 하나 이상의 네트워크 인터페이스가 기본적으로 방화벽을 통해 인터넷에 연결되어 있어야 합니다.

– 운영 체제 이미지를 배포하고 장치 드라이버를 업데이트하려는 경우, eth1 또는 eth0 인터페이스를 사용하도록 선택할 수 있습니다. 그러나 사용하는 인터페이스에 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결이 있어야 합니다.

  **참고:** OS 배포 및 OS 장치 드라이버 업데이트를 위해 분리된 네트워크를 구현한 경우, 데이터 네트워크 대신 해당 네트워크에 연결하도록 두 번째 네트워크 인터페이스를 구성할 수 있습니다. 하지만 각 서버의 운영 체제가 데이터 네트워크에 액세스할 수 없는 경우, 필요 시 OS 배포 및 OS 장치 드라이버 업데이트를 위해 호스트 운영 체제에서 데이터 네트워크로 연결할 수 있도록 서버의 추가 인터페이스를 구성하십시오.

다음 테이블은 사용자 환경에 구현된 네트워크 토폴로지 유형을 기반으로 하여 XClarity Administrator 네트워크 인터페이스에 가능한 구성을 표시합니다. 이 테이블을 사용하여 각 네트워크 인터페이스를 정의하는 방법을 판별하십시오.

***표 3. 네트워크 토폴로지 기준 각 네트워크 인터페이스 역할***

| 네트워크 토폴로지 | 인터페이스 1(eth0)의 역할 | 인터페이스 2(eth1)의 역할 |
|---|---|---|
| 컨버지드 네트워크(OS 배포 및 OS 장치 드라이버 업데이트를 지원하는 관리 및 데이터 네트워크) | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색<br>• OS 배포<br>• OS 장치 드라이버 업데이트 | 없음 |
| 분리형 관리 네트워크(OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원 포함) | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색<br>• OS 배포<br>• OS 장치 드라이버 업데이트 | 데이터 네트워크<br>• 없음 |
| OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원을 포함하는 분리형 관리 네트워크 및 데이터 네트워크 | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색 | 데이터 네트워크<br>• OS 배포<br>• OS 장치 드라이버 업데이트 |

*표 3. 네트워크 토폴로지 기준 각 네트워크 인터페이스 역할 (계속)*

| 네트워크 토폴로지 | 인터페이스 1(eth0)의 역할 | 인터페이스 2(eth1)의 역할 |
|---|---|---|
| OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원을 포함하지 않는 분리형 관리 네트워크 및 데이터 네트워크 | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색 | 데이터 네트워크<br>• 없음 |
| 관리 네트워크만(OS 배포 및 OS 장치 드라이버 업데이트는 지원되지 않음) | 관리 네트워크<br>• 검색 및 관리<br>• 서버 구성<br>• 펌웨어 업데이트<br>• 서비스 데이터 수집<br>• 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능)<br>• 보증 데이터 검색 | 없음 |

XClarity Administrator 네트워크 인터페이스에 대한 자세한 정보는 네트워크 고려사항의 내용을 참조하십시오.

## 절차

네트워크 액세스를 구성하려면 다음 단계를 완료하십시오.

단계 1. 초기 설치 페이지에서 **네트워크 액세스 구성**을 클릭하십시오. 네트워크 액세스 편집 페이지가 표시됩니다.


단계 2. XClarity Administrator를 사용하여 운영 체제를 배포하고 OS 장치 드라이버를 업데이트하는 경우, 운영 체제 관리에 사용할 네트워크 인터페이스를 선택하십시오.

- XClarity Administrator에 한 인터페이스만 정의하는 경우, 해당 인터페이스를 사용하여 하드웨어만 검색하고 관리하는지 또는 해당 인터페이스를 사용하여 운영 체제를 관리하기도 하는지를 선택하십시오.
- XClarity Administrator에 대해 두 개의 인터페이스(Eth0 및 Eth1)를 정의하는 경우, 운영 체제 관리에 사용할 인터페이스를 결정하십시오. "없음"을 선택하는 경우, XClarity Administrator에서 관리되는 서버로 운영 체제 이미지를 배포하거나 OS 장치 드라이버를 업데이트*할 수 없습니다*.

단계 3. IP 설정을 지정하십시오.

a. 첫 번째 인터페이스의 경우 IPv4 주소, IPv6 주소 또는 둘 다를 지정하십시오.

- IPv4. 인터페이스에 IPv4 주소를 할당해야 합니다. 할당된 IP 주소를 고정으로 사용하거나 DHCP 서버에서 IP 주소를 얻도록 선택할 수 있습니다.
- IPv6. 선택적으로 다음 할당 방법을 사용하여 인터페이스에 IPv6 주소를 할당할 수 있습니다.
  - 정적으로 할당된 IP 주소 사용
  - 상태 저장 주소 구성 사용(DHCPv6)
  - 상태 비저장 주소 자동 구성 사용

  **참고:** IPv6 주소 제한에 대한 정보는 IP 구성 제한의 내용을 참조하십시오.

b. 두 번째 인터페이스가 사용 가능한 경우, IPv4 주소, IPv6 주소 또는 두 개 모두 지정하십시오.

  **참고:** 이 인터페이스에 할당되는 IP 주소는 첫 번째 인터페이스에 할당되는 IP 주소와 다른 서브넷에 있어야 합니다. DHCP를 사용하여 두 인터페이스(Eth0 및 Eth1)에 IP 주소를 할당하도록 선택한 경우 DHCP 서버가 두 인터페이스의 IP 주소에 동일한 서브넷을 할당하지 않아야 합니다.

- IPv4. 할당된 IP 주소를 고정으로 사용하거나 DHCP 서버에서 IP 주소를 얻도록 선택할 수 있습니다.
- IPv6. 선택적으로 다음 할당 방법을 사용하여 인터페이스에 IPv6 주소를 할당할 수 있습니다.
  - 정적으로 할당된 IP 주소 사용
  - 상태 저장 주소 구성 사용(DHCPv6)
  - 상태 비저장 주소 자동 구성 사용

c. 기본 게이트웨이를 지정하십시오.

  기본 게이트웨이를 지정하는 경우 이는 올바른 IP 주소여야 하고 네트워크 인터페이스(Eth0 또는 Eth1) 중 하나의 IP 주소와 동일한 네트워크 마스크(동일한 서브넷)를 사용해야 합니다. 단일 인터페이스를 사용하는 경우 기본 게이트웨이는 네트워크 인터페이스와 동일한 서브넷에 있어야 합니다.

  인터페이스가 DHCP를 사용하여 IP 주소를 얻는 경우 기본 게이트웨이도 DHCP를 사용합니다. DHCP 서버에서 수신한 기본 게이트웨이 주소를 재정의하는 기본 게이트웨이 주소를 수동으로 입력하려면 **게이트웨이 재정의** 확인란을 선택합니다.

  **팁:**

- 게이트웨이가 네트워크 인터페이스의 서브넷 중 하나와 일치하는지 확인합니다. 기본 게이트웨이는 해당 네트워크 인터페이스를 통해 자동으로 설정됩니다.
- DHCP 제공 게이트웨이로 돌아가려면 **게이트웨이 재정의** 확인란을 선택 취소합니다.

  **경고:**
  **게이트웨이를 재정의하기로 선택한 경우 올바른 게이트웨이 주소를 입력하도록 주의하시기 바랍니다. 그렇지 않으면 이 관리 서버에 연결할 수 없으며 원격으로 로그인하여 수정할 방법이 없습니다.**

d. **IP 설정 저장**을 클릭하십시오.

단계 4. **옵션:** 고급 설정을 구성하십시오.

a. **고급 라우팅** 탭을 클릭하십시오.


b. **고급 경로 설정** 테이블에 이 인터페이스에서 사용할 하나 이상의 경로 항목을 지정하십시오.

하나 이상의 경로 항목을 정의하려면 다음 단계를 완료하십시오.
1. 인터페이스를 선택하십시오.
2. 다른 호스트 또는 네트워크에 대한 경로가 될 수 있는 경로 유형을 지정하십시오.
3. 경로를 지정할 대상 호스트 또는 네트워크 주소를 지정하십시오.
4. 대상 주소의 서브넷 마스크를 지정하십시오.
5. 패킷을 처리할 게이트웨이 주소를 지정하십시오.

c. **고급 라우팅 저장**을 클릭하십시오.

단계 5. 선택적으로, DNS 및 프록시 설정을 수정하십시오.

a. **DNS 및 프록시** 탭을 클릭하십시오.


b. XClarity Administrator에 사용할 호스트 이름 및 도메인 이름을 지정하십시오.

c. DNS 작동 모드를 선택하십시오. **정적 모드** 또는 DHCP 중 선택 가능합니다.

**주의:** DNS 작동 모드를 변경하는 경우 관리 서버를 다시 시작해야 합니다.

**참고:** DHCP 서버를 사용하여 IP 주소를 얻도록 선택한 경우 다음에 XClarity Administrator가 DHCP 임대를 갱신하면 **DNS 서버** 필드의 변경사항을 덮어씁니다.

d. 사용할 DNS (Domain Name System) 서버 하나 이상의 IP 주소와 각 서버의 우선 순위를 지정하십시오.

e. 직접 연결 또는 HTTP 프록시(XClarity Administrator이(가) 인터넷에 액세스할 수 있을 경우) 중에서 인터넷 액세스 방식을 지정하십시오.

**참고:** HTTP 프록시를 사용하는 경우 다음 요구사항이 충족되는지 확인하십시오.
- 프록시 서버가 기본 인증을 사용하도록 설정되었는지 확인하십시오.
- 프록시 서버가 비종결 프록시(non-terminating proxy)로 설정되었는지 확인하십시오.
- 프록시 서버가 전달 프록시로 설정되었는지 확인하십시오.
- 로드 밸런서가 한 프록시 서버와의 세션을 유지하고 세션 간을 전환하지 않도록 구성되었는지 확인하십시오.

HTTP 프록시를 사용하도록 선택한 경우 필수 필드를 완료하십시오.
1. 프록시 서버 호스트 이름과 포트를 지정하십시오.
2. 인증을 사용할지 여부를 선택하고 필요에 따라 사용자 이름과 암호를 지정하십시오.
3. 프록시 테스트 URL을 지정하십시오.
4. **프록시 테스트**를 클릭하여 프록시 설정이 제대로 구성되어 작동되는지를 확인하십시오.

f. **DNS 및 프록시 저장**을 클릭하십시오.

g. XClarity Administrator 관리 서버 FQDN(정규화된 도메인 이름) 및 DNS 정보를 IMM2, XCC 및 XCC2가 있는 관리되는 서버에 푸시하여 관리되는 서버가 이 정보를 사용하여 관리 서버를 찾을 수 있도록 합니다.
1. **BMC에 FQDN/DNS 푸시**를 클릭합니다.
2. 베이스보드 관리 컨트롤러에서 기존 DNS 항목을 처리하는 방법을 선택합니다.
   - 기존 DNS 항목을 유지하고 사용 가능한 다음 슬롯에 관리 서버 DNS 항목을 추가합니다.
   - 모든 기존 DNS 항목을 관리 서버 DNS 항목으로 바꿉니다.
3. 편집 필드에 **예**를 입력합니다.
4. **적용**을 클릭하십시오.

이 작업을 수행하기 위한 작업이 생성됩니다. **모니터링 → 작업** 카드에서 작업 진행상태를 모니터링할 수 있습니다. 작업이 성공적으로 완료되지 않은 경우에는 작업 링크를 클릭하여 작업에 대한 세부 정보를 표시합니다(XClarity Administrator 온라인 설명서의 작업 관련 작업 참조).

**BMC에서 FQDN/DNS 제거**를 클릭하여 IMM2, XCC 및 XCC2가 있는 관리되는 서버에서 관리 서버 FQDN 및 DNS 정보를 제거할 수도 있습니다. 기타 기존 DNS 항목을 유지하거나, 모든 DNS 항목을 제거하거나, 관리 서버 정보와 일치하는 항목만 제거하도록 선택할 수 있습니다.

단계 6. **뒤로**를 클릭하십시오.

단계 7. **연결 테스트**를 클릭하여 네트워크 설정을 확인하십시오.

# 날짜 및 시간 구성

Lenovo XClarity Administrator의 날짜 및 시간을 수동으로 설정할 수 있지만 XClarity Administrator와 모든 관리 장치 간의 시간 소인을 동기화하는 데 사용할 수 있는 NTP(Network Time Protocol) 서버를 설정하는 것이 더 좋은 방법입니다.

## 시작하기 전에

하나 이상(최대 4개)의 NTP(Network Time Protocol) 서버를 사용하여 관리되는 장치에서 받은 모든 이벤트의 타임 스탬프를 XClarity Administrator와 동기화해야 합니다.

**팁:** NTP 서버는 관리 네트워크(일반적으로 Eth0 인터페이스)를 통해 액세스 가능해야 합니다. XClarity Administrator가 실행 중인 호스트에 NTP 서버를 설정할 것을 고려하십시오.

NTP 서버의 시간을 변경하는 경우 XClarity Administrator가 새 시간과 동기화되는 데 약간의 시간이 걸릴 수 있습니다.

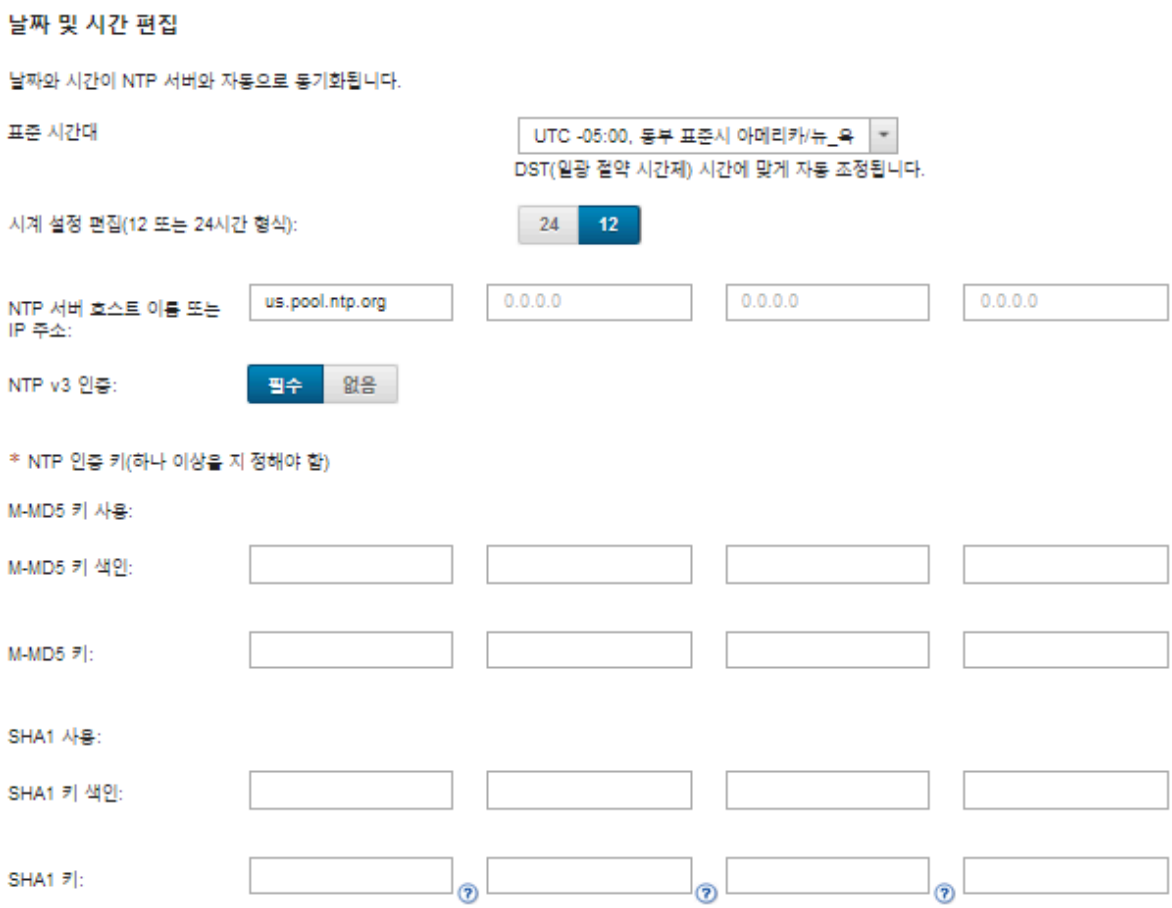
**주의:** XClarity Administrator 가상 어플라이언스와 해당 호스트가 동일한 시간 소스와 동기화되도록 설정해야만 XClarity Administrator와 해당 호스트 간에 부주의하게 수행되는 잘못된 시간 동기화가 방지됩니다. 일반적으로 호스트는 가상 어플라이언스와 시간 동기화를 수행하도록 구성됩니다. XClarity Administrator가 해당 호스트가 아닌 다른 소스와 동기화하도록 설정된 경우 XClarity Administrator 가상 어플라이언스와 해당 호스트 간에 호스트 시간 동기화를 사용 안 함으로 설정해야 합니다.

- ESXi의 경우 VMware – 시간 동기화 사용 안 함 웹 페이지의 다음 지시 사항을 참조하십시오.
- Hyper-V의 경우 Hyper-V 관리자에서 XClarity Administrator 가상 컴퓨터를 마우스 오른쪽 단추로 클릭한 다음 **설정**을 클릭하십시오. 대화 상자의 탐색 분할창에서 **관리 > 통합 서비스**를 클릭한 다음 **시간 동기화**를 선택 취소하십시오.

## 절차

XClarity Administrator에 대한 NTP 서버를 설정하려면 다음 단계를 완료하십시오.

단계 1. 초기 설치 페이지에서 **날짜 및 시간 기본 설정 구성**을 클릭하십시오. 날짜 및 시간 편집 페이지가 표시됩니다.




단계 2. 날짜 및 시간 대화 상자를 지정하십시오.

1. XClarity Administrator의 호스트가 있는 시간대를 선택하십시오.

   선택한 시간대에서 일광절약시간(DST)를 사용하는 경우 시간이 DST에 맞게 자동으로 조정됩니다.
2. 12시간 또는 24시간 시계를 사용하도록 선택하십시오.
3. 네트워크에 있는 각 NTP 서버의 호스트 이름 또는 IP 주소를 지정하십시오. 최대 4개의 NTP 서버를 정의할 수 있습니다.
4. 네트워크 내의 XClarity Administrator와 NTP 서버 간에 NTP v3 인증을 사용하려면 **필수**를 선택하고 NTP v1 인증을 사용하려면 **없음**을 선택하십시오.

   관리되는 Flex System CMM 및 베이스보드 관리 컨트롤러에 v3 인증이 필요한 펌웨어가 있는 경우 및 네트워크 내의 XClarity Administrator와 하나 이상의 NTP 서버 간에 NTP v3 인증이 필요한 경우 v3 인증을 사용할 수 있습니다.
5. NTP v3 인증을 사용하는 경우 각각의 해당 NTP 서버에 대한 인증 키와 색인을 설정하십시오. M-MD5 키, SHA1 키 또는 둘 다를 지정할 수 있습니다. M-MD5 또는 SHA1 키가 모두 지정된 경우, XClarity Administrator가 M-MD5 또는 SHA1 키를 관리되는 Flex System CMM 및 이를 지원하는 관리 컨트롤러로 푸시합니다. XClarity Administrator는 이 키를 사용하여 NTP 서버에 인증합니다.
   - M-MD5 키의 경우, 대소문자(az, AZ), 숫자(0~9) 및 다음 특수 문자(@#)만 포함하는 ASCII 문자열을 지정하십시오.
   - SHA1 키의 경우 40자의 ASCII 문자열(0–9 및 a-f만 해당)을 지정하십시오.
   - 지정된 키 인덱스 및 인증 키는 NTP 서버에 설정된 키 ID 및 암호 값과 일치해야 합니다. 예를 들어 NTP 서버에 입력된 SHA1 키의 키 인덱스가 5이면, XClarity Administrator SHA1 키의 지정된 키 인덱스도 5입니다. 키 ID 및 암호 설정에 대한 자세한 정보는 NTP 서버 설명서를 참조하십시오.
   - 2개 이상의 NTP 서버에서 동일한 키를 사용하는 경우에도 v3 인증을 사용하는 각 NTP 서버에 대한 키를 지정해야 합니다.
   - v3 인증을 사용하지만 NTP 서버에 대한 인증 키와 색인을 제공하지 않으면 기본적으로 v1 인증이 사용됩니다.
   - 여러 개의 NTP 서버를 지정한 경우 NTP 서버는 모두 v3 인증을 받거나 모두 v1 인증을 받아야 합니다. v3 인증과 v1 인증이 혼합된 NTP 서버는 지원되지 않습니다.
   - v3 인증을 받은 여러 개의 NTP 서버를 지정한 경우 키가 같지 않으면 키 인덱스가 고유해야 합니다. 예를 들어, SHA1 키가 NTP 서버 1과 2에서 다른 경우 NTP 서버 1과 2는 SHA1 키 색인 1을 가질 수 없습니다. NTP 서버 중 하나를 재구성하여 다른 NTP 서버의 키 색인과 다른 키 색인을 가진 키를 허용해야 합니다. 그렇지 않으면 키 색인과 연결된 마지막으로 정의된 키가 동일한 키 색인을 가진 모든 NTP 서버에 대해 구성됩니다.

단계 3. **저장**을 클릭하십시오.

---

# 서비스 및 지원 구성

사용 데이터, Lenovo 지원(콜 홈), Lenovo 업로드 기능 및 제품 보증 등의 서비스 및 지원 설정을 구성할 수 있습니다.

## 절차

보안을 구성하려면 다음 단계를 완료하십시오.

단계 1. 초기 설치 페이지에서 **서비스 및 지원 설정 구성**을 클릭하십시오. 서비스 및 지원 페이지가 표시됩니다.


단계 2. Lenovo 개인정보 보호정책을(를) 읽고 동의하십시오.

**참고:** 귀하는 먼저 Lenovo 개인정보 보호정책을(를) 수락하지 않으면 Lenovo에 데이터를 수집하고 전송할 수 없습니다. 개인 정보 보호 정책을 거부하기로 선택한 경우 나중에 **서비스 및 지원 → 콜 홈 구성** 페이지에서 개인 정보 보호 정책을 검토하고 수락할 수 있습니다.

단계 3. 선택적으로 Lenovo XClarity Administrator가 사용 현황 및 하드웨어 정보를 수집할 수 있도록 선택하고 **적용**을 클릭하십시오.

다음 유형의 데이터를 수집하여 Lenovo에 전송할 수 있습니다.

- **사용 현황 데이터**

  Lenovo로 사용 현황 데이터를 전송하도록 동의하면 다음 데이터가 수집되어 매주 전송됩니다. 이 데이터는 *익명*으로 처리됩니다. 개인 데이터(일련 번호, UUID, 호스트 이름, IP 주소 및 사용자 이름 포함)는 수집되거나 Lenovo로 전송되지 않습니다.
  - 수행된 작업 로그
  - 발생한 이벤트 목록 및 발생한 타임 스탬프
  - 발생한 감사 이벤트 목록 및 발생한 타임 스탬프
  - 실행된 작업 목록 및 각 작업의 성공 또는 실패 정보
  - 메모리 사용량, 프로세서 사용량 및 디스크 공간을 포함한 XClarity Administrator 지표
  - 모든 관리 장치에 대한 제한된 인벤토리 데이터

- **하드웨어 데이터**

  Lenovo로 하드웨어 데이터를 전송하도록 동의하면 다음 데이터가 수집되어 매주 전송됩니다. 이 데이터는 *익명으로 처리되지 않습니다*. 하드웨어 데이터에는 UUID 및 일련 번호와 같은 속성이 포함됩니다. IP 주소나 호스트 이름은 포함되지 않습니다.

- **일별 하드웨어 데이터**. 각 인벤토리 변경에 대해 다음 데이터가 포함됩니다.
  - 인벤토리-변경 이벤트(FQXHMDM0001I)
  - 해당 이벤트와 관련된 장치의 인벤토리 데이터 변경
- **주별 하드웨어 데이터**. 모든 관리 장치에 대해 인벤토리 데이터가 포함됩니다.

사용 현황 데이터 및 하드웨어 데이터가 Lenovo로 전송되면 이벤트가 감사 로그에 기록됩니다.

언제든지 이 설정을 변경할 수 있으며 **관리 → 서비스 및 지원**을 클릭한 다음 **정기 데이터 업로드** 탭을 클릭하면 나오는 링크를 사용하여 Lenovo로 수집 및 전송된 마지막 아카이브를 다운로드할 수 있습니다.

단계 4. 선택적으로 **콜 홈 구성**을 클릭하여 Lenovo 지원(콜 홈)에 대한 자동 문제 알림을 설정하십시오. 그런 다음 **적용 및 사용**을 클릭하여 기본 콜 홈 서비스 전달자를 작성하거나 **적용만**을 클릭하여 연락처 정보를 저장하십시오.

Lenovo 지원에 대한 자동 문제 알림 설정 정보에 대해서는 XClarity Administrator 온라인 설명서에서 콜 홈 설정의 내용을 참조하십시오.

단계 5. 선택적으로 **Lenovo 업로드 기능**을 클릭하여 Lenovo 업로드 기능에 대한 자동 문제 알림을 설정하십시오. 그런 다음 **적용 및 사용**을 클릭하여 기본 Lenovo 업로드 기능 서비스 전달자를 작성하거나 **적용만**을 클릭하여 설정 정보를 저장하십시오.

Lenovo 업로드 기능에 대한 자동 문제 알림 설정 정보에 대해서는 XClarity Administrator 온라인 설명서에서 Lenovo 업로드 기능에 자동 문제 알림 설정의 내용을 참조하십시오.

단계 6. 선택적으로 **보증**을 클릭하여 관리되는 장치에 대한 보증 정보를 수집하는 데 필요한 외부 연결을 사용하도록 설정하십시오.

관리되는 장치의 보증 상태(확장된 보증 포함) 보기에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 보증 정보 보기의 내용을 참조하십시오.

단계 7. 필요한 경우 **Lenovo 게시판 서비스**를 클릭하여 Lenovo에서 XClarity Administrator에 서비스 게시판을 보내도록 허용한 후 **적용**을 클릭하십시오.

Lenovo가 전송하는 서비스 게시판 유형에 대해 자세히 알아보려면 XClarity Administrator 온라인 설명서에서 Lenovo에서 게시판 받기의 내용을 참조하십시오.

단계 8. XClarity Administrator가 응답이 없어 복구할 수 없는 경우 서비스 데이터와 로그를 수집하고 다운로드하는 데 사용할 수 있는 서비스 복구 암호를 지정하십시오.

서비스 복구 암호에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 서비스 복구 암호 변경의 내용을 참조하십시오.

단계 9. **초기 설정으로 돌아가기**를 클릭하십시오.

## 보안 구성

역할 그룹, 인증 서버, 사용자 계정 보안 설정, 암호 및 인증서를 포함하여 보안을 구성할 수 있습니다.

### 절차

보안을 구성하려면 다음 단계를 완료하십시오.

단계 1. 초기 설치 페이지에서 **추가 보안 설정 구성**을 클릭하십시오. 보안 페이지가 표시됩니다.

단계 2. 리소스에 대한 권한 부여와 액세스를 관리할 사용자 정의된 역할 그룹을 작성하십시오(XClarity Administrator 온라인 설명서에서 역할 그룹 만들기 참조).

*역할 그룹*은 하나 이상의 역할의 컬렉션이며 이를 사용하여 해당 역할을 여러 사용자에게 할당합니다. 역할 그룹에 구성된 역할은 역할 그룹의 멤버인 각 사용자에게 부여된 액세스 수준을 판별합니다. 각 XClarity Administrator 사용자는 하나 이상의 역할 그룹의 멤버여야 합니다.

단계 3. 인증 서버를 구성하십시오(XClarity Administrator 온라인 설명서의 인증 서버 관리 참조).

*인증 서버*는 사용자 자격 증명을 인증하는 데 사용되는 Microsoft Active Directory(LDAP) 서버입니다. XClarity Administrator는 모든 관리 장치(Flex 스위치 제외)의 중앙 사용자 관리를 위해 단일 인증 서버를 사용합니다. XClarity Administrator에서 장치를 관리하는 경우 관리되는 장치와 설치된 해당 구성 요소(Flex 스위치 제외)는 XClarity Administrator 인증 서버를 사용하도록 구성됩니다. 인증 서버에 정의된 사용자 계정을 사용하여 XClarity Administrator, CMM 및 베이스보드 관리 컨트롤러에 로그인합니다.

관리 노드의 로컬 인증 서버 대신 외부 인증 서버를 사용하도록 선택할 수 있습니다.

단계 4. 암호 복잡도, 계정 잠금 및 웹 세션 비활성 제한시간을 제어하는 사용자 계정 보안 설정을 구성하십시오(XClarity Administrator 온라인 설명서에서 사용자 계정 보안 설정 변경 참조).

단계 5. XClarity Administrator와 관리 장치 간에 보안 통신이 처리되는 방식을 제어하는 통신 모드와 프로토콜을 정의하는 암호 설정을 구성하십시오(XClarity Administrator 온라인 설명서의 암호 모드 및 통신 프로토콜 설정 참조).

단계 6. XClarity Administrator 관리되는 인증 대신 로컬 인증을 사용하여 랙 서버를 관리하려는 경우 관리 프로세스 중에 장치에 로그인하는 데 사용할 수 있는 장치 또는 Active Directory의 활성 사용자 계정에 해당하는 저장된 자격 증명을 하나 이상 만드십시오. 저장된 자격 증명에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 저장된 자격 증명 관리의 내용을 참조하십시오.

단계 7. 사용자 소유 정보가 포함된 사용자 지정된 서버 인증서를 사용하거나 외부에서 서명된 인증서를 사용할 경우 관리 시스템을 시작하기 전에 새 인증서를 생성하여 배포하십시오. 사용자 보안 인증서 생성에 대한 정보는 XClarity Administrator 온라인 설명서에서 보안 인증서 작업의 내용을 참조하십시오.

단계 8. 보안 페이지의 수직 메뉴에서 **초기 설치로 돌아가기**를 클릭하십시오.

# 장치 관리

Lenovo XClarity AdministratorFlex System 섀시, 랙 및 타워 서버, RackSwitch 스위치 및 저장 장치를 비롯한 여러 유형의 시스템을 관리할 수 있습니다. 대량 가져오기 파일을 사용하여 장치에 대한 정보를 가져와서 사용자 환경에 있는 많은 수의 장치를 쉽게 검색하고 관리할 수 있습니다.

## 시작하기 전에

**중요:**

- 최대 300대의 장치를 한 번에 관리할 수 있습니다. 대량 가져오기 파일에 장치를 300대 넘게 포함하지 마십시오.
- 장치 관리 작업을 시작한 후에는 전체 관리 작업이 완료될 때까지 기다렸다가 다른 장치 관리 작업을 시작해야 합니다.

섀시 구성 요소(예, CMM, 컴퓨팅 노드, 스위치 및 스토리지 장치)는 구성 요소가 포함된 섀시를 관리할 때 자동으로 검색되고 관리됩니다. 섀시 구성 요소는 섀시와는 별도로 검색 및 관리할 수 없습니다.

특정 포트는 섀시의 CMM 및 서버의 베이스보드 관리 컨트롤러와 통신하는 데 사용 가능해야 합니다. 시스템 관리를 시도하기 전에 이러한 포트가 사용 가능한지 확인하십시오. 포트에 대한 자세한 정보는 포트 사용 가능성의 내용을 참조하십시오.

XClarity Administrator를 사용하여 관리하려는 각 시스템에 최소 요구 펌웨어가 설치되어 있어야 합니다. 필요한 최소 펌웨어 수준은 XClarity Administrator 지원 – 호환성 웹 페이지에서 **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하여 확인할 수 있습니다.

CMM과의 대역 외 통신에 대해 세 개 이상의 TCP 명령 모드 세션이 설정되어 있어야 합니다. 세션 수 설정에 대한 정보는 CMM 온라인 설명서의 tcpcmdmode 명령의 내용을 참조하십시오.

XClarity Administrator가 관리하는 모든 CMM 및 Flex 스위치에 대해 IPv4 또는 IPv6 주소 구현을 고려하십시오. 일부 CMM 및 Flex 스위치에 대해 IPv4, 다른 것에 대해 IPv6를 구현하는 경우 일부 이벤트는 감사 로그에(또는 감사 트랩으로) 수신되지 않을 수 있습니다.

사용자 환경의 라우터를 비롯하여 ToR(top-of-rack) 스위치에 있는 멀티캐스트 SLP 전달을 사용으로 설정했는지 확인하십시오. 멀티캐스트 SLP 전달이 사용하도록 설정되어 있는지 확인하고 사용하지 않도록 설정된 경우 사용하도록 설정하는 절차를 확인하려면 특정 스위치 또는 라우터와 함께 제공된 설명서를 참조하십시오.

**중요:**

- 스위치가 XClarity Administrator에 의해 검색되고 관리되려면 먼저 RackSwitch 스위치의 펌웨어 버전에 따라 각 RackSwitch 스위치에서 멀티캐스트 SLP 전달 및 SSH를 사용 설정해야 할 수 있습니다. 자세한 정보는 System x 온라인 설명서의 랙 스위치의 내용을 참조하십시오.
- XClarity Administrator에서 검색되도록 하려면 먼저 각 스토리지 장치에서 멀티캐스트 SLP 전달을 사용으로 설정해야 합니다.
- 사용자 소유 정보가 포함된 사용자 지정된 서버 인증서를 사용하거나 외부에서 서명된 인증서를 사용할 경우 관리 시스템을 시작하기 전에 새 인증서를 생성하여 배포하십시오. 사용자 보안 인증서 생성에 대한 정보는 XClarity Administrator 온라인 설명서에서 보안 인증서 작업의 내용을 참조하십시오.
- Lenovo XClarity Administrator 외에 다른 관리 소프트웨어를 사용하여 섀시를 모니터링하려는 경우와 해당 관리 소프트웨어가 SNMPv3 통신을 사용하는 경우, 먼저 적절한 SNMPv3 정보로 구성된 로컬 CMM 사용자 ID를 만든 다음 해당 사용자 ID를 사용하여 CMM에 로그인하여 암호를 변경해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 관리 고려사항의 내용을 참조하십시오.
- SLP 및 SSDP와 같은 서비스 검색 프로토콜을 사용하면 XClarity Administrator에서 관리하려는 장치 유형을 자동으로 검색한 후 적절한 메커니즘을 사용하여 장치를 관리합니다. 일부 장치 유형은 서비스 검색 프로토콜을 지원하지 않으며, 일부 환경에서는 서비스 검색 프로토콜이 의도적으로 사용 중지되어 있습니다. 두 경우 모두 적절한 장치 유형을 선택하여 관리 프로세스를 완료해야 합니다. 다음 장치 유형은 명시적으로 식별되어야 합니다.
  - Lenovo ThinkSystem DB 시리즈 스위치
  - NVIDIA Mellanox 스위치

## 이 작업 정보

XClarity Administrator는 지정된 IP 주소 또는 IP 주소 범위를 사용하거나 스프레드시트에서 정보를 가져와서 XClarity Administrator와 동일한 IP 서브넷에 있는 관리 가능 장치를 프로브함으로써 사용자 환경에서 시스템을 검색할 수 있습니다.

기본적으로 장치는 XClarity Administrator 관리되는 인증을 사용하여 장치에 로그인하도록 관리됩니다. 랙 서버 및 Lenovo 섀시를 관리할 때 로컬 인증 또는 관리 인증을 사용하여 장치에 로그인하도록 선택할 수 있습니다.

- 랙 서버, Lenovo 섀시 및 Lenovo 랙 스위치에 *로컬 인증*을 사용하는 경우, XClarity Administrator는 저장된 자격 증명을 사용하여 장치를 인증합니다. *저장된 자격 증명*은 장치의 활성 사용자 계정 또는 Active Directory 서버의 사용자 계정입니다.

  로컬 인증을 사용하여 장치를 관리하기 전에 장치의 활성 사용자 계정 또는 Active Directory 서버의 사용자 계정과 일치하는 XClarity Administrator다음 위치에 저장된 자격 증명을 만들어야 합니다(XClarity Administrator온라인 설명서의 저장된 자격 증명 관리 참조).

**참고:**

- RackSwitch 장치는 인증을 위해 저장된 자격 증명만 지원합니다. XClarity Administrator 사용자 자격 증명은 지원되지 않습니다.

- *관리되는 인증*을 사용하면 로컬 자격 증명 대신 XClarity Administrator 인증 서버의 자격 증명을 사용하여 여러 장치를 관리하고 모니터링할 수 있습니다. 장치(ThinkServer 서버, System x M4 서버 및 스위치 이외의 장치)에 관리되는 인증을 사용하는 경우 XClarity Administrator는 중앙 집중식 관리를 위해 XClarity Administrator 인증 서버를 사용하도록 장치 및 설치된 구성 요소를 구성합니다.

  - 관리되는 인증을 사용으로 설정하면 수동으로 입력되거나 저장된 자격 증명을 사용하여 장치를 관리할 수 있습니다(XClarity Administrator 온라인 설명서에서 사용자 계정 관리 및 저장된 자격 증명 관리 참조).

    저장된 자격 증명은 XClarity Administrator가 장치에 LDAP 설정을 구성할 때까지만 사용됩니다. 그 후에는 저장된 자격 증명을 변경해도 장치를 관리하거나 모니터링하는 데 아무런 영향을 주지 않습니다.

    **참고:** 장치에 대해 관리되는 인증을 사용하는 경우 XClarity Administrator를 사용하여 해당 장치에 대한 저장된 자격 증명을 편집할 수 없습니다.

  - 로컬 또는 외부 LDAP 서버를 XClarity Administrator 인증 서버로 사용하는 경우 인증 서버에 정의된 사용자 계정은 XClarity Administrator 도메인에서 XClarity Administrator, CMM 및 베이스보드 관리 컨트롤러에 로그인하는 데 사용됩니다. 로컬 CMM 및 관리 컨트롤러 사용자 계정은 사용하지 않습니다.

  - SAML 2.0 ID 공급자를 XClarity Administrator 인증 서버로 사용하는 경우 SAML 계정은 관리되는 장치에 액세스할 수 없습니다. 하지만 SAML ID 공급자와 LDAP 서버를 함께 사용할 때 ID 공급자가 LDAP 서버에 존재하는 계정을 사용하는 경우 LDAP 사용자 계정을 사용하여 관리되는 장치에 로그인할 수 있고 SAML 2.0이 제공하는 고급 인증 방식(예, 다중 인증 및 SSO(Single sign-on))을 사용하여 XClarity Administrator에 로그인할 수 있습니다.

  - SSO(Single sign-on)를 사용하면 XClarity Administrator에 이미 로그인한 사용자가 베이스보드 관리 컨트롤에 자동으로 로그인할 수 있습니다. ThinkSystem 또는 ThinkAgile 서버가 XClarity Administrator에 의해 관리되는 경우 서버가 CyberArk 암호로 관리되지 않는 한 SSO(Single sign-on)는 기본적으로 사용됩니다. 관리되는 모든 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용 또는 사용하지 않도록 전역 설정을 구성할 수 있습니다. 특정 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용하면 모든 ThinkSystem 및 ThinkAgile 서버에 대한 전역 설정이 재정의됩니다(XClarity Administrator 온라인 설명서의 서버 관리 참조).

    **참고:** 인증에 CyberArk ID 관리 시스템을 사용하면 SSO(Single sign-on)가 자동으로 비활성화됩니다.

  - ThinkSystem SR635 및 SR655 서버에 관리되는 인증이 사용되는 경우:

    - 베이스보드 관리 컨트롤러 펌웨어는 최대 5개의 LDAP 사용자 역할을 지원하고 XClarity Administrator는 관리하는 동안 다음 LDAP 사용자 역할을 서버에 추가합니다. **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** 및 **lxc-os-admin**.

      ThinkSystem SR635 및 SR655 서버와 통신하려면 사용자가 지정된 LDAP 사용자 역할 중 하나 이상으로 지정되어야 합니다.

    - 관리 컨트롤러 펌웨어는 서버의 로컬 사용자와 동일한 사용자 이름을 가진 LDAP 사용자를 지원하지 않습니다.

  - ThinkServer 및 System x M4 서버의 경우, XClarity Administrator 인증 서버가 사용되지 않습니다. 대신 장치에 접두사가 "LXCA_"이고 무작위 문자열이 따르는 IPMI 계정이 만들어집니다. (기존 로컬 IPMI 사용자 계정은 사용 안 함으로 설정되지 않습니다.) ThinkServer 서버를 관리 해제하는 경우 "LXCA_" 사용자 계정을 사용할 수 없는 경우 접두사 "LXCA_"가 접두사 "DISABLED_"로 교체됩니다. ThinkServer 서버가 다른 인스턴스로 관리되는지 판별하기 위해 XClarity Administrator는 접두사 "LXCA_"가 있는 IPMI 계정이 있는지 확인합니다. 관리

ThinkServer 서버를 강제 관리하는 경우 "LXCA_" 접두사가 포함된 장치의 모든 IPMI 계정을 사용할 수 없고 이름이 변경됩니다. 더 이상 사용되지 않는 IPMI 계정을 지울 것을 고려해 보십시오.

수동으로 입력한 자격 증명을 사용하는 경우 XClarity Administrator는 저장된 자격 증명을 자동으로 만들고 이 저장된 자격 증명을 사용하여 장치를 관리합니다.

**참고:** 장치에 대해 관리되는 인증을 사용하는 경우 XClarity Administrator를 사용하여 해당 장치에 대한 저장된 자격 증명을 편집할 수 없습니다.

- 수동으로 입력한 자격 증명을 사용하여 장치를 관리할 때마다 이전 관리 프로세스 중에 해당 장치에 대해 다른 저장된 자격 증명이 만들어진 경우에도 새로운 저장된 자격 증명이 만들어집니다.
- 장치를 관리 해제할 때 XClarity Administrator는 관리 프로세스 중에 해당 장치에 대해 자동으로 만들어진 저장된 자격 증명은 삭제하지 않습니다.

시스템이 XClarity Administrator에서 관리되면 XClarity Administrator는 관리되는 각 시스템을 주기적으로 폴링하여 인벤토리, 필수 제품 데이터 및 상태와 같은 정보를 수집합니다. 관리되는 각 시스템을 보고 모니터하고, 관리 작업(예, 시스템 설정 구성, 운영 체제 이미지 배포 및 전원 켜기와 끄기)을 수행할 수 있습니다.

한 번에 하나의 XClarity Administrator만 시스템을 관리할 수 있습니다. 여러 관리자의 관리는 지원되지 않습니다. 한 XClarity Administrator에서 시스템을 관리하는데 다른 XClarity Administrator에서 시스템을 관리하도록 하려면 먼저 현재 XClarity Administrator에서 시스템을 관리 해제해야 합니다. 그런 다음 다른 XClarity Administrator에서 시스템을 관리할 수 있습니다. 시스템 관리 해제에 대한 정보는 XClarity Administrator 온라인 설명서에서 섀시 관리 해제, 서버 관리 해제, RackSwitch 스위치 관리 해제 및 Lenovo Storage 스토리지 시스템 관리 해제의 내용을 참조하십시오.

**참고:** XClarity Administrator는 관리 프로세스 중에 보안 설정 또는 암호 설정(암호화 모드 및 보안 통신에 사용되는 모드)을 수정하지 않습니다. 시스템이 관리되면 암호화 설정을 수정할 수 있습니다(XClarity Administrator 온라인 설명서에서 암호 모드 및 통신 프로토콜 설정 참조).

**참고:** XClarity Administrator는 실제 하드웨어를 시뮬레이션하는 데모 섀시(예, CMM, 컴퓨팅 노드 및 스위치) 및 데모 랙 또는 타워 서버에 대한 하드웨어 인벤토리로 미리 지정할 수 있습니다. 데모 장치는 웹 인터페이스 페이지에 있으며 관리 작업을 시연하는 데 사용할 수 있습니다. 그러나 관리 작업이 실패합니다. 예를 들어 구성 패턴을 만들고 패턴을 데모 서버에 배포할 수 있지만 배포가 실패합니다. 데모 장치를 관리 해제하여 데모 장치를 제거할 수 있습니다(XClarity Administrator 온라인 설명서에서 섀시 관리 해제 및 서버 관리 해제 참조). 데모 장치가 삭제된 후에는 이를 다시 관리 설정할 수 없습니다.

## 절차

대량 가져오기 파일을 사용하여 XClarity Administrator에서 시스템 검색 및 관리하려면, 다음 단계를 완료하십시오.

**참고:** 대량 가져오기를 사용하여 스위치를 관리하는 경우 스위치에서 HTTPS가 사용되고 스위치의 NTP 클라이언트가 관리 서버의 NTP 설정을 사용하도록 구성됩니다. 이 설정을 변경하려면 스위치를 수동으로 관리 설정해야 합니다.

1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.
2. 수신 요청이 XClarity Administrator에서만 허용되도록 관리 프로세스 중에 모든 장치에서 방화벽 규칙을 변경하려면 **모든 미래 관리 장치에서 encapsulation 사용** 선택란을 클릭하십시오.

   **참고:**

   - Encapsulation은 스위치, 스토리지 장치 및 Lenovo 이외 섀시 및 서버에에서 지원되지 않습니다.
   - 관리 네트워크 인터페이스가 DHCP(Dynamic Host Configuration Protocol)를 사용하도록 구성되어 있고 encapsulation이 사용으로 설정된 경우 랙 서버를 관리하는 데 오랜 시간이 걸릴 수 있습니다.

장치를 관리한 후 특정 장치에서 encapsulation을 사용 또는 사용하지 않도록 설정할 수 있습니다.

**주의:** Encapsulation을 사용하고 장치를 관리 해제하기 전에 XClarity Administrator를 사용할 수 없게 되는 경우 encapsulation을 사용하지 않도록 필요한 단계를 취해 장치와의 통신을 설정해야 합니다. 복구 절차는 XClarity Administrator 온라인 설명서에서 관리 서버 오류 후 CMM으로 섀시 관리 복구 및 관리 서버 오류 후 랙 또는 타워 서버 관리 복구의 내용을 참조하십시오.

3. **대량 가져오기**를 클릭하십시오. 대량 가져오기 마법사가 표시됩니다.


4. 데이터 파일 가져오기 페이지에서 **Excel에서** 또는 **CVS에서** 링크를 클릭하여 템플릿 대량 가져오기 파일을 Excel 또는 CSV 형식으로 다운로드하십시오.

   **중요:** 템플릿 파일은 릴리스마다 변경되지 않을 수 있습니다. 항상 최신 템플릿을 사용해야 합니다.

5. 템플릿 파일의 데이터 워크시트를 작성하고 파일을 *쉼표로 구분된* CSV 형식으로 저장하십시오.

   **팁:** Excel 템플릿 파일에는 **데이터** 워크시트와 Readme 워크시트가 포함됩니다. **데이터** 워크시트를 사용하여 장치 데이터를 채우십시오. Readme 워크시트는 **데이터** 워크시트(어떤 필드가 필수인지 포함) 및 샘플 데이터의 각 필드를 작성하는 방법에 대한 정보를 제공합니다.

   **중요:**

   - 장치는 대량 가져오기 파일에 나열된 순서로 관리됩니다.
   - XClarity Administrator는 장치를 관리할 때 장치 구성에 정의된 랙 할당 정보를 사용합니다. XClarity Administrator에서 랙 할당을 변경하면, XClarity Administrator가 장치 구성을 업데이트합니다. 장치를 관리한 후에 장치 구성을 업데이트하면, 변경 내용이 XClarity Administrator에 반영됩니다.
   - 랙을 장치에 할당하기 전에 스프레드 시트에 랙을 명시적으로 작성하는 것이 좋지만 반드시 필요한 것은 아닙니다. 랙이 명시적으로 정의되어 있지 않고 이미 XClarity Administrator에 이미 존재하지 않는 경우, 장치에 대해 지정된 랙 할당 정보는 기본 높이가 52U인 랙을 만드는 데 사용됩니다.

     랙에 다른 높이를 사용하려면, 장치에 할당하기 전에 스프레드시트에서 랙을 명시적으로 정의해야 합니다.

   대량 가져오기 파일에서 장치를 정의하려면, 다음 열을 완료하십시오.

   - (A~C열) 기본 검색의 경우, 장치 유형과 현재 IP 주소 또는 일련 번호를 지정해야 합니다. 다음 유형은 지원되지 않습니다.
     - filler. 관리 해제된 장치의 자리 표시자입니다. 랙 보기에서는 이 장치가 일반 필러 그래픽으로 표시됩니다. 추가 필러 유형은 Excel 템플릿의 Readme 워크시트를 참조하십시오.
     - flexchassis. 10U Flex System 섀시
     - server. XClarity Administrator가 지원하는 랙 및 타워 서버
     - rack. 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, 및 52U 랙. 다른 랙 높이는 지원되지 않습니다. 기본값으로 52U가 사용됩니다.
     - storage. 스토리지 장치

– switch. RackSwitch 스위치

**참고:** Flex System 컴퓨팅 노드, 스위치, 스토리지 장치는 섀시 검색 및 관리 프로세스의 일부로 간주됩니다.

- (D~H열) 저장된 자격 증명(Z열) 또는 ID(AF~AJ열) 대신 수동으로 입력한 자격 증명을 사용하도록 선택한 경우 현재 사용자 이름과 암호를 지정합니다. 수동으로 입력한 자격 증명은 일부 장치의 자격 증명이 다른 경우 유용합니다. 대량 가져오기 파일에 하나 이상의 장치에 대한 자격 증명을 지정하지 않는 경우 대량 가져오기 대화 상자에 지정하는 전역 자격 증명을 대신 사용합니다. 수동으로 입력된 사용자 및 관리 인증에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 사용자 계정 관리의 내용을 참조하십시오.

  **참고:**

  – 수동으로 입력한 자격 증명을 사용하려면 XClarity Administrator 관리되는 인증
  – 일부 필드는 일부 장치에 적용되지 않습니다.
  – (섀시의 경우) 관리되는 인증을 선택한 경우(AA 열 또는 대량 가져오기 대화 상자에서) 대량 가져오기 파일의 G 열 또는 대량 가져오기 대화 상자에서 RECOVERY_ID 암호를 지정해야 합니다. 로컬 인증을 선택하면 복구 암호가 허용되지 않습니다. 대량 가져오기 파일의 G 열 또는 대량 가져오기 대화 상자에 복구 암호를 지정하지 마십시오.
  – (랙 서버의 경우) 관리되는 인증을 선택한 경우(AA 열 또는 대량 가져오기 대화 상자에서) 대량 가져오기 파일의 G 열 또는 대량 가져오기 대화 상자에서 복구 암호를 선택적으로 지정할 수 있습니다. 로컬 인증을 선택하면 복구 암호가 허용되지 않습니다. 대량 가져오기 파일의 G 열 또는 대량 가져오기 대화 상자에 복구 암호를 지정하지 마십시오.
  – (랙 스위치의 경우) RackSwitch 장치는 스위치에 대해 인증하기 위해 저장된 자격 증명(Z열)만 지원합니다. 수동 사용자 자격 증명은 지원되지 않습니다.
- (I ~ U열) 성공적으로 관리하고 장치에 변경 사항을 적용하려는 경우 추가 정보를 선택적으로 제공할 수 있습니다.

  **참고:** 일부 필드는 일부 장치에 적용되지 않습니다. 이러한 필드는 RackSwitch 스위치에 적용되지 않습니다.
- (V~Z열) 랙 이름, 위치, 룸, 가장 낮은 랙 장치 및 높이를 포함하여 랙 생성 및 할당에 대한 정보를 선택적으로 제공할 수 있습니다.

  **참고:**

  – 랙을 만들 때, 랙 이름과 랙 높이를 지정해야 합니다. 지원되는 랙 높이: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, 및 52U. 다른 랙 높이는 지원되지 않습니다.
  – 일반 필러를 만들 때, 랙 이름과 필러 높이를 지정해야 합니다. 지원되는 필러 높이는 1U, 2U 및 4U입니다.
  – 특정 필러를 만들 때, 필러 높이가 무시됩니다. XClarity Administrator는 각 특정 필러의 높이를 알고 있습니다. 필러 유형 및 높이는 템플릿 스프레드시트를 참조하십시오.
  – 장치를 랙에 할당할 때, 장치 높이는 무시됩니다. 장치 높이는 장치 목록에서 검색됩니다.
- (AA열) 다음 오류 조건 중 하나로 인해 관리가 실패한 경우, 강제 관리 옵션을 사용하여 다음 절차를 반복하십시오.

  – 관리 XClarity Administrator가 오류가 발생하여 복구할 수 없는 경우.

    **참고:** 교체 XClarity Administrator 인스턴스가 동일한 IP 주소를 오류가 있는 XClarity Administrator로 사용하는 경우, RECOVERY_ID 계정 및 암호(해당하는 경우)와 강제 관리 옵션을 사용하여 장치를 다시 관리할 수 있습니다.
  – 장치를 관리 해체하기 전에 관리 XClarity Administrator를 작동 중지한 경우.
  – 장치가 성공적으로 관리 해제되지 않은 경우.

한 번에 하나의 XClarity Administrator 인스턴스만 사용해서 장치를 관리할 수 있습니다. 여러 XClarity Administrator 인스턴트를 사용한 관리는 지원되지 않습니다. 한 XClarity Administrator에서 장치를 관리하는데 다른 XClarity Administrator에서 장치를 관리하도록 하려면 먼저 원래 XClarity Administrator에서 장치를 관리 해제하고 이를 새 XClarity Administrator에서 관리하도록 설정하십시오.

**중요:** 서버가 XClarity Administrator에서 관리된 후 서버의 IP 주소를 변경하는 경우 XClarity Administrator는 새 IP 주소를 인식하고 계속해서 서버를 관리합니다. 그러나 XClarity Administrator는 일부 서버의 IP 주소 변경은 인식하지 못합니다. IP 주소가 변경된 후 XClarity Administrator에서 서버가 오프라인 상태임을 표시하는 경우 강제 관리 옵션을 사용하여 서버를 다시 관리하십시오.

- (AB열) 수동으로 입력한 자격 증명(D~H열) 또는 ID(AF~AJ열) 대신 저장된 자격 증명을 사용하도록 선택한 경우 저장된 자격 증명 ID를 지정합니다. XClarity Administrator 메뉴에서 **관리 → 보안**을 클릭한 다음 왼쪽 탐색에서 **저장된 자격 증명**을 클릭하여 저장된 자격 증명 페이지에서 저장된 자격 증명 ID를 찾을 수 있습니다. 저장된 자격 증명 및 로컬 인증에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 저장된 자격 증명 관리의 내용을 참조하십시오.

  **참고:**

  – RackSwtich 장치는 인증을 위해 저장된 자격 증명만 지원합니다. 수동 사용자 자격 증명(D열)은 지원되지 않습니다.

  – 저장된 자격 증명을 사용하여 장치를 관리하고 관리 인증을 사용하는 경우, 저장된 자격 증명을 편집할 수 없습니다.

- (AC열) 섀시 및 랙 서버의 경우 관리되는 인증을 사용하도록 선택한 경우 대량 가져오기 파일의 G열 또는 대량 가져오기 대화 상자에서 RECOVERY_ID 암호를 지정해야 합니다. 로컬 인증을 선택하면 복구 암호가 허용되지 않습니다. 대량 가져오기 파일의 G 열 또는 대량 가져오기 대화 상자에 복구 암호를 지정하지 마십시오.
- (AD 열) 랙 서버의 경우 이 열에 FALSE를 지정하여 XClarity Administrator 관리 인증 대신 로컬 인증을 사용하도록 선택할 수 있습니다. 관리되는 인증 및 로컬 인증에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 인증 서버 관리의 내용을 참조하십시오.
- (AE열) 장치를 보고 관리할 수 있는 역할 그룹 목록을 선택적으로 지정할 수 있습니다. 현재 사용자가 속한 역할 그룹만 지정할 수 있습니다.

  **참고:** 장치를 관리 섀시에 추가하면, 새 장치는 섀시와 동일한 역할 그룹에 속하게 됩니다.

- (AF~AJ열) 수동으로 입력한 자격 증명(D~H열) 또는 저장된 자격 증명(AB열) 대신 ID 관리 시스템을 사용하도록 선택한 경우 관리 대상 서버의 IP 주소 또는 호스트 이름, 사용자 이름을 지정하고 선택적으로 응용 프로그램 ID, 보관함 및 폴더를 지정합니다.

  응용 프로그램 ID를 지정하는 경우 보관함과 폴더(있는 경우)도 지정해야 합니다.

  응용 프로그램 ID를 지정하지 않으면 XClarity Administrator에서 CyberArk를 설정할 때 정의된 경로를 사용하여 CyberArk에 온보딩된 계정을 식별합니다.

  **참고:** ThinkSystem 또는 ThinkAgile 서버만 지원됩니다. ID 관리 시스템은 XClarity Administrator에서 구성되어야 하며, 관리되는 ThinkSystem 또는 ThinkAgile 서버의 Lenovo XClarity Controller은(는) CyberArk와 통합되어야 합니다.

다음 그림에는 대량 가져오기 파일 예제가 표시되어 있습니다.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Required fields (Type + SN or IP) | | | Optional fields | | | | | | | | | | | | | | | |
| Type | Serial Number | Current IP | Current username | Current password | New password | Recovery password | Switch enable password | New IPv4 | IPv4 subnet mask | IPv4 default gateway | IPv4 DNS1 | IPv4 DNS2 | New IPv6 | IPv6 prefix | IPv6 gateway | IPv6 DNS1 | IPv6 DNS2 | Domain |
| server | | 10.1.0.198 | | | | | | | | | | | | | | | | |
| server | P67X30EL | | | | | | | | | | | | | | | | | |
| flexchassis | | 10.1.0.213 | USERID | passw0rdx | Pa55word@ | abcd1234 | | | | | | | | | | | | |
| flexchassis | Z3499DD | | | | Pa55word@ | abcd1234 | | 9.27.20.51 | 255.255.255.0 | 9.27.20.1 | 9.0.148.50 | 9.0.146.50 | | | | | | ebg.lenovo.com |
| server | 35T88XP | | | | | | | | | | | | 2002:939 | 2002:9: | 2002:939: | 2002:9: | 2002:9 | ebg.lenovo.com |
| server | | 10.1.0.214 | | | | | | 10.1.2.213 | 255.255.255.0 | 10.1.2.1 | 9.0.148.50 | 9.0.146.50 | | | | | | ebg.lenovo.com |
| rack | | | | | | | | | | | | | | | | | | |
| rack | | | | | | | | | | | | | | | | | | |
| filler | | | | | | | | | | | | | | | | | | |
| filler | | | | | | | | | | | | | | | | | | |
| filler | | | | | | | | | | | | | | | | | | |

| R | S | T | U | V | W | X | Y | Z | AA | AB | AC | AD | AE | AF | AG | AH | AI | AJ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPv6 DNS2 | Domain | Host name | User-defined name | Rack name | Location | Room | Lowest rack unit | Height | Force | Stored credentials ID | Stored credentials ID for RECOVERY_ID | Managed authentication | Role Groups | IdentityManagementSystemEnabled | IMS type | IMS AppID | Folder | Safe |
| | | | | | | | | | | | | | | TRUE | CyberArk | LXCA | | Test |
| | | | chassis03 | SH3G05A34 | | | 25 | | TRUE | | | | | | | | | |
| | ebg.lenovo.com | chassis01 | chassis01 | SH3G05A34 | | | 5 | | | | | | | | | | | |
| 2002:9 | ebg.lenovo.com | host4 | c02node01 | SH3G05B12 | | | 38 | | | 2 | 3 | FALSE | | | | | | |
| | ebg.lenovo.com | host5 | web02 | SH3G05B12 | | | 10 | | | | | | | | | | | |
| | | | SG2R01A01 | | | | | 37 | | | | | | | | | | |
| | | | SH3G05A34 | | | | | 46 | | | | | | | | | | |
| | | | APC UPS | SH3G05A34 | | | 1 | 4 | | | | | | | | | | |
| | | | FC switch | SH3G05A34 | | | 40 | 2 | | | | | | | | | | |
| | | | KVM switch | SH3G05B12 | | | 22 | 1 | | | | | | | | | | |

6. 대량 가져오기 마법사에서 처리를 위해 파일을 업로드할 CSV 파일의 이름을 입력하십시오. 파일을 쉽게 찾으려면 **찾아보기**를 클릭할 수 있습니다.
7. **업로드**를 클릭하여 파일을 업로드하고 유효성을 검사합니다.
8. **다음**을 클릭하여 관리할 장치 목록이 있는 입력 요약 페이지를 표시합니다.

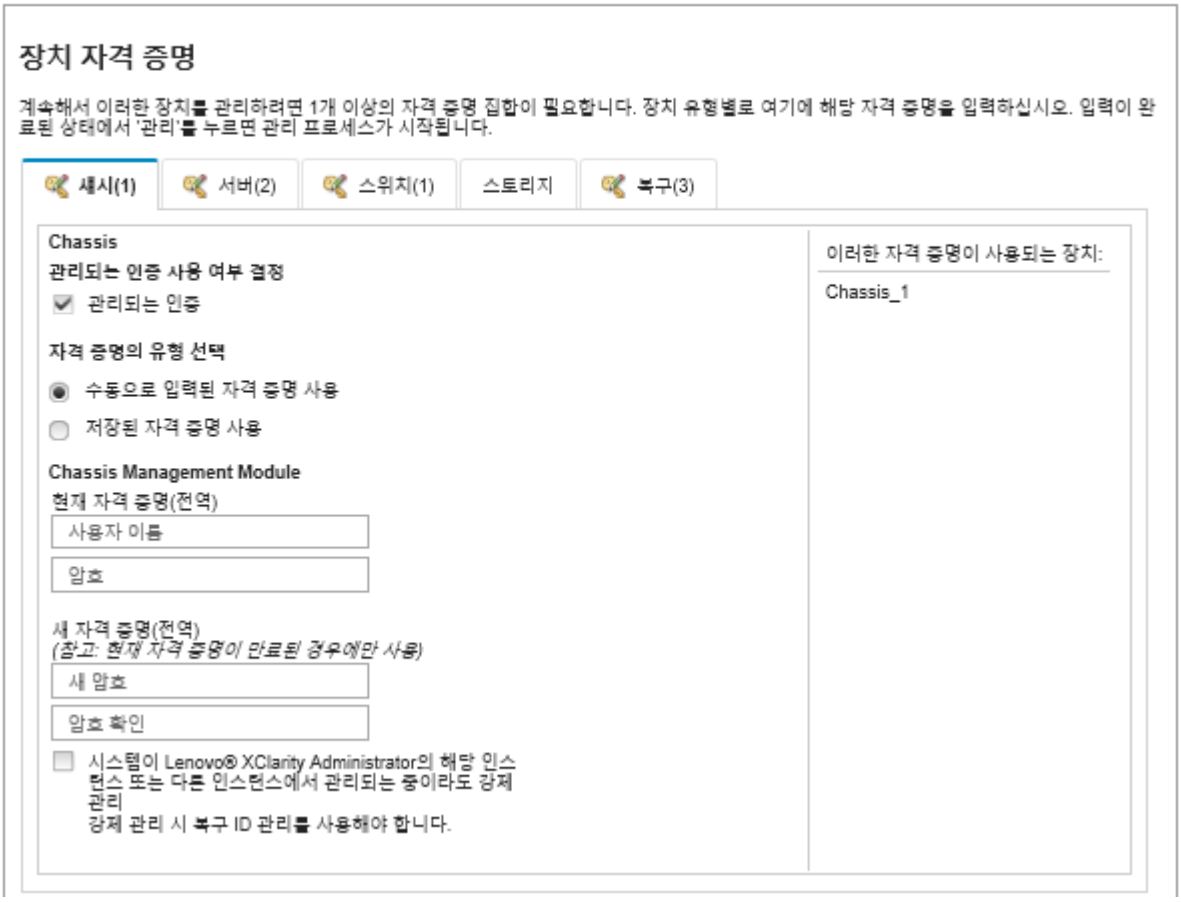

9. 관리하려는 장치의 요약을 검토하십시오.

   **잠재적 문제점이 있는 행만 표시**를 선택하여 불완전한 데이터가 있는 행을 나열합니다. 대량 가져오기 파일의 모든 문제를 해결한 **뒤로**를 클릭하여 수정된 CSV 파일을 업로드하십시오.

   **참고:**

   - 대량 가져오기 파일에 필요한 데이터가 제공되지 않으면, 관련 장치가 관리되지 않습니다.
   - 자격 증명 정보가 없는 입력 요약페이지 플래그 행. 대량 가져오기 파일에서 자격 증명을 지정하지 않는 경우, 대량 가져오기 마법사에서 지정하는 전역 자격 증명을 대신 사용합니다.
10. **다음**을 클릭하여 장치 자격 증명 페이지를 표시하십시오.

일괄 가져오기




11. **옵션:** 각 탭을 클릭하고 선택적으로 특정 유형의 모든 장치에 사용할 전역 설정 및 자격 증명을 지정하십시오. 전역 설정과 자격 증명을 사용할 장치는 각 탭의 오른쪽에 나열됩니다.

    전역 자격 증명을 사용하기로 선택하는 경우, 특정 장치 유형에 대한 자격 증명이 대량 가져오기 파일에 입력된 자격 증명이 없는 동일한 유형의 장치와 동일해야 합니다. 예를 들어 CMM 자격 증명은 모든 섀시에서 동일해야 하고, 스토리지 관리 자격 증명은 모든 스토리지 장치에서 동일해야 합니다. 자격 증명이 동일하지 않은 경우 대량 가져오기 파일에 자격 증명을 입력해야 합니다.

    - **섀시**. 인증 모드 및 자격 증명 유형을 지정하십시오. 대량 가져오기 파일에 정의된 모든 섀시에 로그인하기 위한 현재 자격 증명을 지정하십시오. 현재 CMM 자격 증명이 만료된 경우, 사용할 새 암호를 지정하십시오.

      섀시를 강제 관리하는 경우, 장치 자격 증명에 대한 RECOVERY_ID 계정과 암호를 지정하십시오.
    - **서버**. 인증 모드 및 자격 증명 유형을 지정하십시오. 대량 가져오기 파일에 정의된 모든 랙 및 타워 서버에 로그인하기 위한 현재 자격 증명을 지정하십시오. 현재 베이스보드 관리 컨트롤러 자격 증명이 만료된 경우, 사용할 새 암호를 지정하십시오.

      서버를 강제 관리하는 경우, 장치 자격 증명에 대한 RECOVERY_ID 계정과 암호를 지정하십시오.
    - **스위치**. 대량 가져오기 파일에 정의된 모든 RackSwitch 스위치에 로그인하기 위한 저장된 자격 증명을 지정하십시오. 설정된 경우 스위치에 권한이 있는 실행 모드를 입력하는 데 사용되는 "사용" 암호도 지정하십시오.
    - **스토리지**. 대량 가져오기 파일에 정의된 모든 스토리지 장치에 로그인하기 위한 현재 자격 증명을 지정하십시오.
    - **복구**. 대량 가져오기 파일에 정의된 모든 서버 및 섀시에 로그인하기 위한 복구 암호를 지정하십시오.

로컬 사용자 계정 또는 저장된 복구 자격 증명 중에서 선택하여 사용할 수 있습니다. 두 경우 모두 사용자 이름은 항상 RECOVERY_ID입니다.

암호가 지정되면 RECOVERY_ID 계정이 장치에 생성되고 모든 로컬 사용자 계정이 사용 안 함으로 설정됩니다.

- 섀시의 경우 복구 암호가 필수입니다.
- 서버에서는 관리되는 인증을 사용하도록 선택한 경우 복구 암호는 선택 사항이며 로컬 인증을 사용하도록 선택한 경우에는 복구 암호가 허용되지 않습니다.
- 암호가 장치의 보안 및 암호 정책을 준수하는지 확인하십시오. 보안 및 암호 정책은 다를 수 있습니다.
- 나중에 사용하도록 복구 암호를 기록해야 합니다.
- 복구 계정은 ThinkServer 및 System x M4 서버에서 지원되지 않습니다.

대량 가져오기 파일에 지정하는 정보는 장치 자격 증명 페이지에서 지정한 유사한 정보보다 우선합니다.

다음의 경우, 각 유형의 장치에 대해 관리를 강제하도록 선택할 수 있습니다.

- 장치가 현재 XClarity Administrator 인스턴스 또는 IBM Flex System Manager와 같은 다른 관리 시스템으로 관리되는 경우
- XClarity Administrator를 해체했지만 해체하기 전에 장치를 관리 해제하지 않은 경우
- 장치를 올바로 관리 해제하지 않았고 CIM 구독을 지우지 않은 경우

**참고:** 다른 XClarity Administrator 인스턴스가 장치를 관리한 경우 장치는 강제 관리가 이루어진 후 일정 시간 동안 원래 인스턴스가 관리하는 것으로 표시됩니다. 장치를 관리 해제하여 원래 XClarity Administrator 인스턴스에서 제거할 수 있습니다.

12. **관리**를 클릭하십시오. 모니터링 결과 페이지에는 대량 가져 오기 파일에 있는 각 장치의 관리 상태에 대한 정보가 표시됩니다.

    관리 프로세스를 위해 작업이 생성됩니다. 대량 가져오기 마법사를 닫으면, 관리 프로세스가 백그라운드에서 계속 실행됩니다. 작업 로그에서 관리 프로세스의 상태를 모니터링할 수 있습니다. 작업 로그에 대한 정보는 XClarity Administrator 온라인 설명서에서 작업 모니터링의 내용을 참조하십시오.

    XClarity Administrator가 대량 가져오기 파일에 지정된 자격 증명 또는 대화 상자에 지정된 전역 자격 증명을 사용하여 장치에 로그인할 수 없는 경우 해당 장치의 관리가 실패하고 XClarity Administrator는 대량 가져오기 파일의 다음 장치로 이동합니다.

    **참고:** 다음 오류 조건 중 하나로 인해 관리가 실패한 경우, **강제 관리** 옵션을 사용하여 다음 절차를 반복하십시오.

    - 관리 XClarity Administrator가 오류가 발생하여 복구할 수 없는 경우.

      **참고:** 교체 XClarity Administrator 인스턴스가 동일한 IP 주소를 오류가 있는 XClarity Administrator로 사용하는 경우, RECOVERY_ID 계정 및 암호(해당하는 경우)와 **강제 관리** 옵션을 사용하여 장치를 다시 관리할 수 있습니다.
    - 장치를 관리 해체하기 전에 관리 XClarity Administrator를 작동 중지한 경우.
    - 장치가 성공적으로 관리 해제되지 않은 경우.

    **주의:** 한 번에 하나의 XClarity Administrator 인스턴스만 사용해서 장치를 관리할 수 있습니다. 여러 XClarity Administrator 인스턴트를 사용한 관리는 지원되지 않습니다. 한 XClarity Administrator에서 장치를 관리하는데 다른 XClarity Administrator에서 장치를 관리하도록 하려면 먼저 원래 XClarity Administrator에서 장치를 관리 해제하고 이를 새 XClarity Administrator에서 관리하도록 설정해야 합니다.

13. 대량 가져오기 파일에 새 섀시가 포함되는 경우, 전체 섀시(컴퓨팅 노드 및 Flex 스위치 포함)에 대한 관리 네트워크 설정의 유효성을 검증 및 변경하고 서버 패턴을 만들어 배포함으로써 컴퓨팅 노드 정보, 로컬 스토리지, I/O 어댑터, 부팅 대상 및 펌웨어 설정을 구성하십시오. 자세한 정보는 XClarity

Administrator 온라인 설명서에서 새시에 대한 관리 IP 설정 수정 및 XClarity Administrator를 사용하여 서버 구성의 내용을 참조하십시오.

## 완료한 후에

시스템을 관리한 후에는 다음 작업을 수행할 수 있습니다.

- 추가 시스템을 검색 및 관리하십시오(Lenovo XClarity Administrator 온라인 설명서에서 새시 관리, 랙 관리, 서버 관리, 저장 장치 관리 및 스위치 관리 참조).
- 서버 패턴을 작성하고 배포하여 시스템 정보, 로컬 스토리지, I/O 어댑터, 부팅 설정 및 펌웨어 설정을 구성하십시오(Lenovo XClarity Administrator 온라인 설명서에서 XClarity Administrator를 사용하여 서버 구성 참조).
- 운영 체제가 설치되지 않은 서버에 운영 체제 이미지를 배포하십시오(XClarity Administrator 온라인 설명서에서 운영 체제 이미지 배포 참조).
- 현재 정책을 준수하지 않는 장치에서 펌웨어를 업데이트하십시오(XClarity Administrator 온라인 설명서에서 관리 장치에서 펌웨어 업데이트 참조).
- 새로 관리되는 시스템을 적합한 랙에 추가하여 물리적 환경을 반영하십시오(XClarity Administrator 온라인 설명서에서 랙 관리 참조).
- 하드웨어 상태 및 세부 정보를 모니터링하십시오(XClarity Administrator 온라인 설명서에서 관리 서버의 상태 보기 참조).
- 이벤트 및 경고를 모니터링하십시오(XClarity Administrator 온라인 설명서에서 이벤트 작업 및 경고 작업 참조).
- 관리되는 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용 중지하거나 사용합니다.
  - 모든 관리되는 ThinkSystem 및 ThinkAgile 서버(전역)의 경우에는 XClarity Administrator 메뉴 표시줄에서 **관리 ➡ 보안**을 클릭하고 **활성 세션**을 클릭한 다음 SSO(Single sign-on)를 사용 또는 사용 중지합니다.
  - 특정 ThinkSystem 및 ThinkAgile 서버의 경우에는 XClarity Administrator 메뉴 표시줄에서 **하드웨어 ➡ 서버**를 클릭한 다음 **모든 작업 ➡ 보안 ➡ SSO(Single sign-on) 사용** 또는 **모든 작업 ➡ 보안 ➡ SSO(Single sign-on) 사용 안 함**을 클릭합니다.

  **참고:** SSO(Single sign-on)를 사용하면 XClarity Administrator에 이미 로그인한 사용자가 베이스보드 관리 컨트롤에 자동으로 로그인할 수 있습니다. ThinkSystem 또는 ThinkAgile 서버가 XClarity Administrator에 의해 관리되는 경우 서버가 CyberArk 암호로 관리되지 않는 한 SSO(Single sign-on)는 기본적으로 사용됩니다. 관리되는 모든 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용 또는 사용하지 않도록 전역 설정을 구성할 수 있습니다. 특정 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(single sign-on)를 사용하면 모든 ThinkSystem 및 ThinkAgile 서버에 대한 전역 설정이 재정의됩니다.

# 제 5 장 XClarity Administrator 등록

Lenovo XClarity Administrator의 인스턴스를 등록하면 평가판 만료 및 비준수 라이센스에 대한 경고가 반복 표시되지 않는 상태로 기본 기능을 사용할 수 있습니다. 등록하고 나면 비준수 라이센스 경고가 더 이상 표시되지 않지만, 라이센스가 필요한 모든 기능은 관리되는 장치 수에 따라 라이센스를 구매하고 설치할 때까지 비활성화된 상태로 유지됩니다.

## 이 작업 정보

XClarity Administrator 인스턴스를 등록할 때 연락처 정보를 공유하지 않아도 됩니다. Lenovo는 제공된 정보를 다른 외부 기관과 공유하지 않습니다.

고급 기능에 대한 라이센스를 설치한 경우에는 XClarity Administrator 인스턴스를 등록할 필요가 없습니다. 라이센스 및 고급 기능에 대해 자세히 알아보려면 전체 기능 사용 라이센스 설치의 내용을 참조하십시오.

## 절차

XClarity Administrator을(를) 등록하려면 다음 단계를 완료하십시오.

- XClarity Administrator가 인터넷에 연결된 경우
  1. Lenovo XClarity Administrator메뉴 표시줄에서 **관리 → 등록**을 클릭하여 등록 페이지를 표시합니다.
  2. **등록**을 클릭하여 XClarity Administrator의 새 인스턴스를 등록합니다.
  3. 회사 이름, XClarity Administrator에서 관리할 장치 수, XClarity Administrator이(가) 위치하는 국가를 입력합니다.
  4. **제출**을 클릭하십시오.
- XClarity Administrator가 인터넷에 연결되지 않은 경우
  1. XClarity Administrator을(를) 등록합니다.
     a. 웹 브라우저에서 Lenovo XClarity 등록 웹 포털을(를) 엽니다.
     b. 회사 이름, XClarity Administrator에서 관리할 장치 수, XClarity Administrator가 위치하는 국가를 입력합니다.
     c. **제출**을 클릭하여 등록 토큰을 받습니다.
  2. Lenovo XClarity Administrator메뉴 표시줄에서 **관리 → 등록**을 클릭하여 등록 페이지를 표시합니다.
  3. **가져오기**를 클릭하여 등록 토큰을 가져옵니다.
  4. 1단계에서 받은 등록 토큰을 입력합니다.
  5. **제출**을 클릭하십시오.

# 제 6 장 전체 기능 사용 라이센스 설치

90일 무료 평가판이 만료된 후 Lenovo XClarity Administrator에서 운영 체제 배포와 장치 구성 기능을 계속 사용하려면 고급 기능을 지원하는 모든 관리되는 장치에 대해 Lenovo XClarity Pro 라이센스를 구입하여 설치해야 합니다. XClarity Administrator 서비스와 지원을 이용하려면 *모든* 관리되는 장치에 대한 Lenovo XClarity Pro 라이센스가 있어야 합니다.

**자세히 알아보기:** XClarity Administrator: 라이언스 설치

## 시작하기 전에

다음 라이센스 고려사항을 검토하십시오.

- 라이센스는 특정 장치에 묶여 있지 *않습니다*.
- 섀시 라이센스는 14개의 장치에 대한 라이센스를 제공합니다.
- System x3850 X6(6241) 확장 가능 복합 서버의 경우 파티션에 관계없이 각 서버에 별도의 라이센스가 필요합니다.
- System x3950 X6(6241) 확장 가능 복합 서버의 경우 파티션이 없다면 각 서버에 별도의 라이센스가 필요합니다. 파티션이 있는 경우 각 파티션에 별도의 라이센스가 필요합니다.
- 다음 장치는 고급 기능을 *지원하지 않으므로* 이러한 기능에 대한 라이센스가 *필요하지 않습니다*. 그러나 XClarity Administrator 서비스와 지원을 얻으려면 이러한 각 장치에 대한 라이센스를 구입해야 합니다.
  - ThinkServer 서버
  - System x M4 서버
  - System x X5 서버
  - System x3850 X6 및 x3950 X6(3837) 서버
  - 스토리지 장치
  - 스위치

라이센스를 설치하려면 lxc-supervisor 또는 lxc-security-admin 권한이 있어야 합니다.

## 이 작업 정보

XClarity Administrator는 다음 라이센스를 지원합니다.

- **Lenovo XClarity Pro**. 각 라이센스는 단일 장치에 대해 다음과 같은 권한을 제공합니다.
  - Lenovo XClarity Integrator에 대한 서비스 및 지원
  - XClarity Administrator에 대한 서비스 및 지원
  - XClarity Administrator 내 고급 기능
    - 구성 패턴을 사용하여 서버 구성
    - 운영 체제 배포
    - 콜 홈을 사용하여 XClarity Administrator 문제 보고(하드웨어 경고에 대한 콜 홈은 해당되지 않음)

라이센스의 활성화 기간은 라이센스를 구매하고 인증 코드가 생성되면 시작됩니다.

라이센스 준수는 고급 기능을 지원하는 관리되는 장치의 수에 따라 결정됩니다. 관리되는 장치의 수는 모든 활성 라이센스 키의 총 라이센스 수를 초과해서는 안 됩니다. XClarity Administrator가 설치된 라이센스 수를 준수하지 않는 경우(예: 라이센스가 만료되거나 관리 중인 추가 장치가 총 활성 라이센스 수를 초과하는 경우), 적절한 라이센스를 설치할 수 있는 유예 기간은 90일입니다. XClarity Administrator이

(가) 비준수 상태가 될 때마다 유예 기간이 90일로 재설정됩니다. 라이센스를 준수하기 전에 유예 기간(무료 평가판 포함)이 종료되면 모든 장치에서 고급 기능이 사용 중지됩니다.

예를 들어 기존 XClarity Administrator 인스턴스에서 추가로 100개의 ThinkSystem 서버와 20개의 랙 스위치를 관리하는 경우 90일 이내에 추가로 100개의 라이센스를 구입하고 설치해야 모든 장치의 사용자 인터페이스에서 고급 기능이 사용 중지되지 않습니다. 랙 스위치 20개의 라이센스는 고급 기능을 사용하는 데 필요하지 않지만 서비스 및 지원을 이용하려면 필요합니다. 고급 기능이 사용 중지된 경우 규정을 준수하는 충분한 수의 라이센스를 설치하면 고급 기능을 다시 사용할 수 있습니다.

무료 평가판 라이센스를 사용 중이거나 유예 기간을 준수하고 XClarity Administrator의 최신 버전으로 업그레이드하는 경우 평가판 라이센스 또는 유예 기간이 90 일로 재설정됩니다.

**참고:**

- 유예 기간이 만료되면 서버 구성 및 운영 체제 배포 기능이 비활성화됩니다.
- XClarity Administrator 문제를 위한 콜 홈(소프트웨어 콜 홈 기능)은 라이센스를 준수하지 않는 경우 사용 중지됩니다. 이 기능에 대한 유예 기간은 없습니다. 하지만 하드웨어 경고에 대한 콜 홈은 영향을 받지 않습니다.

라이센스를 이미 설치한 경우 XClarity Administrator의 새 릴리스로 업그레이드할 때 새 라이센스가 필요하지 *않습니다*.

XClarity Administrator 제목 표시줄에서 사용자 작업 메뉴( 

)를 클릭한 후 **정보**를 클릭하여 평가판 라이센스에 남아 있는 기간(일) 등의 라이센스 상태를 판별할 수 있습니다.

**도움말 얻기**

- 문제가 있고 비즈니스 파트너를 사용한 경우, 비즈니스 파트너에게 문의하여 트랜잭션 및 사용을 확인하십시오.
- 전자 권한 증명서, 인증 코드 또는 활성화 키를 받지 못했거나 이러한 사항이 잘못된 사람에게 전송된 경우, 본인 지역의 지역 담당자 중 한 사람에게 문의하십시오.
  - ESDNA@lenovo.com(북미 국가)
  - ESDAP@lenovo.com(아시아 태평양 국가들)
  - ESDEMEA@lenovo.com(유럽, 중동 및 아시아 국가)
  - ESDLA@lenovo.com(중남미 국가)
  - ESDChina@Lenovo.com(중국)
- 내 자격에 대한 정보가 정확하지 않은 경우, SW_override@lenovo.com의 Lenovo 지원으로 문의하고 다음 정보를 포함하십시오.
  - 주문 번호
  - 이메일 주소를 포함한 연락처 정보.
  - 실제 주소
  - 원하는 변경 사항
- 라이센스 다운로드에 관한 문제나 질문이 있는 경우 -eSupport_-_Ops@lenovo.com의 Lenovo 지원으로 문의하십시오.

## XClarity Administrator 웹 인터페이스를 사용하여 전체 기능 사용 라이센스 설치

XClarity Administrator에서 인터넷에 액세스할 수 있다면 XClarity Administrator 웹 인터페이스를 통해 기존 인증에 대한 라이센스를 사용 및 검색한 다음 사용된 라이센스를 가져와서 설치할 수 있습니다.

### 시작하기 전에

활성화하려는 기능과 관리하려는 장치 수에 따라 Lenovo XClarity Pro 라이센스를 구매하려면 Lenovo 담당자 또는 공인 비즈니스 파트너에게 문의하십시오. 라이센스를 구매하면 *전자 자격 증명* 이메일로 인증 코드가 전송됩니다. 인증 코드는 22자의 영숫자 문자열로, 라이센스를 사용하고 설치하는 데 필요합니다. 이메일을 받지 않았으나 비즈니스 파트너를 통해 라이센스를 구매한 경우, 비즈니스 파트너에게 연락하여 인증 코드를 요청하십시오.

Features on Demand 웹 포털에서 **인증 코드 검색**을 클릭하여 인증 코드를 검색할 수도 있습니다.

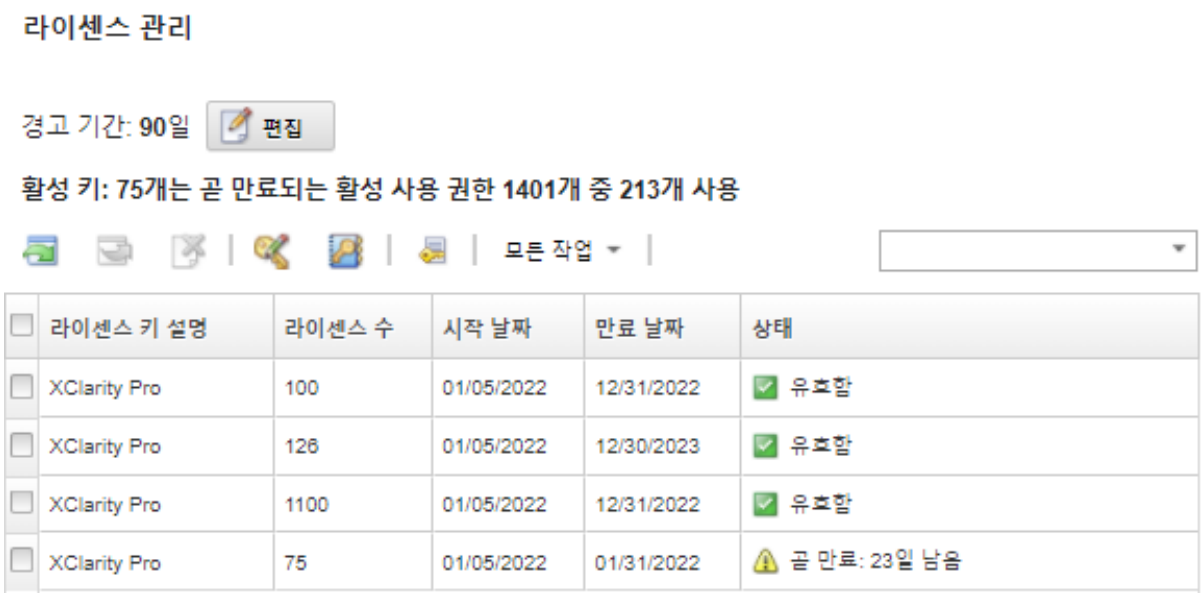
## 절차

관리 서버에 Lenovo XClarity Pro 라이센스를 설치하려면 다음 절차 중 하나를 완료하십시오.

- **단일 인증 코드로 나머지 라이센스 전체 또는 일부 사용 및 설치**

  단일 인증 코드에서 사용 가능한 라이센스 전체 또는 일부를 사용하여 사용된 라이센스에 대한 개별 정보가 포함된 파일인 라이센스 활성화 키를 만들 수 있습니다. 그런 다음 해당 라이센스 활성화 키 파일로 사용된 라이센스를 설치할 수 있습니다.

  1. XClarity Administrator 메뉴 표시줄에서 **관리 ➡ 라이센스**를 클릭하여 라이센스 관리 페이지를 표시하십시오.

  2. **활성화 키 요청** 아이콘()을 클릭하여 활성화 키 요청 대화 상자를 표시합니다.
  3. **단일 인증 코드**를 클릭합니다.
  4. 22자리 인증 코드를 입력하고 **검색**을 클릭하여 Features on Demand 웹 사이트에서 지정된 인증 코드에 대해 구매한 라이센스 관련 정보를 가져옵니다.

     수신한 인증 코드가 승인되지 않으면 Lenovo 지원에 문의하십시오.
  5. **Lenovo 고객 번호** 필드에 10자리의 Lenovo 고객 번호를 입력합니다.
  6. **사용 수량** 필드에 사용하고자 하는 라이센스 수를 입력한 다음 **계속**을 클릭하십시오.

     인증 코드로 사용 가능한 모든 라이센스를 사용하려면 **사용 가능한 라이센스** 필드의 숫자와 일치해야 합니다.

     사용 가능한 라이센스의 일부만 사용하는 경우 동일한 인증 코드를 사용하여 나중에 나머지 라이센스를 사용할 수 있습니다.

     **팁:** 각 XClarity Administrator에서는 최대 1,000개의 관리되는 장치를 지원합니다. 따라서 XClarity Administrator 인스턴스에 설치할 수 있는 하나의 라이센스 활성화 키에 라이센스가 1,000개를 초과할 수 없습니다.

7. 연락처 정보가 정확한지 검토하고 필요한 경우 수정합니다.
8. **요청 제출**을 클릭하여 라이센스를 사용하고 라이센스 활성화 키를 생성합니다.
9. 설치할 라이센스가 포함된 라이센스 활성화 키를 선택합니다.
10. **설치**를 클릭하여 관리 서버에 라이센스를 설치합니다.
11. **닫기**를 클릭하십시오.

- **여러 인증 코드로 남은 모든 라이센스 사용 및 설치**

  여러 인증 코드로 남은 모든 라이센스를 사용할 수 있습니다. 각 인증 코드에 대해 라이센스 활성화 키가 만들어집니다. 그러면 라이센스 활성화 키로 사용된 라이센스를 설치할 수 있습니다. 인증 코드는 제공된 템플릿을 사용하여 CSV 형식의 파일로 제공해야 합니다.

  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 라이센스**를 클릭하여 라이센스 관리 페이지를 표시하십시오.
  2. **활성화 키 요청** 아이콘(  )을 클릭하여 활성화 키 요청 대화 상자를 표시합니다.
  3. **여러 인증 코드**를 클릭합니다.
  4. **템플릿 다운로드** 링크를 클릭하여 Excel 파일을 엽니다. 파일에 각 인증 코드를 추가하고 파일을 CSV 형식으로 로컬 시스템에 저장합니다.
  5. **찾아보기**를 클릭하여 인증 코드 CSV 파일을 찾아 선택한 다음 **검색**을 클릭하여 Lenovo 지원 웹 사이트에서 인증 코드에 대한 정보를 검색합니다.
  6. 구매한 라이센스 및 각 인증 코드와 관련된 사용 가능한 라이센스 활성화 키에 관한 정보를 검토합니다.
  7. **Lenovo 고객 번호** 필드에 10자리의 Lenovo 고객 번호를 입력합니다.
  8. 연락처 정보가 정확한지 검토하고 필요한 경우 수정합니다. 그런 다음 **계속**을 클릭합니다.
  9. **예, 모든 유효한 승인 코드를 사용하겠습니다**를 선택한 다음 **요청 제출**을 클릭하여 라이센스 활성화 키를 생성합니다.
  10. 설치하려는 라이센스 활성화 키를 선택합니다.
  11. **설치**를 클릭하여 관리 서버에 라이센스 활성화 키를 설치합니다.
  12. **닫기**를 클릭하십시오.

- **사용된 라이센스 검색 및 설치**

  Features on Demand 웹 포털에 액세스할 수 있는 XClarity Administrator 인스턴스에서 로컬 시스템으로 라이센스 활성화 키를 다운로드한 후 다른 XClarity Administrator 인스턴스에 해당 라이센스 활성화 키를 가져와 설치할 수 있습니다. 인터넷에 액세스할 수 없는 XClarity Administrator 인스턴스에 라이센스를 설치하거나 XClarity Administrator을(를) 다시 설치했으며 설치된 라이센스를 복원해야 하는 경우 유용합니다.

  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 라이센스**를 클릭하여 라이센스 관리 페이지를 표시하십시오.
  2. **기록 검색** 아이콘(  )을 클릭하여 기록 검색 대화 상자를 표시합니다.
  3. Lenovo 고객 번호 또는 22자리 인증 코드를 입력합니다.
  4. **검색**을 클릭하여 사용 가능한 라이센스와 사용된 라이센스에 대한 정보를 검색합니다.

     수신한 인증 코드가 승인되지 않으면 Lenovo 지원에 문의하십시오.
  5. 설치하려는 라이센스 키 파일을 선택합니다.
  6. **설치**를 클릭하여 XClarity Administrator에 라이센스 활성화 키를 설치합니다.
  7. **닫기**를 클릭하십시오.

- **다른 XClarity Administrator 인스턴스에 사용된 라이센스 가져오기 및 설치**

  하나의 XClarity Administrator 인스턴스에서 라이센스를 사용했으며 해당 라이센스를 다른 XClarity Administrator 인스턴스에 설치하려는 경우 또는 설치된 라이센스를 복원해야 하는 오

류 조건이 발생하는 경우 로컬 시스템에서 다른 XClarity Administrator 인스턴스로 라이센스 키 파일을 가져올 수 있습니다.

1. Features on Demand 웹 포털에 액세스할 수 있는 XClarity Administrator 인스턴스에서 Features on Demand 웹 포털의 라이센스 활성화 키를 검색한 다음 라이센스 활성화 키를 로컬 시스템에 파일로 저장합니다.
   a. XClarity Administrator 메뉴 표시줄에서 **관리 → 라이센스**를 클릭하여 라이센스 관리 페이지를 표시하십시오.
   b. **기록 검색** 아이콘(  )을 클릭하여 기록 검색 대화 상자를 표시합니다.
   c. 22자리 인증 코드를 입력합니다.
   d. **검색**을 클릭하여 해당 인증 코드에 대해 사용 가능한 라이센스와 사용된 라이센스에 대한 정보를 검색합니다.

      수신한 인증 코드가 승인되지 않으면 Lenovo 지원에 문의하십시오.
   e. 설치하려는 라이센스 활성화 키 파일을 선택합니다.
   f. **다운로드**를 클릭하여 라이센스 키 파일을 로컬 시스템에 저장합니다.
2. 라이센스 활성화 키를 설치하려는 XClarity Administrator 인스턴스에서:
   a. XClarity Administrator 메뉴 표시줄에서 **관리 → 라이센스**를 클릭하여 라이센스 관리 페이지를 표시하십시오.
   b. **가져온 후 적용** 아이콘(  )을 클릭하여 라이센스를 가져오고 설치합니다.
   c. **찾아보기**를 클릭하여 설치할 라이센스의 라이센스 활성화 키를 선택합니다.

      여러 개의 라이센스 활성화 키를 가져오려면 .KEY 파일을 ZIP 파일로 압축하고 가져올 ZIP 파일을 선택합니다.
   d. **라이센스 계약에 동의**를 클릭하여 라이센스를 가져와 적용합니다.

      설치가 완료되면 라이센스 활성화 키가 설치된 라이센스 수와 활성화 기간(시작 및 만료 날짜)과 함께 테이블에 나열됩니다.

## 완료한 후에

라이센스 페이지에서 다음 작업을 수행할 수 있습니다.

- **내보내기** 아이콘(  )을 클릭하여 하나 이상의 특정 라이센스 활성화 키를 로컬 시스템에 다운로드합니다.

  **참고:** 여러 개의 라이센스 활성화 키를 내보내면 파일이 단일 ZIP 파일로 다운로드됩니다.
- **삭제** 아이콘(  )을 클릭하여 특정 라이센스 활성화 키를 삭제합니다.
- 페이지 상단에 있는 **편집** 버튼을 클릭하여 라이센스 경고 기간을 구성하십시오. XClarity Administrator이(가) 경고를 트리거할 경우 라이센스 경고 기간은 라이센스 만료 전 남는 일수입니다.

### 도움말 얻기

- 문제가 있고 비즈니스 파트너를 사용한 경우, 비즈니스 파트너에게 문의하여 트랜잭션 및 사용을 확인하십시오.
- 전자 권한 증명서, 인증 코드 또는 활성화 키를 받지 못했거나 이러한 사항이 잘못된 사람에게 전송된 경우, 본인 지역의 지역 담당자 중 한 사람에게 문의하십시오.
  - ESDNA@lenovo.com(북미 국가)
  - ESDAP@lenovo.com(아시아 태평양 국가들)
  - ESDEMEA@lenovo.com(유럽, 중동 및 아시아 국가)
  - ESDLA@lenovo.com(중남미 국가)
  - ESDChina@Lenovo.com(중국)

- 내 자격에 대한 정보가 정확하지 않은 경우, SW_override@lenovo.com의 Lenovo 지원으로 문의하고 다음 정보를 포함하십시오.
  - 주문 번호
  - 이메일 주소를 포함한 연락처 정보.
  - 실제 주소
  - 원하는 변경 사항
- 라이센스 다운로드에 관한 문제나 질문이 있는 경우 -eSupport_-_Ops@lenovo.com의 Lenovo 지원으로 문의하십시오.

## Features on Demand 웹 포털에서 전체 기능 사용 라이센스 설치

XClarity Administrator에서 인터넷에 액세스할 수 *없다면* XClarity Administrator 네트워크에 액세스할 수 있는 다른 시스템의 Features on Demand 웹 포털을(를) 사용하여 기존 인증 코드에 대한 라이센스를 사용하고 검색할 수 있습니다. 이렇게 하면 XClarity Administrator 웹 인터페이스를 통해 사용된 라이센스를 가져오고 설치할 수 있습니다.

### 절차

관리 서버에 Lenovo XClarity Pro 라이센스를 설치하려면 다음 단계를 완료하십시오.

단계 1. 각 관리되는 장치에 대해 Lenovo XClarity Pro 라이센스를 구입합니다.

활성화하려는 기능과 관리하려는 장치 수에 따라 Lenovo XClarity Pro 라이센스를 구매하려면 Lenovo 담당자 또는 공인 비즈니스 파트너에게 문의하십시오. 라이센스를 구매하면 *전자 자격 증명* 이메일로 인증 코드가 전송됩니다. 인증 코드는 22자의 영숫자 문자열로, 라이센스를 사용하고 설치하는 데 필요합니다. 이메일을 받지 않았으나 비즈니스 파트너를 통해 라이센스를 구매한 경우, 비즈니스 파트너에게 연락하여 인증 코드를 요청하십시오.

Features on Demand 웹 포털에서 **인증 코드 검색**을 클릭하여 인증 코드를 검색할 수도 있습니다.

단계 2. 인증 코드를 사용하여 라이센스 전체 또는 일부를 사용합니다. 라이센스가 사용되면 라이센스 활성화 키 파일이 생성됩니다.

1. 웹 브라우저에서 Features on Demand 웹 포털를 연 다음 이메일 주소를 사용자 ID로 포털에 로그인하십시오.
2. **활성화 키 요청**을 클릭합니다.
3. **단일 인증 코드 입력**을 선택하십시오.
4. 22자리 인증 코드를 입력하고 **계속**을 클릭하십시오.
5. **Lenovo 고객 번호** 필드에 Lenovo 고객 번호를 입력하십시오.
6. **사용 수량** 필드에 사용하고자 하는 라이센스 수를 입력한 다음 **계속**을 클릭하십시오.

   이 인증 코드로 사용 가능한 모든 라이센스를 사용하려면 **사용 가능한 라이센스** 필드의 숫자와 일치해야 합니다.

   사용 가능한 라이센스의 일부를 사용하는 경우 동일한 인증 코드를 사용하여 다른 라이센스 활성화 키의 나머지 라이센스를 사용할 수 있습니다.

   **팁:** 각 XClarity Administrator에서는 최대 1,000개의 관리되는 장치를 지원합니다. 따라서 XClarity Administrator 인스턴스에 설치하는 하나의 라이센스 활성화 키에 라이센스가 1,000개를 초과할 수 없습니다.
7. 제품 세부 정보 및 연락처 정보를 입력하라는 메시지에 따라 **계속**을 클릭하여 라이센스 활성화 키를 생성합니다.
8. 라이센스 활성화 키를 수신할 추가 수신자를 지정하는 옵션도 있습니다.
9. **제출**을 클릭하여 라이센스 활성화 키를 전송합니다.

구매 주문서 및 추가 수신자로 지정된 사람은 라이센스 활성화 키가 포함된 이메일을 받게 됩니다. 키는 .KEY 형식의 파일입니다.

**참고:** Features on Demand 웹 포털에서 **기록 검색**을 클릭하고 Lenovo 고객 번호로 라이센스 활성화 키를 찾아 라이센스 활성화 키(개별 또는 일괄)를 다운로드할 수 있으며, 키를 전체 또는 일부만 다운로드할 수도 있습니다. 그런 다음 **이메일**을 클릭하여 키를 이메일로 전송하거나 **다운로드**를 클릭하여 로컬 시스템에 키를 다운로드하십시오.

단계 3. XClarity Administrator에 라이센스를 가져와서 설치합니다.

1. XClarity Administrator 메뉴 표시줄에서 **관리 → 라이센스**를 클릭하여 라이센스 관리 페이지를 표시하십시오.
2. **가져와서 적용하기** 아이콘(  )을 클릭하여 라이센스를 설치하십시오.
3. **찾아보기**를 클릭하여 설치할 라이센스의 라이센스 활성화 키 파일을 선택하십시오.

   **팁:** 여러 개의 라이센스 활성화 키를 가져오려면 .KEY 파일을 ZIP 파일로 압축하고 가져올 ZIP 파일을 선택하십시오.
4. **라이센스 계약에 동의**를 클릭하여 라이센스를 가져와 적용합니다.

   설치가 완료되면 라이센스 활성화 키가 설치된 라이센스 수와 활성화 기간(시작 및 만료 날짜)과 함께 테이블에 나열됩니다.

## 완료한 후에

라이센스 페이지에서 다음 작업을 수행할 수 있습니다.

- **내보내기** 아이콘(  )을 클릭하여 하나 이상의 특정 라이센스 활성화 키를 로컬 시스템에 다운로드합니다.

  **참고:** 여러 개의 라이센스 활성화 키를 내보내면 파일이 단일 ZIP 파일로 다운로드됩니다.
- **삭제** 아이콘(  )을 클릭하여 특정 라이센스 활성화 키를 삭제합니다.
- 페이지 상단에 있는 **편집** 버튼을 클릭하여 라이센스 경고 기간을 구성하십시오. XClarity Administrator이(가) 경고를 트리거할 경우 라이센스 경고 기간은 라이센스 만료 전 남는 일수입니다.

### 도움말 얻기

- 문제가 있고 비즈니스 파트너를 사용한 경우, 비즈니스 파트너에게 문의하여 트랜잭션 및 사용을 확인하십시오.
- 전자 권한 증명서, 인증 코드 또는 활성화 키를 받지 못했거나 이러한 사항이 잘못된 사람에게 전송된 경우, 본인 지역의 지역 담당자 중 한 사람에게 문의하십시오.
  - ESDNA@lenovo.com(북미 국가)
  - ESDAP@lenovo.com(아시아 태평양 국가들)
  - ESDEMEA@lenovo.com(유럽, 중동 및 아시아 국가)
  - ESDLA@lenovo.com(중남미 국가)
  - ESDChina@Lenovo.com(중국)
- 내 자격에 대한 정보가 정확하지 않은 경우, SW_override@lenovo.com의 Lenovo 지원으로 문의하고 다음 정보를 포함하십시오.
  - 주문 번호
  - 이메일 주소를 포함한 연락처 정보.
  - 실제 주소
  - 원하는 변경 사항
- 라이센스 다운로드에 관한 문제나 질문이 있는 경우 -eSupport_-_Ops@lenovo.com의 Lenovo 지원으로 문의하십시오.

# 제 7 장 XClarity Administrator를 로 업데이트

컨테이너로 Lenovo XClarity Administrator을(를) 실행하는 경우 이 업데이트 절차를 사용하여 최신 소프트웨어를 새 컨테이너로 설치하고 원래 컨테이너의 볼륨을 새 컨테이너에 바인딩하십시오.

## 시작하기 전에

XClarity Administrator v3.0 이상의 인스턴스에서만 XClarity Administrator v4.0 이상을 업데이트할 수 있습니다. XClarity Administrator v3.0 이전 버전을 사용하는 경우에는 v4.0으로 업그레이드하기 전에 먼저 v3.0 이상으로 업그레이드해야 합니다.

Lenovo XClarity Orchestrator를 사용하여 XClarity Administrator v4.0 이상의 인스턴스를 관리하려면 XClarity Orchestrator v2.0 이상이 필요합니다. XClarity Administrator를 v4.0 이상으로 업데이트하는 경우 XClarity Orchestrator가 이미 v2.0 이상인지 확인하십시오.

## 이 작업 정보

`docker-compose.yml` 파일은 *원래* 컨테이너를 설치하는 동안 설정하는 다음 환경 변수를 사용합니다. 이러한 환경 변수는 새 컨테이너에서도 사용됩니다.

- CONTAINER_NAME. 각 XClarity Administrator 인스턴스에 대한 Docker 볼륨을 만드는 데 사용되는 고유 컨테이너 이름(예: `CONTAINER_NAME=LXCA-203`)

  XClarity Administrator은(는) 컨테이너 이름을 사용하여 컨테이너의 볼륨을 생성합니다. 새 컨테이너에 동일한 컨테이너 이름을 사용할 경우 새 XClarity Administrator 인스턴스가 동일한 볼륨을 사용하게 되며, 따라서 원래 XClarity Administrator 인스턴스(컨테이너)와 동일한 시스템 데이터 및 설정에 액세스할 수 있습니다.

  컨테이너 이름을 변경할 경우 컨테이너에 새 볼륨이 생성되며 새 XClarity Administrator 인스턴스가 원래 XClarity Administrator 인스턴스(컨테이너)와 동일한 시스템 데이터 및 설정에 액세스할 수 없습니다. 컨테이너 이름 또는 IP 주소를 변경해야 하는 경우 새 컨테이너를 설치하기 전에 원래 XClarity Administrator 인스턴스의 시스템 데이터와 설정을 백업한 다음 해당 백업을 사용하여 새 컨테이너에서 시스템 데이터 및 설정을 복원하십시오.
- ADDRESS. 컨테이너의 고정 IPv4 또는 IPv6 주소(예: `ADDRESS=192.0.2.0`)

  장치를 관리 설정한 후 XClarity Administrator IP 주소를 변경하면 XClarity Administrator에서 장치가 오프라인 상태가 될 수 있습니다. IP 주소를 변경하기 전에 모든 장치가 관리 해제되었는지 확인하십시오.
- BACKUP_MOUNT 및 FIRMWARE_MOUNT. (선택 사항) XClarity Administrator 백업을 저장하는 데 사용하거나 펌웨어 업데이트를 위한 원격 리포지토리로 사용할 수 있는 원격 공유의 경로. 경로는 각각 `/mnt/backup_share` 및 `/mnt/fw_share`여야 합니다.

**참고:** XClarity Administrator는 권한이 있는 컨테이너로 실행되지 *않습니다*.

## 절차

XClarity Administrator 컨테이너를 업데이트하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 다운로드 웹 페이지에서 클라이언트 워크스테이션으로 XClarity Administrator 컨테이너 이미지를 다운로드하십시오. 웹 사이트에 로그온한 후 제공된 액세스 키를 사용하여 이미지를 다운로드하십시오.

단계 2. 다음 명령을 실행하여 XClarity Administrator 컨테이너 이미지를 Docker 호스트로 가져오십시오.

```
docker load -i lnvgy_sw_lxca_110-3.5.0_anyos_noarch
```

단계 3. 원래 컨테이너에 사용된 것과 동일한 docker-compose.yml 파일을 편집하십시오. 2단계의 새 Docker 이미지를 가리키도록 파일 상단의 이미지 속성을 업데이트하십시오. `docker tag` 명령을 사용하여 이미지 태그를 변경할 수 있습니다.

다음은 IPv6이 사용 설정된 yml 파일의 예를 보여줍니다.

```
version: '3.8'

services:

 lxca:
  image: lenovo/lxca:4.1.0-124
  container_name: ${CONTAINER_NAME}
  tty: true
  stop_grace_period: 60s
  volumes:
   #bind mount example
   - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
   - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
   #docker volume mount
   - data:/opt/lenovo/lxca/data
   - postgresql:/var/lib/postgresql
   - log:/var/log
   - confluent-etc:/etc/confluent
   - confluent-log:/var/log/confluent
   - confluent:/var/lib/confluent
   - propconf:/opt/lenovo/lxca/bin/conf
   - ssh:/etc/ssh
   - xcat:/etc/xcat
  networks:
   lan:
    ipv4_address: ${ADDRESS}
    ipv6_address: "2001:8003:7d51:2003::2"
  dns:
   - 192.0.2.10
   - 192.0.2.11
  deploy:
   resources:
    limits:
     cpus: "2.0"
     memory: "8g"

volumes:
 data:
  name: ${CONTAINER_NAME}-data
 postgresql:
  name: ${CONTAINER_NAME}-postgresql
 log:
  name: ${CONTAINER_NAME}-log
 confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
 confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
 confluent:
  name: ${CONTAINER_NAME}-confluent
 propconf:
  name: ${CONTAINER_NAME}-propconf
 ssh:
  name: ${CONTAINER_NAME}-ssh
 xcat:
  name: ${CONTAINER_NAME}-xcat
```

```
networks:
 lan:
  name: lan
  driver: macvlan
  enable_ipv6: true
  driver_opts:
   parent: eth0
  ipam:
   config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
```

단계 4. 다음 명령을 실행하여 *원래* 컨테이너를 종료합니다.

```
docker-compose -p ${CONTAINER_NAME} down
```

단계 5. 다음 명령을 실행하여 *새* 이미지를 Docker에 배포합니다. 여기에서 *<ENV_FILENAME>*은(는) 환경 변수 파일의 이름입니다.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME}
--env-file <ENV_FILENAME> up -d
```

# 제 8 장 XClarity Administrator 제거

Lenovo XClarity Administrator 가상 어플라이언스 또는 컨테이너를 제거하려면 다음 단계를 완료하십시오.

## 절차

XClarity Administrator 가상 어플라이언스를 설치 제거하려면 다음 단계를 완료하십시오.

단계 1. 현재 XClarity Administrator에서 관리하는 모든 장치를 관리 해제하십시오. (XClarity Administrator 온라인 문서의 섀시 관리, 서버 관리, and 스위치 관리 참조)

단계 2. 운영 체제에 따라 다음과 같이 XClarity Administrator를 설치 제거하십시오.

- Docker-compose컨테이너를 중지하고 네트워크 및 볼륨을 제거하려면 다음 명령을 실행하십시오.
  ```
  docker-compose down -v
  ```
- CentOS, Red Hat, Rocky 및 Ubuntu
  1. 가상 컴퓨터 관리자를 사용하여 호스트에 연결하십시오.
  2. 가상 컴퓨터를 마우스 오른쪽 버튼으로 클릭하고 **시스템 종료 → 강제 끄기**를 클릭하십시오.
  3. 가상 컴퓨터를 다시 마우스 오른쪽 단추로 클릭하고 **삭제**를 클릭하십시오. 삭제 확인 대화 상자가 표시됩니다.
  4. 확인란을 모두 선택하고 **삭제**를 클릭하십시오.
- ESXi
  1. VMware vSphere Client를 통해 호스트에 연결하십시오.
  2. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 **전원 → 전원 끄기**를 클릭하십시오.
  3. 가상 컴퓨터를 다시 마우스 오른쪽 단추로 클릭하고 **디스크에서 삭제**를 클릭하십시오.
- Hyper-V
  1. Server Manager 대시보드에서 Hyper-V를 클릭하십시오.
  2. 서버를 마우스 오른쪽 단추로 클릭하고 Hyper-V Manager를 클릭하십시오.
  3. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 **시스템 종료**를 클릭하십시오.
  4. 가상 컴퓨터를 다시 마우스 오른쪽 단추로 클릭하고 **삭제**를 클릭하십시오.