Lenovo XClarity Administrator 사용 설명서

버전 4.0.0

초판 (2023년 2월)

목차

표

변경사항 요약

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

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

이 버전은 관리 소프트웨어에 대한 다음 향상 기능을 지원합니다.

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

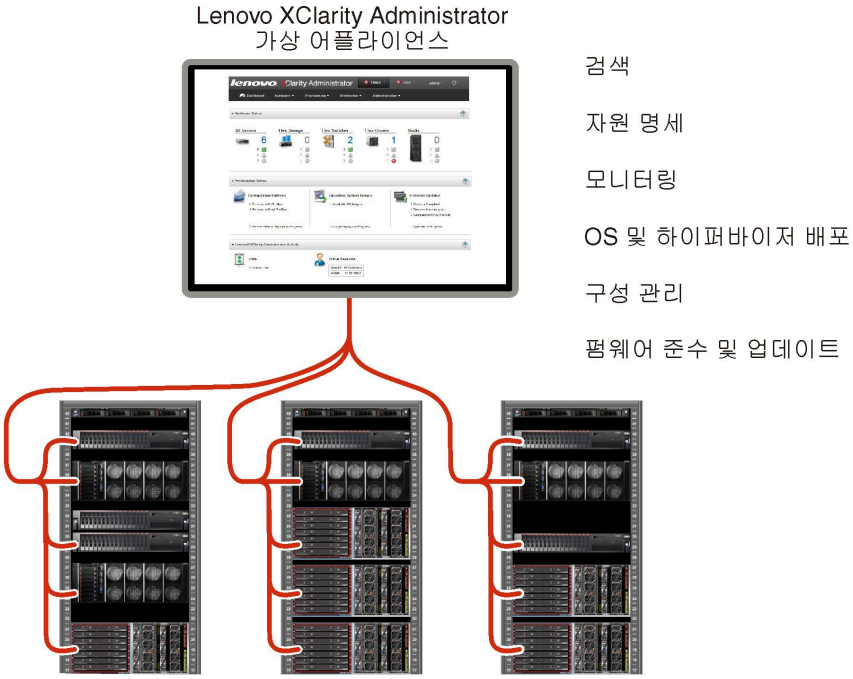
기능	설명
관리	XClarity Administrator 관리 서버 FQDN(정규화된 도메인 이름) 및 DNS 정보를 IMM2, XCC 및 XCC2가 있는 관리되는 서버에 푸시하여 관리되는 서버가 이 정보를 사용하여 관리 서버를 찾을 수 있도록 할 수 있습니다(네트워크 액세스 구성 참조).
모니터링	영구 메모리(PMEM) 구성 요소에 대한 추가 인벤토리 데이터를 볼 수 있습니다(관리 서버의 세부 정보 보기 참조). 스토리지 장치에 대한 추가 인벤토리 데이터를 볼 수 있습니다(관리 서버의 세부 정보 보기 참조).
장치 관리	XClarity Administrator와 별도로 특정 서버의 보안 모드를 보고 구성할 수 있습니다(관리되는 서버의 보안 설정 구성 및 관리 서버의 암호화 설정 구성). 해당하는 ThinkSystem 서버의 베이스보드 관리 컨트롤러에 대해 보조 IP 주소가 지원됩니다(관리 서버의 세부 정보 보기 참조).
펌웨어 업데이트	IBM TS4300 테이프 라이브러리에서 펌웨어를 업데이트할 수 있습니다(관리 장치에서 펌웨어 업데이트 참조).
운영 체제 배포	관리되는 서버에 다음 운영 체제를 배포할 수 있습니다(지원되는 운영 체제 참조). • Microsoft Windows Client 10 21H2, 10 22H2 및 11 22H2 • RedHat Enterprise Linux 9.x • Ubuntu 서버 22.04.x

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 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 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 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 구성 패턴을 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 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 베어메탈 서버에 운영 체제 설치의 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 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 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 사용자 지정 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 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 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 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 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 제

공업체 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 XClarity Administrator 온라인 설명서에서 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

XClarity Administrator에 로그인

지원되는 웹 브라우저를 사용하여 Lenovo XClarity Administrator 웹 인터페이스에 로그인하십시오.

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

다음 단계를 완료하여 XClarity Administrator 웹 인터페이스에 로그인하십시오.

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` 명령

을 사용하여 영역 인덱스를 찾으십시오. 영역 인덱스는 어댑터의 **링크 로컬 IPv6 주소** 필드에서 백분율 기호(%) 다음에 나옵니다. 다음 예에서는 영역 인덱스는 "30"입니다.

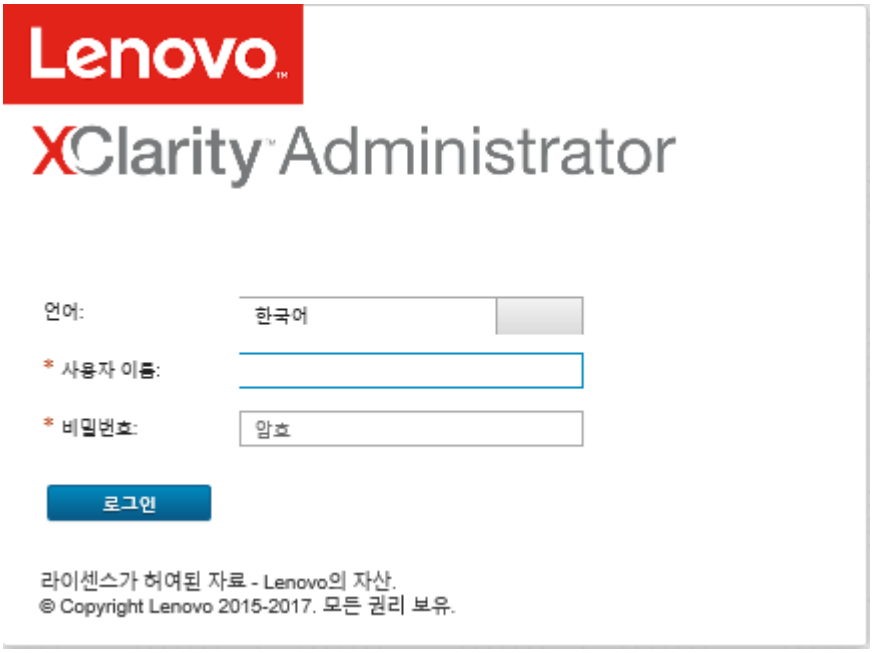
```
PS C:> ipconfig
Windows IP 구성

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
```

XClarity Administrator 초기 로그인 페이지가 표시됩니다.



단계 2. **언어** 드롭다운 목록에서 원하는 언어를 선택하십시오.

참고: 관리 장치에서 영어로 된 구성 설정 및 값만 제공할 수 있습니다.

단계 3. 유효한 사용자 ID 및 암호를 입력하고 **로그인**을 클릭하십시오.

처음 사용자 계정으로 로그인할 때 암호를 변경해야 합니다. 암호는 다음 기준을 충족해야 합니다.

- (1) 알파벳 문자를 하나 이상 포함해야 하며 알파벳 문자, 숫자 및 QWERTY 키보드 키 시퀀스를 포함하여 세 개 이상의 순차적 문자를 포함해서는 안됩니다(예: "abc", "123", "asd"는 허용되지 않습니다).
- (2) 숫자(0~9)를 하나 이상 포함해야 합니다.
- (3) 다음 문자 중 *두 개* 이상이 포함되어야 합니다.
  - 알파벳 대문자(A – Z)
  - 알파벳 소문자(a – z)

  - 특수 문자 ; @ _ ! ' $ & +
- (4) 사용자 이름을 반복하거나 거꾸로 쓸 수 없습니다.
- (5) 동일한 문자를 세 개 이상 연속해서 포함할 수 없습니다(예: "aaa", "111", "..."는 허용되지 않습니다).

완료한 후에

XClarity Administrator 대시보드 페이지가 표시됩니다.

참고: 호스트 운영 체제가 예기치 않게 종료되는 경우 XClarity Administrator에 로그인을 시도할 때 인증 오류를 받을 수 있습니다. 이 문제를 해결하려면 최종 백업에서 XClarity Administrator를 복원하여 관리 서버에 액세스합니다(Lenovo XClarity Administrator 백업 참조).

XClarity Administrator 제목 표시줄의 사용자 작업 메뉴(ADMIN_USER)에서 다음 작업을 수행할 수 있습니다.

- **도움말**을 클릭하여 포함된 도움말 시스템에서 XClarity Administrator 사용 방법에 대한 정보를 찾습니다.

  XClarity Administrator 설명서(영어)는 온라인에서 정기적으로 업데이트됩니다. 최신 정보와 절차에 대해서는 XClarity Administrator 온라인 설명서의 내용을 참조하십시오.
- **라이센스**를 클릭하여 XClarity Administrator 라이센스를 봅니다.
- **정보**를 클릭하여 XClarity Administrator 릴리스에 대한 정보를 봅니다.
- **언어 변경**을 클릭하여 사용자 인터페이스의 언어를 변경합니다.
- **로그아웃**을 클릭하여 현재 세션에서 로그아웃합니다.
- **아이디어 제출** 또는 **피드백 제출**을 클릭하여 XClarity Administrator에 대한 아이디어를 제출하거나 피드백을 제공할 수 있습니다.
- **포럼 방문**을 클릭하여 Lenovo XClarity 커뮤니티 포럼 웹 사이트에서 질문을 하고 답변을 찾습니다.

사용자 인터페이스 팁 및 기술

Lenovo XClarity Administrator 사용자 인터페이스를 사용할 때 다음 팁과 기술을 고려합니다.

페이지별로 많거나 적은 데이터 보기

표의 오른쪽 하단에 있는 링크를 사용하여 각 페이지별로 표시되어 있는 행의 수를 변경할 수 있습니다. 10개, 25개, 50개, 또는 모든 행을 표시할 수 있습니다.

큰 목록에서 데이터 찾기

대부분의 필드는 최대 128자를 허용합니다.

특정 기준에 따라 큰 목록의 서브세트를 표시하는 몇 가지 방법이 있습니다.

- 열 머리글을 클릭하여 테이블 행을 정렬할 수 있습니다.

  테이블 열의 정렬 순서를 바꾸면 사용자 세션을 변경해도 지속됩니다.
- 일부 페이지에서 표시되는 **다음으로 분류** 아이콘 및 **표시** 드롭다운 목록을 사용하여 선택한 기준에 따라 일부 데이터 결과를 표시할 수 있습니다.
- 사용 가능한 모든 열에 있는 데이터를 찾기 위해 **필터** 필드에 (이름 또는 IP 주소와 같은) 텍스트를 입력해서 결과를 구체화 할 수 있습니다.

  필터 필드의 드롭 다운 메뉴에서 검색을 선택하여, 검색 기록 10개 중에서 선택할 수 있습니다. 페이지의 마지막 활성 검색 기록은 사용자 세션을 변경해도 지속됩니다.

열 데이터 보기

열 크기로 인해 모든 정보가 테이블 셀에 표시되지 않는 경우(줄임표로 표시됨) 셀의 텍스트 위로 마우스를 가져가면 팝업에서 전체 정보를 볼 수 있습니다.

테이블 열 구성

중요한 정보를 표시하도록 테이블을 구성할 수 있습니다.

- 모든 **작업 → 열 전환**을 클릭하여 표시하거나 숨길 열을 선택할 수 있습니다.
- 열 머리글을 원하는 위치로 끌어 열을 다시 정렬할 수 있습니다.

사용자 인터페이스의 언어 변경

처음 로그인할 때 사용자 인터페이스의 언어를 설정하는 옵션이 있습니다.

로그인한 후 사용자 작업 메뉴(

)를 클릭한 다음 **언어 변경**을 클릭하여 사용자 인터페이스의 언어를 변경할 수 있습니다. 표시하려는 언어를 선택하십시오.

참고: 도움말 시스템은 사용자 인터페이스에 설정된 동일한 언어로 표시됩니다.

도움말 얻기

XClarity Orchestrator 는 사용자 인터페이스에 대한 도움말을 얻을 수 있는 몇 가지 방법을 제공합니다.

- 일부 페이지에서는 **도움말** 아이콘()을 사용하여 특정 필드나 상태에 대한 자세한 정보를 볼 수 있습니다. 아이콘 위에 커서를 놓으면 유용한 정보가 포함된 팝업이 표시됩니다.
- 사용자 인터페이스에서 특정 작업을 수행하는 방법에 대한 도움말을 보려면 사용자 작업 메뉴(

)를 클릭한 다음 **도움말**을 클릭하십시오.

Lenovo XClarity Mobile 앱 사용

Lenovo XClarity Administrator는 Android 및 iOS 장치용 모바일 앱을 제공합니다. Lenovo XClarity Mobile앱을 사용하여 물리적 시스템을 안전하게 모니터링하고 실시간 상태 알림 및 통지를 받으며 일반 시스템 수준 작업에 대한 조치를 취할 수 있습니다. 이 앱은 활성화된 USB 포트를 통해 ThinkSystem 서버에 직접 연결하여 가상 LCD 기능을 제공할 수도 있습니다.

자세히 알아보기: Lenovo XClarity Mobile 앱 개요

XClarity Mobile 앱을 사용하여 다음 활동을 수행할 수 있습니다.
- 네트워크 설정 및 속성 구성
- 연결된 각 XClarity Administrator의 상태 요약을 봅니다.
- 모든 관리되는 장치의 상태 요약을 봅니다.
- 섀시, 랙 서버 및 스토리지 장치에 대한 그래픽 보기(맵)을 표시합니다.
- XClarity Administrator에 정의된 리소스 그룹을 봅니다.
- 랙 스위치 포트 정보를 보고 구성된 포트 상태를 변경합니다.
- 각 관리되는 장치의 인벤토리 및 세부 상태를 모니터링합니다.
- 감사 이벤트, 하드웨어 및 관리 이벤트, 경고 및 작업을 모니터링합니다.
- 관리되는 장치의 위치 LED를 켜거나 끕니다.
- 전원을 키거나 끄거나, 관리 장치를 다시 장착하십시오.
- 진단 데이터의 수집을 트리거합니다.
- 기기 보증 정보 및 상태 보기
- 콜 홈을 통해 자동 문제 알림을 설정합니다.
- 이용 가능한 서비스 티켓 요약 보기 및 서비스 티켓 삭제
- 모바일 장치에 이벤트 알림을 푸시합니다(모바일 장치에 이벤트 전달 참조).
- 활성 사용자 및 시스템 리소스 사용량 개요 보기
- Lenovo 지원에 이 모바일 앱에 대한 피드백을 보냅니다.
- XClarity Mobile 앱(USB 테더링을 지원하는 장치용)을 사용하여 서버를 관리하려면 모바일 장치를 ThinkSystem 서버에 직접 연결하십시오.
- 모바일 장치가 ThinkSystem 서버에 연결되어 있으면 Lenovo XClarity Controller 서비스 데이터를 다운로드하십시오.

또한, ThinkSystem 서버에 모바일 장치를 직접 연결한 다음 XClarity Mobile 앱을 실행하고 동일한 웹 및 CLI 자격 증명을 사용하여 해당 서버의 베이스보드 관리 컨트롤러에 로그인할 수 있습니다. 일부 예로 다음과 같은 추가 정보 및 작업 메뉴가 제공됩니다.

- 서비스
  - 이메일 또는 모바일 장치의 기타 수단을 통해 요약 정보 공유
  - 이벤트 및 감사 로그 지우기
  - 이벤트 및 감사 로그를 모바일 장치 로컬 저장소에 다운로드 하거나, 모바일 장치의 다른 수단을 통해 로그 전송
  - BMC FFDC 서비스 파일을 모바일 장치 로컬 저장소에 다운로드 하거나, 모바일 장치의 다른 수단을 통해 파일 전송
  - 전력, 열 및 시스템 사용에 대한 내역 그래프 데이터 보기
  - 활성화 알림 및 장치 중요 정보를 즉시 요약하여 보여주는 "원터치" 서비스 모드 활성화
- 구성 및 초기 설정
  - 선택한 XClarity Administrator을 사용하여 새로운 장치 구성
  - 초반 작업을 위해 위치 및 연락처 정보와 같은 서버 속성 설정
  - IPv4 및 IPv6 BMC 네트워크 인터페이스 설정 보기 및 변경
  - 부팅 순서 및 일회성 부팅 설정 지정
  - 앞면 패널 USB 포트 배치 변경
  - 서버 재부팅 횟수 및 총 작동 시간 보기
- 전원 작업
  - 서버 전원 켜기, 끄기, 재시작, 또는 NMI 작동

- BMC 재설정

팁: 앱을 연 후 앱을 새로 고쳐 업데이트된 상태, 인벤토리, 이벤트 및 작업을 확인해야 합니다.

전제조건

- iOS 태블릿은 iPhone 화면 해상도로만 지원됩니다. Android 태블릿은 현재 지원되지 않습니다.
- 다음 모바일 운영 체제가 지원됩니다.
  - Android 7~11
  - iOS 10 이상

    참고:

    - Android 5는 XClarity Mobile 2.3.0 이전에만 지원됩니다.
    - iPhone X/XR/XS 장치에서 사용되는 얼굴 인식은 지원되지 않습니다.
- 모바일 장치에서 XClarity Administrator 인스턴스로의 네트워크 연결을 사용할 수 있어야 합니다. 여기에는 VPN 솔루션 사용이 필요할 수 있습니다. 지원을 받으려면 네트워크 관리자에게 문의하십시오.
- 각 XClarity Administrator 인스턴스에 대해 CA 인증서를 가져오십시오.

  중요: 모든 XClarity Administrator 연결은 HTTPS를 사용합니다. 하지만 연결이 신뢰할 수 있는 것으로 간주되고 데이터를 모바일 장치에 전달되기 전에 올바른 인증서 체인이 있어야 합니다. 신뢰할 수 있는 인증서 체인을 만들려면 XClarity Administrator 자체 서명된 인증 기관(CA)을 모바일 장치에 가져와야 합니다.

  *각 XClarity Administrator 인스턴스*에 대한 자체 서명된 CA 인증서를 모바일 장치에 가져오려면 다음 단계를 완료하십시오.

  1. CA 인증서를 로컬 시스템에 다운로드하십시오.
     a. 로컬 시스템에서 웹 브라우저를 사용하여 XClarity Administrator 인스턴스에 연결하십시오.
     b. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.
     c. 인증서 관리 섹션의 **인증 기관**을 클릭하십시오. 인증 기관 페이지가 표시됩니다.
     d. **인증 기관 루트 인증서 다운로드**를 클릭하십시오.

        주의: 일반적으로 이 프로세스를 완료하기 위해 **인증 기관 루트 인증서 다시 생성**을 클릭할 필요가 없습니다. 그렇게 하면 올바른 절차를 따르지 않는 경우 관리되는 장치와의 통신이 중단될 수 있습니다. 자세한 정보는 보안 인증서 작업의 내용을 참조하십시오.
     e. 로컬 시스템에서 CA 인증서를 DER 또는 PEM 파일로 저장하려면 DER로 **저장** 또는 PEM으로 **저장**을 클릭하십시오. 대부분의 경우 PEM 형식이 작동합니다.
  2. CA 인증서를 모바일 장치로 전송하십시오. 예를 들어 액세스 가능한 스토리지 리포지토리(예, Dropbox™), 이메일 또는 연결된 케이블을 통한 파일 전송을 사용할 수 있습니다.
  3. 신뢰할 수 있는 CA 인증서를 가져오십시오.
     - (Android) 일반적으로 전화 스토리지에서 **설정 → 보안 → 설치**를 선택한 다음 사용자가 다운로드한 인증서 파일을 선택하여 수행됩니다.

       중요: 성공적으로 설치된 CA 인증서가 타사의 서명을 받지 않은 경우 알 수 없는 타사에서 네트워크를 모니터링할 수 있음 메시지가 Android 장치에 표시됩니다. 신뢰할 수 있는 환경에서 CA 인증서가 생성되기 때문에 이 메시지가 안전하게 무시됩니다. 메시지를 무시하려면 메시지가 XClarity Administrator CA 인증서에 대한 것이어야 합니다.
     - (iOS) 모바일 장치에서 이메일을 열고 이메일의 문서 링크를 클릭하여 신뢰할 수 있는 CA 인증서를 가져오십시오.

주의: iOS 10.3 이상 버전의 경우, 가져온 인증서는 신뢰할 수 없는 것이 기본값입니다. 인증서를 신뢰할 수 있는 인증서로 설정하려면 **설정 → 일반 → 정보 → 인증서 신뢰 설정**을 선택한 후 인증서 신뢰를 사용으로 설정하십시오.

설치 및 설정

1. iTunes App Store(iOS) 또는 Google Play Store(Android)에서 XClarity Mobile 앱을 다운로드하십시오.
2. 앱을 설치하려면 모바일 장치에 대한 지시사항을 따르십시오.

   중요: XClarity Mobile 앱을 사용하려면 화면 액세스를 잠금 해제하기 위한 모바일 OS 수준의 보안 코드가 필요합니다. 아직 설정하지 않은 경우 설치 중 설정 지시사항을 따르십시오.
3. **설정**을 클릭하고 자동 검색을 사용하거나 IP 주소 및 사용자 자격 증명을 제공하여 여러 XClarity Administrator 인스턴스에 연결을 추가하거나 편집하고 앱에 대한 PIN 코드를 설정하고 이벤트 및 감사 로그 설정을 변경하고 선호하는 언어를 선택하십시오.

ThinkSystem 서버에 직접 연결

Lenovo Think System에 포함된 앞면 패널 USB 포트는 모바일 장치에 연결 시 다른 Lenovo 서버의 LCD 시스템 정보 디스플레이 패널에서 제공된 유사 기능을 구현하는 데 사용할 수 있습니다.

서버에 직접 연결해서 ThinkSystem 서버를 관리하려면 다음 과정을 차례로 완료하십시오.

1. 다음 과정 중 한 가지 단계를 수행하여 호스트에서 BMC로 서버 앞면 패널 USB를 전환하십시오.
   a. 관리 컨트롤러 CLI에서 `usbfp` 명령을 실행합니다
   b. 관리 컨트롤러 웹 인터페이스에서 BMC **구성 → 네트워크 → 앞면 패널 USB 포트 관리**를 클릭합니다.
   c. 파란색 표시등이 2초에 1회씩 깜박일 때까지 앞면 패널의 파란색 ID 위치 LED를 적어도 3초 이상 길게 누릅니다.
2. ThinkSystem 서버의 앞면 패널 USB 포트에 휴대폰 USB 케이블을 연결합니다.
3. 모바일 장치에서 USB 테더링을 사용합니다.
   a. iOS의 경우 **설정 → 셀룰러 → 개인용 핫스팟**을 클릭하십시오.
   b. Android의 경우 **설정 → 모바일 핫스팟 및 테더링 → USB 테더링**을 클릭합니다.
4. 모바일 장치에서 XClarity Mobile 앱을 실행합니다.
5. 자동 검색을 사용하지 않는 경우 USB 검색 페이지의 **검색**을 클릭하여 서버의 관리 컨트롤러에 연결하고 인벤토리, 상태, 펌웨어, 네트워크 구성, 최신 활성 이벤트 목록 등의 정보를 수집하십시오.

팁:

- 데이터 및 전원이 지원되는 고품질 USB 케이블을 사용해야 합니다. 모바일 장치와 함께 지급되는 일부 케이블은 충전 전용이라는 것을 알아 두십시오.

  참고: ThinkSystem SD530에 연결하려면 고품질의 micro USB to USB 케이블 또는 어댑터도 사용해야 합니다.
- USB 연결 서버는 요약 상태 카드의 전압, 온도 및 사용 통계 전체를 묶어서 하나로 보고하려 할 경우에 전원 켜기를 해야 합니다.
- USB 연결 서버의 앞면 패널에 외부 "파란색 식별" LED/버튼이 없는 경우 필요에 따라 관리 컨트롤러 웹 인터페이스 또는 CLI를 사용하여 앞면 패널 USB 포트 관리 선택 항목을 변경해야 합니다.
- XClarity Mobile 앱을 통하여 관리 컨트롤러 네트워크 인터페이스에 가한 변경 내용은 관리 컨트롤러를 다시 시작하지 않고서도 즉시 적용됩니다. 예를 들어 IPv4 인터페이스가 고정 주소에서 DHCP로 변경되는 경우 해당 인터페이스는 DHCP 할당 주소를 즉시 획득합니다.
- Newsfeed 탭에서 "최신 활성 이벤트" 카드는 관리 컨트롤러의 활성 이벤트 탭에 나열되는 최대 3개의 활성 이벤트를 처음에 표시합니다. 모바일 앱에서 해당 카드를 누르면 모든 활성 이벤트가 표시됩니다. 단, 이는 모든 이벤트의 전체 목록이 아니라 활성 및 해결된 이벤트의 목록입니다.

데모 모드 사용

설정 페이지에서 **데모 모드**를 사용하여 랙 및 섀시 등 2개의 XClarity Administrator 인스턴스에 대한 데모 데이터로 XClarity Mobile 앱을 구성하십시오. 이 모드에서 XClarity Administrator 인스턴스의 상태 요약을 보고 장치의 세부 상태 및 인벤토리를 보고 이벤트 및 경고를 모니터링할 수 있습니다. 하지만 전원 켜기 및 끄기와 같은 관리 작업은 지원되지 않습니다.

참고:

- 실제 XClarity Administrator 인스턴스 연결이 없는 경우에만 데모 모드를 사용할 수 있습니다.
- 데모 모드를 사용하는 동안 실제 XClarity Administrator 인스턴스에 연결을 추가할 수 없습니다.

검색

검색 필드를 사용하여 관리되는 장치를 특정 이름 또는 상태(위험, 경고 또는 정상)로 표시합니다. 예를 들어 "crit"을 검색하는 경우 위험 상태 및 "crit"이 포함되는 이름의 관리되는 장치가 표시됩니다.

문제 해결

설치 문제:

- Android 모바일 앱은 보안을 강화하기 위해 보안 키로 "서명"되어 있습니다. 새로운 릴리스에서는 보안 키 크기가 증가했습니다. 서명된 앱이 이전 앱 서명과 일치하지 않기 때문에 Android 설치 보안 프로세스가 자동 업데이트를 방지합니다.

  모바일 앱을 업데이트하려면, 현재 버전의 모바일 앱을 제거하고 앱 스토어에서 최신 버전의 Android 앱을 다운로드한 다음 앱을 다시 설치하십시오. 대부분의 Android 장치에서는 **설정 → 응용 프로그램 → 응용 프로그램 관리자** 메뉴 항목을 사용하여 앱을 제거할 수 있습니다.

연결 문제:

- iOS 14, 14.0.1 및 14.0.2에서 USB 테더링 기능이 제대로 작동하지 않습니다. 따라서 이러한 iOS 버전에서는 Lenovo XClarity Mobile 앱 테더링 기능을 사용할 수 없습니다. 이 문제는 데이터 센터의 USB 연결 핸드헬드 관리에만 영향을 줍니다. 셀룰러 및 Wi-Fi 통신을 지원하는 모바일 장치를 사용한 원격 관리는 영향을 받지 않으며 XClarity Administrator의 데이터를 연결 및 수집하고 관리되는 장치에서 관리 작업을 수행하는 데 사용할 수 있습니다.

  USB 연결 핸드헬드 관리 기능이 필요한 경우 iOS 14로 업그레이드하지 마십시오.

  이 알림은 Apple에서 iOS 14 관련 문제를 해결하면 업데이트됩니다.
- XClarity Mobile은 모바일 장치에서 XClarity Administrator 인스턴스로의 네트워크 연결을 사용할 수 있어야 합니다. 여기에는 VPN 솔루션 사용이 필요할 수 있습니다. 지원을 받으려면 네트워크 관리자에게 문의하십시오.
- 모바일 장치에서 각 XClarity Administrator 인스턴스로 연결하려면 신뢰할 수 있는 인증서 체인이 필요합니다. 모바일 장치에서 신뢰할 수 있는 CA 인증서 다운로드 및 설치 지시사항은 온라인 설명서를 참조하십시오.

  성공적으로 설치된 CA 인증서가 타사의 서명을 받지 않은 경우 알 수 없는 타사에서 네트워크를 모니터링할 수 있음 메시지가 표시됩니다. 신뢰할 수 있는 환경에서 CA 인증서가 생성되기 때문에 이 메시지가 안전하게 무시됩니다. 메시지를 무시하려면 메시지가 XClarity Administrator CA 인증서에 대한 것이어야 합니다.
- 모바일 장치를 가상 개인 네트워크(VPN)에서 로컬 네트워크로 또는 그 반대로 전환하는 경우 보안 게이트웨이가 연결 시도를 거부했습니다 메시지가 표시될 수 있습니다. 동일한 또는 다른 보안 게이트웨이에 새로 연결을 시도해야 하는데, 여기에는 재인증이 필요합니다. Lenovo XClarity Mobile에 로그온하여 계속 앱을 사용하십시오.

보안 문제:

- PIN 코드를 잊어버린 경우 XClarity Mobile 앱을 제거하고 다시 설치하십시오. 그런 다음 모든 연결을 다시 구축하십시오.

- Android 장치에서 자격 증명을 지우는 경우 암호화 키가 삭제됩니다. 모든 연결을 다시 구축해야 합니다.

이벤트 문제:

- 기본적으로 이벤트 로그는 최근 24시간 동안 수신된 하드웨어 및 관리 이벤트를 표시하고 감사 로그는 최근 2시간 동안 수신된 감사 이벤트를 표시합니다. 선택한 시간 기간 동안 이벤트가 수신되지 않는 경우 XClarity Mobile의 모니터링 페이지에 이벤트 로그 및 감사 로그가 표시되지 않습니다.
- XClarity Administrator에서 이벤트 전달을 설정하여 이메일 계정에 이벤트를 보내는 경우 이메일의 링크는 Android 장치에서 작동하지 않을 수 있습니다. Android 및 이메일 앱이 하이퍼링크를 지원해야 합니다. 하이퍼링크가 지원되지 않은 경우 다른 이메일 앱을 사용하십시오.

도움말 시스템 문제:

- 일부 장치에서는 도움말 시스템이 화면 크기에 맞게 정확하게 확장되지 않습니다. 도움말 시스템 컨트롤을 사용하여 페이지를 최대화한 다음 최소화하십시오.

제 2 장 Lenovo XClarity Administrator 관리

Lenovo XClarity Administrator에서 사용자 추가 또는 작업 보기 등 여러 가지 관리 작업을 할 수 있습니다.

인증 및 권한 부여 관리

Lenovo XClarity Administrator는 사용자의 자격 증명을 확인하고 리소스 및 작업에 대한 액세스를 제어하는 보안 메커니즘을 제공합니다.

인증 서버 관리

기본적으로 Lenovo XClarity Administrator는 사용자 자격 증명을 인증하는 데 LDAP(Lightweight Directory Access Protocol) 서버를 사용합니다.

이 작업 정보

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.

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(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 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 "관리 서버 오류 후 CMM으로 관리 복구" 201페이지 및 "관리 서버 오류 후 랙 또는 타워 서버 관리 복구" 246페이지의 내용을 참조하십시오.

외부 LDAP 인증 서버 설정

관리 노드의 로컬 Lenovo XClarity Administrator 인증 서버 대신 외부 LDAP 인증 서버를 사용하도록 선택할 수 있습니다.

시작하기 전에

외부 인증 서버를 설정하기 전에 XClarity Administrator 초기 설치가 완료되어야 합니다.

다음 외부 인증 서버가 지원됩니다.

- OpenLDAP
- Microsoft Active Directory. 이 서버는 관리 네트워크, 데이터 네트워크 또는 두 가지 모두에 연결된 아웃보드 Microsoft Windows 서버에 상주해야 합니다.

외부 인증 서버에 필요한 모든 포트가 네트워크와 방화벽에서 열려 있어야 합니다. 포트 요구 사항에 대한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

외부 인증 서버에 정의된 그룹과 일치하도록 로컬 인증 서버에서 역할 그룹을 작성하거나 이름을 바꾸어야 합니다.

로컬 인증 서버에는 lxc-recovery 권한이 있는 하나 이상의 사용자가 있어야 합니다. 외부 LDAP 서버에 통신 오류가 발생하는 경우 이 로컬 사용자 계정을 사용하여 XClarity Administrator에 직접 인증할 수 있습니다.

참고: XClarity Administrator가 외부 인증 서버를 사용하도록 구성된 경우 XClarity Administrator 웹 인터페이스에서 사용자 관리 페이지를 사용할 수 없습니다.

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

XClarity Administrator는 구성된 외부 LDAP 서버에 대한 연결을 유지하기 위해 5초마다 연결을 검사합니다. LDAP 서버가 여러 개인 환경에서는 이 연결 검사를 수행하는 동안 CPU 사용량이 높아질 수 있습니다. 우수한 성능을 위해서는 도메인에 있는 대부분의 또는 모든 LDAP 서버가 도달 가능해야 하거나, 인증 서버 선택 방법이 **미리 구성된 서버 사용**으로 설정되고 알려진 도달 가능한 LDAP 서버만 지정해야 합니다.

절차

XClarity Administrator를 외부 인증 서버를 사용하도록 구성하려면 다음 단계를 완료하십시오.

단계 1. Microsoft Active Directory 또는 OpenLDAP에 대한 사용자 인증 방법을 설정하십시오.

비보안 인증을 사용하려는 경우 추가 구성이 필요하지 않습니다. Windows Active Directory 또는 OpenLDAP 도메인 컨트롤러는 기본적으로 비보안 LDAP 인증을 사용합니다.

보안 LDAP 인증을 사용하려는 경우, 도메인 컨트롤러를 보안 LDAP 인증을 허용하도록 설정해야 합니다. Active Directory에서 보안 LDAP 인증 구성 설정에 대한 자세한 정보는 Microsoft TechNet의 LDAPS(LDAP over SSL) 인증서 문서 웹 사이트의 내용을 참조하십시오.

Active Directory 도메인 컨트롤러가 보안 LDAP 인증을 사용하도록 구성되었는지 확인하려면 다음과 같이 하십시오.

- 도메인 컨트롤러 이벤트 뷰어 창에서 **지금 SSL(Secure Sockets Layer)을 통해 LDAP 사용 가능** 이벤트를 찾으십시오.
- `ldp.exe` Windows 도구를 사용하여 보안 도메인 컨트롤러와의 보안 LDAP 연결을 테스트하십시오.

단계 2. Active Directory 또는 OpenLDAP 서버 인증서 또는 Active Directory 서버 인증서에 서명한 인증 기관의 루트 인증서를 가져오십시오.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오.
b. 인증서 관리 섹션의 **신뢰할 수 있는 인증서**를 클릭하십시오.
c. **만들기** 아이콘( )을 클릭하여 인증서를 추가하십시오.
d. 파일을 찾아보거나 PEM 형식 인증서 텍스트를 붙여넣으십시오.
e. **만들기**를 클릭하십시오.

단계 3. 다음과 같이 XClarity Administrator LDAP 클라이언트를 구성하십시오.

a. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.
b. 사용자 및 그룹 섹션에서 LDAP **클라이언트**를 클릭하여 LDAP 클라이언트 설정 대화 상자를 표시하십시오.

c. 다음 기준에 따라 대화 상자를 작성하십시오.

1. 이러한 사용자 인증 방법 중 하나를 선택하십시오.

   - **로컬 사용자의 로그온 허용**. 로컬 인증을 사용하여 인증이 수행됩니다. 이 옵션을 선택하면 모든 사용자 계정이 관리 노드의 로컬 인증 서버에 존재합니다.
   - **LDAP 사용자의 로그온 허용**. 외부 LDAP 서버가 인증을 수행합니다. 이 방법을 통해 사용자 계정 원격 관리를 사용할 수 있습니다. 이 옵션을 선택하면 모든 사용자 계정이 외부 LDAP 서버에 원격으로 존재합니다.
   - **로컬 사용자 먼저 허용 후 LDAP 사용자 허용**. 로컬 인증 서버가 인증을 먼저 수행합니다. 실패하면 외부 LDAP 서버가 인증을 수행합니다.

- **LDAP 사용자 먼저 허용 후 로컬 사용자 허용**. 외부 LDAP 서버가 인증을 먼저 수행합니다. 실패하면 로컬 인증 서버가 인증을 수행합니다.

2. 다음과 같이 보안 LDAP를 사용 또는 사용 안 함으로 설정할지 선택하십시오.
   - **보안 LDAP 사용**. XClarity Administrator는 LDAPS 프로토콜을 사용하여 외부 인증 서버에 안전하게 연결합니다. 이 옵션을 선택한 경우 보안 LDAP 지원을 사용하기 위해 신뢰할 수 있는 인증서도 구성해야 합니다.
   - **보안 LDAP 사용 안 함**. XClarity Administrator는 비보안 프로토콜을 사용하여 외부 인증 서버에 연결합니다. 이 설정을 사용하면 보안 공격에 대한 하드웨어의 취약성이 높아질 수 있습니다.
3. 이러한 서버 선택 방법 중 하나를 선택하십시오.
   - **미리 구성된 서버 사용**. XClarity Administrator는 지정된 IP 주소 및 포트를 사용하여 외부 인증 서버를 검색합니다.

     이 옵션을 선택한 경우 최대 4개의 미리 구성된 서버 IP 주소 및 포트를 지정하십시오. LDAP 클라이언트는 첫 번째 서버 주소를 사용하여 인증을 시도합니다. 인증에 실패하면 LDAP 클라이언트가 다음 서버 IP 주소를 사용하여 인증을 시도합니다.

     엔트리에 대한 포트 번호가 3268 또는 3269로 명확하게 설정되지 *않으면* 해당 엔트리는 도메인 컨트롤러를 식별하는 것으로 간주됩니다.

     포트 번호가 3268 또는 3269로 설정되면 해당 엔트리는 글로벌 카탈로그를 식별하는 것으로 간주됩니다. LDAP 클라이언트는 처음으로 구성되는 서버 IP 주소에 대한 도메인 컨트롤러를 사용하여 인증을 시도합니다. 이것이 실패하는 경우 LDAP 클라이언트는 다음 서버 IP 주소에 대한 도메인 컨트롤러를 사용하여 인증을 시도합니다.

     중요: 글로벌 카탈로그를 지정하는 경우에도 하나 이상의 도메인 컨트롤러를 지정해야 합니다. 글로벌 카탈로그만 지정하는 것이 성공한 것으로 보이지만 유효한 구성이 아닙니다.

     암호 모드가 NIST-800-131A로 설정되면, LDAP 서버가 XClarity Administrator의 LDAP 클라이언트로 TLS(Transport Layer Security) 버전 1.2 연결을 설정할 수 없는 경우에는 보안 포트(예, 기본 포트 636에서 LDAPS 사용)를 사용하여 XClarity Administrator를 외부 LDAP 서버에 연결할 수 없습니다.
   - **DNS를 사용하여 LDAP 서버 찾기**. XClarity Administrator는 지정된 도메인 이름 또는 포리스트 이름을 사용하여 외부 인증 서버를 동적으로 검색합니다. 도메인 이름 및 포리스트 이름은 도메인 컨트롤러를 확보하는 데 사용되고 포리스트 이름은 글로벌 카탈로그 서버의 목록을 확보하는 데 사용됩니다.

     주의: DNS를 사용하여 LDAP 서버를 찾는 경우 외부 인증 서버에 인증하는 데 사용할 사용자 계정이 지정된 도메인 컨트롤러에서 호스팅되어야 합니다. 사용자 계정이 하위 도메인 컨트롤러에서 호스팅된 경우 서비스 요청 목록에 하위 도메인 컨트롤러를 포함시키십시오.
4. 이러한 바인딩 방법 중 하나를 선택하십시오.
   - **구성된 자격 증명**. 이 바인딩 방법을 사용하여 클라이언트 이름 및 암호로 XClarity Administrator를 외부 인증 서버에 바인딩하십시오. 바인딩에도 실패하면 인증 프로세스가 실패합니다.

     클라이언트 이름은 고유 이름, AMAccountName, NetBIOS 이름 또는 UserPrincipalName 등 LDAP 서버가 지원하는 모든 이름이 될 수 있습니다. 클라이언트 이름은 최소 읽기 전용 권한이 있는 도메인 내의 사용자 계정이어야 합니다. 예를 들어, 다음과 같습니다.

     ```
     cn=username,cn=users,dc=example,dc=com
     domain\username
     username@domain.com
     username
     ```

주의: 외부 인증 서버에서 클라이언트 암호를 변경하는 경우 XClarity Administrator에서 새 암호도 업데이트해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 XClarity Administrator에 로그인할 수 없음의 내용을 참조하십시오.

- **로그인 자격 증명**. 이 바인딩 방법을 사용하여 Active Directory 또는 OpenLDAP 사용자 이름과 암호로 XClarity Administrator를 외부 인증 서버에 바인딩하십시오.

  사용자가 지정하는 사용자 ID 및 암호는 인증 서버 연결을 테스트하는 데에만 사용됩니다. 성공하는 경우 LDAP 클라이언트 설정은 저장되지만, 사용자가 지정한 테스트 로그인 자격 증명은 저장되지 않습니다. 모든 향후 바인딩은 사용자가 XClarity Administrator에 로그인하는 데 사용한 사용자 이름 및 암호를 사용합니다.

  참고:

  - 완전한 사용자 ID(예, `administrator@domain.com` 또는 `DOMAIN\admin`)를 사용하여 XClarity Administrator에 로그인해야 합니다.
  - 바인딩 방법에 대해 완전한 테스트 클라이언트 이름을 사용해야 합니다.

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

5. 루트 DN 필드에서 여러 개의 도메인이 있는 환경의 경우 특히 루트 고유 이름을 지정하지 않는 것이 좋습니다. 이 필드가 공백인 경우 XClarity Administrator는 이름 지정 컨텍스트에 대해 외부 인증 서버를 쿼리합니다. DNS를 사용하여 외부 인증 서버를 검색하는 경우 또는 여러 서버를 지정하는 경우(예, `dc=example,dc=com`) 선택적으로 LDAP 디렉토리 트리에서 가장 높은 엔트리를 지정할 수 있습니다. 이 경우 지정된 루트 고유 이름을 검색 기반으로 사용하여 검색을 시작합니다.
6. 사용자 이름을 검색하는 데 사용할 특성을 지정하십시오.

   바인딩 방법이 **구성된 자격 증명**으로 설정된 경우 LDAP 서버에 대한 초기 바인딩 후 사용자의 DN, 로그인 권한 및 그룹 멤버십 등 사용자에 대한 특정 정보를 검색하는 검색 요청을 합니다. 이 검색 요청에서는 해당 서버에서 사용자 ID를 나타내는 특성 이름을 지정해야 합니다. 이 특성 이름이 이 필드에서 구성됩니다. 이 필드를 공백으로 둔 경우 기본값은 cn입니다.
7. 사용자가 속한 그룹을 식별하는 데 사용되는 특성 이름을 지정하십시오. 이 필드를 공백으로 둔 경우 필터의 특성 이름 기본값이 memberOf가 됩니다.
8. LDAP 서버가 구성하는 그룹 이름을 식별하는 데 사용되는 속성 이름을 지정하십시오. 이 필드를 공백으로 둔 경우 기본값은 uid입니다.

d. **적용**을 클릭하십시오.

XClarity Administrator는 일반 오류를 감지하기 위해 구성 테스트를 시도합니다. 테스트에 실패하면 오류의 소스를 표시하는 오류 메시지가 표시됩니다. 테스트에 성공하고 지정된 서버 연결이 성공적으로 완료되는 경우에도 다음과 같은 경우 사용자 인증에 실패할 수 있습니다.

- lxc-recovery 권한이 있는 로컬 사용자는 존재하지 않습니다.
- 루트 고유 이름이 올바르지 않습니다.
- 사용자가 XClarity Administrator 인증 서버의 역할 그룹 이름과 일치하는 외부 인증 서버에서 하나 이상의 그룹 멤버가 아닙니다. XClarity Administrator는 루트 DN이 올바른지 감지할 수 없습니다. 하지만 사용자가 하나 이상의 그룹 멤버인지 감지할 수 있습니다. 사용자가 하나 이상의 그룹 멤버가 아닌 경우 사용자가 XClarity Administrator에 로그인을 시도하면 오류 메시지가 표시됩니다. 외부 인증 서버 문제 해결에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 연결 문제의 내용을 참조하십시오.

단계 4. XClarity Administrator에 액세스할 수 있는 외부 사용자 계정을 만드십시오.

a. 외부 인증 서버에서 사용자 계정을 만드십시오. 지시사항은 Active Directory 또는 OpenLDAP 설명서를 참조하십시오.

b. 미리 정의되고 권한 부여된 그룹의 이름으로 Active Directory 또는 OpenLDAP 글로벌 그룹을 만드십시오. 그룹은 LDAP 클라이언트에 정의된 루트 고유 이름의 컨텍스트 내에 존재해야 합니다.

c. Active Directory 또는 OpenLDAP 사용자를 이전에 만든 보안 그룹의 멤버로 추가하십시오.

d. Active Directory 또는 OpenLDAP 사용자 이름을 사용하여 XClarity Administrator에 로그인하십시오.

e. **옵션:** 추가 그룹을 정의하고 만드십시오. 이러한 그룹을 권한 부여하고 사용자 및 그룹 페이지에서 역할을 할당할 수 있습니다.

f. 보안 LDAP를 사용하는 경우, 외부 LDAP 서버에 신뢰할 수 있는 인증서를 가져오십시오(사용자 지정되고 외부 서명된 서버 인증서 설치 참조).

결과

XClarity Administrator는 LDAP 서버 연결을 유효성 검증합니다. 유효성 검증을 통과하면 XClarity Administrator, CMM 및 관리 컨트롤러에 로그인할 때 외부 인증 서버에서 사용자 인증이 발생합니다.

유효성 검증에 실패하면 인증 모드가 **로컬 사용자의 로그온 허용** 설정으로 다시 자동 변경되고 실패의 원인을 설명하는 메시지가 표시됩니다.

참고: 올바른 역할 그룹은 XClarity Administrator에서 구성되어야 하며 사용자 계정을 Active Directory 서버의 역할 그룹 중 하나의 멤버로 정의해야 합니다. 그렇지 않으면 사용자 인증에 실패합니다.

외부 SAML ID 공급자 설정

Security Assertion Markup Language(SAML) 2.0 ID 공급자를 사용하도록 선택하여 Lenovo XClarity Administrator에 대한 인증 및 권한 부여를 수행할 수 있습니다.

시작하기 전에

ID 공급자를 설정하기 전에 XClarity Administrator 초기 설치가 완료되어야 합니다.

ID 공급자는 Microsoft Active Directory Federated Service(AD FS)여야 하고 관리 네트워크, 데이터 네트워크 또는 두 가지에 모두 연결할 수 있습니다. 인증은 웹 브라우저를 통해 수행되므로 웹 브라우저가 XClarity Administrator 및 SAML 서버에 액세스할 수 있어야 합니다.

다음 URL을 사용하여 IDP 메타 데이터를 다운로드할 수 있습니다:
`https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`,
여기서 *<ADFS_IP_Address>*는 AD FS의 IP 주소입니다(예:
https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

외부 인증 서버에 정의된 그룹과 일치하도록 위치 인증 서버에서 역할 그룹을 작성하거나 이름을 바꾸어야 합니다.

SAML ID 공급자를 설정하려면, **lxc_admin** 또는 **lxc_supervisor** 그룹의 멤버인 사용자로 로그인해야 합니다.

이 작업 정보

XClarity Administrator는 사용자를 인증하고 권한 부여하는 데 Security Assertion Markup Language 2.0 ID 공급자 사용을 지원합니다. 사용자 이름과 암호 입력 뿐 아니라 PIN 코드 입력, 스마트 카드 읽기 및 클라이언트 인증서를 사용한 인증과 같이 사용자 ID를 유효성 검증하기 위한 추가 기준이 필요하도록 ID 공급자를 설정할 수 있습니다.

XClarity Administrator가 ID 공급자를 사용하도록 설정되면 인증을 위해 XClarity Administrator 웹 인터페이스로부터의 대화형 로그인 요청이 ID 공급자로 리디렉션됩니다. 사용자가 인증되면 웹 브라우저가 다시 XClarity Administrator로 리디렉션됩니다.

참고: ID 공급자를 사용하는 경우 웹 브라우저에서 XClarity Administrator 로그인 페이지(예: `https://<ip_address>/ui/login.htm`)를 열어서 ID 공급자를 우회하는 방식으로 로컬 또는 외부 LDAP 인증 서버를 사용하여 XClarity Administrator에 로그인할 수 있습니다.

ID 공급자 프로필을 사용하도록 XClarity Administrator를 구성한 경우XClarity Administrator 웹 인터페이스에서 사용자 관리 페이지를 사용할 수 없습니다. 로컬 사용자 계정이 PowerShell 및 REST API 인증을 위해서는 관리되는 섀시나 서버에 직접 로그인해야 합니다(해당 장치에서 Encapsulation을 사용하는 경우는 제외).

절차

외부 SAML ID 공급자(AD FS)를 설정하려면 다음 단계를 완료하십시오.

단계 1. ID 공급자가 사용 불가능한 경우 XClarity Administrator에 로그인하는 데 사용할 수 있는 복구 사용자 계정을 작성하십시오(사용자 계정 관리 참조).

단계 2. ID 공급자에서 ID 공급자(IDP) 메타데이터를 검색하여 이 파일을 XClarity Administrator 호스트에 저장하십시오.

단계 3. XClarity Administrator SAML 클라이언트를 구성하십시오.

a. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

b. 사용자 및 그룹 섹션에서 SAML **설정**을 클릭하여 SAML 설정 대화 상자를 표시하십시오.

c. SAML 설정 페이지에 필드를 지정하십시오.

1. 항목 ID가 XClarity Administrator 관리 서버의 IP 주소와 일치하는지 확인하십시오.
2. 생성되는 메타데이터가 디지털 서명되는지 여부를 선택하십시오.

3. 인증 요청이 서명되는지 여부를 선택하십시오.
4. 인증 응답이 서명되어야 하는지 여부를 택하십시오.
5. 원격 ID 공급자로 보내는 아티팩트-해결 요청이 서명되어야 하는지 여부를 선택하십시오.
6. ID 공급자 에서 생성되고 단계 2 3 23페이지단계에서 검색된 SAML ID 공급자(IDP) 메타데이터를 IDP **메타데이터** 필드에 붙여넣으십시오.

d. **적용**을 클릭하여 변경사항을 적용하고 SP 메타데이터 필드에서 텍스트를 업데이트하십시오.

주의: 이 때 SAML **사용**을 선택하지 *마십시오*. 나중에 SAML을 사용으로 설정하여 XClarity Administrator를 다시 시작할 수 있습니다.

e. SP **메타데이터** 필드의 데이터를 복사하여 파일에 붙여넣고 파일을 .XML 확장자(예, sp_metadata.xml)로 저장하십시오. 이 파일을 AD FS 호스트에 복사하십시오.

단계 4. AD FS를 구성하십시오.

a. AD FS 관리 도구를 여십시오.
b. ADFS ➡ **신뢰 당사자 트러스트**를 클릭하십시오.
c. **신뢰 당사자 트러스트**를 마우스 오른쪽 단추로 클릭한 후 **신뢰 당사자 트러스트 추가**를 클릭하여 마법사를 표시하십시오.
d. **시작**을 클릭하십시오.
e. 데이터 소스 선택 페이지에서 **파일에서 신뢰 당사자에 대한 데이터 가져오기**를 선택한 후 3e 단계에서 저장된 SP 메타데이터를 선택하십시오.
f. 표시 이름을 입력하십시오.
g. 모든 페이지에서 **다음**을 클릭하여 기본값을 선택하십시오.
h. **완료**를 클릭하여 클레임 규칙 페이지를 표시하십시오.
i. LDAP **속성을 클레임으로 보내기**를 기본값으로 그대로 두고 **다음**을 클릭하십시오.
j. 클레임 규칙 이름을 입력하십시오.
k. 속성 저장소에 Active Directory를 선택하십시오.
l. 매핑을 추가하십시오. 왼쪽에서 SAM-Account-Name을 선택하고, 오른쪽에서 발신 클레임 유형에 **이름 ID**를 선택하십시오.
m. 다른 매핑을 추가하십시오. 왼쪽에서 Token-Groups-Unqualified Names를 선택하고, 오른쪽에서 출력 클레임 유형에 **그룹**을 선택하십시오.
n. **확인**을 누르십시오.
o. **신뢰 당사자 트러스트** 목록에서 작성한 트러스트를 찾으십시오.
p. 트러스트를 마우스 오른쪽 단추로 클릭하고 **속성 선택**을 클릭하십시오. 트러스트 속성 대화 상자가 표시됩니다.
q. **고급** 탭을 클릭하여 보안 해시 알고리즘으로 SHA-1을 선택하십시오.

단계 5. AD FS에서 서버 인증서를 저장하십시오.

a. AD FS **콘솔** ➡ **서비스** ➡ **인증서**를 클릭하십시
b. 토큰 서명에서 **인증서**를 선택하십시오.
c. 인증서를 마우스 오른쪽 단추로 클릭하고 **인증서 보기**를 클릭하십시오.
d. **세부 정보** 탭을 클릭하십시오.
e. **파일에 복사**를 클릭하여 인증서를 DER encoded binary X.509 (.CER) 파일로 저장하십시오.
f. 서버 인증서 .CER 파일을 XClarity Administrator 호스트에 복사하십시오.

단계 6. AD FS 신뢰할 수 있는 인증서를 XClarity Administrator 웹 인터페이스로 가져오십시오.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오.
b. 인증서 관리 섹션의 **신뢰할 수 있는 인증서**를 클릭하십시오.
c. **만들기** 아이콘()을 클릭하여 인증서를 추가하십시오.
d. 이전 단계에서 저장된 서버 인증서 .CER 파일을 선택하십시오.
e. **만들기**를 클릭하십시오.

단계 7. 사용자 및 그룹 섹션에서 SAML **설정**을 클릭하여 SAML 설정 대화 상자를 표시하십시오.

단계 8. SAML **사용**을 선택하여 외부 ID 공급자를 사용하는 사용자 계정 관리를 사용으로 설정하십시오. 이 옵션을 선택하면 모든 사용자 계정이 ID 공급자에 원격으로 존재하게 됩니다.

단계 9. **적용**를 클릭하여 변경사항을 적용하고 관리 서버를 다시 시작하십시오.

단계 10. XClarity Administrator가 다시 시작하기까지 몇 분 기다리십시오.

주의: 이 프로세스 중에는 가상 어플라이언스를 수동으로 다시 시작하지 마십시오.

단계 11. 웹 브라우저를 닫고 다시 여십시오.

단계 12. ID 공급자에서 XClarity Administrator 웹 인터페이스에 로그인하십시오.

결과

XClarity Administrator는 일반 오류를 감지하기 위해 구성 테스트를 시도합니다. 테스트에 실패하면 오류의 소스를 표시하는 오류 메시지가 표시됩니다.

XClarity Administrator가 ID 공급자 연결을 유효성 검증합니다. 유효성 검증이 패스되면 XClarity Administrator에 로그인할 때 ID 공급자에서 사용자 인증이 발생합니다.

외부 ID 관리 시스템 설정

*ID 관리 시스템*은 XClarity Administrator 및 XClarity Controller 자격 증명을 저장하기 위해 Lenovo XClarity Administrator에서 선택적으로 사용할 수 있는 외부 암호 저장소입니다. ID 관리 시스템이 XClarity Administrator에 추가되면 XClarity Administrator이(가) 인증 서버 대신 ID 관리 시스템에서 암호를 검색합니다.

이 작업 정보

XClarity Administrator에서는 다음 ID 관리 시스템을 지원합니다.
- CyberArk

CyberArk ID 관리 시스템 설정

CyberArk는 XClarity Administrator 및 Lenovo XClarity Controller 자격 증명을 저장하기 위해 Lenovo XClarity Administrator에서 선택적으로 사용할 수 있는 외부 암호 저장소입니다. 계정 암호가 CyberArk에 저장되면 CyberArk에서 암호를 관리합니다.

이 작업 정보

XClarity Administrator을(를) 사용하면 타사 서비스인 CyberArk에서 제공하는 ID 관리 시스템에 XCC 암호를 저장할 수 있습니다. Lenovo는 CyberArk 서비스에 대한 책임을 지지 않으며, 사용자가 CyberArk에 직접 연락해야 합니다.

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.

절차

CyberArk를 사용하도록 XClarity Administrator을(를) 구성하려면 다음 단계를 완료하십시오.

단계 1. CyberArk를 구성합니다.

1. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오.
2. ID 관리 섹션 아래에서 **CyberArk**를 클릭합니다.
3. 도구 모음에서 **CyberArk 서버 세부 정보 편집**을 클릭합니다.
4. CyberArk 호스트 이름 또는 IP 주소를 지정하고 포트 번호를 지정합니다.
5. **적용**을 클릭하십시오.

단계 2. XClarity Administrator 상호 인증 인증서를 CyberArk로 가져옵니다.

1. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오.
2. 인증서 관리 섹션에서 **서버 인증서**를 클릭합니다.
3. **클라이언트 인증서** 탭을 클릭합니다.
4. 서버 유형으로 **CyberArk**를 선택합니다.
5. **인증서 다시 생성**을 클릭하여 CyberArk에 대한 새로운 TLS 상호 인증 인증서를 생성합니다.

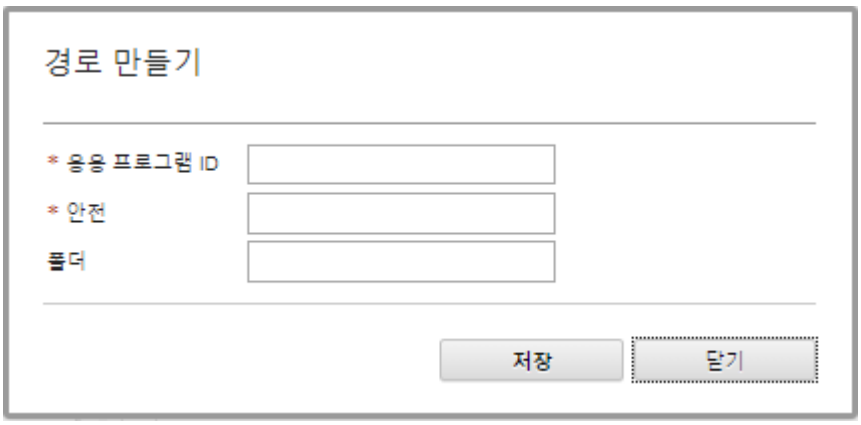
   주의: XClarity Administrator 및 CyberArk 사이의 연결을 설정한 후 CyberArk에 대한 TLS 상호 인증 인증서를 다시 생성하면 CyberArk에 새 인증서를 가져올 때까지 연결이 끊어집니다.
6. **인증서 다운로드**를 클릭한 다음 **DER로 저장** 또는 **PEM으로 저장**을 클릭하여 인증서를 로컬 시스템에 파일로 저장합니다.
7. 다운로드한 인증서를 CyberArk로 가져옵니다.

단계 3. CyberArk 루트 CA 인증서를 XClarity Administrator(으)로 가져옵니다.

1. CyberArk에서 루트 CA 인증서를 다운로드합니다.
2. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오.
3. 인증서 관리 섹션의 **신뢰할 수 있는 인증서**를 클릭하십시오.
4. **만들기** 아이콘( )을 클릭하여 인증서를 추가하십시오.
5. 파일을 찾아보거나 PEM 형식 인증서 텍스트를 붙여넣으십시오.
6. **만들기**를 클릭하십시오.

단계 4. CyberArk에서 온보딩된 사용자 계정의 위치를 식별하는 경로를 추가합니다.

1. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오.
2. ID 관리 섹션 아래에서 **CyberArk**를 클릭합니다.
3. **경로** 탭을 클릭합니다.
4. **만들기** 아이콘( )을 클릭하여 CyberArk 경로 만들기 대화 상자를 표시합니다.



5. CyberArk에 사용자 계정을 저장할 응용 프로그램 ID, 보관함 및 폴더를 선택적으로 지정합니다.

   응용 프로그램 ID와 보관함을 지정하고 선택적으로 폴더를 지정하면 XClarity Administrator이(가) 지정된 위치에서 사용자 계정을 찾습니다.

   응용 프로그램 ID와 보관함이 아닌 필드 조합을 지정하는 경우(예: 응용 프로그램 ID만 지정, 보관함 및 폴더만 지정 또는 응용 프로그램 ID 및 폴더만 지정하는 경우)XClarity Administrator에서 지정된 값을 사용하여 경로를 필터링합니다.
6. **적용**을 클릭하십시오.

완료한 후에

- **편집** 아이콘( )을 클릭하여 선택된 CyberArk 경로를 수정합니다.
- **삭제** 아이콘( )을 클릭하여 선택된 CyberArk 경로를 삭제합니다.

Lenovo XClarity Administrator가 사용하는 인증 방법의 유형 판별

보안 페이지의 LDAP **클라이언트** 및 SAML **설정** 탭에서 현재 사용하고 있는 인증 방법의 유형을 판별할 수 있습니다.

이 작업 정보

*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.

절차

관리 소프트웨어가 사용하고 있는 인증 서버의 유형을 판별하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 LDAP **클라이언트**를 클릭하여 LDAP 클라이언트 설정 대화 상자를 표시하십시오.

선택한 사용자 인증 방법을 확인하십시오.

- **로컬 사용자의 로그온 허용**. 로컬 인증을 사용하여 인증이 수행됩니다. 이 옵션을 선택하면 모든 사용자 계정이 관리 노드의 로컬 인증 서버에 존재합니다.
- LDAP **사용자의 로그온 허용**. 외부 LDAP 서버가 인증을 수행합니다. 이 방법을 통해 사용자 계정 원격 관리를 사용할 수 있습니다. 이 옵션을 선택하면 모든 사용자 계정이 외부 LDAP 서버에 원격으로 존재합니다.
- **로컬 사용자 먼저 허용 후** LDAP **사용자 허용**. 로컬 인증 서버가 인증을 먼저 수행합니다. 실패하면 외부 LDAP 서버가 인증을 수행합니다.
- LDAP **사용자 먼저 허용 후 로컬 사용자 허용**. 외부 LDAP 서버가 인증을 먼저 수행합니다. 실패하면 로컬 인증 서버가 인증을 수행합니다.

단계 3. 사용자 및 그룹 섹션에서 SAML **설정**을 클릭하여 SAML 설정 페이지를 표시하십시오.

SAML **사용**을 선택한 경우 ID 공급자를 사용합니다.

외부 LDAP 서버 오류 후 Lenovo XClarity Administrator 액세스

외부 LDAP 인증 서버를 사용하는 중이고, 서버가 실패하거나 사용 불가능한 경우 관리 노드의 로컬 인증 서버를 사용하여 다음 절차를 따라 Lenovo XClarity Administrator 웹 인터페이스에 대한 액세스를 복구하십시오.

절차

LDAP 클라이언트 설정을 변경하려면 다음 단계를 완료하십시오.

단계 1. lxc-recovery 권한이 있는 사용자 계정을 사용하여 XClarity Administrator 웹 인터페이스에 로그인합니다. 클라이언트 도메인 이름에 대한 자세한 정보는 외부 LDAP 인증 서버 설정의 내용을 참고하십시오.

단계 2. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 3. 사용자 및 그룹 섹션에서 LDAP **클라이언트**를 클릭하여 LDAP 클라이언트 대화 상자를 표시하십시오.

단계 4. 사용자 인증 방법에 대해 **로컬 사용자의 로그온 허용**을 선택하여 사용자 계정의 로컬 관리를 사용하십시오. 이 옵션을 선택하면 모든 사용자 계정이 관리 서버에 로컬로 존재합니다.

단계 5. **적용**을 클릭하십시오.

결과

이제 로컬 인증 서버에서 사용자 계정을 사용하여 XClarity Administrator 관리 서버에 액세스할 수 있습니다. 외부 인증 서버가 복원되고 관리 서버에서 사용 가능하면 LDAP 클라이언트 설정을 다시 외부 인증 서버로 변경할 수 있습니다.

외부 SAML ID 공급자 실패 후 Lenovo XClarity Administrator에 액세스

외부 SAML ID 공급자를 사용하는 중이고, 서버가 실패하거나 사용 불가능한 경우 XClarity Administrator 로컬 인증 서버를 사용하여 다음 절차를 따라 Lenovo XClarity Administrator 웹 인터페이스에 대한 액세스를 복구하십시오.

절차

SAML 클라이언트 설정을 변경하려면 다음 단계를 완료하십시오.

단계 1. 웹 브라우저에서 XClarity Administrator 로그인 페이지(예: https://*<ip_address>*/ui/login.html)를 여십시오.

단계 2. ID 공급자 설정 시 작성한 로컬 복구 사용자 계정을 사용하여 XClarity Administrator 웹 인터페이스에 로그인하십시오.

단계 3. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 4. 사용자 및 그룹 섹션에서 SAML **설정**을 클릭하여 SAML 설정 대화 상자를 표시하십시오.

단계 5. SAML **사용**을 지워서 SAML ID 공급자를 사용 안 함으로 설정하십시오. 이 옵션을 지우면 인증에 로컬 인증 서버 또는 외부 LDAP 서버(구성된 경우)가 사용됩니다.

단계 6. **적용**을 클릭하십시오.

결과

이제 로컬 인증 서버에서 사용자 계정을 사용하여 XClarity Administrator 관리 서버에 액세스할 수 있습니다. 외부 ID 공급자가 복원되어 관리 서버에서 사용 가능하면 인증 방법을 ID 공급자로 변경할 수 있습니다.

사용자 계정 관리

*사용자 계정*을 사용하여 Lenovo XClarity Administrator 및 XClarity Administrator에서 관리하는 모든 섀시와 서버에 로그인하고 관리합니다. XClarity Administrator 사용자 계정은 인증과 권한 부여라는 두 개의 상호 의존적인 프로세스를 거칩니다.

이 작업 정보

*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.

참고: SYSMGR_* 및 SYSRDR_* 사용자 계정(여기서 *는 문자 A-Z 및 0-9에서 생성된 임의로 선택된 접미사)은 XClarity Administrator에 의해 생성되고 서비스 사용자 계정으로 사용되며 관리되는 인증, OS 배포 및 펌웨어 업데이트와 같은 기능에 사용됩니다. SYSMGR_* 및 SYSRDR_* 암호는 XClarity Administrator이(가) 부팅될 때와 암호 만료 기간이 얼마 남지 않았을 때 교체됩니다.

사용자 만들기

사용자 계정을 사용하여 리소스에 대한 권한과 액세스를 관리합니다.

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

XClarity Administrator에 사용자를 추가하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 **로컬 사용자**를 클릭하여 사용자 관리 페이지를 표시하십시오.

단계 3. **만들기** 아이콘( )을 클릭하여 사용자를 작성하십시오. 새 사용자 만들기 대화 상자가 표시됩니다.

단계 4. 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 정의 역할 그룹 작성 방법에 대해서는 사용자 지정 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 5. **만들기**를 클릭하십시오.

완료한 후에

사용자 계정이 사용자 관리 테이블에 표시됩니다. 이 테이블은 각 사용자 계정의 연결된 역할 그룹과 계정 상태를 표시합니다.

사용자 계정을 작성하면 선택한 사용자 계정에 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘( )을 클릭하여 사용자 계정의 사용자 이름, 설명 및 역할을 수정합니다.

- **삭제** 아이콘()을 클릭하여 사용자 계정을 삭제합니다.
- 사용자 계정의 암호를 재설정합니다(사용자 암호 재설정 참조).
- 계정을 잠금 해제합니다(사용자 잠금 해제 참조).
- 사용자 계정을 사용 또는 사용 안 함으로 설정합니다(사용자 사용 또는 사용 안 함 참조).

사용자 사용 또는 사용 안 함

인증 서버에서 로컬 사용자 계정을 사용 또는 사용 안 함 설정을 변경할 수 있습니다.

절차

사용자 계정을 사용 또는 사용 안 함으로 설정하려면 다음 단계를 완료하십시오.

- 로컬 인증 서버를 사용하는 경우:
  1. Lenovo XClarity Administrator 제목 표시줄에서 **관리** → **보안**을 클릭하십시오.
  2. 사용자 및 그룹 섹션에서 **로컬 사용자**를 클릭하여 사용자 관리 페이지를 표시하십시오.
  3. 사용자 계정을 선택하십시오.
  4. 사용자 계정을 사용으로 설정한 경우 **모든 작업** → **선택한 계정 사용 안 함**을 클릭하여 사용자를 사용 안 함으로 설정하십시오. 테이블에서 계정 상태가 Disabled로 변경됩니다.
  5. 사용자 계정을 사용 안 함으로 설정한 경우 **모든 작업** → **선택한 계정 사용**을 클릭하여 사용자를 사용으로 설정하십시오. 테이블에서 계정 상태가 Enabled로 변경됩니다.
- 외부 LDAP 서버를 사용하는 경우 Microsoft Active Directory에서 사용자 계정을 사용 또는 사용 안 함으로 설정하십시오.
- 외부 SAML ID 공급자을 사용하는 경우 ID 공급자에서 사용자 계정을 사용 또는 사용 안 함으로 설정하십시오.

활성 사용자 로그오프

Lenovo XClarity Administrator에서 활성 사용자를 로그오프(종료)할 수 있습니다.

lxc-supervisor 또는 **lxc-security-admin** 권한이 있는 사용자 계정으로 XClarity Administrator에 로그온해야 합니다.

절차

활성 사용자를 로그오프하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 제목 표시줄에서 **관리** → **보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 **활성 세션**를 클릭하여 활성 세션 관리 페이지를 표시하십시오.

단계 3. 하나 이상의 사용자 계정을 선택하십시오.

단계 4. **사용자 로그오프**를 클릭하십시오.

사용자 계정 암호 변경

사용자 계정의 암호를 변경할 수 있습니다.

절차

암호를 변경하려면 다음 단계를 완료하십시오.

- 로컬 인증 서버를 사용하는 경우:
  1. Lenovo XClarity Administrator 제목 표시줄에서 사용자 작업 메뉴(

)를 클릭한 후 **암호 변경**을 클릭하십시오. 암호 변경 대화 상자가 표시됩니다.

2. 현재 암호를 입력하십시오.
3. 새 암호와 새 암호 확인을 입력하십시오. 암호 규칙은 현재 계정 보안 설정을 기반으로 합니다.
4. **변경**을 클릭하십시오.

- 외부 인증 서버를 사용하는 경우 Microsoft Active Directory에서 암호를 변경하십시오.

  주의: XClarity Administrator 를 외부 인증 서버와 바인딩하는 데 사용하는 클라이언트 계정의 새 암호로 Microsoft Active Directory를 업데이트한 경우, XClarity Administrator 웹 인터페이스에서도 새 암호를 업데이트해야 합니다(외부 LDAP 인증 서버 설정 참조).
- 외부 SAML ID 공급자를 사용하는 경우 ID 공급자에서 암호를 변경하십시오.

사용자 암호 재설정

사용자 계정의 암호를 재설정할 수 있습니다.

절차

암호를 재설정하려면 다음 단계를 완료하십시오.

- 로컬 인증 서버를 사용하는 경우 Lenovo XClarity Administrator 웹 인터페이스에서 암호를 재설정하십시오.
  1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.
  2. 사용자 및 그룹 섹션에서 **로컬 사용자**를 클릭하여 사용자 관리 페이지를 표시하십시오.
  3. 테이블에서 사용자 계정을 선택하십시오.
  4. 사용자 계정을 사용으로 설정한 경우 **모든 작업 → 선택한 사용자의 암호 재설정**을 클릭하십시오. 암호 재설정 대화 상자가 표시됩니다.
     a. 새 암호와 새 암호 확인을 입력하십시오. 암호 규칙은 현재 계정 보안 설정을 기반으로 합니다.
     b. (옵션) 사용자가 XClarity Administrator에 처음 로그인할 때 암호를 강제로 변경하도록 하려면 **처음 액세스할 때 변경**을 Yes로 설정하십시오.
     c. **재설정**을 클릭하십시오.
- 외부 LDAP 서버를 사용하는 경우 Microsoft Active Directory에서 암호를 재설정하십시오.

- 외부 SAML ID 공급자를 사용하는 경우 ID 공급자에서 암호를 재설정하십시오.
- 다른 감독자 계정을 사용하여 XClarity Administrator에 로그인할 수 없거나 다른 감독자 계정이 없는 경우 구성 파일이 포함된 ISO 이미지를 새 암호에 탑재하여 복구 또는 감독자 권한이 있는 로컬 사용자의 암호를 재설정할 수 있습니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 로컬 복구 또는 감독자 사용자의 암호를 잊어버림의 내용을 참조하십시오.

사용자 잠금 해제

Lenovo XClarity Administrator에서 잠긴 사용자 계정을 잠금 해제할 수 있습니다. 사용자가 유효하지 않은 로그인을 너무 많이 시도한 경우 사용자 계정이 일시적으로 잠길 수 있습니다.

이 작업 정보

사용자 계정 보안 설정은 잠긴 사용자로 다시 로그인을 시도할 수 있게 되기까지 경과해야 하는 총 시간을 제어합니다. **최대 로그인 실패 횟수 이후 잠금 기간** 설정을 0으로 설정하면 관리자가 명시적으로 잠금 해제할 때까지 사용자 계정이 잠긴 상태로 유지됩니다. 최대 로그인 실패 횟수의 잠금 기간에 대한 자세한 정보는 사용자 계정 보안 설정 변경의 내용을 참조하십시오.

사용자 계정을 영구적으로 사용 안 함 또는 사용으로 설정할 수도 있습니다. 자세한 정보는 사용자 사용 또는 사용 안 함의 내용을 참조하십시오.

참고: 사용자 계정을 잠금 해제하려면 감독자 권한이 있어야 합니다.

팁: XClarity Administrator를 사용하면 로컬 인증 서버를 사용하여 관리되는 사용자 계정을 잠금 해제할 수 있습니다. XClarity Administrator를 사용하여 외부 인증 서버의 사용자 계정을 잠금 해제할 수는 없습니다.

절차

사용자 계정을 잠금 해제하려면 다음 단계를 완료하십시오.

- 로컬 인증 서버를 사용하는 경우:
  1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.
  2. 사용자 및 그룹 섹션에서 **로컬 사용자**를 클릭하여 사용자 관리 페이지를 표시하십시오.
  3. 테이블에서 사용자 계정을 선택하십시오.
  4. **모든 작업 → 선택한 사용자 계정 잠금 해제**를 클릭하십시오.
- 외부 LDAP 서버를 사용하는 경우 Microsoft Active Directory에서 사용자 계정을 잠금 해제하십시오.
- 외부 SAML ID 공급자를 사용하는 경우 ID 공급자에서 사용자 계정을 잠금 해제하십시오.

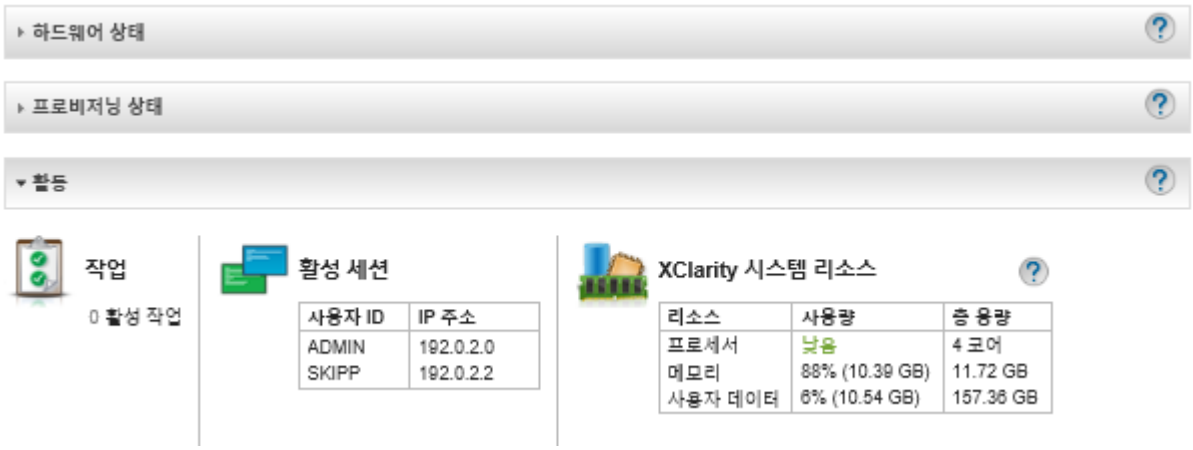
활성 사용자 모니터링

대시보드 페이지에서 Lenovo XClarity Administrator 웹 인터페이스에 로그인한 사용자를 판별할 수 있습니다.

절차

- XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하여 활성 사용자 및 해당 IP 주소 목록을 찾을 수 있습니다.

  활성 사용자 세션은 활동 섹션에 나열되어 있습니다.



- XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭한 후 **활성 세션**을 클릭하여 모든 활성 사용자(현재 사용자 외) 및 해당 IP 주소 목록을 찾을 수 있습니다.

  참고: 특정 시간 이상 비활성 상태인 사용자 세션이 자동으로 로그 아웃됩니다. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**과 계정 보안 설정을 차례로 클릭한 다음 **웹 비활성 세션 시간 제한** 값을 조정하여 비활성 기간을 설정할 수 있습니다. 변경이 활성 사용자 세션 영향을 주지 않습니다. 설정이 변경된 후 시작하는 사용자 세션에만 영향을 줍니다.

저장된 자격 증명 관리

*저장된 자격 증명*은 로컬 인증을 사용하여 Lenovo XClarity Administrator에서 관리되는 섀시 및 서버에 대한 인증 및 액세스를 관리하는 데 사용됩니다.

시작하기 전에

저장된 자격 증명을 작성, 수정 또는 삭제하려면, lxc-supervisor 또는 lxc-security-admin 권한을 가지고 있어야 합니다.

이 작업 정보

저장된 자격 증명은 장치의 로컬 사용자 계정 또는 Active Directory 서버의 사용자 계정이어야 합니다.

XClarity Administrator 관리되는 인증 대신 로컬 인증을 사용하여 장치를 관리하도록 선택한 경우 관리 프로세스 중에 저장된 자격 증명 계정을 선택해야 합니다.

중요: XClarity Administrator는 저장된 자격 증명에 대해 지정한 사용자 이름 및 암호의 유효성을 검증하지 않습니다. 지정된 정보가 로컬 장치 또는 Active Directory의 활성 사용자 계정에 해당하는지를 사용자가 확인해야 합니다(관리되는 장치가 Active Directory를 사용하여 인증하도록 구성된 경우).

주의: 저장된 자격 증명에는 수퍼바이저 액세스 권한이 있거나 장치의 구성을 변경할 수 있는 충분한 권한이 있어야 합니다. 장치에 대한 충분한 권한이 없는 저장된 자격 증명이 있는 서버를 관리하려고 하면, 관리 프로세스가 성공할 수는 있지만 액세스 거부 오류로 인해 장치에 대한 추가 관리 인벤토리 작업이 실패하여 장치에 대한 연결 문제가 감지 될 수 있습니다.

절차

XClarity Administrator에 저장된 자격 증명을 추가하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하십시오. 보안 페이지가 표시됩니다.

단계 2. 관리되는 인증 섹션 아래에서 **저장된 자격 증명**을 클릭하면 저장된 자격 증명 페이지가 표시됩니다.

단계 3. **만들기** 아이콘( )을 클릭하여 저장된 자격 증명을 만드십시오. 새로운 저장된 자격 증명 만들기 대화 상자가 표시됩니다.

단계 4. 대화 상자에서 다음 정보를 입력하십시오.
- 저장된 자격 증명에 대한 사용자 이름과 선택적 설명을 입력하십시오.
- 저장된 자격 증명에 대한 암호를 입력한 다음 확인하십시오.
- 선택적으로 입력한 다음, RECOVERY_ID에 저장된 복구 자격 증명의 암호를 확인하십시오.

단계 5. **저장된 자격 증명 만들기**를 클릭하십시오.

완료한 후에

저장된 자격 증명 계정이 저장된 자격 증명 테이블에 표시됩니다. 이 테이블은 각각의 저장된 자격 증명 계정에 대한 관련 ID와 설명을 보여줍니다.

저장된 자격 증명 페이지에서 선택된 저장된 자격 증명 계정에 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘( )을 클릭하여 저장된 자격 증명 계정에 대한 사용자 이름, 암호 및 설명을 수정하십시오.

  참고: 저장된 자격 증명을 사용하여 장치를 관리하고 관리 인증을 사용하는 경우, 저장된 자격 증명을 편집할 수 없습니다.
- **삭제** 아이콘( )을 클릭하여 저장된 자격 증명 계정을 삭제하십시오.

만료되었거나 유효하지 않은 저장된 자격 증명을 해결하려면, 서버에 대해 만료되었거나 유효하지 않은 저장된 자격 증명 해결의 내용을 참조하십시오.

역할 및 역할 그룹 관리

*역할*을 사용하여 리소스에 대한 사용자 액세스를 제어하고 해당 리소스에서 수행할 수 있는 작업을 제한합니다. *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 Lenovo XClarity Administrator 사용자는 하나 이상의 역할 그룹의 멤버여야 합니다.

사용자 지정 역할 만들기

*역할*은 특정한 작업을 수행하기 위한 *권한* 또는 특권 세트입니다. Lenovo XClarity Administrator에는 미리 정의된 몇 가지 (기본) 역할이 있습니다. 사용자가 수행할 수 있는 고유한 권한 세트를 적용하는 사용자 지정 역할을 만들 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 lxc-supervisor 또는 lxc-security-admin 권한이 있어야 합니다.

이 작업 정보

사용자 지정 역할을 만들려면 만들려는 역할의 범위에서 가장 가까운 하나 이상의 미리 정의된 역할을 선택한 다음 제한할 개별 권한을 지웁니다. 이렇게 하면 의도한 모든 권한을 얻고 종속된 권한으로 역할이 올바르게 구성됩니다.

일부 XClarity Administrator 권한은 관리되는 장치에서 작업을 수행하는 해당 관리 모듈 권한에 따라 다릅니다(관리 모듈 v1 권한 및 관리 모듈 v2 권한 참조). XClarity Administrator 권한을 사용하면 관리되는 장치에 작업을 요청할 수 있지만, CMM, IMM 또는 XCC에 대한 해당 권한이 없는 경우 장치는 요청을 거부합니다. 예를 들어, 관리되는 장치에서 전원 작업을 수행하는 사용자 지정 역할을 만드는 경우 lxc-inventory-modify-device-power-state 권한과 다음을 추가합니다.

- 랙에 있는 ThinkSystem 서버의 경우 mm-power-and-restart-access-v1 권한을 추가합니다.
- 전체 Flex System 섀시(섀시의 장치 포함)의 경우 mm-power-and-restart-access-v1 권한을 추가합니다.
- 섀시에 있는 ThinkSystem 서버의 경우 대상 서버와 일치하는 mm-power-and-restart-access-v1, mm-blade-operator-v2 및 mm-blade-#-scope-v2 권한을 추가합니다.

모든 역할은 읽기 전용 권한을 포함합니다. 사용자 지정 역할은 lxc-operator 역할보다 더 제한적일 수 없습니다.

사용자에게 특정 작업을 수행할 권한이 없으면 해당 작업을 수행하는 메뉴 항목, 도구 모음 아이콘 및 버튼이 비활성화됩니다(회색으로 표시됨).

XClarity Administrator는 역할과 동일한 이름을 사용하여 미리 정의된 각 역할에 대한 역할 그룹을 제공합니다. 만드는 새 역할에 대한 역할 그룹을 만드는 것이 좋습니다. 역할 그룹에 대한 자세한 정보는 사용자 지정 역할 그룹 만들기의 내용을 참조하십시오.

- lxc-supervisor. 이 역할에 할당된 사용자는 관리 서버 및 모든 관리되는 장치에서 사용 가능한 모든 작업을 액세스하고, 구성하고, 수행할 수 있습니다.이 역할에 할당된 사용자는 항상 모든 관리되는 장치에 대한 액세스 권한을 가집니다. 이 역할의 장치에 대한 액세스 권한을 제한할 수 없습니다.
- lxc-admin. 이 역할에 할당된 사용자는 관리 서버에서 관리 서버 업데이트 및 재시작 기능을 포함한 모든 비보안 관련 작업을 수행하고 비보안 관련 설정을 수정할 수 있습니다. 이 역할은 관리 서버와 관리되는 장치에 대한 모든 구성과 상태 정보를 볼 수 있는 기능도 제공합니다.
- lxc-security-admin. 이 역할에 할당된 사용자는 관리 서버와 관리되는 장치에서 보안 관련 작업을 수행하고 보안 관련 설정을 수정할 수 있습니다. 이 역할은 관리 서버와 관리되는 장치에 대한 모든 구성과 상태 정보를 볼 수 있는 기능도 제공합니다.

  이 역할에 할당된 사용자는 항상 모든 관리되는 장치에 대한 액세스 권한을 가집니다. 이 역할의 장치에 대한 액세스 권한을 제한할 수 없습니다.

- lxc-hw-admin. 이 역할에 할당된 사용자는 관리되는 장치에서 관리되는 장치 업데이트 및 재시작 기능을 포함한 모든 비보안 관련 작업을 수행하고 비보안 관련 설정을 수정할 수 있습니다. 이 역할은 관리 서버와 모든 관리되는 장치에 대한 모든 구성과 상태 정보를 볼 수 있는 기능도 제공합니다.
- lxc-fw-admin. 이 역할에 할당된 사용자는 펌웨어 정책을 작성하고 해당 정책을 관리되는 장치에 배포할 수 있습니다. 이 역할이 할당되지 않는 사용자는 정책 정보를 보는 것만 가능합니다.
- lxc-os-admin. 이 역할이 할당되는 사용자는 운영 체제 및 장치 드라이버 업데이트를 관리되는 서버로 다운로드하고 배포할 수 있습니다. 이 역할이 할당되지 않는 사용자는 운영 체제 및 장치 드라이버 정보를 보는 것만 가능합니다.
- lxc-service-admin. 이 역할이 할당된 사용자는 XClarity Administrator 및 관리되는 장치에 대한 서비스 파일을 수집하고 다운로드할 수 있습니다. 이 역할이 할당되지 않은 사용자는 서비스 데이터를 수집할 수는 있지만 다운로드할 수는 없습니다.
- lxc-hw-manager. 이 역할에 할당된 사용자는 새 장치를 검색하고 해당 장치를 XClarity Administrator의 관리 제어 하에 둘 수 있습니다. 이 역할은 새 장치를 검색하고 관리하는 데 필요한 작업을 제외하고 사용자가 관리 서버 및 관리되는 장치에서 구성 설정을 수정하거나 작업을 수행하지 못하게 합니다.
- lxc-operator. 이 역할에 할당된 사용자는 관리 서버와 관리되는 장치에 대한 모든 구성 및 상태 정보를 볼 수 있습니다. 이 역할은 사용자가 관리 서버 및 관리되는 장치에서 구성 설정을 수정하거나 작업을 수행하지 못하게 합니다.
- lxc-recovery. 이 역할에 할당된 사용자는 관리 서버에서 보안 관련 작업을 수행하고 보안 관련 설정을 수정할 수 있습니다. 이러한 사용자는 인증 방법이 외부 LDAP 서버로 설정된 경우에도 XClarity Administrator에 직접 인증할 수도 있습니다. 이 역할은 "로그인 자격 증명" 구성을 사용하는 외부 LDAP 서버에서 통신 오류가 발생하는 경우 복구 메커니즘을 제공합니다.

  이 역할에 할당된 사용자는 항상 모든 관리되는 장치에 대한 액세스 권한을 가집니다. 이 역할의 장치에 대한 액세스 권한을 제한할 수 없습니다.

다음 미리 정의된 역할은 *예약*되어 있으며 이를 사용하여 새 역할 그룹을 작성하거나 새 사용자에 할당할 수 없습니다.
- lxc-sysrdr
- lxc-sysmgr

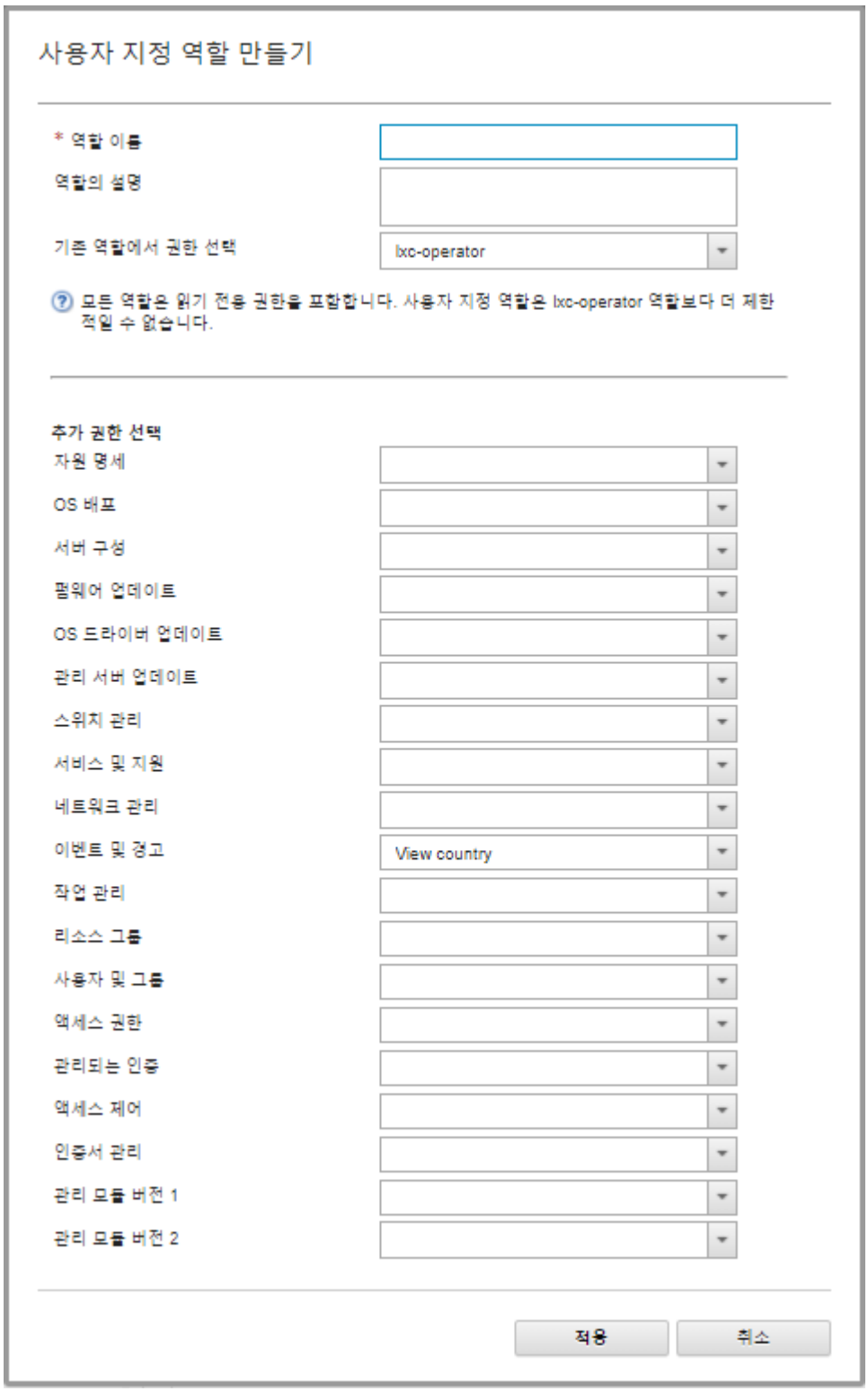
절차

사용자 지정 역할을 작성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 **역할**을 클릭하여 역할 관리 페이지를 표시하십시오.

단계 3. **만들기** 아이콘( )을 클릭하여 역할을 만드십시오. 사용자 지정 역할 만들기 대화 상자가 표시됩니다.



단계 4. 역할 이름과 설명을 입력하십시오.

단계 5. 이 사용자 지정 역할의 시작 지점으로 사용할 미리 정의된 역할을 선택하십시오.

기존 역할을 선택하면 해당 역할과 연결된 권한이 대화 상자에서 선택됩니다.

단계 6. **추가 권한 선택** 드롭 다운 메뉴에서 권한을 선택하거나 선택 취소하여 이 새 역할에 대한 권한을 수정하십시오.

참고: 특정 범주의 모든 권한을 선택하고 XClarity Administrator를 업데이트하거나 업그레이드할 때 해당 범주에 권한이 추가되면 새 권한이 사용자 지정 역할에 자동으로 추가됩니다.

단계 7. **만들기**를 클릭하십시오. 새 역할이 역할 관리 페이지의 테이블에 추가됩니다.

결과

다음 작업을 수행할 수도 있습니다.

- 역할을 선택하고 **보기** 아이콘()을 클릭하여 특정 역할과 연결된 권한을 확인합니다.
- **편집** 아이콘()을 클릭하여 사용자 지정 역할을 편집하거나 이름을 바꿉니다. 사용자 지정 역할을 편집할 때 선택한 권한, 설명 및 역할과 연결된 사용자 목록을 변경할 수 있습니다.

  참고: 미리 정의된 역할은 수정할 수 없습니다.
- **삭제** 아이콘()을 클릭하여 미리 정의된 역할 또는 사용자 지정 역할을 삭제합니다.
- 역할 그룹에서 역할을 추가하거나 제거합니다(역할 그룹에서 여러 사용자 추가 및 제거 참조).
- **모든 작업 → 기본 역할 복원**을 클릭하여 삭제된 미리 정의된 역할을 모두 복원합니다.

미리 정의된 권한

Lenovo XClarity Administrator는 사용자가 특정 작업을 수행할 수 있도록 하는 *권한*(특권) 세트입니다. 권한은 작업 유형에 따라 범주로 구성됩니다.

액세스 권한

다음 권한은 암호화 및 SSL/TLS 모드를 수정할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-sec-apply-crypto-settings	암호화 설정 적용	lxc-recovery, lxc-security-admin, lxc-supervisor

원격 제어 권한

다음 권한은 리소스에 대한 액세스를 제어할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-sec-modify-resource-access-control	리소스 액세스 제어 설정 편집	lxc-recovery, lxc-security-admin, lxc-supervisor

인증서 관리 권한

다음 권한은 Lenovo XClarity Administrator에서 보안 인증서를 관리할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-sec-add-external-certificates	외부 인증서 추가	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	신뢰할 수 있는 인증서 추가	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-certificate-signing	인증서 서명 요청 생성	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	기존 외부 인증서 삭제	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	기존 인증서 삭제	lxc-recovery, lxc-security-admin, lxc-supervisor

권한 이름	권한 설명	기본 역할
lxc-sec-download-ca	인증 기관 루트 인증서 다운로드	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	서버 인증서 다운로드	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	인증서 해지 목록 수정 또는 바꾸기	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	인증 기관 루트 인증서 다시 생성	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	인증 기관 루트 인증서 다시 생성	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	서버 인증서 다시 생성	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	신뢰할 수 없는 인증서 해결	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	서버 인증서 업로드	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_view_certpol_settings	인증서 정책 설정 보기	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_apply_certpol_settings	인증서 정책 설정 적용	lxc-security-admin, lxc-supervisor

모니터링 및 이벤트 권한

다음 권한은 이벤트 및 경고를 관리할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-event-audit	이벤트 및 감사 로그 관리	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	이벤트 전달자 만들기 및 수정	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	푸시 서비스 만들기 및 수정	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-event-forwarders	이벤트 전달자 삭제	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-push-services	푸시 서비스 삭제	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	이벤트 임계값 설정	lxc-admin, lxc-hw-admin, lxc-supervisor

펌웨어 업데이트 권한

다음 권한은 펌웨어 업데이트 및 UpdateXpress System Pack를 관리하고 적용할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-fwUpdates-apply-assign-policy	장치에 펌웨어 준수 정책 할당	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	펌웨어 업데이트 수행	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	펌웨어 준수 정책 만들기, 복사, 편집 및 가져오기	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	준수 정책 삭제	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	펌웨어 업데이트 패키지 삭제	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	펌웨어 업데이트 패키지 다운로드/가져오기 및 펌웨어 업데이트 패키지 새로 고침	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	펌웨어 업데이트 패키지 내보내기	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

리소스 그룹 권한

다음 권한은 리소스 그룹을 사용할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-resource-create-edit-group	리소스 그룹 만들기 및 수정	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	리소스 그룹 삭제	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

인벤토리 권한

다음 권한은 장치를 검색 및 관리하고 장치 인벤토리를 볼 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-dm-manage-device	섀시, 서버, 스토리지 및 스위치 관리	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	동일한 서브넷에서 중복 IP 주소에 대한 검사 사용 또는 사용 안 함	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	캐니스터, cmms, 노드, 스토리지 및 스위치 전원 상태 수정	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	캐비넷, 캐니스터, 섀시, cmms, 노드, 스토리지 및 스위치 속성 수정	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	예측된 장애 경고(PFA) 구성 설정 수정	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

작업 관리 권한

다음 권한은 작업을 관리할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-tasks-remove-jobs	작업 삭제	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	작업 예약	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

관리되는 인증 권한

다음 권한은 저장된 자격 증명을 포함하여 인증을 관리할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-sec-delete-stored-credentials	저장된 자격 증명 삭제	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	기존 저장된 자격 증명 편집	lxc-recovery, lxc-security-admin, lxc-supervisor

관리 모듈 v1 권한

이러한 권한은 랙 서버 및 전체 Flex System 섀시(해당 섀시의 모든 장치 포함)에 대한 관리 모듈에 의해 적용되는 LDAP 권한 비트(비트 문자열)와 관련됩니다.

Lenovo XClarity Administrator에서는 이러한 권한을 적용하지 않습니다. 이러한 권한은 XClarity Administrator 사용자 계정을 사용하는 관리되는 장치에 의해 적용됩니다.

장치가 *관리되는 인증*(인증을 위해 로컬 인증 서버 사용)을 사용하여 관리되는 경우 로컬 인증 서버는 이러한 권한을 사용하여 장치에 로그인할 때 사용자에게 부여할 권한을 관리되는 장치에 지정합니다.

외부 LDAP 서버에서 이와 동일한 권한을 구성합니다. XClarity Administrator에서 외부 LDAP 서버를 사용하는 경우 XClarity Administrator의 역할 그룹 이름과 동일한 이름을 사용하는 외부 LDAP 서버에 그룹을 추가하고 외부 LDAP 사용자가 이러한 그룹 중 하나 이상에 추가되어야 합니다. 외부 LDAP 사용자는 관리 모듈 비트 문자열과 관련된 역할을 포함하는 XClarity Administrator 역할 그룹과 동일한 이름의 LDAP 그룹에 속해야 합니다. XClarity Administrator에서는 이러한 그룹을 사용하여 외부 LDAP 사용자를 XClarity Administrator의 역할 그룹 및 관리 모듈에서 시행하는 비트 문자열에 연결합니다. 그런 다음 사용자가 외부 LDAP 사용자 계정을 사용하여 관리되는 장치에 로그인하면 관리 모듈에서 사용자에게 감독자 또는 운영자 권한을 부여할지 여부를 파악합니다.

참고: 관리 모듈 v1 권한은 Secure IOM 사용 설정이 되지 않은 FlexSystem 스위치, RackSwitch 스위치, 스토리지 장치 및 ThinkServer 서버에서 지원되지 않습니다.

각 관리 모듈의 LDAP 권한 비트에 대한 정보는 온라인 설명서를 참조하십시오.
- CMM 및 CMM2 온라인 설명서의 LDAP 구성
- IMM 및 IMM2 온라인 설명서의 LDAP 구성
- XCC 온라인 설명서의 LDAP 구성

권한 이름	권한 설명	기본 역할
mm-advanced-adaptor-configuration-v1	고급 어댑터 구성	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	기본 구성	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

권한 이름	권한 설명	기본 역할
mm-clear-event-logs-v1	이벤트 로그 지우기	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	항상 거부	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	네트워킹 및 보안	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	서버 및 Flex 스위치의 전원/재시작 액세스	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	서버에 대한 원격 제어 액세스	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	서버에 대한 원격 콘솔 및 가상 미디어 액세스	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	감독자 액세스	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	사용자 관리	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

관리 모듈 v2 권한

이러한 권한은 개별 FlexSystem 및 섀시의 ThinkSystem 장치(섀시, 서버 및 Secure IOM 사용 스위치)에 대한 관리 모듈에 의해 적용되는 LDAP 권한 비트(비트 문자열)와 관련됩니다.

Lenovo XClarity Administrator에서는 이러한 권한을 적용하지 않습니다. 이러한 권한은 XClarity Administrator 사용자 계정을 사용하는 관리되는 장치에 의해 적용됩니다.

장치가 *관리되는 인증*(인증을 위해 로컬 인증 서버 사용)을 사용하여 관리되는 경우 로컬 인증 서버는 이러한 권한을 사용하여 장치에 로그인할 때 사용자에게 부여할 권한을 관리되는 장치에 지정합니다.

외부 LDAP 서버에서 이와 동일한 권한을 구성합니다. XClarity Administrator에서 외부 LDAP 서버를 사용하는 경우 XClarity Administrator의 역할 그룹 이름과 동일한 이름을 사용하는 외부 LDAP 서버에 그룹을 추가하고 외부 LDAP 사용자가 이러한 그룹 중 하나 이상에 추가되어야 합니다. 외부 LDAP 사용자는 관리 모듈 비트 문자열과 관련된 역할을 포함하는 XClarity Administrator 역할 그룹과 동일한 이름의 LDAP 그룹에 속해야 합니다. XClarity Administrator에서는 이러한 그룹을 사용하여 외부 LDAP 사용자를 XClarity Administrator의 역할 그룹 및 관리 모듈에서 시행하는 비트 문자열에 연결합니다. 그런 다음 사용자가 외부 LDAP 사용자 계정을 사용하여 관리되는 장치에 로그인하면 관리 모듈에서 사용자에게 감독자 또는 운영자 권한을 부여할지 여부를 파악합니다.

참고:

- 또한 전체 섀시에 대해서는 관리 모듈 v1 권한을 지정해야 합니다(관리 모듈 v1 권한 참조).
- Secure IOM을 사용하지 않는 FlexSystem 스위치에 대해서는 관리 모듈 v2 권한이 지원되지 않습니다.
- Lenovo ThinkSystem 섀시의 경우 사용자 지정 역할이 "노드 관리"를 수행하도록 IMM2를 설정해야 합니다. 사용자 지정 역할이 Lenovo ThinkSystem 섀시의 모든 장치를 제어하도록 하려면 사용자 지정 역할이 "노드 X 범위"도 포함할 수 있도록 IMM2를 설정해야 합니다.

각 관리 모듈의 LDAP 권한 비트에 대한 정보는 온라인 설명서를 참조하십시오.
- CMM 및 CMM2 온라인 설명서의 LDAP 구성
- IMM 및 IMM2 온라인 설명서의 LDAP 구성
- XCC 온라인 설명서의 LDAP 구성

권한 이름	권한 설명	기본 역할
mm-blade-1-scope-v2	노드 1 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	노드 2 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	노드 3 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	노드 4 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	노드 5 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	노드 6 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	노드 7 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-8-scope-v2	노드 8 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	노드 9 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	노드 10 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	노드 11 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	노드 12 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	노드 13 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	노드 14 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	노드 관리	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

권한 이름	권한 설명	기본 역할
mm-blade-configuration-v2	노드 구성	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	블레이드 운영자	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	노드 원격 관리	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	섀시 관리	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	섀시 구성	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	섀시 로그 계정 관리	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	섀시 운영자	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	섀시 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	사용자 관리	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	항상 거부	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	I/O 모듈 1 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	I/O 모듈 2 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-3-scope-v2	I/O 모듈 3 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	I/O 모듈 4 범위	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	스위치 관리	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	스위치 구성	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

권한 이름	권한 설명	기본 역할
mm-switch-operator-v2	스위치 운영자	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	감독자 액세스	lxc-admin, lxc-hw-admin, lxc-supervisor

관리 서버 권한

다음 권한은 관리 서버를 업데이트할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-mgmtserverupdates-delete-updates	관리 서버 업데이트 삭제	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	관리 서버 업데이트 다운로드/가져오기 및 관리 서버 카탈로그 새로 고침	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	관리 서버 업데이트 수행	lxc-admin, lxc-fw-admin, lxc-supervisor

네트워크 관리 권한

다음 권한은 네트워크 설정을 구성할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-network-edit	네트워크 액세스 수정	lxc-admin, lxc-supervisor

OS 배포 권한

다음 권한은 운영 체제를 관리하고 배포할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-osdeploy-create-edit-remote-file-server	원격 파일 서버 항목 만들기 및 편집	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	OS 이미지 및 사용자 지정 파일 만들기, 가져오기, 내보내기 및 편집	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	OS 이미지 및 사용자 지정 파일 삭제	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	원격 파일 서버 항목 삭제	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-global-settings	전역 설정 대화 상자에서 정보 편집 **참고:** 전역 IP 할당 설정을 변경하면 네트워크 설정에 영향을 줍니다. 따라서 전역 IP 할당 설정을 변경하려면 lxc-osdeploy-edit-settings-and-deploy-os-images 권한도 가지고 있어야 합니다.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	배포 설정 수정 및 하나 이상의 서버에 OS 이미지 배포	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

OS 드라이버 업데이트 권한

다음 권한은 OS 장치 드라이버 업데이트를 관리하고 적용할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-osDriverUpdates-apply-assign-uxsp	장치에 OS 장치 드라이버 UXSP 할당	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	OS 인증 검사	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	OS 장치 드라이버 준수 검사	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	OS 장치 드라이버 업데이트 수행	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	OS 장치 드라이버 업데이트 패키지 삭제	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	OS 장치 드라이버 업데이트 패키지 다운로드/가져오기 및 OS 장치 드라이버 UXSP 카탈로그 새로 고침	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

사용자 및 그룹 권한

다음 권한은 사용자 계정 및 그룹을 관리할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-sec-apply-saml-settings	SAML 설정 적용	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	역할 그룹 삭제	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	역할 삭제	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-users	사용자 삭제	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	계정 보안 설정 수정	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	LDAP 설정 적용	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	역할 그룹 수정	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	역할 수정	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	사용자 수정	lxc-recovery, lxc-security-admin, lxc-supervisor

서버 구성 권한

다음 권한은 구성 패턴을 사용하여 서버를 프로비저닝하거나 사전 프로비저닝할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-cp-edit-management-ip	섀시의 관리 IP 주소 수정	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	구성 패턴 기본 설정 지정	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	주소 풀 관리	lxc-admin, lxc-hw-admin, lxc-supervisor

권한 이름	권한 설명	기본 역할
lxc-cp-manage-patterns	패턴 관리	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	자리 표시자 관리	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	패턴 배포, 섀시에 자리 표시자 배포 및 프로필 관리	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	로컬 스토리지 재설정 및 Intel Optane DCPMM 보안 작업 적용	lxc-admin, lxc-hw-admin, lxc-supervisor

서비스 권한

다음 권한은 각 관리되는 장치에 대한 지원 연락처를 정의하고, 서비스 파일을 수집하여 Lenovo 지원 센터로 보내고, 특정 장치에서 특정 서비스 가능 이벤트가 발생하는 경우의 서비스 공급자에 대한 자동 알림을 설정하고, 서비스 티켓 상태 및 보증 정보를 보고, 서비스 데이터를 수집 및 전달할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-ss-alter-backup-credentials	백업 FFDC 자격 증명 수정	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	콜 홈 수행	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-recovery-password	서비스 복구 암호 변경	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	서비스 티켓 수정	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	서비스 티켓 삭제	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	서비스 전달자 실행	lxc-admin, lxc-hw-admin, lxc-supervisor

스위치 구성 권한

다음 권한은 스위치를 구성하고 스위치 구성 데이터를 백업 및 복원할 수 있는 권한을 제공합니다.

권한 이름	권한 설명	기본 역할
lxc-netcfg-template-management	스위치 구성 템플릿 만들기, 수정, 삭제 및 배포와 스위치 구성 배포 삭제	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	스위치 구성 데이터 파일 백업, 복원, 삭제, 내보내기 및 가져오기	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	스위치 포트 상태 수정	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

사용자 지정 역할 그룹 만들기

*역할 그룹*은 역할 세트이며, 동일한 역할 세트의 멤버인 사용자 세트입니다. 역할 그룹의 각 사용자에게 부여되는 액세스 수준은 해당 역할 그룹에 할당된 역할을 기반으로 합니다. XClarity Administrator는 미리 정의된 각 역할에 해당하는 다음과 같은 미리 정의된 역할 그룹을 제공합니다. 또한 사용자 지정 역할 그룹을 만들 수도 있습니다.

이 작업 정보

각 XClarity Administrator 사용자는 하나 이상의 역할 그룹의 멤버여야 합니다.

다음 역할 그룹은 XClarity Administrator에서 미리 정의되어 있습니다.

- LXC-SUPERVISOR. lxc-supervisor 역할을 포함합니다.
- LXC-ADMIN. lxca-admin 역할을 포함합니다.
- LXC-SECURITY-ADMIN. lxc-security-admin 역할을 포함합니다.
- LXC-HW-ADMIN. lxc-hw-admin 역할을 포함합니다.
- LXC-FW-ADMIN. lxc-fw-admin 역할을 포함합니다.
- LXC-OS-ADMIN. lxc-os-admin 역할을 포함합니다.
- LXC-SERVICE-ADMIN. lxc-service-admin 역할을 포함합니다.
- LXC-HW-MANAGER. lxc-hw-manager 역할을 포함합니다.
- LXC-OPERATOR. lxc-operator 역할을 포함합니다.
- LXC-RECOVERY. lxc-recovery 역할을 포함합니다.

다음 미리 정의된 역할은 *예약*되어 있으며 이를 사용하여 새 역할 그룹을 작성하거나 새 사용자에 할당할 수 없습니다.
- lxc-sysrdr
- lxc-sysmgr

절차

역할 그룹을 작성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리** → **보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 **역할 그룹**을 클릭하여 그룹 관리 페이지를 표시하십시오.

단계 3. **만들기** 아이콘( )을 클릭하여 역할 그룹을 작성하십시오. 새 역할 그룹 만들기 대화 상자가 표시됩니다.

단계 4. 그룹 이름과 설명을 입력하십시오.

참고: 팁: 그룹 이름의 경우 문자, 숫자, 공백, 밑줄, 대시 및 마침표를 사용할 수 있습니다.

단계 5. 이 역할 그룹에 할당할 역할을 하나 이상 선택하십시오.

단계 6. 하나 이상의 사용자를 이 역할 그룹의 멤버로 선택하십시오.

단계 7. **만들기**를 클릭하십시오. 새 역할 그룹은 그룹 관리 페이지의 테이블에 추가됩니다.

결과

역할 그룹은 역할 그룹 테이블에 표시됩니다. 이 테이블은 연결된 권한 부여 역할과 각 역할 그룹의 멤버를 표시합니다.

역할 그룹을 작성하면 선택한 역할 그룹에 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘()을 클릭하여 이 그룹에 할당된 역할을 추가하거나 제거하십시오.
- 사용자를 역할 그룹의 멤버로 추가하거나 제거합니다("역할 그룹에서 여러 사용자 추가 및 제거" 52페이지 참조).
- **모든 작업** → **CSV로 내보내기**를 클릭하여 액세스 권한을 포함한 역할 그룹에 대한 정보를 내보냅니다.
- **삭제** 아이콘()을 클릭하여 역할 그룹을 삭제합니다.미리 정의된 역할 그룹은 삭제할 수 없습니다.

역할 그룹을 작성, 편집 또는 삭제하면 해당 변경 사항은 관리되는 각 장치에 즉시 프로비저닝됩니다.

역할 그룹에서 여러 사용자 추가 및 제거

여러 사용자를 추가하거나 제거하여 역할 그룹에서 멤버십을 변경할 수 있습니다.

절차

역할 그룹에서 사용자를 추가하고 제거하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 바에서 **관리** → **보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 **역할 그룹**을 클릭하여 그룹 관리 페이지를 표시하십시오.

단계 3. **편집** 아이콘()을 클릭하여 역할 그룹을 수정하십시오. 역할 그룹 편집 대화 상자가 표시됩니다.

단계 4. **사용자 목록** 드롭 다운 목록을 클릭하여 이 역할 그룹에 포함할 사용자를 선택하거나 역할 그룹에서 제외할 사용자를 지우십시오.

단계 5. **저장**을 클릭하십시오. **사용자 목록** 열은 역할 그룹의 현재 사용자 멤버십을 표시합니다.

장치에 대한 액세스 관리

장치에 대한 액세스 제어는 기본적으로 사용 안 함으로 설정되며 이를 사용 설정하기 전에는 적용되지 않습니다

Lenovo XClarity Administrator에서 장치를 처음 관리하는 경우 미리 정의된 역할 그룹 세트에는 기본적으로 장치에 액세스할 수 있는 권한이 있습니다. 미리 정의된 세트는 구성될 때까지 기본적으로 비어 있습니다.

특정한 관리되는 장치에 액세스할 수 있는 역할 그룹을 변경합니다. 특정 역할 그룹에 권한이 부여되면 해당 역할 그룹의 구성원인 사용자만 특정 장치를 보고 해당 장치에 대한 작업을 수행할 수 있습니다.

특정 장치에 대한 액세스 제어

Lenovo XClarity Administrator에서 장치를 처음 관리하는 경우 미리 정의된 역할 그룹 세트에는 기본적으로 장치에 액세스할 수 있는 권한이 있습니다. 특정한 관리되는 장치에 액세스할 수 있는 역할 그룹을 변경합니다. 특정 역할 그룹에 권한이 부여되면 해당 역할 그룹의 구성원인 사용자만 특정 장치를 보고 해당 장치에 대한 작업을 수행할 수 있습니다.

시작하기 전에

lxc-supervisor, lxc-security-admin 또는 lxc-recovery 권한이 있는 사용자만 이 작업을 수행할 수 있습니다.

이 작업 정보

액세스 제어는 개별 장치에서 설정됩니다. 랙 및 리소스 그룹과 같은 컨테이너에 대해 설정되지 않습니다.

섀시 또는 인클로저의 구성 요소의 경우, 사용자는 적어도 해당 섀시 또는 인클로저의 보기 구성 요소에 대한 섀시 또는 인클로저에 대한 읽기 전용 액세스 권한이 있어야 합니다. 섀시 또는 인클로저에 대해 읽기 전용 액세스 이상의 권한이 없는 경우, 해당 사용자는 일부 보기에서 섀시 구성 요소를 계속 볼 수 있지만 모든 보기에서 섀시 구성 요소를 볼 수는 없습니다.

lxc-supervisor 권한이 있는 사용자는 해당 리소스에 대한 액세스 권한이 주어진 역할 그룹에 있는지 여부에 관계없이 모든 리소스를 보고 리소스에 대한 작업을 수행할 수 있습니다. 리소스에 대한 lxc-supervisor 역할 그룹의 액세스 권한을 제거할 수 없습니다.

특정 관리되는 장치에 대한 액세스 권한이 있는 역할 그룹의 구성원이 아닌 경우 사용자는 해당 특정 장치를 볼 수 없거나 해당 장치에 대한 작업을 수행할 수 없습니다. 여기에는 Lenovo XClarity Administrator를 통한 관리 컨트롤러 웹 인터페이스 실행이 포함됩니다. 또한 Flex 및 System x 장치의 경우 사용자는 액세스할 수 없는 CMM 또는 관리 컨트롤러에 직접 로그인할 수 없습니다.

XClarity Administrator에서 장치를 처음 관리하는 경우와 특정 장치에 대한 액세스 권한을 기본 설정으로 다시 설정하는 경우 기본 액세스 제어 설정을 사용하여 장치에 대한 액세스 권한을 설정합니다. 기본 액세스 제어 설정을 변경해도 이미 관리되는 장치에 대한 액세스 권한은 자동으로 변경되지 않습니다.

중요:

- 사용자가 둘 이상의 역할 그룹의 구성원이고 역할 그룹이 다른 장치에 할당된 경우 사용자가 각 장치에서 수행할 수 있는 작업이 다를 수 있습니다. 예를 들어 사용자가 기본 역할 그룹 LXC-FW-ADMIN 및 LXC-OS-ADMIN의 구성원인 경우, LXC-FW-ADMIN이 서버 A에 대한 액세스 권한을 부여받았지만 LXC-OS-ADMIN이 서버 A에 대한 액세스 권한을 부여받지 못했으면 사용자는 서버 A에서 펌웨어를 업데이트할 수 있지만 서버 A에 운영 체제를 배포할 수는 없습니다. LXC-OS-ADMIN이 서버 B에 대한 액세스 권한을 부여받았지만 LXC-FW-ADMIN이 서버 B에 대한 액세스 권한을 부여받지 못했으면 동일한 사용자는 서버 B에 운영 체제를 배포할 수 있지만 서버 B에서 펌웨어를 업데이트할 수는 없습니다.

- 상위 리소스(예, Flex Chasis의 서버 또는 스위치)가 있는 장치에 대한 액세스를 제한할 경우 장치와 완전히 상호 작용하려면 사용자는 최소한 상위 리소스에 대한 읽기 전용 권한을 가지고 있어야 합니다. 사용자가 최소한 장치에 대한 읽기 전용 액세스 권한은 가지고 있지만 상위 리소스에 대한 권한은 가지고 있지 않은 경우 사용자는 장치 인벤토리 보기를 볼 수 없지만 작업 및 이벤트와 같은 일부 보기에서 장치를 볼 수 있습니다.

  예를 들어 상위 리소스에 대한 역할 그룹을 만들고 해당 역할 그룹에 lxc-operator 역할을 할당할 수 있습니다. 해당 역할 그룹의 하위 리소스(예, Flex Chasis의 서버 또는 스위치)에 액세스할 수 있어야 하는 모든 사용자를 포함시키십시오. 그런 다음 해당 역할 그룹을 상위 리소스에 액세스할 수 있는 그룹 중 하나로 포함시키십시오.

절차

역할 그룹을 해당 장치와 연결하여 특정 장치에 대한 액세스를 제어하려면 다음 절차를 완료하십시오.

단계 1. 기본 Lenovo XClarity Administrator 메뉴에서 **관리 → 보안**을 클릭하십시오.

단계 2. 왼쪽 탐색 창에서 **리소스 보기**를 클릭하십시오. 리소스 보기 페이지가 표시됩니다.

특정 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **리소스 유형** 드롭 다운 메뉴에서 장치 유형을 선택하고 **역할 그룹** 드롭 다운 메뉴에서 역할 그룹을 선택하고 **리소스 그룹** 드롭 다운 메뉴에서 리소스 그룹을 선택하고 **필터** 필드에 텍스트(예, 리소스 이름 또는 유형)를 입력하여 선택한 기준을 충족하는 장치만 나열할 수 있습니다.

단계 3. 액세스를 제어할 장치를 하나 이상 선택하십시오.

단계 4. **편집** 아이콘()을 클릭하십시오. 리소스 편집 대화 상자가 표시되고 **리소스 이름** 필드에 대상 장치가 나열됩니다.

단계 5. **역할 그룹** 드롭 다운 목록에서 대상 장치에 액세스할 수 있는 역할 그룹을 선택하십시오.

참고: 장치에 상위 리소스(예, Flex Chassis의 서버 또는 스위치)가 있는 경우 장치(오른쪽 열)와 상위 리소스(왼쪽 열) 모두에 대한 액세스를 지정할 수 있습니다.

단계 6. **공용 액세스**를 No로 설정하십시오. 즉, 선택한 역할 그룹의 구성원인 사용자만 대상 장치에 액세스할 수 있습니다.

단계 7. **저장**을 클릭하십시오.

단계 8. 권한 할당을 완료한 후 **사용 안 함** 토글을 클릭하여 **리소스 액세스 제어**를 사용으로 변경하십시오.

특정 장치에 대한 액세스를 구성하기 전이나 후에 언제든지 리소스 액세스 제어를 사용으로 설정할 수 있습니다. 이 설정을 사용하면 감독자가 아닌 사용자가 액세스할 수 있는 그룹이 없는 모든 장치에 대해 액세스를 거부하는 것을 포함하여 테이블에 표시된 구성이 적용됩니다.

완료한 후에

다음 작업을 수행하여 장치에 대한 액세스를 제어할 수도 있습니다.

- **편집** 아이콘()을 클릭하고 **기본값으로 재설정**을 클릭하여 권한을 기본 역할 그룹 및 공용 액세스 설정으로 변경하십시오.
- 기본 역할 그룹 및 공용 액세스 설정을 변경하십시오(기본 권한 변경 참조).
- **리소스 액세스 제어**를 사용 안 함으로 변경하기 위해 **사용** 토글을 클릭하여 리소스 액세스 제어를 사용 안 함으로 설정하십시오. 즉, 모든 역할 그룹이 모든 관리되는 장치에 액세스할 수 있습니다.

리소스 액세스 제어 사용 안 함

모든 장치 또는 특정 장치에 대한 액세스 제어를 사용 안 함으로 설정하면 모든 사용자가 해당 장치를 보고 장치에 대한 작업을 수행할 수 있습니다.

이 작업 정보

lxc-supervisor, lxc-security-admin 또는 lxc-recovery 권한이 있는 사용자만 이 작업을 수행할 수 있습니다.

절차

리소스 액세스 제어를 사용 안 함으로 설정하려면 다음 단계를 완료하십시오.

- 모든 관리되는 장치의 경우
  1. 기본 Lenovo XClarity Administrator 메뉴에서 **관리 → 보안**을 클릭하십시오.
  2. 왼쪽 탐색 창에서 **리소스 보기**를 클릭하십시오. 리소스 보기 페이지가 표시됩니다.
  3. **사용** 토글을 클릭하여 **리소스 액세스 제어**를 사용 안 함으로 변경하십시오.
- 특정한 관리되는 장치의 경우
  1. 기본 XClarity Administrator 메뉴에서 **관리 → 보안**을 클릭하십시오.
  2. 왼쪽 탐색 창에서 **리소스 보기**를 클릭하십시오. 리소스 보기 페이지가 표시됩니다.

     특정 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **리소스 유형** 드롭 다운 메뉴에서 장치 유형을 선택하고 **역할 그룹** 드롭 다운 메뉴에서 역할 그룹을 선택하고 **리소스 그룹** 드롭 다운 메뉴에서 리소스 그룹을 선택하고 **필터** 필드에 텍스트(예, 리소스 이름 또는 유형)를 입력하여 선택한 기준을 충족하는 장치만 나열할 수 있습니다.
  3. 액세스를 변경할 장치를 하나 이상 선택하십시오.
  4. **편집** 아이콘( )을 클릭하십시오. 리소스 편집 대화 상자가 표시되고 **리소스 이름** 필드에 선택한 장치가 나열됩니다.
  5. **공용 액세스**를 Yes로 설정하십시오. 즉, 모든 역할 그룹은 **역할 그룹** 드롭 다운 목록에 나열된 역할 그룹에 상관 없이 대상 장치에 액세스할 수 있습니다.
  6. **저장**을 클릭하십시오.

기본 권한 변경

Lenovo XClarity Administrator에서 장치를 처음 관리할 때 역할 그룹이 장치에 액세스할 수 있는지 여부를 판별하는 공용 액세스와 역할 그룹이라는 두 가지 설정이 있습니다. 공용 액세스 설정은 모든 역할 그룹 세트 또는 특정 역할 그룹 세트만 대상 장치에 액세스할 수 있는지 여부를 결정합니다. 기본적으로 이 설정은 Yes로 설정되며 이는 모든 역할 그룹이 대상 장치에 액세스할 수 있음을 의미합니다. 공용 액세스 설정을 No로 변경한 후 대상 장치에 액세스할 수 있는 역할 그룹 세트를 선택하여 기본 동작을 변경할 수 있습니다.

이 작업 정보

lxc-supervisor, lxc-security-admin 또는 lxc-recovery 권한이 있는 사용자만 이 작업을 수행할 수 있습니다.

lxc-supervisor, lxc-security-admin 또는 lxc-recovery 권한을 가진 사용자는 모든 관리 장치에 액세스할 수 있습니다. 해당 역할 그룹의 모든 장치에 대한 액세스를 제거할 수 없습니다.

XClarity Administrator에서 장치를 처음 관리하는 경우와 특정 장치에 대한 액세스 권한을 기본 설정으로 다시 설정하는 경우 기본 액세스 제어 설정을 사용하여 장치에 대한 액세스 권한을 설정합니다. 기본 액세스 제어 설정을 변경해도 이미 관리되는 장치에 대한 액세스 권한은 자동으로 변경되지 않습니다.

절차

기본 액세스 제어를 변경하려면 다음 절차를 완료하십시오.

단계 1. 기본 XClarity Administrator 메뉴에서 **관리 → 보안**을 클릭하십시오.

단계 2. 왼쪽 탐색 창에서 **리소스 보기**를 클릭하십시오. 리소스 보기 페이지가 표시됩니다.

특정 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **리소스 유형** 드롭 다운 메뉴에서 장치 유형을 선택하고 **역할 그룹** 드롭 다운 메뉴에서 역할 그룹을 선택하고 **리소스 그룹** 드롭 다운 메뉴에서 리소스 그룹을 선택하고 **필터** 필드에 텍스트(예, 리소스 이름 또는 유형)를 입력하여 선택한 기준을 충족하는 장치만 나열할 수 있습니다.

단계 3. **모든 작업 → 기본 리소스 편집**을 클릭하십시오. 기본 리소스 편집 대화 상자가 표시됩니다.

단계 4. **역할 그룹** 드롭 다운 목록에서 기본 세트로 정의할 역할 그룹을 선택하십시오.

단계 5. 기본 **공용 액세스** 설정을 선택하십시오.

- **예**. 장치를 처음 관리할 때 모든 역할 그룹은 **역할 그룹** 드롭 다운 목록에 나열된 역할 그룹에 상관 없이 해당 장치에 액세스할 수 있습니다.
- **아니요**. 장치를 처음 관리할 때 기본적으로 **역할 그룹** 드롭 다운 목록에 나열된 역할 그룹만 해당 장치에 액세스할 수 있습니다.

단계 6. **저장**을 클릭하십시오.

보안 환경 구현

사용자 환경의 보안 요구사항을 평가하고, 모든 보안 위험을 이해하고, 이러한 위험을 최소화하는 것이 중요합니다. Lenovo XClarity Administrator에는 사용자 환경을 보호하는 데 도움을 줄 수 있는 몇 가지 기능이 있습니다. 다음 정보를 사용하면 사용자 환경의 보안 계획을 구현하는 데 도움을 줄 수 있습니다.

이 작업 정보

중요: 사용자는 사용자 시스템의 보안 기능, 관리 절차 및 적합한 제어를 평가, 선택 및 구현할 책임이 있습니다. 이 섹션에 설명되어 있는 보안 기능 구현은 사용자 환경을 완전히 보호하지는 못합니다.

사용자 환경의 보안 필요사항을 평가하는 경우 다음 정보를 고려하십시오.

- 사용자 환경의 물리적 보안은 중요합니다. 시스템 관리 하드웨어가 보관되는 룸과 랙에 대한 액세스를 제한하십시오.
- 소프트웨어 기반 방화벽을 사용하여 바이러스 및 무단 액세스와 같은 알려진 긴급한 보안 위협으로부터 네트워크 하드웨어 및 데이터를 보호하십시오.
- 네트워크 스위치와 pass-thru 모듈에 대한 기본 보안 설정을 변경하지 마십시오. 해당 구성 요소에 대한 공장 출하 기본 설정에서 비보안 프로토콜은 사용 안 함으로 설정되고 서명된 펌웨어 업데이트에 대한 요구사항은 사용으로 설정되어 있습니다.
- CMM, 베이스보드 관리 컨트롤러, FSP 및 스위치에 대한 관리 응용 프로그램은 신뢰할 수 있는 펌웨어만 설치하도록 해당 구성 요소에 서명된 펌웨어 업데이트 패키지만 허용합니다.
- 펌웨어 구성 요소를 업데이트할 권한이 있는 사용자만 업데이트 펌웨어 권한을 가지고 있어야 합니다.
- 최소한 중요 펌웨어 업데이트는 설치되어야 합니다. 변경한 후에는 구성을 항상 백업하십시오.
- DNS 서버의 모든 보안 관련 업데이트는 즉시 설치하여 최신 상태를 유지해야 합니다.
- 사용자에게 신뢰할 수 없는 인증서는 승인되지 않음을 알립니다. 자세한 정보는 보안 인증서 작업의 내용을 참조하십시오.
- Flex System 하드웨어에 변조 표시 옵션을 사용할 수 있습니다. 하드웨어가 잠기지 않은 랙에 설치되거나 개방된 공간에 있는 경우 변조 표시 옵션을 설치하여 침입을 방지하고 식별하십시오. 변조 표시 옵션에 대한 자세한 정보는 Flex System 제품과 함께 제공되는 설명서를 참조하십시오.
- 가능하거나 실용성이 있을 경우 시스템 관리 하드웨어를 별도의 서브넷에 설치하십시오. 일반적으로 관리자만 시스템 관리 하드웨어에 대한 액세스 권한을 가져야 하고 기본 사용자에게는 액세스 권한을 부여하면 안됩니다.
- 암호를 선택하는 경우 "password" 또는 회사 이름과 같이 추측하기 쉬운 표현은 사용하지 마십시오. 암호는 보안이 가능한 위치에 보존하고 암호에 대한 액세스를 제한해야 합니다. 회사의 암호 정책을 구현하십시오.

중요: 항상 기본 사용자 이름과 암호를 변경하십시오. 모든 사용자에게 강력한 암호 규칙이 필요합니다.

- 데이터에 대한 액세스 권한이 있고 서버에 프로그램을 설치하는 사용자를 제어하는 방식으로 사용자에 대한 시동 암호를 구축하십시오. 시동 암호에 대한 자세한 정보는 서버와 함께 제공되는 설명서를 참조하십시오.
- 사용자 환경의 여러 사용자에게 사용 가능한 여러 권한 수준을 사용하십시오. 모든 사용자가 동일한 감독자 사용자 ID를 사용하여 작업하지 않도록 하십시오.
- 사용자 환경이 보안 통신을 지원하는 다음 NIST 800-131A 기준을 충족하는지 확인하십시오.
  - TLS v1.2 프로토콜을 통해 SSL(Secure Sockets Layer)을 사용하십시오.
  - 디지털 서명에는 SHA-256 또는 더 강력한 해시 기능, 다른 응용 프로그램에는 SHA-1 또는 더 강력한 해시 기능을 사용하십시오.
  - RSA-2048 이상을 사용하거나 224비트 이상인 NIST 승인 Elliptic Curve를 사용합니다.
  - 길이가 최소 128비트인 키가 있는 NIST 승인 대칭적 암호화를 사용합니다.
  - NIST 승인 무작위 숫자 생성기를 사용합니다.
  - 가능한 경우 Diffie-Hellman 또는 Elliptic Curve Diffie-Hellman 키 교환 메커니즘을 지원합니다.

  암호 표기법 설정에 대한 자세한 정보는 관리 서버의 암호화 설정 구성의 내용을 참조하십시오. NIST 설정에 대한 자세한 정보는 NIST SP 800-131A 준수 구현의 내용을 참조하십시오.

사용자 계정 보안 설정 변경

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

절차

현재 사용자 계정 보안 설정을 덮어쓰려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 2. 사용자 및 그룹 섹션에서 **계정 보안 설정**을 클릭하여 사용자 관리 페이지를 표시하십시오.

단계 3. 변경해야 할 다음 설정에 각각 새 값을 선택하십시오.

표 1. 계정 보안 설정

보안 설정	설명	허용되는 값	기본값
암호 만료 기간	변경 시기 이전에 사용자가 암호를 사용할 수 있는 총 시간(일 수). 값이 작을수록 공격자가 암호를 추정할 수 있는 총 시간이 줄어듭니다. 0으로 설정하면 암호가 만료되지 않습니다. **참고:** 이 설정은 로컬 인증 서버를 사용하여 사용자 계정을 관리하는 경우에만 적용됩니다. 외부 인증 서버를 사용하는 경우에는 사용되지 않습니다.	0 – 365	90
암호 만료 경고 기간	사용자가 암호 만료 임박에 대한 경고를 받기 시작하게 될 암호 만료 날짜 전 시간(일 수) 0으로 설정하면 경고를 받지 않습니다. **참고:** 이 설정은 로컬 인증 서버를 사용하여 사용자 계정을 관리하는 경우에만 적용됩니다. 외부 인증 서버를 사용하는 경우에는 사용되지 않습니다.	0 – ***최대 암호 만료 설정***	5

표 1. 계정 보안 설정 (계속)

보안 설정	설명	허용되는 값	기본값
최소 암호 재사용 사이클	사용자가 암호를 다시 사용하기 위해 암호 변경 시 고유한 암호를 입력해야 하는 최소 횟수 0으로 설정하면 암호를 즉시 재사용할 수 있습니다.	0 – 10	5
최소 암호 변경 기간	암호 변경 후 다시 변경할 수 있게 되기까지 경과해야 하는 최소 시간(시간 단위). 이 설정에 대해 지정되는 값은 암호 만료 기간에 지정된 값을 초과할 수 없습니다. 0으로 설정하면 암호를 즉시 변경할 수 있습니다.	0 – 1440	24
최대 로그인 실패 횟수	사용자 계정이 잠기기 전에 사용자가 잘못된 암호로 로그인을 시도할 수 있는 최대 횟수. 최대 로그인 실패 후 잠금 시간으로 지정되는 숫자에 따라 사용자 계정이 잠기는 시간이 결정됩니다. 잠긴 계정은 유효한 암호를 사용해도 시스템 액세스에 사용할 수 없습니다. 0으로 설정하면 계정이 잠기지 않습니다. 로그인 성공 후 로그인 실패 카운터가 0으로 재설정됩니다.	0 – 100	20
최대 로그인 실패 횟수 이후 잠금 기간	잠긴 사용자로 다시 로그인을 시도할 수 있게 되기까지 경과해야 하는 최소 시간(분 단위) 0으로 설정하면 관리자가 명백히 잠금을 해제할 때까지 계정이 잠깁니다. 0으로 설정하면 고의적인 로그인 시도 실패를 통해 계정을 영구적으로 잠그는 심각한 서비스 거부 공격에 더 쉽게 노출됩니다. **팁:** 감독자 역할의 사용자는 사용자 계정을 잠금 해제할 수 있습니다. 자세한 정보는 사용자 잠금 해제의 내용을 참조하십시오. **참고:** 이 설정은 로컬 인증 서버를 사용하여 사용자 계정을 관리하는 경우에만 적용됩니다. 외부 인증 서버를 사용하는 경우에는 사용되지 않습니다.	0 – 2880	60
웹 비활성 세션 시간 제한	사용자가 로그아웃하기 전에 XClarity Administrator로 구축된 사용자 세션이 비활성화될 수 있는 총 시간(분 단위) 0으로 설정하면 웹 세션이 만료되지 않습니다. **참고:** 이 값을 변경하면, 설정을 변경한 후 시작하는 사용자 세션만 영향을 받습니다.	0 – 1440	1440
최소 암호 길이	유효한 암호를 지정하는 데 사용할 수 있는 최소 글자 수	8 – 20	8
새 비밀번호를 만들 때 지켜야 하는 복잡성 규칙 수	새 비밀번호를 만들 때 지켜야 하는 복잡성 규칙 수 규칙은 규칙 1부터 지정된 규칙 수까지 적용됩니다. 예를 들어, 암호 복잡성이 4로 설정된 경우 규칙 1, 2, 3 및 4를 따라야 합니다. 암호 복잡성이 2로 설정된 경우 규칙 1 및 2를 따라야 합니다. XClarity Administrator는 다음 암호 복잡성 규칙을 지원합니다. • (1) 알파벳 문자를 하나 이상 포함해야 하며 알파벳 문자, 숫자 및 QWERTY 키보드 키 시퀀스를 포함하여 세 개 이상의 순차적 문자를 포함해서는 안됩니다(예: "abc", "123", "asd"는 허용되지 않습니다). • (2) 숫자(0~9)를 하나 이상 포함해야 합니다.	0 – 5	4

표 1. 계정 보안 설정 (계속)

보안 설정	설명	허용되는 값	기본값
	• (3) 다음 문자 중 *두 개* 이상이 포함되어야 합니다. – 알파벳 대문자(A – Z) – 알파벳 소문자(a – z) – 특수 문자 ; @ _ ! ' $ & + • (4) 사용자 이름을 반복하거나 거꾸로 쓸 수 없습니다. • (5) 동일한 문자를 세 개 이상 연속해서 포함할 수 없습니다(예: "aaa", "111", "..."는 허용되지 않습니다). 0으로 설정하면 암호가 복잡성 규칙을 준수할 필요가 없습니다.		
특정 사용자의 최대 활성 세션	지정된 시간에 허용되는 특정 사용자에 대한 최대 활성 세션 수 0으로 설정하면 특정 사용자에 대해 허용된 활성 세션의 수가 제한되지 않습니다.	1 – 20	3
처음 액세스할 때 암호 변경 강제	사용자가 처음으로 XClarity Administrator에 로그인할 때 암호를 변경해야 하는지 여부를 표시	**예** 또는 **아니요**	**예**

단계 4. **적용**을 클릭하십시오.

완료한 후에

이를 저장하면 새 설정이 즉시 적용됩니다. 웹 비활성 세션 시간 제한 설정을 변경하면 활성 세션이 영향을 받습니다.

암호 정책을 변경하는 경우 해당 정책은 다음에 사용자가 로그인하거나 암호를 변경할 때 적용됩니다.

관리 서버의 암호화 설정 구성

관리 서버의 SSL/TLS 버전 및 암호 설정을 구성할 수 있습니다.

시작하기 전에

관리 서버의 설정을 수정하기 전에 암호화 고려 사항을 검토하십시오(XClarity Administrator 온라인 설명서의 암호화 관리 참조).

이 작업 정보

암호 모드는 XClarity Administrator와 모든 관리되는 모든 시스템 간에 보안 통신이 처리되는 방식을 결정합니다. 보안 통신을 구현하는 경우 사용할 암호화 키 길이를 설정합니다.

참고: 선택하는 암호 모드와 관계 없이 NIST가 승인한 Digital Random Bit Generator를 항상 사용하고 대칭 암호화에 128비트 또는 더 긴 키만 사용합니다.

관리되는 장치의 보안 설정을 변경하려면 관리되는 서버의 보안 설정 구성의 내용을 참조하십시오.

절차

관리 서버의 암호 설정을 변경하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리 → 보안**을 클릭하십시오.

단계 2. 보안 통신에 사용할 다음 암호 모드 중 하나를 선택하십시오.

- **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(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 NIST SP 800-131A 준수 구현의 내용을 참조하십시오.

단계 3. 다른 서버(LDAP 서버 등)에 대한 클라이언트 연결에 사용할 최소 TLS 프로토콜 버전을 선택하십시오. 다음 옵션을 선택할 수 있습니다.

- TLS1.2. TLS v1.2 암호화 프로토콜을 적용합니다.
- TLS1.3. TLS v1.3 암호화 프로토콜을 적용합니다.

단계 4. 서버트 연결(예, 웹 서버)에 사용할 최소 TLS 프로토콜 버전을 선택하십시오. 다음 옵션을 선택할 수 있습니다.

- TLS1.2. TLS v1.2 암호화 프로토콜을 적용합니다.
- TLS1.3. TLS v1.3 암호화 프로토콜을 적용합니다.

단계 5. 최소 TLS 모드는 XClarity Administrator 운영 체제 배포 및 OS 장치 드라이버 업데이트에 사용할 최소 TLS 프로토콜 버전을 선택합니다. 다음 옵션을 선택할 수 있습니다.

- TLS1.2. TLS v1.2 암호화 프로토콜을 적용합니다.
- TLS1.3. TLS v1.3 암호화 프로토콜을 적용합니다.

참고: 선택한 암호화 알고리즘이나 강력한 암호화 알고리즘을 지원하는 설치 프로세스를 갖춘 운영 체제만 XClarity Administrator를 통해 배포되고 업데이트될 수 있습니다.

단계 6. 루트 CA 인증서, 서버 인증서 및 외부 서명 인증서의 CSR을 포함하여 인증서의 모든 부분에 사용할 암호화 키 길이 및 해시 알고리즘을 선택하십시오.

- RSA 2048비트/SHA-256(기본)

  이 모드는 관리되는 장치가 호환성, NIST SP 800-131A 또는 표준 보안 모드일 때 사용 가능합니다. 이 모드는 하나 이상의 관리되는 장치가 Enterprise Strict **보안** 모드일 경우 사용 *불가합니다*.
- RSA 3072비트/SHA-384

  이 모드는 관리되는 장치가 Enterprise Strict **보안** 모드인 경우에 필요합니다.

  중요: XCC2가 있는 서버만 RSA-3072/SHA-384 인증서 서명을 지원합니다. XClarity Administrator를 RSA-3072/SHA-384 기반 인증서로 구성한 후에는 비 XCC2 장치가 관리되지 않습니다. 비 XCC2 장치를 관리하려면 별도의 XClarity Administrator 인스턴스가 필요합니다.

단계 7. **적용**을 클릭하십시오.

단계 8. XClarity Administrator를 다시 시작하십시오(XClarity Administrator 다시 시작 참조).

단계 9. 암호화 키 길이를 변경한 경우에는 올바른 키 길이 및 해시 알고리즘을 사용하여 인증 기관 루트 인증서를 다시 생성하십시오(Lenovo XClarity Administrator 자체 서명된 서버 인증서 다시 생성 또는 복원 또는 Lenovo XClarity Administrator에 사용자 지정된 서버 인증서 배포 참조).

완료한 후에

관리되는 장치에 대해 서버 인증서를 신뢰할 수 없다는 경고를 수신하는 경우 신뢰할 수 없는 서버 인증서 해결의 내용을 참조하십시오.

관리되는 서버의 보안 설정 구성

관리되는 서버의 SSL/TLS 버전 및 암호 설정을 구성할 수 있습니다.

이 작업 정보

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

절차

특정 관리되는 서버의 보안 설정을 변경하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴에서 **하드웨어** → **서버**를 클릭하십시오. 모든 관리되는 서버의 표 형식 보기와 함께 서버 페이지가 표시됩니다.

단계 2. 하나 이상의 서버를 선택하십시오.

단계 3. 보안 모드를 구성합니다.

1. **모든 작업 → 보안 → 시스템 보안 모드 설정**을 클릭하여 시스템 보안 모드 설정 대화 상자를 표시하십시오.

   대화 상자에는 각 모드로 설정할 수 있는 서버 수가 나열됩니다. 각 번호 위로 커서를 가져가면 해당 서버 이름 목록이 있는 팝업이 표시됩니다.

2. 보안 모드를 선택합니다. 이는 다음 값 중 하나입니다.

   - **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.

3. **적용**을 클릭하십시오.

단계 4. 최소 TLS 버전을 구성합니다.

1. **모든 작업 → 보안 → System TLS 버전 설정**을 클릭하여 System TLS 버전 설정 대화 상자를 표시하십시오.

2. 다른 서버에 대한 클라이언트 연결(예: LDAP 서버에 대한 LDAP 클라이언트 연결)에 사용할 최소 TLS 프로토콜 버전을 선택합니다. 값은 이 설정을 지원하는 선택된 장치에서 구성됩니다. 다음 옵션을 선택할 수 있습니다.
   - TLS1.2. TLS v1.2 암호화 프로토콜을 적용합니다.
   - TLS1.3. TLS v1.3 암호화 프로토콜을 적용합니다.

   참고: System x 및 CMM 장치는 TLS v1.2만 지원합니다.
3. **적용**을 클릭하십시오.

보안 인증서 작업

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.

시작하기 전에

이 섹션은 SSL 표준 및 SSL 인증서의 정의 및 관리 방법을 포함하여 이에 대한 기본적인 지식이 있는 관리자를 대상으로 합니다. 공개 키 인증서에 대한 일반적인 정보는 Wikipedia의 X.509 웹 페이지 및 인터넷 X.509 공개 키 인프라 인증서 및 CRL(인증서 해지 목록) 프로필(RFC5280) 웹 페이지에서 확인하십시오.

이 작업 정보

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.

XClarity Administrator에서는 수신 SSL/TLS 연결을 수락하는 몇 가지 서비스를 제공합니다. 관리되는 장치 또는 웹 브라우저와 같은 클라이언트가 이러한 서비스 중 하나에 연결하면 XClarity Administrator은(는) 연결을 시도하는 클라이언트가 식별할 수 있도록 *서버 인증서*를 제공합니다. 클라이언트는 신뢰하는 인증서 목록을 유지 관리해야 합니다. XClarity Administrator의 서버 인증서가 클라이언트 목록에 포함되어 있지 않으면 클라이언트는 XClarity Administrator와의 연결을 끊어 보안에 민감한 정보를 신뢰할 수 없는 출처와 교환하지 않도록 합니다.

XClarity Administrator는 관리 장치 및 외부 서비스와 통신할 때 클라이언트의 역할을 합니다. XClarity Administrator이(가) 장치 또는 외부 서비스에 연결하면 장치 또는 외부 서비스는 XClarity Administrator에서 식별할 수 있도록 서버 인증서를 제공합니다. XClarity Administrator은(는) 신뢰할 수 있는 인증서 목록을 유지 관리합니다. 관리되는 장치 또는 외부 서비스에서 제공하는 *신뢰할 수 있는 인증서*가 나열되지 않으면 XClarity Administrator는 관리되는 장치 또는 외부 서비스와의 연결을 끊어 보안에 민감한 정보를 신뢰할 수 없는 출처와 교환하지 않도록 합니다.

다음 인증서 범주는 XClarity Administrator 서비스에서 사용되며 여기에 연결하는 모든 클라이언트가 신뢰할 수 있어야 합니다.

- **서버 인증서**. 최초 부팅 중에 고유 키 및 자체 서명된 인증서가 생성됩니다. 이러한 인증서는 기본 루트 인증 기관으로 사용되며 인증 기관 페이지의 XClarity Administrator 보안 설정에서 관리할 수 있습니다. 키가 유출된 경우 또는 조직에 모든 인증서를 주기적으로 교체해야 한다는 정책이 있는 경우가 아니라면 이 루트 인증서를 다시 생성하지 않아도 됩니다(Lenovo XClarity Administrator 자체 서명된 서버 인증서 다시 생성 또는 복원 참고).

  또한 초기 설정 중에 별도의 키가 생성되고 내부 인증 기관에서 서명하는 서버 인증서가 만들어집니다. 이 인정서는 기본 XClarity Administrator 서버 인증서로 사용됩니다. 인증서에 서버의 올바른 주소가 포함될 수 있도록 XClarity Administrator에서 네트워킹 주소(IP 또는 DNS 주소)가 변경되었음을 감지할 때마다 자동으로 다시 생성됩니다. 필요 시 사용자 지정 및 생성할 수 있습니다(Lenovo XClarity Administrator 자체 서명된 서버 인증서 다시 생성 또는 복원 참조).

  CSR(인증서 서명 요청)을 생성하고, 개인 또는 상업용 인증서 루트 인증 기관에서 CSR에 서명하도록 한 후, 전체 인증서 체인을 XClarity Administrator(으)로 가져와서 기본 자체 서명된 서버 인증서 대신 외부 서명된 서버 인증서를 사용하도록 선택할 수 있습니다(Lenovo XClarity Administrator에 사용자 지정된 서버 인증서 배포 참고).

  기본 자체 서명된 서버 인증서를 사용하도록 선택하는 경우 웹 브라우저에 신뢰하는 루트 기관으로 서버 인증서를 가져와 브라우저에서 인증서 오류 메시지가 표시되지 않도록 하는 것이 좋습니다(웹 브라우저에 인증 기관 인증서 가져오기 참고).
- **OS 배포 인증서**. 운영 체제 배포 서비스가 별도의 인증서를 사용하여 운영 체제 설치 프로그램이 운영 체제 설치 프로세스 중에 배포 서비스에 안전하게 연결하도록 할 수 있습니다. 키가 유출된 경우 관리 서버를 다시 시작하여 다시 생성할 수 있습니다.

다음 인증서 범주(신뢰 저장소)는 XClarity Administrator 클라이언트가 사용합니다.

- **신뢰할 수 있는 인증서**.

  이 신뢰 저장소는 XClarity Administrator이(가) 클라이언트 역할을 할 때 로컬 리소스에 대한 보안 연결을 설정하는 데 사용되는 인증서를 관리합니다. 로컬 리소스의 예로는 관리되는 장치, 이벤트 전달 시 로컬 소프트웨어 및 외부 LDAP 서버가 있습니다.
- **외부 서비스 인증서**. 이 신뢰 저장소는 XClarity Administrator이(가) 클라이언트 역할을 할 때 외부 서비스와의 보안 연결을 설정하는 데 사용되는 인증서를 관리합니다. 외부 서비스의 예로는 보증 정보를 검색하거나 서비스 티켓을 만드는 데 사용되는 온라인 Lenovo 지원 서비스, 이벤트를 전달할 수 있는 외부 소프트웨어(예: Splunk), iOS 또는 Android 장치에 Lenovo XClarity Mobile 푸시 알림이 사용 설정된 경우 Apple 및 Google 푸시 알림 서버가 있습니다. 여기에는 Digicert 및 Globalsign과 같이 일반적으로 신뢰할 수 있고 잘 알려진 특정 인증 기관 공급자의 루트 인증 기관에서 받은 미리 구성된 신뢰할 수 있는 인증서가 포함됩니다.

  다른 외부 서비스에 연결해야 하는 기능을 사용하기 위해 XClarity Administrator을(를) 구성하는 경우 설명서를 참고하여 이 신뢰 저장소에 인증서를 수동으로 추가해야 하는지 확인하십시오.

  이 신뢰 저장소의 인증서는 기본 신뢰할 수 있는 인증서 신뢰 저장소에 추가하지 않는 한 다른 서비스(예: LDAP)에 대한 연결을 설정할 때 신뢰하지 않습니다. 이 신뢰 저장소에서 인증서를 제거하면 이러한 서비스가 성공적으로 작동하지 않습니다.

XClarity Administrator은(는) RSA-3072/SHA-384, RSA-2048/SHA-256 및 ECDSA p256/SHA-256 인증서 서명을 지원합니다. 구성에 따라 SHA-1 이상 또는 SHA 해시와 같은 다른 알고리즘도 지원될 수 있습니다. XClarity Administrator에서 선택된 암호화 모드(관리 서버의 암호화 설정 구성 참조), 관리되는 서버에 선택된 보안 설정(관리되는 서버의 보안 설정 구성), 사용자 환경의 다른 소프트웨어 및 장치의 기능을 고려하십시오. 일부 타원 곡선(p256 포함)을 기반으로 하지만 모든 타원 곡선은 아닌 ECDSA 인증서는 신뢰할 수 있는 인증서 페이지와 XClarity Administrator 인증서의 서명 체인에서 지원되지만 현재 XClarity Administrator 서버 인증서에서 사용하도록 지원되지는 *않습니다*.

참고: XClarity Administrator는 Strict 모드에서 XCC2가 있는 서버에 RSA- 3072/SHA-384 인증서 서명을 사용합니다.

사용자 지정되고 외부 서명된 서버 인증서 설치

개인 또는 상업용 인증 기관(CA)가 서명한 서버 인증서를 사용할 수 있습니다.

시작하기 전에

루트 인증 기관이 조직에서 생성되었으며 조직 내에서 인증서 서명에 사용되거나 일반적으로 신뢰할 수 있고 알려진 인증 기관인지 확인합니다(신뢰할 수 있는 인증 기관 웹 페이지 목록 참고).

루트 CA 인증서의 키 및 서명에 대한 알고리즘이 지원되는지 확인합니다. RSA-3072/SHA-384 및 RSA-2048/SHA-256 서명만 지원됩니다. RSA-PSS 서명은 현재 지원되지 않습니다.

모든 관리 장치에는 관리 장치 간의 연결에 영향을 줄 수 있는 작업을 시작하기 전에 최신 펌웨어가 설치되어 있어야 합니다. 관리되는 장치에서 펌웨어를 업그레이드하려면 관리 장치에서 펌웨어 업데이트의 내용을 참조하십시오.

하드웨어를 클릭한 다음 장치 유형(섀시 또는 서버)을 클릭하여 XClarity Administrator가 모든 관리 장치와 성공적으로 통신하고 있는지 확인하십시오. 페이지가 해당 유형의 모든 관리 장치 표 보기와 함께 표시됩니다. 상태가 "오프라인"인 장치가 있는 경우 관리 서버와 장치 사이에 네트워크 연결이 작동하고 있는지 확인하고 필요한 경우 신뢰할 수 없는 서버 인증서를 해결하십시오(신뢰할 수 없는 서버 인증서 해결 참조).

이 작업 정보

XClarity Administrator 또는 베이스보드 관리 컨트롤러나 CMM에 사용자 지정되고 외부에서 서명된 서버 인증서를 설치하는 경우 전체 CA 서명 체인이 포함된 인증서 번들을 제공해야 합니다.

XClarity Administrator가 관리하지 않는 섀시 또는 서버에 사용자 지정 서버 인증서를 설치하는 경우 CMM의 모든 관리 컨트롤러에 설치하기 전에 CMM에 인증서 번들을 설치하십시오.

사용자 지정 서버 인증서를 관리 섀시에 설치하는 경우 먼저 CA 서명 체인을 XClarity Administrator 신뢰 저장소에 추가하고 모든 관리 컨트롤러 및 CMM에 서버 인증서를 설치한 다음 서버 인증서를 XClarity Administrator에 업로드하십시오. 모든 루트 CA 인증서를 신뢰하거나 추가하여 쉽게 우회할 수 있지만, 모든 관리되는 장치의 모든 인증서 체인이 해당하는 것은 아닙니다. 가져온 인증서의 수는 루트 CA 인증서의 수(루트 CA 인증서 + 모든 중간 CA 인증서)와 같아야 합니다. 자세한 정보는 관리 장치에 사용자 지정된 서버 인증서 배포의 내용을 참조하십시오.

CA 루트 인증서 및 모든 중간 인증서를 XClarity Administrator 신뢰 저장소에 한 번에 추가해야 합니다. 순서는 상관이 없습니다. 각 인증서는 한 번 설치해야 하기 때문에 모든 장치가 동일한 CA 및 중간 인증서를 사용하는 경우 CA 및 각 중간 인증서는 XClarity Administrator 신뢰 저장소에 한 번에 설치되어야 합니다. 하나 이상의 CA 또는 중간 CA를 사용하는 경우 관리 장치의 서명 체인에 사용되는 각 고유 CA 루트 인증서 또는 중간 인증서를 다음 단계에 따라 가져옵니다.

팁: 새 서버 인증서가 신뢰할 수 있는 타사의 서명을 받지 않은 경우 다음에 XClarity Administrator에 연결할 때 브라우저에는 보안 메시지와 새 인증서를 브라우저에 허용하는 대화 상자가 표시됩니다. 보안 메시지를 방지하려면 다운로드한 서버 인증서를 웹 브라우저의 신뢰할 수 있는 인증서 목록에 가져올 수 있습니다. 서버 인증서 가져오기에 대한 자세한 정보는 웹 브라우저에 인증 기관 인증서 가져오기의 내용을 참조하십시오.

Lenovo XClarity Administrator에 사용자 지정된 서버 인증서 배포

사용자 조직의 인증 기관 또는 타사 인증 기관의 서명을 받을 인증서 서명 요청(CSR)을 생성할 수 있습니다. CSR은 전체 인증서 체인을 가져와 고유 기본 내부 서명된 인증서 대신에 사용할 수 있는 전체 인증서를 만듭니다.

시작하기 전에

인증서 세부 정보에 다음 요구 사항이 포함되어 있는지 확인합니다.

- 키 사용은 다음을 포함해야 합니다.
  - 키 계약
  - 디지털 서명

  - 키 암호화
- 향상된 키 사용은 다음을 포함해야 합니다.
  - 서버 인증(1.3.6.1.5.5.7.3.1)
  - 클라이언트 인증(1.3.6.1.5.5.7.3.2)

이 작업 정보

주의: NIST SP 800-131A이(가) 사용 설정되어 있으며(NIST SP 800-131A 준수 구현 참조) NIST에서 사용자 지정 또는 외부 서명된 인증서를 사용 중이거나 사용할 계획인 경우 체인의 모든 인증서는 SHA-256 해시 기능을 기반으로 해야 합니다.

서버 인증서가 업로드되면 XClarity Administrator는 새 CA 인증서를 모든 관리되는 장치에 프로비저닝하도록 시도합니다. 프로비저닝 프로세스가 성공하면 XClarity Administrator가 새 서버 인증서를 즉시 사용하기 시작합니다. 프로세스가 실패하면 새로 가져온 서버 인증서를 적용하기 전에 수동으로 문제를 해결하도록 지시하는 오류 메시지가 제공됩니다. 오류가 수정된 후 이전에 업로드한 인증서의 설치를 완료합니다.

참고: XClarity Administrator가 이미 동일한 루트 기관이 서명한 인증서를 사용하고 있는 경우 CA는 장치에 보낼 필요가 없고 XClarity Administrator가 즉시 인증서를 사용하기 시작합니다.

XClarity Administrator v1.1.0 이전에 인증서를 업로드한 후 웹 서버가 다시 시작되고 자동으로 모든 브라우저 세션을 종료했습니다. XClarity Administrator v1.1.1 이상은 기존 세션을 종료하지 않고 새 인증서를 사용하기 시작합니다. 모든 새 세션은 새 인증서를 사용하여 설정됩니다. 사용 중인 새 인증서를 보려면 웹 브라우저를 다시 시작하십시오.

절차

사용자 지정 외부 서명된 서버 인증서를 생성하여 Lenovo XClarity Administrator에 배포하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator에 대한 인증서 서명 요청(CSR)을 만들어 다운로드하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

b. 인증서 관리 섹션의 **서버 인증서**를 클릭하여 서버 인증서 페이지를 표시하십시오.

c. **인증서 서명 요청(CSR) 생성** 탭을 클릭하십시오.

d. 요청에 대한 필드를 채우십시오.
   - 국가/지역
   - 주/도
   - 시/군
   - 조직
   - 조직 단위(옵션)
   - 일반 이름

   주의: XClarity Administrator가 관리 장치에 연결하는 데 사용하는 IP 주소 또는 호스트 이름과 일치하는 일반 이름을 선택하십시오. 올바른 값을 선택하지 않으면 연결이 신뢰할 수 없게 될 수 있습니다.

e. CSR이 생성 될 때 X.509 "subjectAltName" 확장자에 추가되는 SAN(Subject Alternative Name)을 사용자 정의하십시오.

   기본적으로 XClarity AdministratorXClarity Administrator 게스트 운영 체제의 네트워크 인터페이스에 의해 검색되는 IP 주소 및 호스트 이름을 기반으로 CSR에 대한 SAN(Subject Alternative Name)을 자동으로 정의합니다. 이러한 SAN 값을 사용자 정의, 삭제 또는 추가할 수 있습니다.

   선택한 유형에 대해 지정한 이름이 유효해야 합니다.

- directoryName(예, cn=lxca-example,ou=dcg,dc=company,dc=com)
- dNSName(예, lxca-example.dcg.company.com)
- ipAddress(예, 192.0.2.0)
- registeredID(예, 1.2.3.4.55.6.5.99)
- rfc822Name(예, example@company.com)
- uniformResourceIdentifier(예, https://lxca-dev.dcg.company.com/example)

참고: 다음 단계에서 CSR을 생성한 후에만 표에 나열된 모든 SAN을 유효성 검사, 저장 및 CSR에 추가할 수 있습니다.

f. **CSR 파일 생성**을 클릭하십시오. 서버 인증서는 인증서 서명 요청 대화 상자에 표시됩니다.

g. **파일에 저장**을 클릭하여 서버 인증서를 호스트 서버에 저장하십시오.

단계 2. CSR을 신뢰할 수 있는 인증 기관(CA)에 제공하십시오. CA는 CSR에 서명하고 서버 인증서로 응답합니다.

단계 3. 외부 서명된 서버 인증서를XClarity Administrator에 업로드하십시오. 인증서 컨텐츠는 CA의 루트 인증서, 모든 중간 인증서 및 서버 인증서가 포함된 번들이어야 합니다.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

b. 인증서 관리 섹션의 **서버 인증서**를 클릭하십시오.

c. **인증서 업로드** 탭을 클릭하십시오.

d. **인증서 업로드**를 클릭하여 인증서 업로드 대화 상자를 표시하십시오.

e. 인증서 번들 파일을 PEM, DER 또는 PKCS7 형식으로 지정하거나 인증서 번들을 PEM 형식으로 붙여넣으십시오.

f. **업로드**를 클릭하여 서버 인증서를 업로드하고 인증서를 XClarity Administrator 신뢰 저장소에 저장하십시오.

관리 장치에 사용자 지정된 서버 인증서 배포

해당 장치에 대한 CMM 및 관리 컨트롤러로 외부 서명된 인증서 번들을 업로드 및 설치하여 사용자 지정된 서버 인증서를 관리 장치에 배포할 수 있습니다.

시작하기 전에

모든 관리 장치에 최신 펌웨어가 설치되어 있어야 합니다(관리 장치에서 펌웨어 업데이트 참조).

사용자 지정 인증서에 대한 인증서 서명 요청(CSR)을 생성할 때 장치를 식별하는 데 사용되는 IP 주소 또는 호스트 이름과 일치하는 일반 이름을 선택해야 합니다. 올바른 값을 선택하지 않으면 연결이 신뢰할 수 없게 될 수 있습니다.

최종 서버 인증서에서 전체 인증서 트러스트 체인을 확인하는 데 사용할 수 있는 신뢰할 수 있는 CA의 루트(기본) 인증서로 전체 서명 체인이 포함되는 인증서 번들을 획득해야 합니다.

관리 장치가 "오프라인"인 동안에는 Lenovo XClarity Administrator 서버 인증서를 변경하지 마십시오. Lenovo XClarity Administrator를 수정하기 전에 연결을 수리해야 하며 그렇게 하지 않으면 연결 문제 수리에 추가 단계가 필요할 수 있습니다(신뢰할 수 없는 서버 인증서 해결 참조).

이 작업 정보

이 섹션에는 Lenovo XClarity Administrator와 관리 장치 사이에 성공적인 통신이 지속되도록 하기 위한 권장 사항이 포함되어 있습니다. CSR을 생성하고 서명된 인증서를 가져오는 방법에 대한 자세한 지침은 장치 설명서를 참조하십시오.

Lenovo XClarity Administrator가 하나 이상의 섀시, 랙 서버 및 타워 서버를 관리하고 있는 경우 기본 Lenovo XClarity Administrator 내부 서명된 인증서는 현재 Lenovo XClarity Administrator 및 관리 장치에 설치되고 사용자 지정 서버 인증서를 배포할 수 있습니다.

Lenovo XClarity Administrator로 장치 관리를 시도하기 *전*에 장치에 외부 서명된 서버 인증서가 설치되는 경우 추가 단계가 필요하지 않습니다. Lenovo XClarity Administrator 관리로 관리되는 장치에 사용자 지정 서버 인증서를 배포하려면 다음 단계 중 하나를 수행하여 관리 서버와 관리 장치 사이에 연결이 계속되도록 해야 합니다.

절차

다음 옵션 중 하나를 완료하여 사용자 지정 외부 서명된 서버 인증서를 관리 섀시 또는 서버에 배포하십시오.

- Lenovo XClarity Administrator가 동일한 인증 기관에서 관리 장치로 서명된 인증서를 사용하는 경우 관리 장치에 인증서를 설치하기 *전*에 Lenovo XClarity Administrator에 사용자 지정된 서버 인증서 배포의 단계를 수행하십시오. 동일한 CA에서 Lenovo XClarity Administrator 인증서를 먼저 설치하면 인증서 체인이 Lenovo XClarity Administrator 신뢰 저장소에 있고 Lenovo XClarity Administrator가 외부 서명된 인증서를 거기에 설치한 후 장치를 신뢰할 수 있게 됩니다.
- CA 서명 체인의 외부 서명된 인증서를 Lenovo XClarity Administrator 신뢰 저장소에 추가하십시오.

  CA 루트 인증서 및 모든 중간 인증서를 Lenovo XClarity Administrator 신뢰 저장소에 한 번에 추가해야 합니다. 순서는 상관이 없습니다. 각 인증서는 한 번 설치해야 하기 때문에 모든 장치가 동일한 CA 및 중간 인증서를 사용하는 경우 CA 및 각 중간 인증서는 Lenovo XClarity Administrator 신뢰 저장소에 한 번에 설치되어야 합니다. 하나 이상의 CA 또는 중간 CA를 사용하는 경우 관리 장치의 서명 체인에 사용되는 각 고유 CA 루트 인증서 또는 중간 인증서를 다음 단계에 따라 가져옵니다.

  참고: 이러한 단계에서는 최종, CA 외 서버 인증서를 추가하지 마십시오.

  번들의 각 인증서에 대해 다음 단계를 수행하십시오.

  1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.
  2. 왼쪽 탐색의 인증서 관리에서 **신뢰할 수 있는 인증서**를 클릭하십시오.
  3. **만들기** 아이콘( )을 클릭하여 인증서 추가 대화 상자를 표시하십시오.
  4. 인증서 파일을 PEM 또는 DER 형식으로 지정하거나 인증서를 PEM 형식으로 붙여넣으십시오.
  5. 인증서를 만들려면 **만들기**를 클릭하십시오.

  CA 서명 체인이 설치된 후 Lenovo XClarity Administrator는 외부 서명된 서버 인증서가 설치된 CMM 및 관리 컨트롤러의 CIM 서버 연결을 신뢰합니다.
- 외부 서명된 인증서를 관리 장치에 가져오십시오.

  참고: 필요한 인증서가 Lenovo XClarity Administrator 신뢰 저장소에 없는 경우 Lenovo XClarity Administrator와 관리 장치 간에 연결이 끊어집니다. 연결을 수리하려면 신뢰할 수 없는 서버 인증서 해결의 단계를 수행하십시오.

  중요: 이 옵션으로 일시적으로 연결이 끊어질 수 있으므로 이전 옵션 중 하나를 권장합니다.

Lenovo XClarity Administrator 자체 서명된 서버 인증서 다시 생성 또는 복원

XClarity Administrator에서 현재 사용자 지정 외부 서명된 서버 인증서를 사용하는 경우 새 인증 기관 또는 서버 인증서를 생성하여 현재 자체 서명된 인증서를 교체하거나 Lenovo XClarity Administrator에서 생성한 인증서를 복구할 수 있습니다. 그러면 XClarity Administrator의 인증, HTTPS 및 CIM 서버가 자체 서명된 새로운 서버 인증서를 사용합니다. 또한 모든 관리 장치에 자동으로 프로비저닝됩니다.

시작하기 전에

XClarity Administrator 인증서를 다시 생성하거나 업로드하면 XClarity Administrator이(가) 다시 시작됩니다.

새 CA 인증서가 생성되는 경우 새 CA 인증서는 각 CMM의 신뢰 저장소와 모든 관리 섀시, 랙 서버 및 타워 서버의 베이스보드 관리 컨트롤러에 자동으로 배포되어 시노리할 수 있는 인증 서버 연결을 유지합니다. CA 루트 인증서를 배포하는 동안 오류가 발생하는 경우 인증 기관 페이지에서 다운로드하여 새 서버 인증서를 생성하기 전에 성공적으로 프로비저닝되지 않은 관리 장치의 신뢰 저장소에 수동으로 가져오십시오.

CA 인증서를 다시 생성하려는 계획인 경우 단시간 내에 CA를 다시 생성할 시간을 예약하고 프로비저닝 오류를 해결하고 서버 인증서를 다시 생성하십시오.

새 CA 루트 인증서를 생성한 후 통신 오류가 발생하거나, 서버 인증서가 다시 생성되고 서명될 때까지 장치에 로그인하지 못할 수 있습니다.

중요: XClarity Administrator v1.1.1 이전의 경우 각 CMM 및 관리 컨트롤러의 신뢰 저장소에 CA 루트 인증서를 가져와야 합니다. CA 루트 인증서 가져오기에 대한 자세한 정보는 CMM 및 관리 컨트롤러 설명서를 참조하십시오.

절차

XClarity Administrator에서 자체 서명된 서버 인증서를 복원하려면 다음 단계를 완료하십시오.

참고: 현재 XClarity Administrator에서 사용 중인 서버 인증서는 자체 서명 또는 외부 서명과는 무관하게 새 서버 인증서가 다시 생성되고 서명될 때까지 계속 사용됩니다.

단계 1. **옵션:** 새 CA 루트 인증서를 생성하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

b. 인증서 관리 섹션의 **인증 기관**을 클릭하십시오.

c. **인증 기관 루트 인증서 다시 생성**을 클릭하십시오.

CA 키와 인증서가 성공적으로 다시 생성되면 해당 인증서를 모든 CMM 및 관리 컨트롤러에 LDAP 신뢰할 수 있는 인증서로 프로비저닝하기 위한 작업 상태가 표시된 대화 상자가 표시됩니다(Converged, NeXtScale 및 System x 서버의 경우). 이 대화 상자와 작업 모니터링 페이지에는 해당 각 프로비저닝 작업의 성공 또는 실패가 표시됩니다.

프로비저닝 작업 중 실패한 것이 있으면 다음 단계를 완료하여 CA 루트 인증서를 다운로드한 다음 루트 인증서를 작업이 실패한 장치에서 신뢰할 수 있는 LDAP 인증서로 가져오십시오.

단계 2. **옵션:** CA 루트 인증서를 호스트 시스템에 다운로드하고 웹 브라우저에 가져오십시오.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

b. 인증서 관리 섹션의 **인증 기관**을 클릭하십시오.

c. **인증 기관 루트 인증서 다운로드**를 클릭하십시오. 현재 CA 루트 인증서는 인증 기관 루트 인증서 대화 상자에 표시됩니다.

d. **파일에 저장**을 클릭하여 CA 루트 인증서를 호스트 시스템에 저장하십시오.

e. 인증서를 신뢰할 수 있는 루트 기관으로 가져오려면 사용자의 웹 브라우저와 XClarity Administrator에 액세스할 다른 사용자의 웹 브라우저에 대한 지침을 따르십시오.

단계 3. 새 서버 인증서를 다시 생성하고 새 CA 루트 인증서로 인증서에 서명하십시오.

a. 보안 페이지에서 인증서 관리 섹션의 **서버 인증서**를 클릭하십시오.

b. **서버 인증서 다시 생성** 탭을 클릭하십시오.

c. 서버 인증서 다시 생성 페이지의 필드를 작성하십시오.
   - 국가/지역

- 주/도
- 시/군
- 조직
- 조직 단위
- 일반 이름
- 유효하지 않은 이전 날짜
- 유효하지 않은 이전 시간
- 유효하지 않은 이후 날짜
- 유효하지 않은 이후 시간

d. **인증서 다시 생성**을 클릭하십시오.

e. 관리되는 CMM 및 관리 컨트롤러(Converged, NeXtScale, ThinkSystem 및 System x 서버의 경우)에서 자체 서명된 인증서를 다시 생성하는 경우 각 장치에서 인증서를 다시 생성한 후 새 장치 인증서를 XClarity Administrator 신뢰 저장소로 가져오십시오(신뢰할 수 없는 서버 인증서 해결 참조). 또는 장치에서 인증서를 수동으로 다운로드하여 신뢰할 수 있는 인증서 페이지의 XClarity Administrator에 가져오십시오.

XClarity Administrator v1.1.0 이전의 경우 웹 서버가 다시 시작되고 인증서를 다시 생성한 후 자동으로 모든 브라우저 세션이 종료됩니다. XClarity Administrator v1.1.1 이후의 경우 XClarity Administrator는 기존 세션을 종료하지 않고 새 인증서를 사용하기 시작합니다. 새 세션은 새 인증서를 사용하여 설정됩니다. 사용 중인 새 인증서를 보려면 웹 브라우저를 다시 시작하십시오.

단계 4. 관리되는 CMM 및 관리 컨트롤러(Converged, NeXtScale, ThinkSystem 및 System x 서버의 경우)에서 자체 서명된 인증서를 다시 생성하는 경우 각 장치에서 인증서를 다시 생성한 후 새 장치 인증서를 XClarity Administrator 신뢰 저장소로 가져오십시오(신뢰할 수 없는 서버 인증서 해결 참조). 또는 장치에서 인증서를 수동으로 다운로드하여 신뢰할 수 있는 인증서 페이지의 XClarity Administrator에 가져오십시오.

신뢰할 수 없는 서버 인증서 해결

관리 장치와의 보안 연결을 설정하는 데 사용되는 서버 인증서는 신뢰할 수 없는 상태가 될 수 있습니다. 문제의 원인이 Lenovo XClarity Administrator 신뢰 저장소에 장치 CA 루트 인증서 또는 장치 자체 서명된 인증서의 하위 레벨 버전이 있기 때문인 경우 XClarity Administrator가 신뢰할 수 없는 서버 인증서를 해결할 수 있습니다.

이 작업 정보

관리 장치가 신뢰할 수 없는 상태가 되면 XClarity Administrator가 해당 장치와의 통신을 방지하여 해당 장치에서 관리 또는 인벤토리 작동을 수행하지 못하게 됩니다.

절차

관리 장치에 대한 신뢰할 수 없는 서버 인증서를 해결하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어**를 클릭한 다음 장치 유형을 클릭하십시오(**섀시**, **서버**, **스토리지** 또는 **스위치**). 페이지가 해당 유형의 모든 관리 장치 표 보기와 함께 표시됩니다.

단계 2. "오프라인" 상태에서 특정 장치를 선택하십시오.

단계 3. **모든 작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하십시오.

단계 4. **인증서 설치**를 클릭하십시오.

XClarity Administrator는 대상 장치에서 현재 인증서를 검색합니다. 해당 인증서가 XClarity Administrator 신뢰 저장소에 있는 해당 장치의 신뢰할 수 있는 인증서와 다른 경우 새 인증서는 XClarity Administrator 신뢰 저장소에 저장되어 해당 장치의 이전 인증서를 재정의합니다.

이렇게 해도 문제가 해결되지 않는 경우 XClarity Administrator와 장치 사이에 네트워크 연결이 작동하고 있는지 확인하십시오.

서버 인증서 다운로드

현재 서버 인증서의 사본을 로컬 시스템에 PEM 또는 DER 형식으로 다운로드할 수 있습니다. 그런 다음 인증서를 웹 브라우저 또는 다른 응용 프로그램(Lenovo XClarity Mobile 또는 Lenovo XClarity Integrator)에 가져올 수 있습니다.

절차

서버 인증서를 다운로드하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

단계 2. 인증서 관리 섹션의 **서버 인증서**를 클릭하십시오. 서버 인증서 페이지가 표시됩니다.

단계 3. **인증서 다운로드** 탭을 클릭하십시오.

단계 4. **인증서 다운로드**를 클릭하십시오.

단계 5. 로컬 시스템에서 서버 인증서를 DER 또는 PEM 파일로 저장하려면 **DER로 저장** 또는 **PEM으로 저장**을 클릭하십시오.

웹 브라우저에 인증 기관 인증서 가져오기

Lenovo XClarity Administrator에 액세스할 때 웹 브라우저에서 보안 경고 메시지를 방지하려면 현재 인증 기관(CA) 인증서 사본을 로컬 시스템에 PEM 또는 DER 형식으로 다운로드한 다음 웹 브라우저의 신뢰할 수 있는 인증서 목록에 인증서를 가져올 수 있습니다.

이 작업 정보

XClarity Administrator은(는) RSA-3072/SHA-384, RSA-2048/SHA-256 및 ECDSA p256/SHA-256 인증서 서명을 지원합니다. 구성에 따라 SHA-1 이상 또는 SHA 해시와 같은 다른 알고리즘도 지원될 수 있습니다. XClarity Administrator에서 선택된 암호화 모드(관리 서버의 암호화 설정 구성 참조), 관리되는 서버에 선택된 보안 설정(관리되는 서버의 보안 설정 구성), 사용자 환경의 다른 소프트웨어 및 장치의 기능을 고려하십시오. 일부 타원 곡선(p256 포함)을 기반으로 하지만 모든 타원 곡선은 아닌 ECDSA 인증서는 신뢰할 수 있는 인증서 페이지와 XClarity Administrator 인증서의 서명 체인에서 지원되지만 현재 XClarity Administrator 서버 인증서에서 사용하도록 지원되지는 *않습니다*.

참고: XClarity Administrator는 Strict 모드에서 XCC2가 있는 서버에 RSA- 3072/SHA-384 인증서 서명을 사용합니다.

절차

서버 인증서를 다운로드하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

단계 2. 인증서 관리 섹션의 **인증 기관**을 클릭하십시오. 인증 기관 페이지가 표시됩니다.

단계 3. **인증 기관 루트 인증서 다운로드**를 클릭하십시오.

단계 4. 로컬 시스템에서 서버 인증서를 DER 또는 PEM 파일로 저장하려면 **DER로 저장** 또는 **PEM으로 저장**을 클릭하십시오.

단계 5. 다운로드한 인증서를 브라우저의 신뢰할 수 있는 루트 기관 인증서 목록에 가져오십시오.

- Firefox:
  1. 브라우저를 열고 **도구 → 옵션 → 고급**을 클릭하십시오.
  2. **인증서** 탭을 클릭하십시오.
  3. **인증서 보기**를 클릭하십시오.

4. **가져오기**를 클릭하고 인증서가 다운로드된 위치를 살펴보십시오.
5. 인증서를 선택하고 **열기**를 클릭하십시오.

- Internet Explorer:
  1. 브라우저를 열고 **도구 → 인터넷 옵션 → 컨텐츠**을 클릭하십시오.
  2. 현재 신뢰할 수 있는 모든 인증서의 목록을 보려면 **인증서**를 클릭하십시오.
  3. 인증서 가져오기 마법사를 표시하려면 **가져오기**를 클릭하십시오.
  4. 인증서를 가져오려면 마법사를 완료하십시오.

인증서 해지 목록 추가 및 교체

*인증서 해지 목록*은 취소되어 더 이상 신뢰할 수 없는 인증서의 목록입니다. 인증서는 CA에서 잘못 발행되었거나 키가 누출, 분실, 도난된 경우 해지될 수 있습니다.

절차

다음 단계를 완료하여 새 인증서 해지 목록을 추가하거나 기존 인증서 해지 목록을 교체하십시오

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

단계 2. 왼쪽 탐색의 인증서 관리에서 **인증서 해지 목록**을 클릭하십시오. 인증서 해지 목록 페이지는 모든 인증서 해지 목록과 함께 표시됩니다.

단계 3. 인증서 해지 목록을 추가하려면 **CLR 추가/교체**를 클릭하고 CRL을 교체하려면 **CLR 추가/교체**를 클릭하십시오.

단계 4. 인증서 해지 목록 파일을 PEM 또는 DER 형식으로 지정하거나 인증서를 PEM 형식으로 붙여넣으십시오.

단계 5. 인증서 해지 목록을 만들려면 **만들기**를 클릭하십시오.

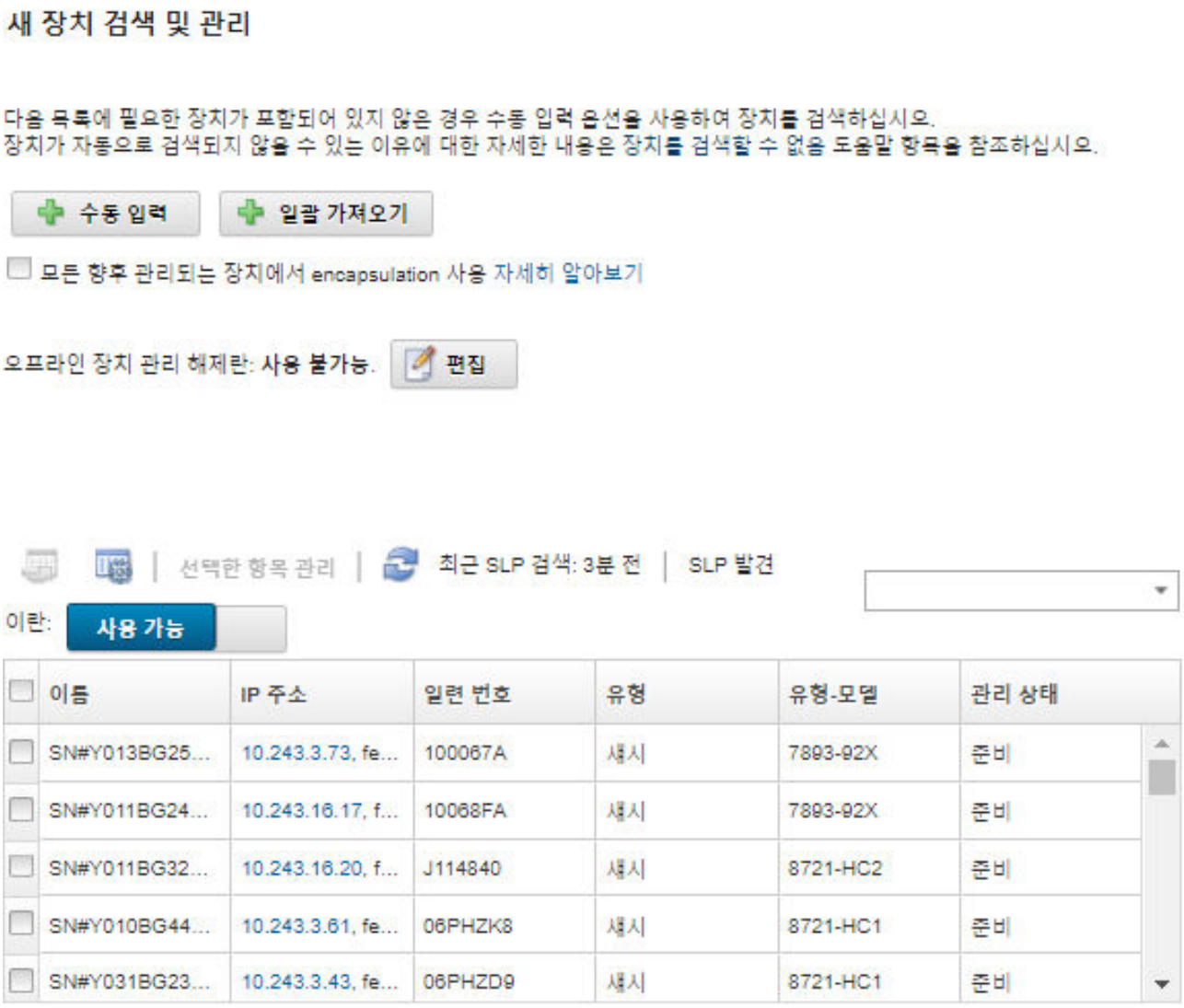
Encapsulation 사용

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.

새 장치 검색 및 관리 페이지의 **모든 향후 관리되는 장치에서 Encapsulation 사용** 선택란을 선택하여 관리 프로세스 중에 모든 장치에 대해 encapsulation을 사용 또는 사용 안 함으로 설정할 수 있습니다. Encapsulation은 기본적으로 사용하지 않습니다.



또한 장치 요약 페이지를 탐색하고 장치를 선택하고 **작업 → Encapsulation 사용** 또는 **작업 → Encapsulation 사용 안 함**을 클릭하여 언제든지 특정 관리되는 장치에 대해 개별적으로 Encapsulation을 사용 또는 사용 안 함으로 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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.

참고: Encapsulation은 스위치, 스토리지 장치 및 Lenovo 이외 섀시 및 서버에에서 지원되지 않습니다.

NIST SP 800-131A 준수 구현

NIST SP 800-131A를 준수해야 하는 경우 Lenovo XClarity Administrator를 사용하여 완벽하게 준수하는 환경을 목표로 작업을 시작할 수 있습니다.

이 작업 정보

미국표준기술연구소(National Institute of Standards and Technology) 특수 출판물 800-131A(NIST SP 800-131A)는 보안 통신을 취급해야 하는 방식을 지정합니다. 표준은 알고리즘을 강화하고 키 길이를 늘려 보안을 개선합니다. NIST SP 800-131A 표준에 따르면 사용자를 표준을 엄격하게 적용하도록 구성해야 합니다.

참고: 다음 Flex System 구성 요소는 현재 NIST SP 800-131A를 지원하지 않습니다. XClarity Administrator 또는 CMM과 준수하지 않는 이러한 구성 요소 간의 통신은 다음과 같습니다.
- Flex System EN4023 10Gb 확장 가능형 스위치
- Flex System EN6131 40Gb 이더넷 스위치
- Flex System FC3171 8Gb SAN 스위치
- Flex System FC5022 16Gb SAN 확장 가능형 스위치
- Flex System IB6131 인피니밴드 스위치

참고: SAML ID 공급자를 인증에 사용하는 경우 XClarity Administrator가 SHA-1을 사용하여 메타데이터에 서명을 합니다. 디지털 서명에 SHA-1 알고리즘을 사용하는 것은 NIST SP 800-131A를 준수하지 않습니다.

절차

NIST SP 800-131A 준수를 구현하려면 다음 단계를 완료하십시오.

단계 1. 장치는 다음 조건을 충족해야 합니다.

- TLS v1.2 프로토콜을 통해 SSL(Secure Sockets Layer)을 사용하십시오.
- 디지털 서명에는 SHA-256 또는 더 강력한 해시 기능, 다른 응용 프로그램에는 SHA-1 또는 더 강력한 해시 기능을 사용하십시오.
- RSA-2048 이상을 사용하거나 224비트 이상인 NIST 승인 Elliptic Curve를 사용합니다.
- 길이가 최소 128비트인 키가 있는 NIST 승인 대칭적 암호화를 사용합니다.
- NIST 승인 무작위 숫자 생성기를 사용합니다.
- 가능한 경우 Diffie-Hellman 또는 Elliptic Curve Diffie-Hellman 키 교환 메커니즘을 지원합니다.

단계 2. Lenovo XClarity Administrator에서 암호 설정을 구성합니다. NIST SP 800-131A 준수와 관련된 다음 두 개의 설정이 있습니다.

- *SSL/TLS 모드*는 보안 통신에 사용될 프로토콜을 지정합니다. XClarity Administrator는 **TLS 1.2 서버 및 클라이언트**의 설정을 지원하여 XClarity Administrator 및 모든 관리 장치에서 TLS 1.2에 암호 프로토콜을 제한합니다.
- 보안 통신을 구현하는 경우 ***암호화 모드***가 사용할 암호화 키 길이를 설정합니다. 암호화 모드를 NIST SP 800-131A로 설정할 수 있습니다. 그러나 일부 운영 체제 설치 프로그램이 제한된 설정을 지원하지 않기 때문에 XClarity Administrator를 통해 일부 운영 체제를 배포하지 못할 수 있습니다. 운영 체제 배포를 지원하려면 운영 체제 배포에 대한 예외를 허용할 수 있습니다.

  암호 설정을 변경하면 XClarity Administrator는 관리되는 모든 장치에 새 설정을 프로비저닝하고 해당 장치에서 새로운 인증서 해결을 시도합니다.

  참고: 변경 사항을 적용하고 손실된 서비스를 복원하기 위해서는 암호 설정이 변경된 후 XClarity Administrator를 수동으로 다시 시작해야 합니다(XClarity Administrator 다시 시작 참조).

  이러한 설정에 대한 자세한 정보는 관리 서버의 암호화 설정 구성의 내용을 참조하십시오.

단계 3. TLS1.2 프로토콜 및 SHA-256 해싱 기능을 지원하는 웹 브라우저를 사용하고 웹 브라우저에서 해당 설정을 사용으로 설정하십시오.

  참고: 사용자 지정 또는 외부 서명된 인증서를 사용 중이거나 사용할 계획인 경우 체인의 모든 인증서는 SHA-256 해시 기능을 기반으로 해야 합니다.

단계 4. 모든 통신에 대한 암호화된 프로토콜을 사용하십시오. XClarity Administrator 관리 장치와의 원격 통신에 Telnet, FTP 및 VNC와 같은 암호화되지 않은 프로토콜을 사용 설정하지 마십시오.

VMware 도구 사용

VMware 도구 패키지는 VMware ESXi 기반 환경에 Lenovo XClarity Administrator를 설치하면 가상 컴퓨터의 게스트 운영 체제에 설치됩니다. 이 패키지는 최적화된 가상 어플라이언스 백업 및 마이그레이션을 지원하는 동시에 응용 프로그램 상태 및 연속성을 보존하는 VMware 도구의 서브세트를 제공합니다.

VMware 도구 사용에 대한 정보는 VMware vSphere Documentation Center의 VMware Tools 구성 유틸리티 사용의 내용을 참조하십시오.

네트워크 액세스 구성

Lenovo XClarity Administrator를 처음 설치할 때 최대 2개의 네트워크 인터페이스를 구성합니다. 또한 그러한 인터페이스 중 운영 체제를 배포하는 데 사용할 것을 지정해야 합니다. 초기 설정 후 이러한 설정을 수정할 수 있습니다.

시작하기 전에

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.

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 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 • 검색 및 관리 • 서버 구성 • 펌웨어 업데이트 • 서비스 데이터 수집 • 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능) • 보증 데이터 검색 • OS 배포 • OS 장치 드라이버 업데이트	없음
분리형 관리 네트워크(OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원 포함)	관리 네트워크 • 검색 및 관리 • 서버 구성 • 펌웨어 업데이트 • 서비스 데이터 수집 • 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능) • 보증 데이터 검색 • OS 배포 • OS 장치 드라이버 업데이트	데이터 네트워크 • 없음
OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원을 포함하는 분리형 관리 네트워크 및 데이터 네트워크	관리 네트워크 • 검색 및 관리 • 서버 구성 • 펌웨어 업데이트 • 서비스 데이터 수집 • 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능) • 보증 데이터 검색	데이터 네트워크 • OS 배포 • OS 장치 드라이버 업데이트
OS 배포 및 OS 장치 드라이버 업데이트에 대한 지원을 포함하지 않는 분리형 관리 네트워크 및 데이터 네트워크	관리 네트워크 • 검색 및 관리 • 서버 구성 • 펌웨어 업데이트 • 서비스 데이터 수집 • 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능) • 보증 데이터 검색	데이터 네트워크 • 없음
관리 네트워크만(OS 배포 및 OS 장치 드라이버 업데이트는 지원되지 않음)	관리 네트워크 • 검색 및 관리 • 서버 구성 • 펌웨어 업데이트 • 서비스 데이터 수집 • 자동 문제점 통지(예, 콜 홈 및 Lenovo 업데이트 기능) • 보증 데이터 검색	없음

IPv6 주소 한계 등 XClarity Administrator 네트워크 인터페이스에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 네트워크 고려사항의 내용을 참조하십시오.

절차

네트워크 액세스를 구성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 바에서 **관리 → 네트워크 액세스**를 클릭하십시오. 현재 네트워크 설정이 표시됩니다.

단계 2. 원하는 경우 **중복 IP 주소 검사** 토글을 클릭하여 동일한 서브넷에서 중복 IP 주소 검사를 사용 설정할 수 있습니다.

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.

단계 3. **네트워크 액세스 편집**을 클릭하여 네트워크 액세스 편집 페이지를 표시하십시오.

단계 4. 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 5. (XClarity Administrator을(를) 가상 어플라이언스로 사용하는 경우만 해당) IP 설정을 수정합니다.

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 XClarity Administrator 온라인 설명서에서 IPv6 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 6. (XClarity Administrator을(를) 가상 어플라이언스로 사용하는 경우만 해당) 원하는 경우 고급 설정을 수정합니다.

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 7. 선택적으로, DNS 및 프록시 설정을 수정하십시오.

XClarity Administrator이(가) 컨테이너로 설정되어 있으면 웹 인터페이스에서 프록시 설정만 수정할 수 있습니다. DNS 설정은 컨테이너에서 정의됩니다.

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(참조).

BMC에서 FQDN/DNS 제거를 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 8. **다시 시작**을 클릭하여 관리 서버를 다시 시작하십시오.

단계 9. **연결 테스트**를 클릭하여 네트워크 설정을 확인하십시오.

날짜 및 시간 설정

Lenovo XClarity Administrator에 사용할 날짜 및 시간을 설정할 수 있습니다.

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.

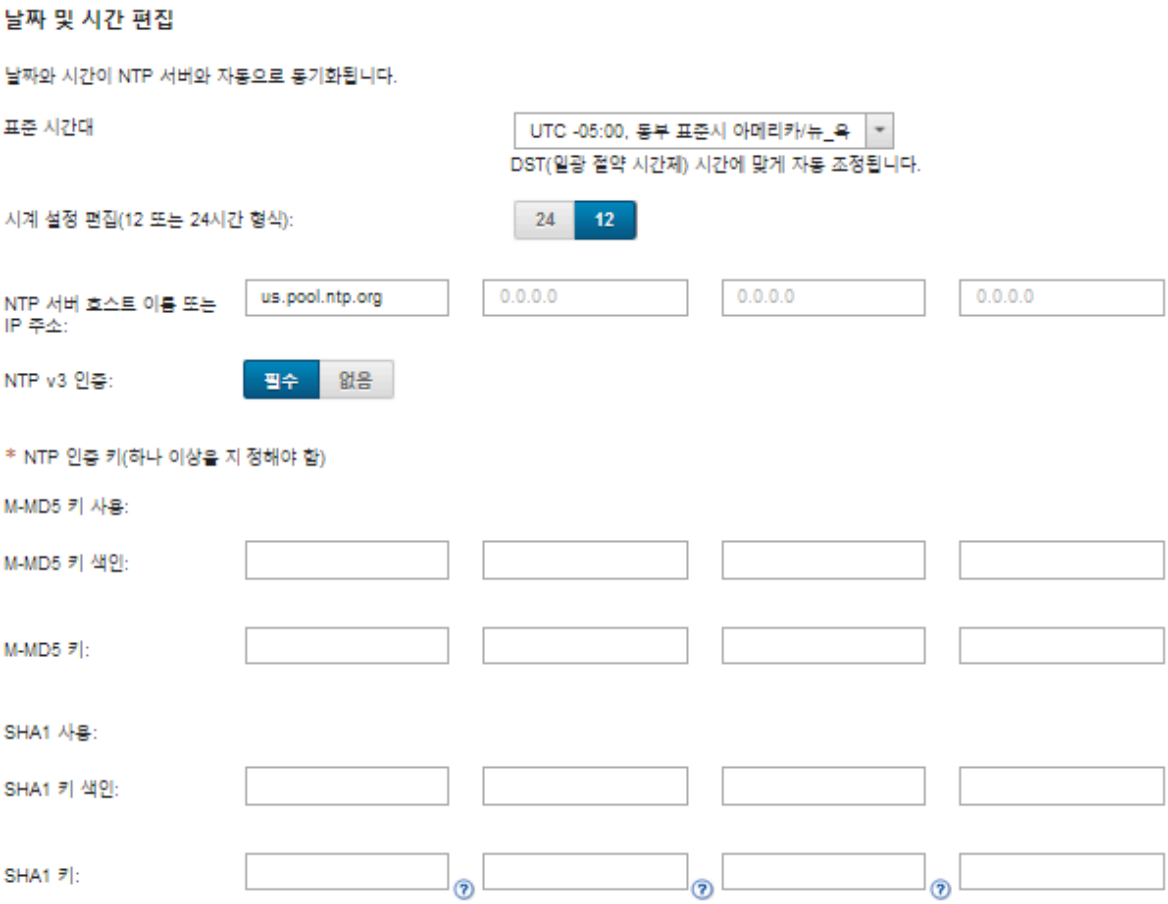
- ESXi의 경우 VMware – 시간 동기화 사용 안 함 웹 페이지의 다음 지시 사항을 참조하십시오.
- Hyper-V의 경우 Hyper-V 관리자에서 XClarity Administrator 가상 컴퓨터를 마우스 오른쪽 단추로 클릭한 다음 **설정**을 클릭하십시오. 대화 상자의 탐색 분할창에서 **관리 > 통합 서비스**를 클릭한 다음 **시간 동기화**를 선택 취소하십시오.

절차

XClarity Administrator에 대한 날짜 및 시간을 설정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 날짜 및 시간**을 클릭하십시오. 날짜 및 시간 페이지가 표시됩니다. 이 페이지에는 XClarity Administrator에 대한 현재 날짜 및 시간이 표시됩니다.

단계 2. 날짜 및 시간 편집 페이지를 표시하려면 **날짜 및 시간 편집**을 클릭하십시오.



단계 3. 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 4. **저장**을 클릭하십시오.

인벤토리 기본 설정 지정

장치 이름을 표시하는 데 사용할 속성을 포함하여 관리되는 장치에 대한 인벤토리 기본 설정을 지정할 수 있습니다.

절차

관리되는 장치의 인벤토리 기본 설정을 지정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 인벤토리 기본 설정**을 클릭하십시오. 인벤토리 기본 설정 페이지가 표시됩니다.

단계 2. Lenovo XClarity Administrator 사용자 인터페이스에서 표시되는 장치 이름에 사용할 속성을 선택하십시오. 다음 속성 중 하나를 선택할 수 있습니다.
- **미리 정의된 순서(기본값)**
- **사용자 정의된 이름**
- **DNS 호스트 이름**
- **호스트 이름**
- **IPv4 주소**
- **일련 번호**

미리 정의된 시퀀스를 선택하면 이전 목록에 있는 속성 순서에 따라 표시되는 장치 이름이 선택됩니다. 예를 들어 장치에 사용자 정의 이름이 있으면 해당 이름이 표시됩니다. 장치에 사용자 정의 이름이 없으면 DNS 호스트 이름이 표시됩니다. 장치에 사용자 정의 이름 또는 DNS 호스트 이름이 없으면 호스트 이름 표시됩니다.

참고: 기본값이 아닌 다른 값을 선택하면 Lenovo XClarity Administrator 사용자 인터페이스에 표시되는 모든 장치의 이름이 선택된 속성으로 변경됩니다. 장치에 할당된 사용자 정의 이름은 변경되지 않습니다.

단계 3. 선택적으로 **사용**을 클릭하여 장치 이름에 선택한 값으로 그리드(테이블)를 정렬하도록 선택하십시오.

단계 4. 랙 번호 매기기 순서 기본 설정(위에서 아래로(예: 1–52) 또는 아래에서 위로(예: 52–1))을 선택하십시오.

참고: 번호 순서 기본 설정을 변경해도 랙에서 장치의 위치는 변경되지 않습니다.

단계 5. **적용**을 클릭하십시오.

완료한 후에

ThinkSystem 또는 ThinkServer 서버의 SSD 수명과 같은 특정 값이 경고 또는 위험 수준을 초과할 때 경고와 이벤트를 발생시키는 임계값을 설정할 수 있습니다(경고 및 이벤트 생성을 위한 임계값 기본 설정 지정 참조).

경고 및 이벤트 생성을 위한 임계값 기본 설정 지정

ThinkSystem 또는 ThinkServer 서버의 SSD 수명과 같은 특정 값이 경고 또는 위험 수준을 초과할 때 경고와 이벤트를 발생시키는 임계값을 설정할 수 있습니다.

절차

서비스 공급자에게 특정 서비스 파일을 전달하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 경고**를 클릭하여 경고 페이지를 표시하십시오.

단계 2. **임계값 설정** 아이콘()을 클릭하여 임계값 설정 대화 상자를 표시하십시오.

단계 3. ThinkSystem 및 ThinkServer 서버에서 SSD의 남은 수명에 대한 경고 및 위험 임계값을 수정하십시오.

SSD의 남은 수명은 공급업체 SMART 카운터를 사용하여 계산됩니다. 기본값은 경고 임계값의 경우 30%이고 위험 임계값의 경우 20%입니다.

단계 4. **사용** 토글을 선택하여 각 임계값에 도달할 때 경고와 이벤트를 생성하도록 하십시오.

단계 5. **적용**을 클릭하십시오.

Lenovo 지원에 대한 자동 문제 알림 설정(콜 홈)

특정 관리되는 장치에서 복구 불가능한 메모리와 같은 특정 서비스 가능 이벤트를 받으면 문제를 해결하기 위해 콜 홈을 사용하여 관리되는 장치의 서비스 데이터를 Lenovo 지원로 자동으로 보내는 서비스 전달자를 만들 수 있습니다. 이 서비스 전달자의 이름은 "기본 콜 홈"입니다.

Lenovo는 보안에 중점을 둡니다. 사용 설정되면 장치가 하드웨어 오류를 보고하거나 사용자가 수동 콜 홈을 시작하도록 선택하는 경우 콜 홈 Lenovo 지원 센터. 일반적으로 Lenovo 지원 센터에 수동으로 업로드하는 서비스 데이터는 TLS 1.2 이상을 사용하여 HTTPS를 통해 자동으로 Lenovo 지원 센터로 전송됩니다. 사용자의 비즈니스 데이터는 절대로 전송되지 않습니다. Lenovo 지원 센터의 서비스 데이터에 대한 액세스는 공인 서비스 담당자로 제한됩니다.

시작하기 전에

주의: Lenovo 지원 센터에 데이터를 전송하기 전에 Lenovo 개인정보 보호정책을/를 수락해야 합니다.

콜 홈을 사용 설정하기 전에 Lenovo XClarity Administrator에서 필요한 모든 포트(콜 홈에 필요한 포트 포함)가 사용 가능한지 확인하십시오. 포트에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

콜 홈에 필요한 인터넷 주소에 연결되어 있는지 확인하십시오. 방화벽에 대한 정보는 XClarity Administrator 온라인 설명서에서 방화벽 및 프록시 서버의 내용을 참조하십시오.

XClarity Administrator이 HTTP 프록시를 통해 인터넷에 액세스하는 경우 프록시 서버가 기본 인증을 사용하도록 구성되었는지와 비종결 프록시(non-terminating proxy)로 설정되었지를 확인하십시오.

프록시 설정에 대한 자세한 정보는 네트워크 액세스 구성XClarity Administrator 온라인 설명서에서 네트워크 액세스 구성의 내용을 참조하십시오.

콜 홈을(를) 구성하면 **기본 Lenovo 콜 홈** 서비스 전달자가 서비스 전달자 페이지에 추가됩니다. 이 전달자를 편집하여 이 전달자와 연결할 장치를 비롯한 추가 설정을 구성할 수 있습니다. 모든 장치는 기본적으로 매치됩니다. 장치를 지정하지 않으면 콜 홈에서 문제 알림을 Lenovo 지원에 전달하지 *않습니다*.

이 작업 정보

서비스 전달자는 서비스 가능한 이벤트가 발생한 경우 서비스 데이터 파일을 보낼 위치 정보를 정의합니다. 최대 50개의 서비스 전달자를 정의할 수 있습니다.

- **콜 홈 서비스 전달자가 구성되지 않은 경우**, 새 서비스 요청 웹 페이지의 지시사항을 따라 수동으로 서비스 티켓을 열고 서비스 파일을 Lenovo 지원 센터로 보낼 수 있습니다. 서비스 파일 수집 및 다운로드에 대한 정보는 XClarity Administrator 온라인 설명서에서 XClarity Administrator 진단 파일 다운로드 및 장치에 대한 진단 파일 수집 및 다운로드의 내용을 참조하십시오.
- **콜 홈 서비스 전달자가 구성되었지만 사용 설정되지 않은 경우**, 언제든지 콜 홈 기능을 사용하여 *수동으로* 서비스 티켓을 열고 서비스 파일을 수집하여 Lenovo 지원 센터로 전송할 수 있습니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 서비스 티켓 열기의 내용을 참조하십시오.
- **콜 홈 서비스 전달자가 구성되고 사용 설정된 경우**, 문제를 해결할 수 있도록 서비스 가능 이벤트가 발생하면 XClarity Administrator가 *자동으로* 서비스 데이터를 수집하고 서비스 티켓을 열어 서비스 파일을 Lenovo 지원 센터로 전송합니다.

  중요: 콜 홈 서비스 전달자를 Lenovo XClarity Administrator에서 사용 설정하는 경우 중복 문제 레코드가 작성되지 않도록 각 관리되는 장치에서 콜 홈이 사용 안 함으로 설정됩니다. XClarity Administrator를 사용한 장치 관리를 중단하려고 하거나 XClarity Administrator에서 콜 홈을 사용 안 함으로 설정하려는 경우, 나중에 개별 장치에 대해 콜 홈을 다시 사용 설정하는 대신 XClarity Administrator의 모든 관리 장치에서 콜 홈을 다시 사용 설정할 수 있습니다. 콜 홈의 서비스 전달자가 비활성화된 경우 모든 관리되는 장치에서 콜 홈을 활성화하는 방법에 대한 정보는 XClarity Administrator에서 모든 관리 장치에서 콜 홈 다시 사용 가능하도록 설정의 내용을 참조하십시오.XCC2가 있는 서버의 경우 XClarity Administrator가 서비스 데이터를 리포지토리의 파일 두 개에 저장합니다.

  - **서비스 파일**. (.zip) 이 파일에는 서비스 정보와 인벤토리가 쉽게 읽을 수 있는 형식으로 포함되어 있습니다. 이 파일은 서비스 가능한 이벤트가 발생할 경우 자동으로 Lenovo 지원 센터로 전송됩니다.
  - **디버그 파일**. (.tzz) 이 파일에는 Lenovo 지원에서 사용할 모든 서비스 정보, 인벤토리 및 디버그 로그가 포함되어 있습니다. 문제를 해결하기 위해 추가 정보가 필요한 경우 이 파일을 Lenovo 지원에 수동으로 보낼 수 있습니다.

  다른 장치의 경우에는 XClarity Administrator가 서비스 데이터(서비스 정보, 인벤토리 및 디버그 로그 포함)를 리포지토리의 단일 서비스 파일에 저장합니다. 이 파일은 서비스 가능한 이벤트가 발생할 경우 Lenovo 지원 센터로 전송됩니다.

  XClarity Administrator에서는 ThinkAgile 및 ThinkSystem 장치에 콜 홈을(를) 지원하지만 일부 ThinkAgile 및 ThinkSystem 장치의 베이스보드 관리 컨트롤러에서는 콜 홈을(를) 지원하지 않습니다. 따라서 해당 장치 자체에서는 콜 홈을 활성화하거나 비활성화할 수 없습니다. 콜 홈은 XClarity Administrator 수준의 장치에만 사용할 수 있습니다.

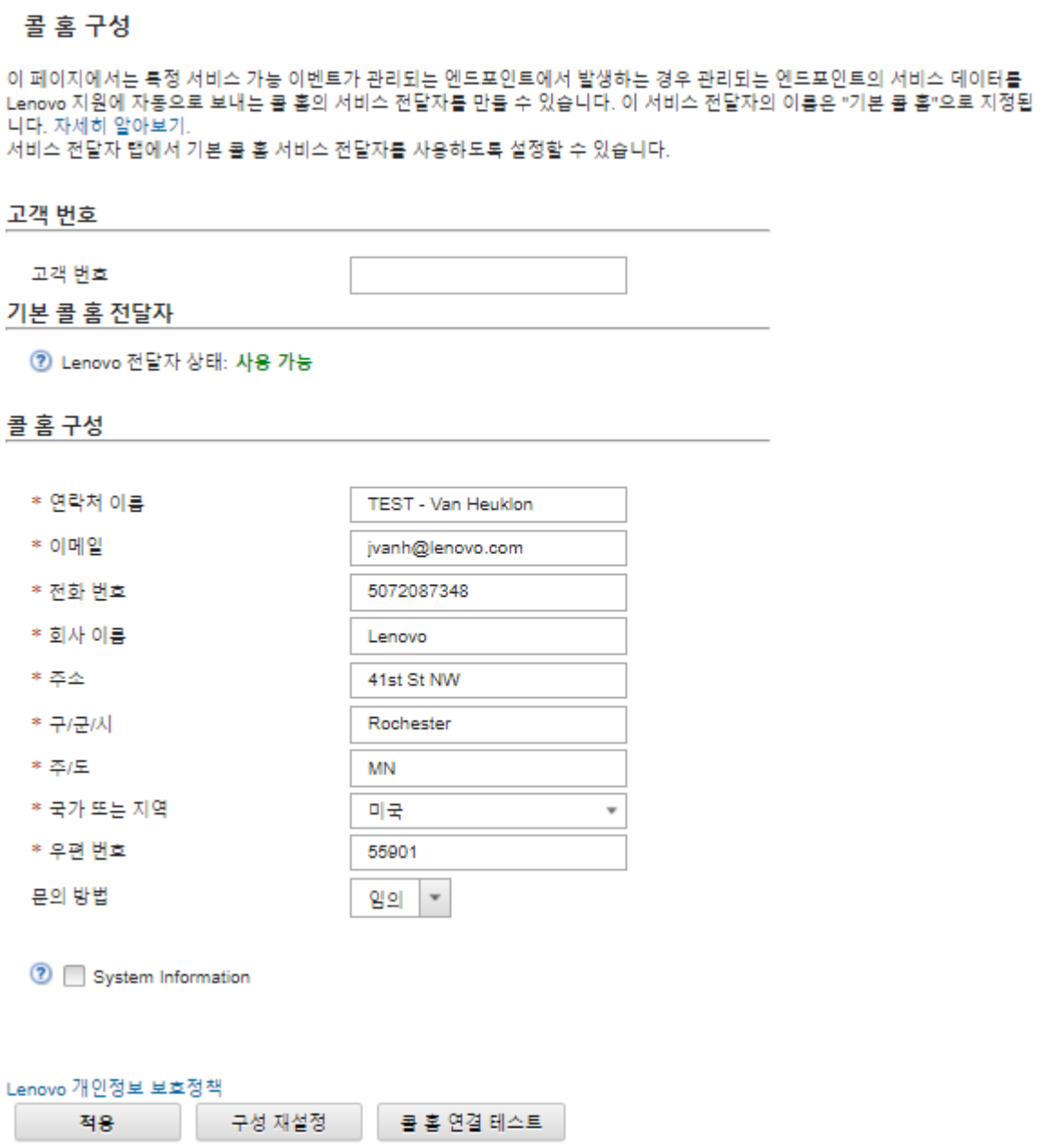
  해당 장치에서 해당 이벤트에 대한 서비스 티켓이 열려 있으면 모든 장치의 반복되는 이벤트에 대해 콜 홈이 억제됩니다. 해당 장치에서 어떤 이벤트에 대한 서비스 티켓이 열려 있으면 모든 ThinkAgile 및 ThinkSystem 장치의 비슷한 이벤트에 대해 콜 홈이 억제됩니다. ThinkAgile 및 ThinkSystem 이벤트는 *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx*(예: 806F010D0401FFFF)와 같은 형식의 16자 문자열입니다. 읽기 유형, 센서 유형 및 엔티티 ID가 동일한 이벤트는 유사합니다. 예를 들어, 특정 ThinkAgile 또는 ThinkSystem 장치에서 이벤트 806F010D0401FFFF에 대한 서비스 티켓이 열려 있으면 해당 장치에 발생하는 이벤트 중 *xx*6F01*xx*04*xxxxxx*(*x*는 영숫자)와 같은 이벤트 ID가 있는 모든 이벤트가 억제됩니다.

콜 홈 서비스 전달자에서 자동으로 연 서비스티켓 보기에 대한 정보는 XClarity Administrator 온라인 설명서에서 서비스 티켓 및 상태 보기의 내용을 참조하십시오.

절차

콜 홈의 서비스 전달자를 설정하려면 다음 단계를 완료하십시오.

- 이 절차는 모든 관리되는 장치(현재 및 이후)에 대해 콜 홈을 설정합니다.
  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 서비스 및 지원**을 클릭하십시오.
  2. 왼쪽 탐색 분할창에서 **콜 홈 구성**을 클릭하여 콜 홈 구성 페이지를 표시하십시오.



  3. (옵션) XClarity Administrator에 대한 문제를 보고할 때 사용할 기본 Lenovo 고객 번호를 지정하십시오.

     팁: Lenovo XClarity Pro를 구입할 때 받은 자격 증명 이메일에서 고객 번호를 찾을 수 있습니다.

4. 연락처 및 위치 정보를 지정하십시오.
5. Lenovo 지원 센터에서 연락할 기본 방법을 선택하십시오.
6. (옵션) 시스템 정보를 지정하십시오.
7. **적용**을 클릭하십시오.

   지정된 연락처 정보를 사용하여 모든 관리되는 장치에 대해 이름이 "기본 콜 홈"인 콜 홈 서비스 전달자가 작성됩니다.
8. "기본 콜 홈" 서비스 전달자를 사용 설정하고 테스트하십시오.
   a. 왼쪽 탐색 분할창에서 **서비스 전달자**를 클릭하여 서비스 전달자 페이지를 표시하십시오.
   b. "기본 콜 홈" 서비스 전달자의 **상태** 열에서 **사용**을 선택하십시오.
   c. "기본 콜 홈" 서비스 전달자를 선택하고 **서비스 전달자 테스트**를 클릭하여 서비스 전달자에 테스트 이벤트를 생성하고 XClarity Administrator가 Lenovo 지원 센터와 통신 가능한지 확인하십시오.

      XClarity Administrator 메뉴 표시줄에서 **모니터링 → 작업**을 클릭하여 테스트 진행 상태를 모니터링할 수 있습니다.

      참고: 서비스 전달자를 테스트하려면 먼저 사용으로 설정되어야 합니다.

- 특정 관리되는 장치에 대한 콜 홈 설정:
  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 서비스 및 지원**을 클릭하십시오.
  2. 왼쪽 탐색 분할창에서 **서비스 전달자**를 클릭하여 서비스 전달자 페이지를 표시하십시오.
  3. **서비스 전달자 만들기** 아이콘( )을 클릭하여 새 서비스 전달자 대화 상자를 표시하십시오.
  4. **일반** 탭을 클릭하십시오.

     a. **콜 홈**을 서비스 전달자로 선택하십시오.
     b. 서비스 전달자 이름과 설명을 입력하십시오.
     c. 자동 알림 재시도 횟수를 지정하십시오. 기본값은 2입니다.
     d. 재시도 간 최소 시간(분)을 지정하십시오. 기본값은 2입니다.
     e. (옵션) 서비스 데이터 파일을 전송하기 전에 검사하려면 **서비스 데이터 검사 필요**를 클릭하고 서비스 파일이 검사되어야 할 때 이를 알릴 담당자의 이메일 주소를 선택적으로 지정하십시오.
  5. **특정** 탭을 클릭하고 연락처 및 시스템 정보를 지정하십시오.

     팁: 콜 홈 구성 페이지에서 구성한 것과 동일한 연락처 및 위치 정보를 사용하려면 **구성** 드롭 다운 메뉴에서 **일반 구성**을 선택하십시오.

6. **장치** 탭을 클릭하고, 해당 서비스 전달자가 서비스 파일을 전달할 관리 장치와 자원 그룹을 선택합니다.

   팁: 모든 관리되는 장치(현재 또는 이후)의 서비스 파일을 전달하려면, **모든 장치 일치** 확인란을 선택하십시오.
7. **만들기**를 클릭하십시오. 서비스 전달자가 서비스 및 지원 페이지에 추가됩니다.
8. 서비스 전달자 페이지의 **상태** 열에서 **사용**을 선택하여 서비스 전달자를 사용 설정하십시오.
9. 서비스 전달자를 선택하고 **서비스 전달자 테스트**를 클릭하여 서비스 전달자에 대한 테스트 이벤트를 생성하고 XClarity Administrator가 Lenovo 지원 센터와 통신 가능한지 확인하십시오.

   XClarity Administrator 메뉴 표시줄에서 **모니터링 → 작업**을 클릭하여 테스트 진행 상태를 모니터링할 수 있습니다.

   참고: 서비스 전달자를 테스트하려면 먼저 사용으로 설정되어야 합니다.

완료한 후에

서비스 및 지원 페이지에서 다음 작업을 수행할 수도 있습니다.

- **서비스 데이터 검사 필요**를 선택하고 서비스 전달자와 연결된 관리되는 장치 중 하나에서 서비스 가능 이벤트를 받은 경우 서비스 파일을 서비스 공급자로 전달하기 전에 이 파일을 검사해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 Lenovo 지원에 진단 파일 전송의 내용을 참조하십시오.
- 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭하고 **콜 홈 상태** 열에서 상태를 확인하여 관리되는 장치에서 콜 홈이(가) 사용 또는 사용 안 함으로 설정되어 있는지 여부를 판별합니다.

  팁: 콜 홈 상태 열에서 "알 수 없는 상태"가 표시되는 경우, 웹 브라우저를 새로 고쳐서 올바른 상태가 표시되도록 합니다.
- 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭하고 장치를 선택한 후 **연락처 프로필 만들기** 아이콘( )또는 **연락처 프로필 편집** 아이콘( )을 클릭하여 특정 관리되는 장치에 대한 지원 연락처 및 위치 정보를 정의합니다. 관리되는 장치의 연락처 및 위치 정보는 콜 홈이 Lenovo 지원 센터로 보내는 서비스 티켓에 포함되어 있습니다. 관리 장치에 대해 고유한 연락처 및 위치 정보가 지정되면, 해당 정보가 서비스 티켓에 포함됩니다. 그렇지 않으면 XClarity Administrator 콜 홈 구성(**콜 홈 구성** 페이지 또는 **서비스 전달자** 페이지)에 대해 지정된 일반 정보가 사용됩니다. 자세한 정보는 Lenovo 지원 센터의 내용을 참조하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치에 대한 지원 연락처 정의의 내용을 참조하십시오.
- 왼쪽 탐색 분할창에서 **서비스 티켓 상태**를 클릭하여 Lenovo 지원 센터에 제출된 서비스 티켓을 확인합니다. 이 페이지는 콜 홈 서비스 전달자에서 자동 또는 수동으로 연 서비스 티켓, 상태 및 Lenovo 지원 센터로 전송된 서비스 파일을 나열합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 서비스 티켓 및 상태 보기의 내용을 참조하십시오.
- 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭하고 장치를 선택한 후 **서비스 데이터 수집** 아이콘( )을 클릭하여 특정 장치에 대한 서비스 데이터를 수집합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치에 대한 진단 파일 수집 및 다운로드의 내용을 참조하십시오.
- 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭하고 장치를 선택한 후 **모든 작업 → 수동으로 콜 홈 수행**을 클릭하여 Lenovo 지원 센터에서 서비스 티켓을 열고 특정 장치에 대한 서비스 데이터를 수집하며 해당 파일을 Lenovo 지원 센터(으)로 보냅니다.Lenovo 지원 센터에 추가 데이터가 필요한 경우 Lenovo 지원에서 해당 장치나 다른 장치에 대한 서비스 데이터를 다시 수집하라고 요청할 수 있습니다.

  자세한 정보는 XClarity Administrator 온라인 설명서에서 서비스 티켓 열기의 내용을 참조하십시오.
- 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭한 후 **모든 작업 → 모든 장치에서 콜 홈 사용**을 클릭하여 모든 관리되는 장치에서 콜 홈을(를) 다시 사용하도록 설정합니다.

  콜 홈 서비스 전달자를 Lenovo XClarity Administrator에서 사용 설정하는 경우 중복 문제 레코드가 작성되지 않도록 각 관리되는 장치에서 콜 홈이 사용 안 함으로 설정됩니다. XClarity Administrator를 사용한 장치 관리를 중단하려고 하거나 XClarity Administrator에서 콜 홈을 사용 안 함으로 설정

하려는 경우, 나중에 개별 장치에 대해 콜 홈을 다시 사용 설정하는 대신 XClarity Administrator의 모든 관리 장치에서 콜 홈을 다시 사용 설정할 수 있습니다.

자세한 정보는 XClarity Administrator 온라인 설명서에서 모든 관리 장치에서 콜 홈 다시 사용 가능하도록 설정의 내용을 참조하십시오.

선호 서비스 공급자에 대한 자동 문제 알림 설정

서비스 가능한 특정 이벤트(예, 복구 불가능한 메모리 오류)가 관리 대상 장치에서 발생하는 경우, 선호하는 서비스 공급자(콜 홈을 사용하는 Lenovo 지원 포함)에게 해당하는 관리 대상 장치 그룹의 진단 파일을 자동으로 보내도록 Lenovo XClarity Administrator를 구성하여 문제를 해결할 수 있습니다.

시작하기 전에

주의: Lenovo 지원 센터에 데이터를 전송하기 전에 Lenovo 개인정보 보호정책을/를 수락해야 합니다.

서비스 전달자를 설정하기 전에 XClarity Administrator에서 필요한 모든 포트(콜 홈에 필요한 포트 포함)가 사용 가능한지 확인하십시오. 포트에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

서비스 공급자에 필요한 인터넷 주소에 연결되어 있는지 확인하십시오.

Lenovo 지원를 사용하도록 선택한 경우 콜 홈에서 필요한 인터넷 주소에 연결되어 있는지 확인하십시오. 방화벽에 대한 정보는 XClarity Administrator 온라인 설명서에서 방화벽 및 프록시 서버의 내용을 참조하십시오.

XClarity Administrator가 HTTP 프록시를 통해 인터넷에 액세스하는 경우 프록시 서버가 비종결 프록시(non-terminating proxy)로 설정되어 있는지 확인하십시오. 프록시 설정에 대한 자세한 정보는 네트워크 액세스 구성XClarity Administrator 온라인 설명서에서 네트워크 액세스 구성의 내용을 참조하십시오.

이 작업 정보

서비스 전달자는 서비스 가능한 이벤트가 발생한 경우 서비스 데이터 파일을 보낼 위치 정보를 정의합니다. 최대 50개의 서비스 전달자를 정의할 수 있습니다.

각 서비스 전달자에 대해 Lenovo 지원(*콜 홈*), Lenovo 업로드 기능 또는 다른 서비스 공급자(SFTP 사용)에 서비스 데이터를 자동으로 보내도록 선택할 수 있습니다. 콜 홈의 서비스 전달자 설정에 대한 정보는 Lenovo 지원에 대한 자동 문제 알림 설정(콜 홈) 및 선호 서비스 공급자에 대한 자동 문제 알림 설정의 내용을 참조하십시오. Lenovo 업로드 기능의 서비스 전달자 설정에 대한 정보는 XClarity Administrator 온라인 설명서에서 Lenovo 업로드 기능에 자동 문제 알림 설정의 내용을 참조하십시오.

서비스 전달자가 구성되고 SFTP에 사용 설정된 경우 XClarity Administrator는 ***자동으로*** 서비스 데이터를 수집하고 서비스 파일을 선호하는 서비스 공급자의 지정된 SFTP 사이트로 전송합니다.

XCC2가 있는 서버의 경우 XClarity Administrator가 서비스 데이터를 리포지토리의 파일 두 개에 저장합니다.

- **서비스 파일**. (.zip) 이 파일에는 서비스 정보와 인벤토리가 쉽게 읽을 수 있는 형식으로 포함되어 있습니다. 이 파일은 서비스 가능한 이벤트가 발생할 때 선호하는 서비스 공급자에 자동으로 전송됩니다.
- **디버그 파일**. (.tzz) 이 파일에는 Lenovo 지원에서 사용할 모든 서비스 정보, 인벤토리 및 디버그 로그가 포함되어 있습니다. 문제를 해결하기 위해 추가 정보가 필요한 경우 이 파일을 Lenovo 지원에 수동으로 보낼 수 있습니다.

다른 장치의 경우에는 XClarity Administrator가 서비스 데이터(서비스 정보, 인벤토리 및 디버그 로그 포함)를 리포지토리의 단일 서비스 파일에 저장합니다. 이 파일은 서비스 가능한 이벤트가 발생할 때 선호하는 서비스 공급자에 전송됩니다.

참고: 동일한 장치에 여러 SFTP 서비스 전달자가 설정되면 서비스 전달자 중 하나만 서비스 데이터를 전송합니다. 사용되는 주소 및 포트는 처음 트리거되는 서비스 전달자에 따라 다릅니다.

절차

서비스 전달자를 정의하고 사용 설정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 서비스 및 지원**을 클릭하십시오. 서비스 및 지원 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 **서비스 전달자**를 클릭하여 서비스 전달자 페이지를 표시하십시오.

단계 3. **서비스 전달자 만들기** 아이콘( )을 클릭하여 새 서비스 전달자 대화 상자를 표시하십시오.

단계 4. General 탭을 클릭하십시오.

1. 서비스 전달자에 대해 SFTP를 선택하십시오.
2. 서비스 전달자 이름과 설명을 입력하십시오.
3. 자동 알림 재시도 횟수를 지정하십시오. 기본값은 2입니다.
4. 재시도 간 최소 시간(분)을 지정하십시오. 기본값은 2입니다.
5. (옵션) 서비스 파일을 전송하기 전에 검사하려면 **서비스 데이터 검사 필요**를 클릭하고 서비스 파일이 검사되어야 할 때 이를 알릴 담당자의 이메일 주소를 선택적으로 지정하십시오.

단계 5. **특정** 탭을 클릭하고 다음 정보를 지정하십시오.
- SFTP 서버의 IP 주소와 포트 번호
- SFTP 서버에 인증하기 위한 사용자 ID 및 암호

단계 6. **장치** 탭을 클릭하고, 해당 서비스 전달자가 서비스 데이터를 전달할 관리 장치와 자원 그룹을 선택합니다.

팁: 모든 관리되는 장치(현재 또는 이후)의 서비스 데이터를 전달하려면 **모든 장치 일치** 확인란을 선택하십시오.

단계 7. **만들기**를 클릭하십시오. 서비스 전달자가 서비스 및 지원 페이지에 추가됩니다.

단계 8. 서비스 및 지원 페이지의 **상태** 열에서 **사용**을 선택하여 서비스 전달자를 사용 설정하십시오.

단계 9. 제외된 이벤트 목록에 있는 서비스 가능한 이벤트가 문제 보고서를 자동으로 열지 않도록 하려면 **제외된 이벤트로 문제 보고서를 여시겠습니까?**라는 질문 다음에 **아니요**를 선택하십시오.

단계 10. 서비스 전달자를 선택하고 **서비스 전달자 테스트**를 클릭하여 서비스 전달자에 대한 테스트 이벤트를 생성하고 XClarity Administrator가 각 서비스 공급자와 통신할 수 있는지 확인하십시오.

참고: 서비스 전달자를 테스트하려면 먼저 사용으로 설정되어야 합니다.

완료한 후에

서비스 및 지원 페이지에서 다음 작업을 수행할 수도 있습니다.

- **서비스 데이터 검사 필요**를 선택하고 서비스 전달자와 연결된 관리되는 장치 중 하나에서 서비스 가능 이벤트를 받은 경우 서비스 파일을 서비스 공급자로 전달하기 전에 이 파일을 검사해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 진단 파일 검사의 내용을 참조하십시오.
- 왼쪽 탐색 분할창에서 **서비스 전달자**를 클릭하고 **서비스 전달자 편집** 아이콘()을 클릭하여 서비스 전달자 정보를 수정합니다.
- **서비스 전달자**를 클릭하고 **상태** 열에서 **사용** 또는 **사용 안 함**을 선택하여 서비스 공급자를 사용 또는 사용 안 함으로 설정합니다.
- **서비스 전달자**를 클릭하고 **서비스 전달자 삭제** 아이콘()을 클릭하여 서비스 공급자를 삭제합니다.
- 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭하고 장치를 선택한 후 **연락처 프로필 만들기** 아이콘() 또는 **연락처 프로필 편집** 아이콘()을 클릭하여 특정 관리되는 장치에 대한 지원 연락처 및 위치 정보를 정의합니다. 관리되는 장치의 연락처 및 위치 정보는 콜 홈이 Lenovo 지원 센터에 작성하는 문제 레코드에 포함되어 있습니다. 관리되는 장치에 고유한 연락처 및 위치 정보가 지정되면 해당 정보가 문제 레코드에 포함됩니다. 그렇지 않은 경우 XClarity Administrator 콜 홈 구성(**콜 홈 구성** 페이지 또는 **서비스 전달자** 페이지)에 지정된 일반 정보가 사용됩니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치에 대한 지원 연락처 정의의 내용을 참조하십시오.
- **엔드포인트 작업**을 클릭하고 장치를 선택한 후 **서비스 데이터 수집** 아이콘()을 클릭하여 특정 장치에 대한 서비스 데이터를 수집합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치에 대한 진단 파일 수집 및 다운로드의 내용을 참조하십시오.

이러한 서비스 및 지원 작업에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 서비스 및 지원 작업의 내용을 참조하십시오.

TruScale 포털에 허브로 XClarity Administrator 연결

Lenovo TruScale 포털에 관리 허브로 Lenovo XClarity Administrator을(를) 연결할 수 있습니다.

시작하기 전에

주의: 이 구성 단계는 Lenovo 서비스 담당자만 수행할 수 있습니다.

절차

TruScale 포털에 XClarity Administrator을(를) 연결하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 허브 구성**을 클릭하여 허브 구성 페이지를 표시하십시오.

단계 2. **등록 요청 생성**을 클릭하여 등록 키를 만드십시오. 등록 요청 생성 대화 상자가 표시됩니다.

단계 3. **클립보드에 복사**를 클릭하여 등록 키를 복사한 다음 대화 상자를 닫으십시오.

단계 4. **등록 키 설치**를 클릭하여 등록 키 설치 대화 상자를 표시하십시오.

단계 5. **등록 키** 필드에 등록 키를 붙여넣으십시오.

단계 6. **제출**을 클릭하십시오.

완료한 후에

구성 재설정을 클릭하여 등록 키를 제거할 수 있습니다.

시스템 데이터와 설정 백업, 복원 및 마이그레이션

Lenovo XClarity Administrator를 사용하여 시스템 데이터 및 설정과 가져온 파일(예: 운영 체제 이미지, 펌웨어 업데이트 및 OS 장치 드라이버)을 백업하고 복원할 수 있습니다.

Lenovo XClarity Administrator 백업

가상 호스트에 대해 이미 백업 절차를 실행하고 있는 경우 절차에는 Lenovo XClarity Administrator가 포함되어야 합니다.

시작하기 전에

주의: 백업 절차를 시작하기 전에 모든 활성 사용자에게 알리십시오. XClarity Administrator는 데이터가 수정되지 않도록 절차 중에 정지됩니다. 따라서 백업 절차가 실행되는 동안에는 XClarity Administrator에 액세스할 수 없습니다.

XClarity Administrator 가상 어플라이언스에서 인증 기관 인증서를 다운로드하고 사용자의 웹 브라우저로 가져왔는지 확인하십시오(웹 브라우저에 인증 기관 인증서 가져오기 참조).

실행 중인 모든 작업이 완료되었으며 보류 중인 작업이 없는지 확인하십시오. 작업이 실행 중인 경우, 실행 중인 작업을 중지하고 백업 만들기를 계속하도록 선택할 수 있습니다.

DNS 서버가 올바르게 설정되었는지 확인하십시오. 그렇지 않으면 백업 복원 후 SMTP 및 NTP가 올바르게 작동하지 않을 수 있습니다.

백업을 위해 관리 서버에서 사용 가능한 디스크 공간이 충분한 지 확인하십시오. 그렇지 않은 경우 이전 백업을 포함하여 더 이상 필요하지 않은 XClarity Administrator 리소스를 삭제하여 디스크 공간을 확보하거나(디스크 공간 관리 참조) 운영 체제 이미지, 펌웨어 업데이트 파일 및 OS 장치 드라이버를 포함하지 않는 새 백업을 만드십시오.

OS 이미지를 백업하려면 OS 배포가 적절한 네트워크 인터페이스(eth1 또는 eth0)에 구성되어 있는지 확인하십시오(네트워크 액세스 구성 참조).

이 작업 정보

초기 설정을 수행한 후와 다음과 같은 중요 구성 변경을 한 후 XClarity Administrator를 백업하십시오.
- 업데이트하기 전에 – XClarity Administrator
- 새 섀시 또는 랙 서버를 관리하는 경우
- XClarity Administrator에 사용자를 추가하는 경우
- 새 구성 패턴 만들고 배포하는 경우

정기적으로 XClarity Administrator를 백업해야 합니다.

로컬 시스템에 백업을 다운로드하는 것이 좋습니다. 호스트 운영 체제가 예기치 않게 종료되는 경우 호스트 운영 체제를 다시 시작한 후 XClarity Administrator를 인증하지 못할 수도 있습니다. 이 문제를 해결하려면 로컬 시스템의 마지막 백업에서 XClarity Administrator를 복원하십시오(Lenovo XClarity Administrator 복원 참조).

절차

다음 단계를 완료하여 XClarity Administrator를 백업하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 데이터 백업 및 복원**을 클릭하십시오.
데이터 백업 및 복원 페이지가 표시됩니다.

단계 2. **백업** 아이콘()을 클릭하십시오. 데이터 및 설정 백업 대화 상자가 표시됩니다.

단계 3. 이 백업에 대한 설명을 입력하십시오.

단계 4. 백업을 만들 위치를 선택하십시오. 위치는 로컬 리포지토리 또는 원격 공유입니다.

백업은 기본적으로 로컬 리포지토리에 만들어집니다. **백업 복사** 아이콘()을 클릭하여 로컬 리포지토리에서 원격 공유로 백업을 복사할 수 있습니다.

원격 공유를 선택하면 백업이 먼저 로컬 리포지토리에 만들어집니다. 그런 다음, 선택한 원격 공유로 백업이 복사되고 로컬 사본은 삭제됩니다. 자세한 정보는 원격 공유 관리의 내용을 참조하십시오.

단계 5. 운영 체제 이미지, 펌웨어 업데이트, 및 OS 장치 드라이버를 포함하도록 선택하십시오.

단계 6. 백업의 암호화 암호를 지정하십시오.

주의: 암호화 암호를 기록하십시오. 이 암호는 해당 XClarity Administrator 인스턴스 또는 다른 인스턴스에 대한 백업을 복원하는 데 필요합니다. 암호를 잊어버린 경우 복구할 방법이 없습니다.

단계 7. **백업**을 클릭하여 데이터 및 설정을 즉시 백업하거나 **일정**을 클릭하여 이 백업이 나중에 실행되도록 예약하십시오.

주의: 즉시 백업되도록 선택한 경우 프로세스가 완료되기 전에 웹 브라우저 탭 또는 창을 닫거나 새로 고치지 마십시오. 그렇지 않으면 백업이 생성되지 않을 수 있습니다.

백업 생성에는 다소 시간이 걸릴 수 있습니다. 진행률 표시줄에 작업 상태가 표시됩니다.

원격 공유에 백업을 만들도록 선택한 경우 작업 페이지에서 진행 상황을 모니터링할 수 있습니다(작업 모니터링 참조).

백업을 예약하면 관리 서버가 백업 프로세스 중에 일시적으로 종료됩니다. 관리 서버가 다시 온라인 상태가 되면 작업 페이지에서 백업 프로세스의 상태를 모니터링할 수 있습니다.

단계 8. XClarity Administrator에 로그인하여 장치 관리를 계속할 수 있습니다.

완료한 후에

데이터 백업 및 복원 페이지에서 다음 작업을 수행할 수 있습니다.

- **백업 복사** 아이콘()을 클릭하여 XClarity Administrator 백업을 원격 공유에(서) 복사하십시오.
- **백업 삭제** 아이콘()을 클릭하여 더 이상 필요하지 않은 선택한 백업을 로컬 리포지토리 또는 원격 공유에서 삭제하십시오.
- 시스템 데이터와 설정을 이 관리 서버에 복원하십시오(Lenovo XClarity Administrator 복원 참조).
- **백업 가져오기** 아이콘() 또는 **백업 내보내기** 아이콘()을 클릭하여 로컬 시스템에서 백업을 가져오거나 내보내십시오.
- 선택한 백업을 새 XClarity Administrator 인스턴스에 푸시하십시오(시스템 데이터 및 설정을 다른 XClarity Administrator 인스턴스로 마이그레이션 참조).

Lenovo XClarity Administrator 복원

백업된 데이터 및 설정을 사용하여 Lenovo XClarity Administrator를 이전 상태로 복원할 수 있습니다.

시작하기 전에

주의: 백업 절차를 시작하기 전에 모든 활성 사용자에게 알리십시오. XClarity Administrator는 데이터가 수정되지 않도록 절차 중에 정지됩니다. 따라서 백업 절차가 실행되는 동안에는 XClarity Administrator에 액세스할 수 없습니다.

XClarity Administrator 가상 어플라이언스에서 인증 기관 인증서를 다운로드하고 인증서를 웹 브라우저로 가져오십시오(웹 브라우저에 인증 기관 인증서 가져오기 참조).

실행 중인 모든 작업이 완료되었으며 보류 중인 작업이 없는지 확인하십시오.

백업을 만드는 데 사용된 동일한 XClarity Administrator 버전에만 백업을 복원할 수 있습니다.

이 작업 정보

주의:

- 백업이 생성된 이후의 모든 변경 사항은 손실됩니다.
- 데이터를 복원하기 위해 가상 어플라이언스는 원래의 클린 상태로 재설정됩니다. 모든 현재 설정, 장치 인벤토리 및 파일(운영 체제 이미지 및 펌웨어 업데이트 및 운영 체제 장치 드라이버)은 백업의 데이터를 복원하기 전에 삭제됩니다. 백업의 데이터 및 설정은 가상 어플라이언스의 현재 데이터 및 설정과 혼합되지 않습니다. 장치 인벤토리, 운영 체제 이미지, 펌웨어 업데이트 및 OS 장치 드라이버를 복원하지 않기로 선택한 경우에는 복원 조작이 완료된 후 기본 XClarity Administrator 데이터만 남습니다.

백업을 복원한다고 해서 XClarity Administrator 인스턴스에서 백업을 삭제하지는 않습니다.

백업을 복원해도 관리되는 장치의 데이터나 설정은 변경되지 않습니다. 예를 들어, 장치를 관리 해제한 다음 XClarity Administrator에서 장치가 여전히 관리되는 이전 백업을 복원하는 경우 복원 작업이 완료된 후에 해당 장치에 연결 문제가 발생할 수 있습니다. 마찬가지로 장치가 여전히 관리 해제 상태인 경우 장치를 관리 설정하고 이전 백업을 복원하려고 하면 관리되는 상태를 실행 취소하기 위해 장치의 구성으로 수동으로 수정하거나 XClarity Administrator에서 장치를 다시 관리하려고 하면 **강제** 옵션을 사용해야 할 수 있습니다.

절차

XClarity Administrator를 복원하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **관리 → 데이터 백업 및 복원**을 클릭하십시오. 데이터 백업 및 복원 페이지가 표시됩니다.

단계 2. 백업 패키지를 로컬 시스템으로 내보내고 이를 XClarity Administrator에서 삭제한 경우 다음 단계를 완료하십시오.

a. 데이터 백업 및 복원 페이지에서 **백업 가져오기** 아이콘()을 클릭하여 백업 가져오기 대화 상자를 표시하십시오.

b. **찾아보기**를 클릭하여 XClarity Administrator 인스턴스에서 내보낸 백업을 찾으십시오.

c. **가져오기**를 클릭하여 백업을 XClarity Administrator로 업로드하십시오.

백업 가져오기에는 다소 시간이 걸릴 수 있습니다. 진행률 표시줄에 작업 상태가 표시됩니다.

주의: 업로드가 완료되기 전에 웹 브라우저 탭 또는 창을 닫거나 새로 고치면 프로세스가 실패할 수 있습니다.

d. 가져오기가 완료되면 백업에 대한 암호화 암호를 지정하십시오.

참고: 암호화 암호가 없는 경우 XClarity Administrator에 새 백업을 만들어야 합니다(Lenovo XClarity Administrator 백업 참조).

단계 3. 복원할 백업을 선택하고 **백업 복원** 아이콘()을 클릭하십시오. 데이터 복원 대화 상자가 표시됩니다.

단계 4. 백업의 암호화 암호를 지정하십시오.

단계 5. **확인**을 클릭하십시오.

단계 6. 데이터 복원 확인 대화 상자에서 대화 상자의 정보가 올바른지 확인하십시오.

단계 7. 복원 옵션 대화 상자에서 선택적으로 운영 체제 이미지, 펌웨어 업데이트, OS 장치 드라이버, 네트워크 설정 및 장치 인벤토리를 가져오도록 선택합니다.

주의: 이 대화 상자에 표시된 모든 경고를 주의 깊게 읽어야 합니다.

단계 8. **확인**을 클릭하여 데이터 복원을 시작하십시오.

데이터 및 설정 복원에는 다소 시간이 걸릴 수 있습니다. 진행률 표시줄에 작업 상태가 표시됩니다.

복원 프로세스가 완료되면 로그인 페이지로 리디렉션됩니다.

주의: 프로세스가 완료되기 전에 웹 브라우저 탭 또는 창을 닫거나 새로 고치면 프로세스가 실패할 수 있습니다.

단계 9. XClarity Administrator에 로그인하여 장치 관리를 계속할 수 있습니다.

시스템 데이터 및 설정을 다른 XClarity Administrator 인스턴스로 마이그레이션

백업된 시스템 데이터 및 설정을 동일하거나 다른 네트워크에 있는 새 Lenovo XClarity Administrator(으)로 마이그레이션할 수 있습니다.

시작하기 전에

대상 관리 서버는 백업을 만드는 데 사용된 관리 서버와 동일한 버전의 *새* XClarity Administrator 인스턴스여야 하며 단계가 완료되지 않은 채 초기 설정 마법사에 있어야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 XClarity Administrator 설치 및 설정의 내용을 참조하십시오.

백업 절차를 시작하기 전에 모든 활성 사용자에게 알리십시오. XClarity Administrator는 데이터가 수정되지 않도록 절차 중에 정지됩니다. 따라서 백업 절차가 실행되는 동안에는 XClarity Administrator에 액세스할 수 없습니다.

XClarity Administrator에서 인증 기관 인증서를 다운로드하고 인증서를 웹 브라우저로 가져오십시오(XClarity Administrator 온라인 설명서에서 디스크 공간 관리 참고).

소스 관리 서버 백업 리포지토리의 백업은 대상 관리 서버로 마이그레이션되지 않습니다. 데이터 및 설정을 마이그레이션하기 전에 필요한 모든 백업을 로컬 시스템으로 내보내십시오.

이 작업 정보

백업을 만든 후 소스 관리 서버에 대한 변경 사항은 대상 관리 서버로 마이그레이션되지 않습니다.

백업을 복원해도 관리되는 장치의 데이터나 설정은 변경되지 않습니다. 예를 들어, 장치를 관리 해제한 다음 XClarity Administrator에서 장치가 여전히 관리되는 이전 백업을 복원하는 경우 복원 작업이 완료된 후에 해당 장치에 연결 문제가 발생할 수 있습니다. 마찬가지로 장치가 여전히 관리 해제 상태인 경우 장치를 관리 설정하고 이전 백업을 복원하려고 하면 관리되는 상태를 실행 취소하기 위해 장치의 구성으로 수동으로 수정하거나 XClarity Administrator에서 장치를 다시 관리하려고 하면 **강제** 옵션을 사용해야 할 수 있습니다.

참고: XClarity Administrator을(를) 컨테이너로 실행하면 한 컨테이너의 호스트에서 생성된 볼륨을 다른 컨테이너에서 볼륨으로 사용할 수 있습니다. 볼륨이 새(대상) 컨테이너에 바인딩된 후에는 초기(소스) 컨테이너에서 더 이상 사용할 수 없습니다.

1. 대상 컨테이너가 소스 컨테이너와 동일한 IP 주소 및 컨테이너 이름을 사용하도록 하려면 `docker-compose.yml` 파일을 구성합니다.
2. 다음 명령을 사용하여 소스 컨테이너를 중지하십시오.
   `docker-compose -p ${CONTAINER_NAME} down`
3. 다음 명령을 사용하여 대상 컨테이너를 시작합니다. 여기에서 *<env_filename>*은(는) 환경 변수 파일의 이름입니다. 대상 컨테이너가 시작되면 볼륨이 대상 XClarity Administrator 컨테이너에 바운딩되며 XClarity Administrator에서 해당 볼륨의 시스템 데이터 및 설정을 사용합니다.
   `COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

절차

XClarity Administrator를 복원하려면 다음 단계를 완료하십시오.

단계 1. 소스 및 대상 XClarity Administrator가 동일한 네트워크에 있는 경우 다음 단계를 완료하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **관리 → 데이터 백업 및 복원**을 클릭하십시오. 데이터 백업 및 복원 페이지가 표시됩니다.

b. **백업 푸시** 아이콘()을 클릭하여 데이터 푸시 대화 상자를 표시하십시오.

c. 대상 XClarity Administrator의 현재 IP 주소를 지정하십시오.

d. **계속**을 클릭하여 백업을 대상 XClarity Administrator에 업로드하십시오.

백업 업로드에는 다소 시간이 걸릴 수 있습니다. 진행률 표시줄에 작업 상태가 표시됩니다.

주의: 업로드가 완료되기 전에 웹 브라우저 탭 또는 창을 닫거나 새로 고치면 패키지가 업로드되지 않을 수 있습니다.

단계 2. 소스 및 대상 XClarity Administrator가 동일한 네트워크에 *있지 않은* 경우 다음 단계를 완료하십시오.

a. 소스 XClarity Administrator 메뉴 표시줄에서 **관리 → 데이터 백업 및 복원**을 클릭하십시오. 데이터 백업 및 복원 페이지에서 **백업 내보내기** 아이콘()을 클릭하여 백업을 로컬 시스템으로 내보내십시오.

백업 내보내기에는 다소 시간이 걸릴 수 있습니다.

b. 내보낸 백업을 소스 관리 서버에서 대상 관리 서버와 동일한 네트워크의 시스템으로 복사하십시오.

c. 대상 XClarity Administrator의 마법사 페이지에서 **백업 가져오기** 아이콘()을 클릭하여 데이터 패키지 가져오기 대화 상자를 표시하십시오.

d. **찾아보기**를 클릭하여 소스 XClarity Administrator에서 내보낸 백업을 찾으십시오.

e. **업로드**을 클릭하여 백업을 대상 XClarity Administrator로 가져오십시오.

백업 가져오기에는 다소 시간이 걸릴 수 있습니다. 진행률 표시줄에 작업 상태가 표시됩니다.

주의: 업로드가 완료되기 전에 웹 브라우저 탭 또는 창을 닫거나 새로 고치면 프로세스가 실패할 수 있습니다.

단계 3. 가져오기가 완료되면 백업에 대한 암호화 암호를 지정하십시오.

참고: 암호화 암호가 없는 경우 소스 XClarity Administrator에 새 백업을 만들어야 합니다 (Lenovo XClarity Administrator 백업 참조).

단계 4. 데이터 복원 확인 대화 상자에서 모든 정보가 올바른지 확인하십시오.

단계 5. **확인**을 클릭하여 시스템 데이터 및 설정을 로드하십시오.

단계 6. 복원 옵션 대화 상자에서 선택적으로 운영 체제 이미지, 펌웨어 업데이트, OS 장치 드라이버, 네트워크 설정 및 장치 인벤토리를 가져오도록 선택합니다.

주의: 이 대화 상자에 표시된 모든 경고를 주의 깊게 읽어야 합니다.

단계 7. 네트워크 설정 또는 장치 인벤토리를 가져오도록 선택한 경우 **관리 → 관리 서버 종료 → 종료**를 클릭하여 소스 XClarity Administrator에서 소스 관리 서버를 종료하십시오.

계속하기 전에 소스 가상 어플라이언스가 종료되었는지 확인하십시오.

단계 8. 대상 XClarity Administrator에서 **확인**을 클릭하여 패키지에서 데이터 및 설정을 로드하십시오.

네트워크 설정을 가져오기로 선택한 경우 마이그레이션이 완료된 후 소스 XClarity Administrator의 IP 주소가 대상 XClarity Administrator에 다시 할당됩니다.

주의: 소스 XClarity Administrator에서 DHCP를 사용하는 경우 대상 XClarity Administrator MAC 주소를 DHCP 서버의 해당 소스 XClarity Administrator IP 주소에 바인딩해야 합니다. 계속하기 전에 DHCP 서버가 수정된 후 최소 15분 동안 기다리십시오.

단계 9. 패키지에서 데이터 및 설정 로드 진행률 표시줄이 완료될 때까지 기다리십시오.

데이터 마이그레이션 프로세스가 완료되면 로그인 페이지로 리디렉션됩니다.

주의: 업로드가 완료되기 전에 웹 브라우저 탭 또는 창을 닫거나 새로 고치면 프로세스가 실패할 수 있습니다.

단계 10. 대상 XClarity Administrator에 로그인하여 장치 관리를 계속할 수 있습니다.

디스크 공간 관리

원격 공유에 즉시 필요하지 않은 대용량 데이터 파일을 이동하거나 더 이상 필요하지 않은 리소스를 삭제하여 Lenovo XClarity Administrator에서 사용하는 디스크 공간 크기를 관리할 수 있습니다.

이 작업 정보

현재 사용 중인 디스크 공간의 양을 판별하려면 XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 리포지토리 및 원격 공유의 디스크 공간 사용량은 XClarity Administrator 활동 섹션에 나열되어 있습니다.

절차

디스크 공간을 확보하려면 다음의 단계 중 하나 이상을 완료합니다. 파일을 원격 공유로 옮기고 필요 없는 리소스는 삭제합니다.

- **필요 없는 자원 삭제**

  다음의 단계를 통해 더 이상 필요 없는 파일을 로컬 저장소에서 신속히 삭제할 수 있습니다.

  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 디스크 정리**를 클릭하여 디스크 정리 페이지를 표시합니다.
  2. 삭제하려는 파일을 선택합니다. 섹션 헤더에서 파일 삭제 시 확보되는 공간을 확인할 수 있습니다.
     - **운영 체제 관련 파일**

       OS 이미지, 부티 옵션 파일 및 소프트웨어 파일을 삭제할 수 있습니다.
     - **펌웨어 업데이트**

       UpdateXpress System Pack (UXSP)와 관련된 모든 OS 장치 드라이버 및 다운로드 한 개인 장치 드라이버에 대한 페이로드 파일을 삭제할 수 있습니다.

개인 펌웨어 업데이트를 다운로드 했고, 펌웨어 호환성 정책에 해당되지 않는다면 해당 업데이트에 대한 페이로드 파일을 삭제할 수 있습니다.

다운로드 한 관리 서버 업데이트 관련 페이로드 파일을 삭제할 수 있습니다.

참고: 펌웨어 업데이트 리포지토리가 원격 공유에 있는 경우에는 디스크 정리 기능을 사용해 개별 펌웨어 업데이트 및 UXSP를 삭제할 수 없습니다.

- **서비스 데이터 파일**

  서비스 이벤트가 장치에서 발생하는 경우 해당 장치에 대한 서비스 데이터가 자동으로 수집됩니다. XClarity Administrator에서 예외가 발생하는 경우 관리 서버 서비스 데이터가 자동으로 저장됩니다. XClarity Administrator 및 관리 장치가 문제없이 작동된다면, 이러한 파일들을 주기적으로 삭제하는 것을 권장합니다.

  관리 서버 업데이트가 성공적으로 적용되면 업데이트 파일은 리포지토리에서 자동으로 제거됩니다.

3. **선택한 항목 삭제**을 클릭하십시오.
4. 선택한 파일 목록을 검토하고 **삭제**를 클릭하십시오.

- **펌웨어 업데이트 패키지를 원격 리포지토리로 이동**

  기본적으로Lenovo XClarity Administrator은(는) 펌웨어 업데이트를 저장하기 위해 로컬(내부) 리포지토리를 사용합니다. SSHFS(SSH 파일 시스템)를 통해 탑재된 원격 공유를 원격 리포지토리로 사용하여 XClarity Administrator 로컬 리포지토리에 사용 가능한 디스크 공간을 확보할 수 있습니다. 이렇게 하면 원격 리포지토리에서 직접 펌웨어 업데이트 파일을 사용하여 장치의 펌웨어 준수를 유지 관리할 수 있습니다. 자세한 정보는 펌웨어 업데이트에 원격 리포지토리 사용의 내용을 참조하십시오.

  펌웨어 업데이트 리포지토리의 위치를 변경할 때 원래 리포지토리의 모든 펌웨어 업데이트를 새 리포지토리로 복사할 수 있습니다.

  위치를 전환한 후에 원본 리포지토리의 펌웨어 업데이트 파일이 자동으로 정리되지는 *않습니다*.

  팁: 원격 업데이트 리포지토리를 여러 XClarity Administrator 관리 서버에서 공유할 수 있습니다.

  펌웨어 업데이트를 원격 펌웨어 업데이트 리포지토리로 이동하려면 다음 단계를 완료하십시오.

  1. XClarity Administrator에 원격 공유를 추가합니다(원격 공유 관리참조).
  2. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하십시오. 펌웨어 업데이트 리포지토리 페이지가 표시됩니다.
  3. **모든 작업 → 리포지토리 위치 전환**을 클릭하여 리포지토리 위치 전환 대화 상자를 표시합니다.
  4. **리포지토리 위치** 드롭 다운 목록에서 방금 생성한 원격 공유를 선택합니다.
  5. **현재 리포지토리에서 새 리포지토리로 업데이트 패키지 복사**를 선택하여 리포지토리 위치를 전환하기 전에 펌웨어 업데이트 파일을 새 리포지토리 위치에 복사합니다.
  6. **확인**을 누르십시오.

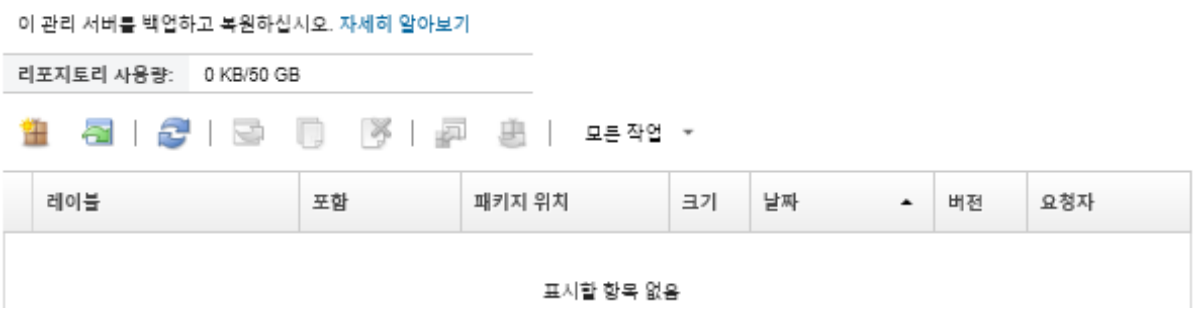
     펌웨어 업데이트 패키지를 새 리포지토리에 복사하기 위한 작업이 만들어집니다. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 작업**을 클릭하여 작업 진행 상태를 모니터링할 수 있습니다.
  7. 로컬 리포지토리에서 펌웨어 업데이트 파일을 정리합니다.
     a. **모든 작업 → 리포지토리 위치 전환**을 클릭하여 로컬 리포지토리로 위치를 전환하고 리포지토리 위치로 **로컬 리포지토리**를 선택한 후 **확인**을 클릭합니다.
     b. **개별 업데이트** 탭을 클릭하고 테이블의 모두 선택 확인란을 클릭하여 모든 펌웨어 업데이트를 선택한 다음 **전체 업데이트 패키지 삭제** 아이콘( )을 클릭합니다.
     c. UpdateXpress System Pack(UXSP) 탭을 클릭하고 테이블의 모두 선택 확인란을 클릭하여 모든 UXSP를 선택한 다음 **UXSP 및 관련 정책 삭제** 아이콘( )을 클릭합니다.
     d. **모든 작업 → 리포지토리 위치 전환**을 클릭하고 리포지토리 위치로 새 원격 리포지토리를 선택한 후 **확인**을 클릭하여 원격 리포지토리로 위치를 다시 전환합니다.

- **XClarity Administrator 백업을 원격 공유로 이동**

  XClarity Administrator 백업을 원격 공유로 이동하므로 XClarity Administrator 로컬 저장소에 있는 디스크 공간을 확보할 수 있습니다. 그러나 원격 공유에서 파일을 직접 사용할 수는 없습니다. 파일을 사용하려면 파일을 다시 XClarity Administrator 로컬 리포지토리로 이동해야 합니다. 원격 공유에 대한 자세한 정보는 원격 공유 관리의 내용을 참조하십시오.

  중요: XClarity Administrator에 있는 백업을 삭제하기 전에, 백업을 로컬 시스템에 다운로드하거나 원격 공유에 복사하는 것이 권장됩니다.

  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 데이터 백업 및 복원**을 클릭하여 데이터 백업 및 복원 페이지를 표시하십시오.

     패키지 위치 열은 XClarity Administrator 로컬 리포지토리에 로컬로 또는 원격 공유에 백업이 저장되는지 여부를 식별합니다.
  2. 백업을 선택하고 **백업 복사** 아이콘( )을 클릭하여 백업 복사 대화 상자를 표시하십시오.
  3. 백업을 저장할 원격 공유를 선택하십시오.
  4. **복사**를 클릭하십시오.
  5. 작업 페이지에서 복사 진행 상황을 모니터링하십시오. 복사가 완료되면 백업을 다시 선택하고 **백업 삭제** 아이콘( )을 클릭하여 백업 삭제 대화 상자를 표시하십시오.
  6. 위치에 "로컬"을 선택하십시오.
  7. **삭제**를 클릭하십시오.

원격 공유 관리

원격 공유을(를) 탑재한 후 로컬 리포지토리에서 원격 공유로 Lenovo XClarity Administrator 백업 및 펌웨어 업데이트와 같은 대용량 데이터 파일을 이동하여 관리 서버에 사용 가능한 디스크 공간을 관리할 수 있습니다.

시작하기 전에

XClarity Administrator을(를) 컨테이너로 실행하는 경우 설치하는 동안 yml 파일을 사용하여 컨테이너에 원격 공유가 탑재됩니다(XClarity Administrator 온라인 설명서의 VMware ESXi 기반 환경에 XClarity Administrator 설치 참조).

XClarity Administrator을(를) 가상 어플라이언스로 실행할 때 원격 공유을(를) 탑재 또는 탑재 해제하려면 lxc-supervisor 권한이 있어야 합니다.

파일 서버와 XClarity Administrator 간의 네트워크 속도가 빠르고 안정적인지 확인하십시오.

XClarity Administrator을(를) 컨테이너로 실행할 때는 원격 공유가 지원되지 않습니다.

이 작업 정보

XClarity Administrator 백업 및 펌웨어 업데이트를 저장하려면 별도의 원격 공유를 사용해야 합니다.

원격 공유에서 직접 XClarity Administrator 백업 파일을 사용할 수 없습니다. 백업 파일을 사용하려면 파일을 다시 로컬 리포지토리로 이동해야 합니다.

현재 SSHFS만 지원됩니다.

절차

XClarity Administrator을(를) 가상 어플라이언스로 실행할 때 원격 공유을(를) 추가하려면 다음 단계를 완료하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **관리 → 원격 공유**를 클릭하십시오. 원격 공유 페이지가 표시됩니다.
2. **만들기**( ) 아이콘을 클릭하여 원격 공유를 만드십시오. 원격 공유 만들기 대화 상자가 표시됩니다.
3. 원격 공유를 호스트하는 파일 서버의 IP 주소를 지정하십시오.
4. 원격 공유에 액세스하는 데 사용할 저장된 자격 증명을 지정하십시오.

   팁: 저장된 자격 증명을 만들려면 저장된 자격 증명 관리의 내용을 참조하십시오.
5. 관리 서버에서 원격 공유를 탑재하는 데 사용할 탑재 지점(로컬 디렉토리)을 지정하십시오.

   중요: 이 경로는 "/mnt"로 시작해야 합니다.
6. 관리 서버에서 원격 공유로 탑재할 공유 디렉토리(원격 서버 경로)를 지정하십시오.
7. **만들기**를 클릭하십시오.

완료한 후에

- 원격 공유를 선택하고 **삭제**( ) 아이콘을 클릭하여 원격 공유를 탑재 해제하십시오.
- 원격 공유로 또는 원격 공유에서 XClarity Administrator 백업 파일을 이동하십시오(디스크 공간 관리 참고).
- 원격 공유를 펌웨어 업데이트 리포지토리로 사용하려면 XClarity Administrator을(를) 구성하십시오(펌웨어 업데이트에 원격 리포지토리 사용 참조).

사용자 인터페이스의 언어 변경

로그인 한 후 사용자 인터페이스의 언어를 변경할 수 있습니다.

절차

Lenovo XClarity Administrator 제목 표시줄에서 사용자 작업 메뉴(ADMIN_USER)를 클릭한 다음 **언어 변경**을 클릭하십시오. 표시할 언어를 선택한 다음 **닫기**를 클릭하십시오.

참고: 도움말 시스템은 사용자 인터페이스에 설정된 동일한 언어로 표시됩니다.

XClarity Administrator 시스템 종료

Lenovo XClarity Administrator이 종료하면 Lenovo XClarity Administrator에 대한 연결이 끊깁니다.

시작하기 전에

XClarity Administrator 가상 어플라이언스를 종료하려면 lxc-supervisor 또는 lxc-admin 권한이 있어야 합니다.

현재 실행 중인 작업이 없음을 확인하십시오. 현재 실행 중인 모든 작업은 시스템 종료 프로세스 중에 취소됩니다. 작업 로그를 보려면 작업 모니터링의 내용을 참조하십시오.

절차

Lenovo XClarity Administrator를 시스템 종료하려면 다음 단계를 완료하십시오.

- **컨테이너**

  컨테이너를 중지하려면 다음 명령을 실행하십시오.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```
- **가상 어플라이언스**
  1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 관리 서버 종료**를 클릭하십시오.

     현재 실행 중인 작업 목록이 있는 확인 대화 상자가 표시됩니다. XClarity Administrator를 시스템 종료하면 작업이 취소됩니다.
  2. **시스템 종료**를 클릭하십시오.

완료한 후에

시스템 종료 후에 XClarity Administrator를 다시 시작하려면 XClarity Administrator 다시 시작의 내용을 참조하십시오.

XClarity Administrator 다시 시작

시스템 종료 후에 웹 인터페이스 또는 하이퍼바이저에서 Lenovo XClarity Administrator를 다시 시작할 수 있습니다.

시작하기 전에

XClarity Administrator을(를) 다시 시작하려면 **lxc-supervisor** 또는 **lxc-admin** 권한이 있어야 합니다.

현재 실행 중인 작업이 없음을 확인하십시오. 현재 실행 중인 모든 작업은 재시작 프로세스 동안 취소됩니다. 작업 로그를 보려면 작업 모니터링의 내용을 참조하십시오.

이 작업 정보

다음과 같이 Lenovo XClarity Administrator를 다시 시작해야 하는 특정한 상황이 있습니다.
- 서버 인증서를 다시 생성하는 경우
- 새 서버 인증서를 업로드하는 경우

절차

Lenovo XClarity Administrator을(를) 다시 시작하려면 다음 절차 중 하나를 완료하십시오.

- **컨테이너**

  다음 명령을 실행하여 컨테이너를 중지한 다음 시작하십시오. 여기에서 *<env_filename>*은(는) 환경 변수 파일의 이름입니다.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
  ```
- **가상 어플라이언스**
  - 웹 인터페이스에서 Lenovo XClarity Administrator를 다시 시작하십시오.
    1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 관리 서버 종료**를 클릭하십시오.

현재 실행 중인 작업 목록이 있는 확인 대화 상자가 표시됩니다. Lenovo XClarity Administrator를 다시 시작하면 작업이 취소됩니다.

2. **다시 시작**을 클릭하십시오.

   Lenovo XClarity Administrator이 종료하면 Lenovo XClarity Administrator에 대한 연결이 끊깁니다.

3. Lenovo XClarity Administrator가 다시 시작될 때까지 몇 분 정도 기다린 후에 다시 로그인하십시오.

– 시스템 종료 후 하이퍼바이저에서 Lenovo XClarity Administrator를 다시 시작하십시오.

  – Microsoft Hyper-V

    1. Server Manager 대시보드에서 **Hyper-V**를 클릭하십시오.
    2. 서버를 마우스 오른쪽 단추로 클릭하고 **Hyper-V Manager**를 클릭하십시오.
    3. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 **시작**을 클릭하십시오. 가상 컴퓨터가 시작되면 다음 예에서와 같이 각 인터페이스에 대해 IPv4 및 IPv6 주소가 나열됩니다.

       XClarity Administrator eth0 관리 포트는 기본적으로 DHCP IP 주소를 사용합니다. XClarity Administrator 부팅 프로세스의 끝에서 아래 예와 같은 메시지가 표시되면 1을 입력하여 eth0 관리 포트에 대해 고정 IP 주소를 설정하도록 선택할 수 있습니다. 로그인 프롬프트가 표시될 때까지 150초 동안 이 프롬프트를 사용할 수 있습니다. 지연없이 로그인 프롬프트로 진행하려면 프롬프트에 x를 입력하십시오.

       중요:

       - 고정 IP 주소 설정을 변경하는 경우 최대 60초 동안 새 설정을 입력할 수 있습니다. 계속하기 전에 필요한 IP 정보가 있는지 확인하십시오.
         – IPv4 설정의 경우 IP 주소, 서브넷 마스크 및 게이트웨이 IP 주소가 있어야 합니다.
         – IPv6 설정의 경우 IP 주소와 접두사 길이가 있어야 합니다.
       - DHCP 서버를 사용하지 않는 경우 구성 파일을 사용하여 XClarity Administrator에 액세스하는 데 사용할 XClarity Administrator eth0 관리 포트에 대한 IP 설정을 지정할 수 있습니다. 자세한 정보는 아래 "다음 작업" 섹션을 참조하십시오.
       - 콘솔에서 IP 주소 설정을 변경하는 경우 XClarity Administrator가 다시 시작되어 새 설정을 적용합니다.
       - 로그인하는 데 작업이 필요하지 않습니다. 콘솔 로그인 메시지를 무시하십시오. 콘솔 인터페이스는 고객이 사용할 수 없습니다.
       - 콘솔에 `TCP: eth0: 드라이버에서 GRO 구현을 의심하고 TCP 성능이 저하될 수 있음` 메시지가 표시될 수 있습니다. 가상 컴퓨터의 성능에 영향을 주지 않으므로 이 경고를 무시할 수 있습니다.

       주의: 장치를 관리 설정한 후 XClarity Administrator 관리 포트의 IP 주소를 변경하면 XClarity Administrator에서 장치가 오프라인 상태가 될 수 있습니다. XClarity Administrator가 작동되어 실행된 후에 IP 주소를 변경하도록 선택한 경우 IP 주소를 변경하기 전에 모든 장치가 관리 해제된 상태인지 확인하십시오.

```
---------------
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
 ... ...
```

4. Lenovo XClarity Administrator에 로그인하십시오(XClarity Administrator에 로그인 참조).

– VMware ESXi

1. VMware vSphere Client를 통해 호스트에 연결하십시오.
2. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 **전원 → 전원 켜기**를 클릭하십시오.
3. **콘솔** 탭을 클릭하십시오. 가상 컴퓨터가 시작되면 다음 예에서와 같이 각 인터페이스에 대해 IPv4 및 IPv6 주소가 나열됩니다.

   XClarity Administrator eth0 관리 포트는 기본적으로 DHCP IP 주소를 사용합니다. XClarity Administrator 부팅 프로세스의 끝에서 아래 예와 같은 메시지가 표시되면 1을 입력하여 eth0 관리 포트에 대해 고정 IP 주소를 설정하도록 선택할 수 있습니다. 로그인 프롬프트가 표시될 때까지 150초 동안 이 프롬프트를 사용할 수 있습니다. 지연없이 로그인 프롬프트로 진행하려면 프롬프트에 x를 입력하십시오.

   중요:

   - 고정 IP 주소 설정을 변경하는 경우 최대 60초 동안 새 설정을 입력할 수 있습니다. 계속하기 전에 필요한 IP 정보가 있는지 확인하십시오.
     – IPv4 설정의 경우 IP 주소, 서브넷 마스크 및 게이트웨이 IP 주소가 있어야 합니다.
     – IPv6 설정의 경우 IP 주소와 접두사 길이가 있어야 합니다.
   - DHCP 서버를 사용하지 않는 경우 구성 파일을 사용하여 XClarity Administrator에 액세스하는 데 사용할 XClarity Administrator eth0 관리 포트에 대한 IP 설정을 지정할 수 있습니다. 자세한 정보는 아래 "다음 작업" 섹션을 참조하십시오.
   - 콘솔에서 IP 주소 설정을 변경하는 경우 XClarity Administrator가 다시 시작되어 새 설정을 적용합니다.
   - 로그인하는 데 작업이 필요하지 않습니다. 콘솔 로그인 메시지를 무시하십시오. 콘솔 인터페이스는 고객이 사용할 수 없습니다.
   - 콘솔에 `TCP: eth0: 드라이버에서 GRO 구현을 의심하고 TCP 성능이 저하될 수 있음` 메시지가 표시될 수 있습니다. 가상 컴퓨터의 성능에 영향을 주지 않으므로 이 경고를 무시할 수 있습니다.

   주의: 장치를 관리 설정한 후 XClarity Administrator 관리 포트의 IP 주소를 변경하면 XClarity Administrator에서 장치가 오프라인 상태가 될 수 있습니다. XClarity Administrator가 작동되어 실행된 후에 IP 주소를 변경하도록 선택한 경우 IP 주소를 변경하기 전에 모든 장치가 관리 해제된 상태인지 확인하십시오.

```
---------------
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
 ... ...
```

4. Lenovo XClarity Administrator에 로그인하십시오(XClarity Administrator에 로그인 참조).

완료한 후에

Lenovo XClarity Administrator가 다시 시작되면 각 관리 장치에 대한 인벤토리를 다시 수집합니다. 펌웨어 업데이트, 구성 패턴 배포 또는 운영 체제 배포를 시도하기 전에 관리되는 장치 수에 따라 약 30-45분 정도 기다리십시오.

제 3 장 장치 및 활동 모니터링

대시보드, 경고 및 감사 로그와 작업 로그를 통해 장치 및 활동을 모니터링할 수 있습니다.

환경의 요약 보기

대시보드에는 모든 관리되는 장치의 상태, 모든 프로비저닝 관련 작업의 개요, Lenovo XClarity Administrator 리소스 및 활동에 대한 정보가 표시됩니다.

자세히 알아보기: XClarity Administrator: 모니터링

절차

단계 1. XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오.

단계 2. 이러한 각 영역에 대한 자세한 정보를 확보하려면 하드웨어 상태, 프로비저닝 상태 또는 관리자 활동 섹션을 확장하십시오.

하드웨어 상태의 요약 보기

하드웨어 상태 영역은 모든 관리되는 장치에 대한 상태를 표시합니다.

절차

해당 유형의 모든 장치에 대한 자세한 정보를 확보하려면 장치 유형에 나열된 숫자를 클릭하십시오.

해당 유형 및 상태의 장치에 대한 자세한 정보만 보려면 각 상태 아이콘 옆의 아이콘 또는 숫자를 클릭하십시오.

- **서버**. XClarity Administrator가 관리하는 서버(컴퓨팅 노드, 랙 서버 및 타워 서버)의 총 수와 정상, 경고 및 위험 상태의 서버 수를 표시합니다. 자세한 정보는 관리 서버의 상태 보기의 내용을 참조하십시오.
- **스토리지**. XClarity Administrator가 관리하는 스토리지 장치의 총 수와 정상, 경고 및 위험 상태의 스토리지 장치 수를 표시합니다. 자세한 정보는 스토리지 장치의 상태 보기의 내용을 참조하십시오.
- **스위치**. XClarity Administrator가 관리하는 RackSwitch 및 Flex System 스위치의 총 수와 정상, 경고 및 위험 상태의 스위치 수를 표시합니다. 자세한 정보는 스위치의 상태 보기의 내용을 참조하십시오.
- **섀시**. XClarity Administrator가 관리하는 Flex 섀시의 총 수와 정상, 경고 및 위험 상태의 Flext 섀시 수를 표시합니다. 자세한 정보는 관리 섀시의 상태 보기의 내용을 참조하십시오.
- **랙**. XClarity Administrator에서 만든 랙 수와 가장 높은 상태가 정상, 경고 및 위험인 장치의 랙 수를 표시합니다. 자세한 정보는 랙의 장치 상태 보기의 내용을 참조하십시오.
- **리소스 그룹**. XClarity Administrator에서 관리하는 리소스 그룹 수와 장치의 최상위 상태가 정상, 경고 및 위험인 리소스 그룹 수를 표시합니다. 자세한 정보는 리소스 그룹의 장치 상태 보기의 내용을 참조하십시오.

대시 보드에 표시된 하드웨어 리소스를 사용자 정의하려면, **사용자 정의** 아이콘()을 클릭하십시오. 표시하거나 숨길 장치 유형을 선택할 수 있습니다. 서버를 단일 요약으로 집계할지, 각 유형의 서버(랙 및 타워, Flex System, ThinkServer 및 NeXtScale 서버)에 대한 별도의 요약을 표시할지 아니면 특정 유형의 서버를 생략할지 여부를 선택할 수도 있습니다.

프로비저닝 상태의 요약 보기

프로비저닝 상태 영역은 프로비저닝 장치와 관련된 모든 작업의 요약을 제공합니다.

절차

- **구성 패턴**. 다음 통계를 포함하여 프로필이 있는 서버 수에 대한 세부 정보를 표시합니다.

  참고: 관리 서버가 라이센스를 준수하지 않는 경우 모든 값은 0입니다(XClarity Administrator 온라인 설명서에서 전체 기능 사용 라이센스 설치 참조).

  - 해당 서버 프로필을 준수하는 서버 수. 번호를 클릭하여 준수 서버 목록이 있는 구성 패턴: 서버 프로필 페이지를 표시할 수 있습니다.
  - 해당 서버 프로필을 준수하지 않는 서버 수. 번호를 클릭하여 비준수 서버 목록이 있는 구성 패턴: 서버 프로필 페이지를 표시할 수 있습니다.
  - 준수 상태를 알 수 없는 장치의 수. 수를 클릭하여 준수가 확인되지 않은 서버 목록이 있는 구성 패턴: 서버 프로필 페이지를 표시할 수 있습니다.

    참고: 일반적으로 부분 프로필 배포 후 Lenovo XClarity Administrator이(가) 서버에서 구성 정보를 수집하지 않으면 준수 상태를 알 수 없습니다. 서버 인벤토리를 새로 고치거나 서버 프로필 세부 정보 페이지를 다시 방문하여 서버에서 구성 정보를 강제로 수집하십시오.
  - 서버 프로필이 할당된 서버 수. 수를 클릭하여 프로필이 포함되지 않은 서버 목록이 있는 구성 패턴: 서버 프로필 페이지를 표시할 수 있습니다.
  - 서버 프로필이 할당되지 않은 서버 수. 수를 클릭하여 프로필이 없는 서버에 배포할 수 있는 서버 패턴 목록이 있는 구성 패턴: 서버 패턴 페이지를 표시할 수 있습니다.
  - 현재 배포중인 서버 패턴 수.

  구성 패턴에 대한 추세 데이터를 보려면 **추세 데이터 보기**를 클릭하십시오(프로비저닝 상태의 추세 모니터링 참조).

  구성 패턴 및 서버 프로필에 대한 자세한 정보는 구성 패턴을 사용하여 서버 구성의 내용을 참조하십시오.
- **운영 체제 이미지**. 다음 통계를 포함하여 운영 체제 배포에 대한 세부 정보를 표시합니다.

  참고: 관리 서버가 라이센스를 준수하지 않는 경우 모든 값은 0입니다(XClarity Administrator 온라인 설명서에서 전체 기능 사용 라이센스 설치 참조).

  - 리포지토리에 있는 OS 이미지 수입니다. 이 숫자를 클릭하면 운영 체제 목록이 있는 운영 체제 배포: OS 이미지 관리 페이지를 표시할 수 있습니다.
  - 진행 중인 현재 OS 배포 수입니다. 이 숫자를 클릭하면 운영 체제가 설치되는 장치 목록이 있는 운영 체제 배포: OS 이미지 배포 페이지를 표시할 수 있습니다.
- **펌웨어 업데이트**. 다음 통계를 포함하여 펌웨어 업데이트에 대한 세부 정보를 표시합니다.
  - 준수 장치의 수. 수를 클릭하여 준수 장치 목록이 있는 펌웨어 업데이트: 적용 / 활성화 페이지를 표시할 수 있습니다.
  - 비준수 장치의 수. 수를 클릭하여 비준수 장치 목록이 있는 펌웨어 업데이트: 적용 / 활성화 페이지를 표시할 수 있습니다.
  - 할당된 펌웨어 준수 정책이 없는 장치의 수. 수를 클릭하여 준수 정책이 없는 장치의 목록이 있는 펌웨어 업데이트: 적용 / 활성화 페이지를 표시할 수 있습니다.

    이 페이지에서 **할당된 준수 정책** 열에서 정책을 선택하여 각 장치에 펌웨어 준수 정책을 할당할 수 있습니다.
  - 업데이트가 지원되지 않는 장치 수입니다. 수를 클릭하여 업데이트가 지원되지 않는 장치의 목록이 있는 펌웨어 업데이트: 적용 / 활성화 페이지를 표시할 수 있습니다.
  - 진행 중인 업데이트의 수.
  - 보류 중인 펌웨어가 있는 장치의 수. 수를 클릭하여 업데이트 활성화가 보류 중인 장치의 목록이 있는 펌웨어 업데이트: 적용 / 활성화 페이지를 표시할 수 있습니다.

  펌웨어 업데이트에 대한 추세 데이터를 보려면 **추세 데이터 보기**를 클릭하십시오(프로비저닝 상태의 추세 모니터링 참조).

펌웨어 업데이트 및 준수 정책에 대한 자세한 정보는 관리 장치에서 펌웨어 업데이트의 내용을 참조하십시오.

Lenovo XClarity Administrator 활동의 요약 보기

XClarity Administrator 활동 영역은 XClarity Administrator의 활성 작업, 활성 세션 및 시스템 리소스에 대한 정보를 표시합니다.

절차

- **작업**. 현재 진행 중인 활성 작업의 수를 표시합니다. 작업에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.
- **활성 세션**. 각 활성 XClarity Administrator 세션에 대한 사용자 ID 및 IP 주소를 표시합니다. 사용자에 대한 자세한 정보는 사용자 계정 관리의 내용을 참조하십시오.
- **리소스 사용량**. 호스트 시스템 및 원격 파일 공유의 프로세서 사용량, 메모리 사용량 및 디스크 용량을 표시합니다. 시스템 리소스에 대한 자세한 정보는 시스템 리소스 모니터링의 내용을 참조하십시오.

시스템 리소스 모니터링

대시보드 페이지에서 호스트 시스템의 프로세서 사용량, 메모리 사용량 및 디스크 용량을 판별할 수 있습니다.

시작하기 전에

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 디스크 공간 관리의 내용을 참조하십시오.

절차

Lenovo XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오.

호스트 시스템 리소스 사용량은 XClarity Administrator 활동 섹션에 나열되어 있습니다.

프로세서
사용량 측정값은 호스트의 프로세스에 동시 액세스하는 XClarity Administrator 프로세스의 수를 나타냅니다.

팁: 사용량 측정값은 간혹 높음 또는 매우 높음으로 급증할 수 있습니다. 사용량이 30분 이상 이러한 수준으로 남는 경우 작업 로그를 확인하여 오래 실행 중인 작업이 진행 중인지 확인하십시오(작업 모니터링 참조).

총 용량 측정값은 호스트에서 사용할 수 있는 프로세서의 수를 나타냅니다.

메모리
사용량 측정값은 현재 XClarity Administrator가 사용하고 있는 메모리의 양을 나타냅니다.

총 용량 측정값은 호스트에서 사용할 수 있는 프로세서의 수를 나타냅니다.

사용자 데이터
사용량 측정값은 현재 호스트 시스템에서 XClarity Administrator가 사용하고 있는 디스크 공간의 크기를 나타냅니다.

총 용량 측정값은 운영 체제 및 펌웨어 업데이트와 같이 사용자 데이터에 할당된 전체 공간 크기(사용된 크기 및 사용되지 않은 크기)를 나타냅니다.

디스크 공간 관리에 대한 자세한 정보는 디스크 공간 관리의 내용을 참조하십시오.

주의: 할당된 리소스가 성능이 좋은 관리 장치의 현재 수를 처리하는 데 부족한 경우, 리소스 할당을 늘리는 것을 고려하십시오. 환경의 관리 장치 수에 따른 권장 하드웨어 요구사항에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 지원되는 호스트 시스템의 내용을 참조하십시오.

프로비저닝 상태의 추세 모니터링

Lenovo XClarity Administrator는 일정 기간 동안 추세를 모니터링할 수 있도록 모든 관리되는 장치의 펌웨어 업데이트 및 구성 패턴에 대한 준수 및 활성 작업을 포함하여 정기적으로 프로비저닝 상태를 수집합니다.

이 작업 정보

추세 데이터를 보려면 lxc_admin 또는 lxc-supervisor 권한이 있어야 합니다.

다음 데이터가 수집됩니다.

- **펌웨어 업데이트**
  - **준수 장치**. 할당된 펌웨어 준수 정책을 준수하는 장치 수
  - **비준수 장치**. 할당된 펌웨어 준수 정책을 준수하지 않는 장치 수
  - **정책이 없는 장치**. 할당된 펌웨어 준수 정책이 없는 장치 수
  - **업데이트가 지원되지 않는 장치**. 펌웨어 업데이트가 지원되지 않는 장치 수
  - **업데이트 진행 중**. 펌웨어 업데이트가 진행 중인 장치 수
- **구성 패턴**
  - **프로필이 있는 서버**. 서버 프로필이 할당된 장치 수
  - **프로필이 없는 서버**. 서버 프로필이 할당되지 않은 장치 수
  - **준수 서버**. 할당된 서버 프로필을 준수하는 장치 수
  - **비준수 서버**. 할당된 서버 프로필을 준수하지 않는 장치 수
  - **서버 패턴 진행 중**. 구성 패턴 업데이트가 진행 중인 장치 수

절차

프로비저닝 상태의 추세를 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하여 대시보드 페이지를 표시하십시오.

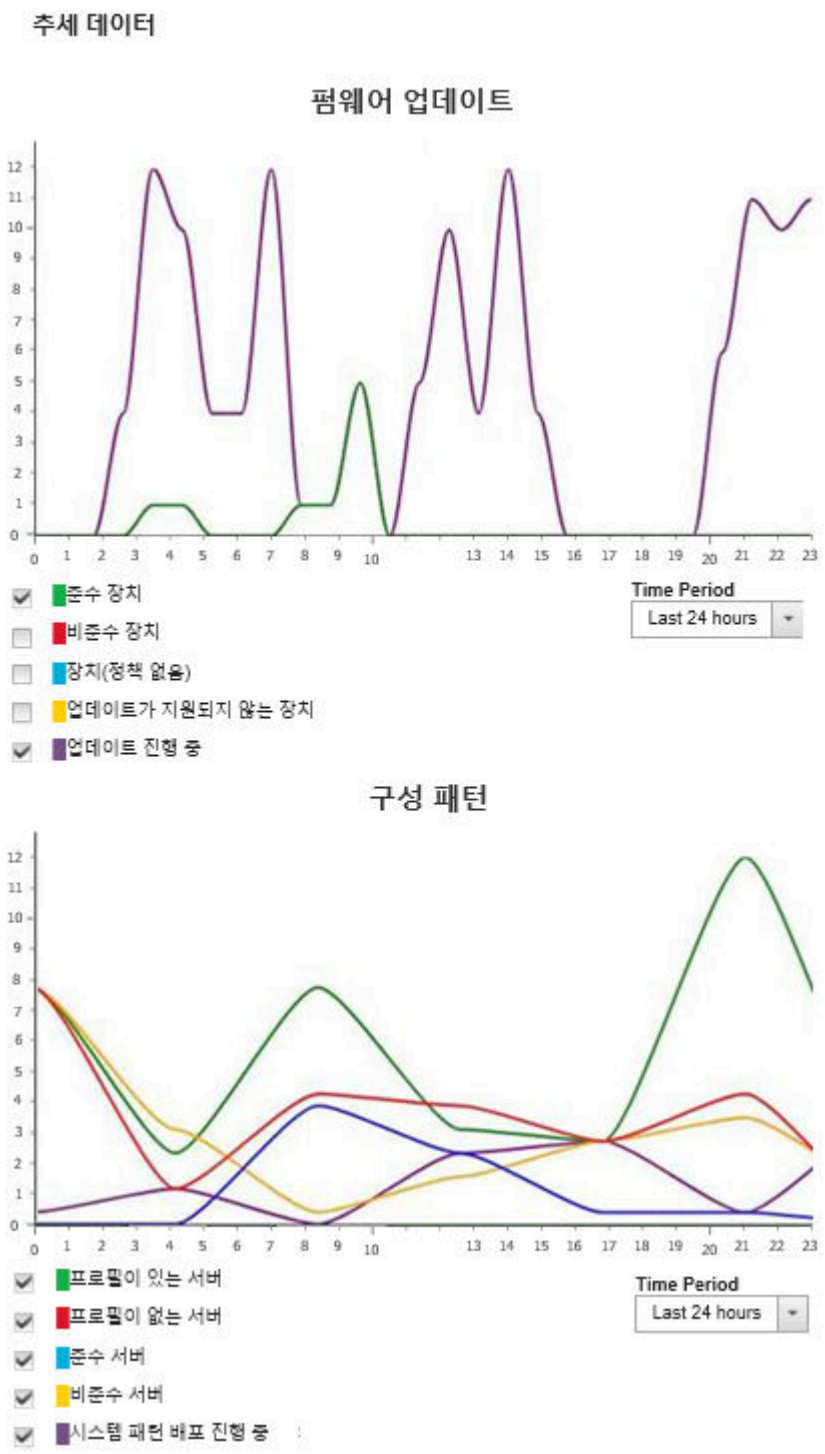
단계 2. **데이터 추세** 링크를 클릭하여 임계값 설정 페이지를 표시하십시오.

단계 3. 보려는 데이터를 지우거나 선택하십시오.

단계 4. 보려는 기간을 선택하십시오.

- **24시간**. 지난 24시간 동안의 데이터를 표시합니다. 각 데이터 포인트는 1시간 동안의 평균입니다.
- **1개월**. 지난 30일 동안의 데이터를 표시합니다. 각 데이터 포인트는 24시간 동안의 평균입니다.

추세 데이터는 선택한 기간 동안 그래프로 표시됩니다.



기록 메트릭 모니터링

Lenovo XClarity Administrator에서 관리되는 ThinkSystem 및 ThinkAgile 장치에 대한 메트릭 데이터를 정기적으로 수집하므로 사용자는 환경의 현재 상태를 분석할 수 있습니다.

시작하기 전에

기록 메트릭은 ThinkSystem 서버(SR635, SR645, SR655 및 SR665 제외)에만 지원됩니다.

2019년 4월 이후 출시된 XCC 펌웨어를 실행하는 ThinkAgile 및 ThinkSystem 서버(SR635 및 SR655 제외)의 SSD만 지원됩니다.

온보드 SATA 드라이버는 지원되지 않습니다.

NVMe 드라이브는 NVMe 관리 인터페이스(NVMe-MI) 사양을 지원해야 합니다.

이 작업 정보

다음 메트릭을 수집합니다.

- **SSD 모니터링** 이 보고서 카드에는 다음 통계와 그래프가 포함됩니다.
  - 관리되는 장치의 총 SSD 수(범위 기반).
  - 분석된 SSD 수
  - 분석 대상이 아닌 SSD 수
  - 특정 범위에서 수명이 남은 SSD가 있는 장치 수를 보여주는 원형 그래프.
    - 남은 수명 <= 10%. 남은 수명이 10% 이하인 SSD 수
    - 남은 수명 11~50%. 남은 수명이 11~50%인 SSD 수
    - 남은 수명 51~100%. 남은 수명이 50%를 초과하는 SSD 수
- **시스템 사용률** 이 보고서 카드에는 다음 통계와 그래프가 포함됩니다.
  - 현재 프로세서 사용량(%)
  - 현재 메모리 사용량(%)
  - 시간 경과에 따른 프로세서 및 메모리 사용량을 보여주는 선 그래프
- **소비 전력** 이 보고서 카드에는 다음 통계와 그래프가 포함됩니다.
  - 모든 전원 공급 장치의 현재 총 전원 입력(와트)
  - 시간 경과에 따른 총 전원 입력을 보여주는 선 그래프
- **장치 온도** 이 보고서 카드에는 다음 통계와 그래프가 포함됩니다.
  - 흡입구 공기의 현재 최고 온도(섭씨)
  - 시간 경과에 따른 최고 온도를 보여주는 선 그래프

원형 그래프의 색상 선, 선 그래프의 포인트 또는 각 메트릭 옆에 있는 숫자 위로 마우스를 가져가면 메트릭에 대한 자세한 정보를 볼 수 있습니다. 범례에서 색상 아이콘을 클릭하여 그래프에서 메트릭을 표시하거나 숨길 수 있습니다. 또한 연결된 숫자 또는 카드 오른쪽 상단의 **설정** 아이콘( )에 있는 옵션을 클릭하여 선택한 기준을 충족하는 메트릭이 있는 모든 장치 목록을 볼 수도 있습니다.

절차

특정 활동에 대한 플로우 다이어그램을 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 기록 메트릭**을 클릭하면 각 메트릭 유형의 보고서 카드가 포함된 기록 메트릭 페이지가 표시됩니다.

단계 2. 범위를 장치의 전체 또는 특정 그룹으로 설정합니다.

장치를 유지 관리 모드로 설정

장치가 유지 관리 모드인 경우 Lenovo XClarity Administrator는 이벤트 및 경고가 표시된 모든 페이지에서 해당 장치에 대한 모든 이벤트와 경고를 제외합니다. 제외된 경고는 계속 로깅되지만 보기에는 표시되지 않습니다.

이 작업 정보

장치가 유지 관리 모드에 있던 중에 장치에 대해 발생한 이벤트 및 알림만 제외됩니다. 장치가 유지 관리 모드로 전환되기 전에 발생한 이벤트 및 알림은 표시됩니다.

관리되는 장치를 유지 관리 모드로 설정한 후 다시 서비스 모드로 설정하면 해당 장치의 인벤토리가 만료될 수 있습니다. 이상이 생긴 경우 장치 페이지에서 수동으로 인벤토리를 새로 고침할 수 있는데, 장치를 선택하고 모든 **작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 그렇게 할 수 있습니다.

절차

다음 단계 중 하나를 완료하여 장치를 유지 관리 모드로 설정하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 서비스 및 지원**을 클릭하십시오. 서비스 및 지원 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 **엔드포인트 작업**을 클릭하여 엔드포인트 작업 페이지를 표시하십시오.

단계 3. 유지 관리 모드로 설정할 하나 이상의 장치를 선택하십시오.

단계 4. **작업 → 유지 관리**를 클릭하여 유지 관리 모드 대화 상자를 표시하십시오.

단계 5. 장치를 유지 관리 모드에서 해제하고 다시 서비스 모드로 설정하기 위한 날짜와 시간을 선택하십시오.

장치를 다시 서비스 모드로 설정하지 않으려면 **무한**으로 선택하십시오.

단계 6. **확인**을 클릭하십시오. 테이블에서 해당 장치에 대한 유지 관리 열이 예로 변경됩니다.

완료한 후에

장치의 유지 관리가 완료되면 장치를 선택하고 **작업 → 유지 관리**를 클릭한 후 대화 상자에서 **유지 관리 해제**를 클릭하여 장치를 되돌릴 수 있습니다. 수동으로 장치를 다시 서비스 모드로 설정하지 않으면 지정된 종료 날짜와 시간이 만료된 후 자동으로 서비스 모드로 설정됩니다.

경고 작업

*경고*는 조사와 사용자 작업이 필요한 하드웨어 또는 관리 조건입니다. Lenovo XClarity Administrator는 관리 장치를 비동기식으로 폴링하고 그러한 장치에서 수신된 경고를 표시합니다.

자세히 알아보기: XClarity Administrator: 모니터링

이 작업 정보

일반적으로 경고가 수신되면 해당 이벤트가 이벤트 로그에 저장됩니다. 경고는 이벤트 로그에 해당 이벤트가 포함되지 않을 수 있습니다(로그가 래핑되는 경우에도). 예를 들어 섀시를 관리하기 전에 발생하는 이벤트가 이벤트 로그에 표시되지 않습니다. 그러나 Lenovo XClarity Administrator는 섀시를 관리한 후 CMM을 폴링하기 때문에 섀시 경고는 경고 로그에 섀시가 표시됩니다.

활성 경고 보기

모든 활성 하드웨어 및 관리 경고 목록을 볼 수 있습니다.

이 작업 정보

참고: Lenovo Storage 장치에 대한 경고는 Lenovo XClarity Administrator의 로케일이 다른 언어로 설정된 경우에도 영어로만 표시됩니다. 필요한 경우 외부 번역 시스템을 사용하여 메시지를 수동으로 번역하십시오.

절차

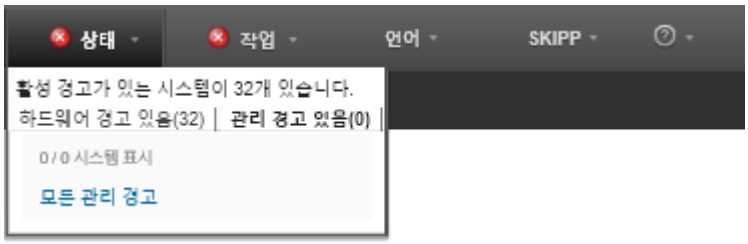
이러한 절차 중 하나를 완료하여 활성 경고를 보십시오.

- 관리 장치 경고(*하드웨어 경고*라고도 함)만 보려면 다음과 같이 하십시오.

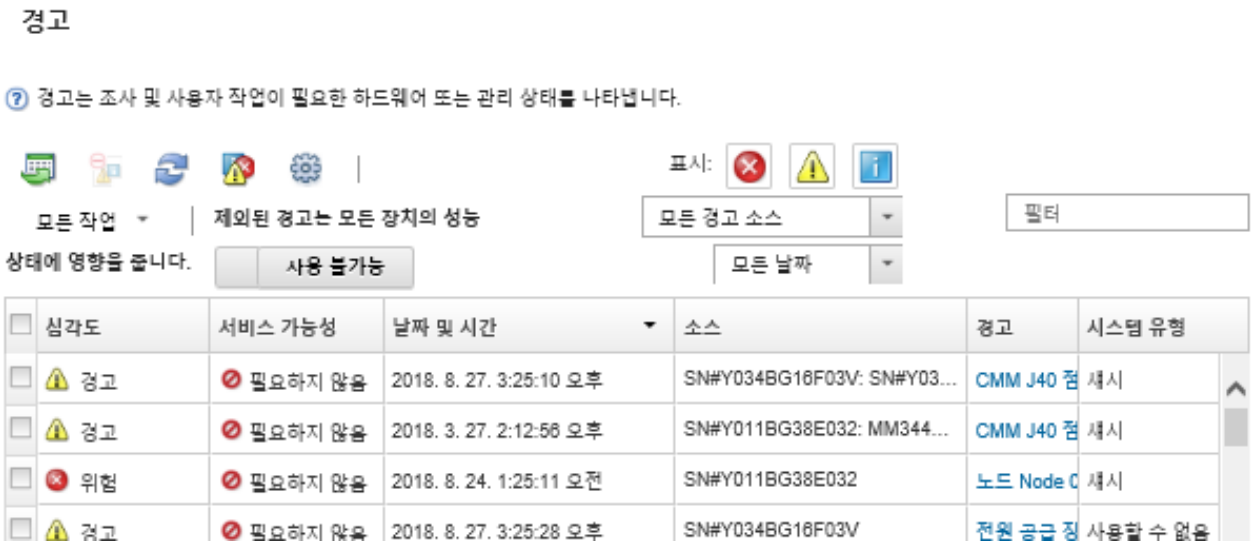
1. XClarity Administrator 제목 표시줄에서 **상태** 풀다운을 클릭하여 하드웨어 및 관리 경고의 요약을 표시하십시오.
2. **하드웨어 경고 있음** 탭을 클릭하여 각 관리 장치의 경고 요약을 보십시오.

3. 해당 탭 아래에 나열된 장치 위에 커서를 놓아 해당 장치에 대한 경고 목록을 표시하십시오.
4. **모든 하드웨어 경고** 링크를 클릭하여 모든 하드웨어 경고의 필터링된 목록으로 경고 페이지를 표시하십시오.

- XClarity Administrator의 경고(*관리 경고*라고도 함)만 보려면 다음과 같이 하십시오.
  1. XClarity Administrator 제목 표시줄에서 **상태** 풀다운을 클릭하여 하드웨어 및 관리 경고의 요약을 표시하십시오.
  2. **관리 경고 있음** 탭을 클릭하여 모든 CMM 및 XClarity Administrator 경고의 요약을 보십시오.



  3. 해당 탭 아래에 나열된 장치 위에 커서를 놓아 해당 장치에 대한 경고 목록을 표시하십시오.
  4. **모든 관리 경고** 링크를 클릭하여 모든 CMM 및 XClarity Administrator 경고의 필터링된 목록으로 경고 페이지를 표시하십시오.
- XClarity Administrator에서 모든 경고를 보려면 XClarity Administrator 메뉴 표시줄에서 **모니터링 → 경고**를 클릭하십시오. 경고 페이지는 모든 활성 경고 목록과 함께 표시됩니다.



- 특정 장치에 대한 경고를 보려면 다음과 같이 하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어**를 클릭한 다음 장치 유형을 클릭하십시오. 페이지가 해당 유형의 모든 관리 장치 표 보기와 함께 표시됩니다. 예를 들어 **하드웨어 → 서버**를 클릭하여 서버 페이지를 표시하십시오.
  2. 특정 장치를 클릭하여 장치의 요약 페이지를 표시하십시오.
  3. 상태 아래에서 **경고**를 클릭하여 해당 장치와 관련된 모든 경고 목록을 표시하십시오.

     참고: 다음 경우 서비스 가능성 열에는 "사용 불가능"이 표시될 수 있습니다.

     – XClarity Administrator가 관리를 시작하기 전에 장치에 대한 경고 발생
     – 이벤트 로그가 래핑되었고 해당 경고와 관련된 이벤트는 더 이상 이벤트 로그에 있지 않습니다.

결과

경고 페이지에서 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 경고 목록을 새로 고치십시오.

  팁: 새 경고가 감지되는 경우 경고 로그가 30초마다 자동으로 새로 고쳐집니다.
- **경고** 열의 링크를 클릭하여 특정 경고(설명 및 사용자 작업 포함) 및 경고의 원인인 장치(예, Universally Unique Identifier)에 대한 정보를 보십시오. 경고 속성 및 세부 정보에 대한 정보가 포함된 대화 상자가 표시됩니다.

  참고: 경고에 대한 설명 및 복구 작업이 **세부 정보** 탭 아래에 표시되는 경우 Lenovo Flex System 온라인 설명서로 이동하여 경고 ID(예, FQXHMSE0004G)를 검색하십시오. 웹 사이트는 항상 최신 정보를 제공합니다.
- 기본적으로 제외된 경고는 관리되는 장치의 상태에 영향을 주지 않습니다. 제외된 경고가 경고 페이지에서 관리 장치의 상태에 영향을 줄 수 있도록 하려면, 토글을 클릭하여 **제외된 경고가 모든 장치의 상태에 영향을 줌**을 사용으로 설정하십시오.
- ThinkSystem 또는 ThinkServer 서버의 SSD 수명과 같은 특정 값이 경고 또는 위험 수준을 초과할 때 경고와 이벤트를 발생시키는 임계값을 설정할 수 있습니다(경고 및 이벤트 생성을 위한 임계값 기본 설정 지정 참조).
- **CSV로 내보내기** 아이콘()을 클릭하여 경고 로그를 내보내십시오.

  참고: 내보낸 로그의 타임스탬프는 웹 브라우저에서 지정한 현지 시간을 사용합니다.
- 경고가 표시된 모든 표이지에서 특정 경고를 제외하십시오(경고 제외 참조).

- 현재 페이지에 표시된 경고 목록으로 압축하십시오.
  - 다음 아이콘을 클릭하여 특정 심각도의 경고를 표시 또는 숨기십시오.
    - **위험 경고** 아이콘()
    - **경고 경고** 아이콘()
    - **정보 경고** 아이콘()
  - 특정 원인의 경고만 표시하십시오. 드롭다운 목록에서 다음 옵션 중 하나를 선택할 수 있습니다.
    - 모든 경고 소스
    - 하드웨어 이벤트
    - 관리 이벤트
    - 서비스 센터 이벤트
    - 고객이 서비스 가능한 이벤트
    - 서비스 불가능 이벤트
  - 특정 날짜 및 시간의 경고만 표시하십시오. 드롭다운 목록에서 다음 옵션 중 하나를 선택할 수 있습니다.
    - 모든 날짜
    - 이전 2시간
    - 이전 24시간
    - 지난주
    - 지난달
  - **필터** 필드에 텍스트를 입력하여 특정 텍스트가 포함된 경고만 나열하십시오.
  - 열 표제를 클릭하여 경고를 열 기준으로 정렬하십시오.

경고 제외

관심 없는 특정 경고는 경고가 표시되는 모든 페이지에서 제외할 수 있습니다. 제외된 경고는 로그에 계속 남아 있지만 로그 보기 및 장치 상태를 포함하여 경고가 표시된 모든 페이지에서 숨겨집니다.

이 작업 정보

제외된 경고는 구성을 설정하는 사용자뿐만 아니라 모든 사용자에 대해 숨겨집니다.

장치를 유지 관리 모드로 설정하여 해당 장치에 대한 모든 이벤트 및 경고가 제외되도록 할 수 있습니다 (장치를 유지 관리 모드로 설정 참조).

제한: 관리 권한이 있는 사용자만 경고를 제외 또는 복원할 수 있습니다.

중요: 상태 경고를 제외하는 경우 장치 요약의 장치 상태와 세부 페이지가 변경되지 않습니다.

절차다음 단계를 완료하여 경고 로그에서 경고를 제외하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 경고**를 클릭하십시오. 경고 페이지가 표시됩니다.

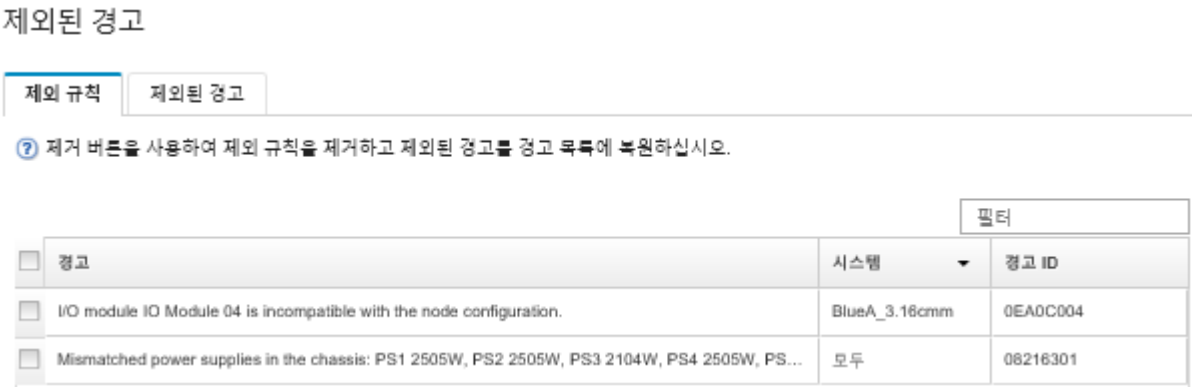
단계 2. 제외할 경고를 선택하고 **경고 제외** 아이콘()을 제외하십시오. 경고 제외 대화 상자가 표시됩니다.

단계 3. 다음 옵션 중 하나를 선택하십시오.
- **모든 시스템에서 선택한 경고 제외**. 모든 관리 장치에서 선택된 경고를 제외합니다.
- **선택한 인스턴스 범위의 시스템에서 경고만 제외**. 선택된 경고가 적용되는 관리 장치에서 선택된 경고를 제외합니다.

단계 4. **저장**을 클릭하십시오.

완료한 후에

경고를 제외하는 경우 Lenovo XClarity Administrator는 사용자가 제공하는 정보에 따라 제외 규칙을 생성합니다. **제외/확인된 경고 표시** 아이콘( )을 클릭하여 경고 페이지에서 제외 규칙과 제외된 경고 목록을 볼 수 있습니다. 제외/확인된 경고 대화 상자에서 **제외 규칙** 탭을 클릭하여 제외 규칙 목록을 보거나 **제외된 경고** 탭을 클릭하여 제외된 경고 목록을 보십시오.



기본적으로 제외된 경고는 관리되는 장치의 상태에 영향을 주지 않습니다. 제외된 경고가 경고 페이지에서 관리 장치의 상태에 영향을 줄 수 있도록 하려면, 토글을 클릭하여 **제외/확인된 경고 표시**를 사용으로 설정하십시오.

적절한 제외 규칙을 제거하여 경고 로그에서 제외된 경고를 복원할 수 있습니다. 제외 규칙을 제거하려면 **제외된 경고 표시** 아이콘( )을 클릭하여 제외된 경고 대화 상자를 표시하고, 복원할 제외 규칙 또는 제외된 경고를 선택한 후, **제거**를 클릭하십시오.

경고 해결

Lenovo XClarity Administrator는 경고를 해결하기 위해 수행해야 하는 적절한 작업에 대한 정보를 제공합니다.

절차다음 단계를 완료하여 경고를 해결하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 경고**를 클릭하여 경고 페이지를 표시하십시오.

단계 2. 경고 로그에서 경고를 찾으십시오.

단계 3. **경고** 열의 링크를 클릭하여 경고에 대한 정보(설명 및 복구 작업 포함) 및 경고의 원인인 장치의 속성(Universally Unique Identifier 등)을 보십시오.

단계 4. **세부 정보** 탭 아래에 나열된 복구 작업을 완료하여 경고를 해결하십시오. 다음 예는 이벤트에 대한 복구 작업을 보여줍니다.

참조 관리 섀시에서 보안 정책 설정을 변경하여 관리 서버에서 현재 보안 정책과 일치시키십시오.

섀시에서 보안 정책을 변경하려면 Chassis Management Module(CMM)에서 명령행 인터페이스 세션을 열고 다음 명령 중 하나를 실행하십시오.

- 보안 정책 수준을 `Secure`로 변경:
  `security -p secure -T mm[p]`
- 보안 정책 수준을 `Legacy`로 변경:
  `security -p legacy -T mm[p]`

참고: 경고에 대한 설명 및 복구 작업이 **세부 정보** 탭 아래에 표시되는 경우 Lenovo Flex System 온라인 설명서로 이동하여 경고 ID(예, `FQXHMSE0004G`)를 검색하십시오. 웹 사이트는 항상 최신 정보를 제공합니다.

권장 작업을 따라도 문제가 지속되면 Lenovo 지원에 문의하십시오.

경고 확인

활성 경고가 확인되면 경고가 표시되는 페이지에 경고가 나열되지만 해당 장치의 심각도 상태에는 영향을 주지 않습니다.

절차

다음 단계를 완료하여 경고를 확인하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링** → **경고**를 클릭하십시오. 경고 페이지가 표시됩니다.

단계 2. 확인할 경고를 선택하십시오.

단계 3. **경고 확인** 아이콘()을 클릭하십시오.

완료한 후에

- **제외/확인된 경고 표시** 아이콘()을 클릭하여 제외/확인된 경고 대화 상자를 표시한 후 **확인된 경고** 탭을 클릭하여 경고 페이지에서 확인된 경고 목록을 볼 수 있습니다.
- **제외/확인된 경고 표시** 아이콘()을 클릭하여 제외/확인된 경고 대화 상자를 표시하고 **확인된 경고** 탭을 클릭하고 경고를 선택한 후 **확인 제거** 아이콘()을 클릭하여 활성 경고에 대한 확인을 제거할 수 있습니다.

이벤트 작업

Lenovo XClarity Administrator에서 이벤트 로그 및 감사 로그에 액세스할 수 있습니다.

자세히 알아보기: XClarity Administrator: 모니터링

이 작업 정보

*이벤트 로그*는 모든 하드웨어 및 관리 이벤트의 기록 목록을 제공합니다.

*감사 로그*는 Lenovo XClarity Administrator에 로그인, 새 사용자 만들기, 사용자 암호 변경과 같은 사용자 작업의 기록 레코드를 제공합니다. 감사 로그를 사용하여 인증 및 IT 시스템의 제어 장치를 추적 및 문서화할 수 있습니다.

이벤트 로그에서 이벤트 모니터링

*이벤트 로그*는 모든 하드웨어 및 관리 이벤트의 기록 목록을 제공합니다.

이 작업 정보

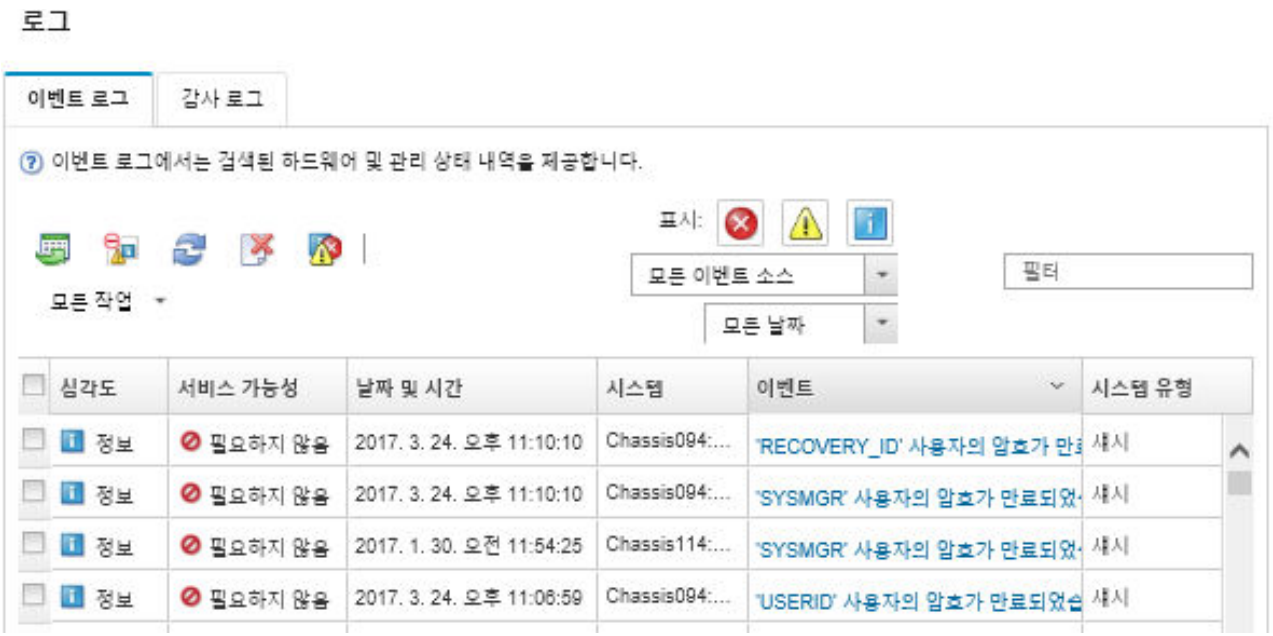
이벤트 로그에는 정보 및 정보 이외 이벤트가 포함됩니다. 이러한 각 이벤트의 번호는 이벤트 로그에서 최대 50,000개의 이벤트에 도달할 때까지 달라집니다. 그 시점에서는 최대 25,000개의 정보 이벤트와 25,000개의 정보 이외 이벤트가 있습니다. 예를 들어 처음에는 이벤트 로그에 0개의 이벤트가 있습니다. 20,000개의 정보 이벤트와 30,000개의 정보 이외 이벤트가 수신되도록 이벤트가 수신되는 것으로 가정합니다. 다음 이벤트를 수신하면 정보 이외 이벤트가 더 오래되었더라도 가장 오래된 정보 이벤트가 폐기됩니다. 결국 각 유형의 이벤트가 25,000개 있도록 로그의 균형이 맞춰집니다.

Lenovo XClarity Administrator는 이벤트 로그가 최대 크기의 80%에 도달할 때 이벤트를 전송하고 이벤트와 감사 로그의 합이 최소 크기의 100%에 도달할 때 다른 이벤트를 전송합니다.

팁: 모든 하드웨어 및 관리 이벤트에 대한 전체 레코드를 확보할 수 있도록 이벤트 로그를 내보낼 수 있습니다. 이벤트 로그를 내보내려면 CSV로 **내보내기** 아이콘()을 클릭하십시오.

절차

이벤트 로그를 보려면 Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 로그**를 클릭하고 **이벤트 로그** 탭을 클릭하십시오. 이벤트 로그 페이지가 표시됩니다.



서비스 가능성 열은 장치에 서비스가 필요한지 여부를 식별합니다. 이 열에는 다음 값 중 하나가 포함될 수 있습니다.

- **필요하지 않음**. 이벤트는 정보이며 서비스가 필요하지 않습니다.
- **사용자**. 문제 해결을 위한 적절한 복구 조치를 취하십시오.

  특정 이벤트에 대한 정보를 보려면 **이벤트** 열의 링크를 클릭하십시오. 대화 상자는 이벤트를 전송한 장치의 속성, 이벤트에 대한 세부 정보 및 복구 작업에 대한 정보와 함께 표시됩니다.
- **지원**. Lenovo XClarity Administrator에서 콜 홈이 사용으로 설정되어 있는 경우 장치에 대해 동일한 이벤트 ID에 대한 열린 서비스 티켓이 이미 존재하지 않는 한 이벤트가 일반적으로 Lenovo 지원 센터에 제출됩니다.

  콜 홈이 사용으로 설정되어 있지 않으면 수동으로 서비스 티켓을 열어 문제를 해결하는 것이 좋습니다(Lenovo XClarity Administrator 온라인 설명서에서 서비스 티켓 열기 참조).

결과

이벤트 로그 페이지에서 다음 작업을 수행할 수 있습니다.

- **소스** 열의 링크를 클릭하여 이벤트 소스를 확인합니다.
- **새로 고침** 아이콘()을 클릭하여 이벤트 목록을 새로 고치십시오.

  팁: 새 이벤트가 감지되는 경우 이벤트 로그는 30초마다 자동으로 새로 고쳐집니다.
- **모든 작업 → 이벤트 로그 지우기**를 선택하여 이벤트 로그의 모든 이벤트를 지웁니다.
- **이벤트** 열의 링크를 클릭하고 **세부 정보** 탭을 클릭하여 특정 이벤이벤트에 대한 세부 정보를 보십시오.
- CSV로 **내보내기** 아이콘()을 클릭하여 이벤트 로그를 내보내십시오.

참고: 내보낸 로그의 타임스탬프는 웹 브라우저에서 지정한 현지 시간을 사용합니다.

- 이벤트가 표시된 모든 페이지에서 특정 이벤트를 제외하십시오(이벤트 제외 참조).
- 현재 페이지에 표시된 하드웨어 및 관리 이벤트 목록으로 압축하십시오.
  - 다음 아이콘을 클릭하여 드롭다운 목록에서 특정 심각도의 이벤트를 표시 또는 숨기십시오.
    - **중요 이벤트** 아이콘()
    - **경고 이벤트** 아이콘()
    - **정보 이벤트** 아이콘()
  - 특정 원인의 이벤트만 표시하십시오. 드롭다운 목록에서 다음 옵션 중 하나를 선택할 수 있습니다.
    - 모든 경고 소스
    - 하드웨어 이벤트
    - 관리 이벤트
    - 서비스 가능 이벤트
    - 고객이 서비스 가능한 이벤트
    - 서비스 불가능 이벤트
  - 특정 날짜 및 시간의 이벤트만 표시하십시오. 다음 옵션 중 하나를 선택할 수 있습니다.
    - 모든 날짜
    - 이전 2시간
    - 이전 24시간
    - 지난주
    - 지난달
    - Custom

    사용자 지정을 선택하면, 사용자 지정 시작 날짜와 현재 날짜 사이에 일어난 하드웨어 및 관리 이벤트를 필터링할 수 있습니다.
  - **필터** 필드에 텍스트를 입력하여 특정 텍스트가 포함된 이벤트만 나열하십시오.
  - 열 표제를 클릭하여 이벤트를 열 기준으로 정렬하십시오.

감사 로그에서 이벤트 모니터링

*감사 로그*는 Lenovo XClarity Administrator에 로그인, 새 사용자 만들기, 사용자 암호 변경과 같은 사용자 작업의 기록 레코드를 제공합니다. 감사 로그를 사용하여 인증 및 IT 시스템의 제어 장치를 추적 및 문서화할 수 있습니다.

이 작업 정보

감사 로그에는 최대 50,000개의 이벤트가 포함될 수 있습니다. 최대 크기에 도달하면 로그에서 가장 오래된 이벤트가 제거되고 새 이벤트가 로그에 추가됩니다.

XClarity Administrator는 감사 로그가 최대 크기의 80%에 도달할 때 이벤트를 전송하고 이벤트와 감사 로그의 합이 최대 크기의 100%에 도달할 때 다른 이벤트를 전송합니다.

팁: 모든 감사 이벤트에 대한 전체 레코드를 확보할 수 있도록 감사 로그를 내보낼 수 있습니다. 감사 로그를 내보내려면 **CSV로 내보내기** 아이콘()을 클릭하십시오.

절차

감사 로그를 보려면 XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 로그**를 클릭하고 **감사 로그** 탭을 클릭하십시오. 감사 로그 페이지가 표시됩니다.

로그

특정 감사 이벤트에 대한 정보를 보려면 **이벤트** 열의 링크를 클릭하십시오. 대화 상자는 이벤트를 전송한 장치의 속성, 이벤트에 대한 세부 정보 및 복구 작업에 대한 정보와 함께 표시됩니다.

결과

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **소스** 열의 링크를 클릭하여 감사 이벤트 소스를 확인합니다.
- **새로 고침** 아이콘()을 클릭하여 감사 이벤트 목록을 새로 고치십시오.

  팁: 새 이벤트가 감지되는 경우 이벤트 로그는 30초마다 자동으로 새로 고쳐집니다.
- **이벤트** 열의 링크를 클릭한 다음 **세부 정보** 탭을 클릭하여 특정 감사 이벤이벤트에 대한 세부 정보를 보십시오.
- CSV로 **내보내기** 아이콘()을 클릭하여 감사 로그를 내보내십시오.

  참고: 내보낸 로그의 타임스탬프는 웹 브라우저에서 지정한 현지 시간을 사용합니다.
- 이벤트가 표시된 모든 페이지에서 특정 감사 이벤트를 제외하십시오(이벤트 제외 참조).
- 현재 페이지에 표시된 감사 이벤트 목록으로 압축하십시오.
  - 다음 아이콘을 클릭하여 특정 심각도의 이벤트를 표시 또는 숨기십시오.
    - **중요 이벤트** 아이콘()
    - **경고 이벤트** 아이콘()
    - **정보 이벤트** 아이콘()
  - 특정 날짜 및 시간의 이벤트만 표시하십시오. 드롭다운 목록에서 다음 옵션 중 하나를 선택할 수 있습니다.
    - 모든 날짜
    - 이전 2시간
    - 이전 24시간
    - 지난주
    - 지난달
    - Custom

    사용자 지정을 선택하면, 사용자 지정 시작 날짜와 현재 날짜 사이에 일어난 하드웨어 및 관리 이벤트를 필터링할 수 있습니다.
  - **필터** 필드에 텍스트를 입력하여 특정 텍스트가 포함된 이벤트만 나열하십시오.

– 열 표제를 클릭하여 이벤트를 열 기준으로 정렬하십시오.

이벤트 해결

Lenovo XClarity Administrator는 이벤트를 해결하기 위해 수행해야 하는 적절한 작업에 대한 정보를 제공합니다.

절차

다음 단계를 완료하여 이벤트를 해결하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 로그**를 클릭하여 로그 페이지를 표시하십시오.

단계 2. **이벤트 로그** 탭을 클릭하십시오.

단계 3. 이벤트 로그에서 이벤트를 찾으십시오.

단계 4. **이벤트** 열의 링크를 클릭하여 이벤트에 대한 정보(설명 및 복구 작업 포함) 및 해당 이벤트의 원인인 장치를 보십시오.

단계 5. **세부 정보** 탭을 클릭하십시오.

단계 6. **세부 정보** 탭 아래의 복구 작업을 완료하여 이벤트를 해결하십시오.

참고: 이벤트에 대한 설명 및 복구 작업이 표시되지 않는 경우 Lenovo Flex System 온라인 설명서로 이동하여 이벤트 제목을 검색하십시오. 웹 사이트는 항상 최신 정보를 제공합니다.

권장 작업을 따라도 문제가 지속되면 Lenovo 지원에 문의하십시오.

이벤트 제외

관심 없는 특정 이벤트는 이벤트가 표시되는 모든 페이지에서 제외할 수 있습니다. 제외된 이벤트는 로그에 계속 남아 있지만 이벤트가 표시된 모든 페이지에서 숨겨집니다.

이 작업 정보

제외된 이벤트는 구성을 설정하는 사용자뿐만 아니라 모든 사용자에 대해 숨겨집니다.

장치를 유지 관리 모드로 설정하여 해당 장치에 대한 모든 이벤트 및 경고가 제외되도록 할 수 있습니다 (장치를 유지 관리 모드로 설정 참조).

제한: 관리 권한이 있는 사용자만 이벤트를 제외 또는 복원할 수 있습니다.

절차

다음 단계를 완료하여 이벤트 로그에서 이벤트를 제외하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 로그**를 클릭하고 **이벤트 로그** 탭을 클릭하십시오. 이벤트 로그가 표시됩니다.

단계 2. 제외할 이벤트를 선택하고 **제외된 이벤트** 아이콘( )을 클릭하십시오. 이벤트 제외 대화 상자가 표시됩니다.

단계 3. 다음 옵션 중 하나를 선택하십시오.
- **모든 시스템에서 선택한 이벤트 제외**. 모든 관리 장치에서 선택된 이벤트를 제외합니다.
- **선택한 인스턴스 범위의 시스템에서 이벤트만 제외**. 선택된 이벤트가 적용되는 관리 장치에서 선택된 이벤트를 제외합니다.

단계 4. **저장**을 클릭하십시오.

완료한 후에

이벤트를 제외하는 경우 Lenovo XClarity Administrator는 사용자가 제공하는 정보에 따라 제외 규칙을 생성합니다.

- **제외된 이벤트 표시** 아이콘()을 클릭하여 로그 페이지에서 제외 규칙 및 제외된 이벤트 목록을 확인하십시오. 제외된 이벤트 대화 상자에서 **제외 규칙** 탭을 클릭하여 제외 규칙을 보거나 **제외된 이벤트** 탭을 클릭하여 제외된 이벤트를 보십시오.

- 적절한 제외 규칙을 제거하여 이벤트 로그에서 제외된 이벤트를 복원하십시오. 제외 규칙을 제거하려면 **제외된 이벤트 표시** 아이콘()을 클릭하여 제외된 이벤트 대화 상자를 표시하고 복원할 제외 규칙을 선택한 후 **제외 제거**를 클릭하십시오.
- Lenovo XClarity Administrator 메뉴 표시줄에서 **관리 → 서비스 및 지원**을 클릭하고 **서비스 전달자** 탭을 클릭한 후 **제외된 이벤트로 문제 보고서를 여시겠습니까?**라는 질문 다음에 **아니요**를 선택하여 제외된 이벤트 목록에 있는 서비스 가능 이벤트가 문제 보고서를 자동으로 열 수 없도록 합니다.

이벤트 전달

Lenovo XClarity Administrator를 하드웨어 환경에 대한 하드웨어 상태 및 런타임 문제를 취합하고 모니터링하기 위해 환경에 있는 모바일 장치 및 연결된 응용 프로그램에 이벤트를 전달하도록 구성할 수 있습니다.

자세히 알아보기: XClarity Administrator: 모니터링

syslog, 원격 SNMP 관리자, 이메일 또는 기타 이벤트 서비스에 이벤트 전달

Lenovo XClarity Administrator를 하드웨어 환경에 대한 하드웨어 상태 및 런타임 문제를 취합하고 모니터링하기 위해 환경에 있는 연결된 응용 프로그램에 이벤트를 전달하도록 구성할 수 있습니다. 장치, 이벤트 클래스, 이벤트 심각도 및 구성 요소에 따라 전달할 이벤트의 범위를 정의할 수 있습니다.

이 작업 정보

Lenovo XClarity Administrator는 하나 이상의 장치에 대한 이벤트를 전달할 수 있습니다. 감사 이벤트의 경우 모든 감사 이벤트를 전달하거나 하나도 전달하지 않을 수 있습니다. 특정 감사 이벤트를 전달할 수는 없습니다. 하드웨어 및 관리 이벤트의 경우 하나 이상의 심각도(중요, 경고 및 정보) 및 하나 이상의 구성 요소(예, 디스크 드라이브, 프로세서 및 어댑터)에 대한 이벤트를 전달할 수 있습니다.

Lenovo XClarity Administrator는 이벤트 전달자를 사용하여 이벤트를 전달합니다. ***이벤트 전달자***에는 사용할 프로토콜, 수신자, 모니터할 장치 및 전달할 이벤트에 대한 정보가 포함됩니다. 이벤트 전달자를 만들어 활성화하면 Lenovo XClarity Administrator는 필터 기준에 따라 수신 이벤트에 대한 모니터링을 시작합니다. 일치하는 것을 찾으면 연결된 프로토콜을 사용하여 이벤트를 전달합니다.

다음 프로토콜은 지원되지 않습니다.

- **Azure Log Analytics**. Lenovo XClarity Administrator는 네트워크를 통해 모니터링되는 이벤트를Microsoft Azure Log Analytics로 전달합니다.
- **이메일**. Lenovo XClarity Administrator는 SMTP를 사용하여 하나 이상의 이메일 주소에 모니터링되는 이벤트를 전달합니다. 이메일에는 이벤트, 소스 장치의 호스트 이름 및 Lenovo XClarity Administrator 웹 인터페이스 및 Lenovo XClarity Mobile 앱의 링크가 포함됩니다.
- FTP. 네트워크를 통해 모니터링되는 이벤트를 FTP 서버로 전달합니다.
- REST. Lenovo XClarity Administrator는 네트워크를 통해 REST Web Service에 모니터링되는 이벤트를 전달합니다.
- SNMP. Lenovo XClarity Administrator는 네트워크를 통해 원격 SNMP 관리자에 모니터링되는 이벤트를 전달합니다. SNMPv1 및 SNMPv3 트랩은 지원되지 않습니다.

  Lenovo XClarity Administrator가 생성하는 SNMP 트랩을 설명하는 관리 정보 기반(MIB) 파일에 대한 정보는 lenovoMgrAlert.mib 파일Lenovo XClarity Administrator 온라인 설명서에서 lenovoMgrAlert.mib 파일의 내용을 참조하십시오.
- Syslog. Lenovo XClarity Administrator는 중앙 로그 서버를 통해 기본 도구를 Syslog 모니터링에 사용할 수 있는 중앙 로그 서버에 모니터링되는 이벤트를 전달합니다.

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게 RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

참고: 예를 들어 Lenovo XClarity Administrator와 이벤트 전달자 간의 연결이 끊기거나 포트가 차단된 경우 이벤트가 전달되지 않습니다.

Azure Log Analytics에 대한 이벤트 전달 설정

Lenovo XClarity Administrator을 설정하여 Azure Log Analytics로 특정 이벤트를 전달하게 할 수 있습니다.

이 작업 정보

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

참고: XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게 RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

절차

Azure Log Analytics에 대한 이벤트 전달자를 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **이벤트 전달자** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 이벤트 전달자 대화 상자의 **일반** 탭이 표시됩니다.

단계 4. Azure Log Analytics를 이벤트 전달자 유형으로 선택하고 프로토콜 특정 정보를 입력하십시오.

- 이벤트 전달자에 대한 이름 및 선택적 설명을 입력하십시오.
- Azure Log Analytics 인터페이스의 기본 키를 입력하십시오.
- 요청에 대한 제한 시간(초)을 입력하십시오. 기본값은 30초입니다.
- **옵션**: 인증이 필요한 경우 다음 인증 유형 중 하나를 선택하십시오.
  - **기본**. 지정된 사용자 ID 및 암호를 사용하여 지정된 서버에 인증합니다.
  - **없음**. 인증이 사용되지 않습니다.

단계 5. **출력 형식**을 클릭하여 전달할 이벤트 데이터의 출력 형식을 선택하십시오. 정보는 이벤트 전달자의 각 유형에 따라 다릅니다.

다음 예제 출력 형식은 Azure Log Analytics 수신자의 기본 형식입니다. 이중 대괄호 사이의 모든 단어는 이벤트가 전달될 때 실제 값으로 대체되는 변수입니다. Azure Log Analytics 수신자가 사용할 수 있는 변수는 출력 형식 대화 상자에 나열되어 있습니다.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

기본값으로 재설정을 클릭하여 출력 형식을 기본 필드로 다시 변경하십시오.

단계 6. **제외된 이벤트 허용** 토글을 클릭하여 제외된 이벤트를 전달하도록 허용하거나 금지합니다.

단계 7. 이 이벤트 전달자에 대한 이벤트 전달을 활성화하려면 **이 전달자 사용**을 선택하십시오.

단계 8. **장치** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 9. 이 이벤트 전달자를 모니터링할 장치 및 그룹을 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

단계 10. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 11. 이 이벤트 전달자에 사용할 필터를 선택하십시오.

- **이벤트 범주별 일치**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
  2. 모든 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  3. 모든 상태 변경 이벤트를 전달하려면, **상태 변경 이벤트 포함**을 선택하십시오.

4. 모든 상태 업데이트이벤트를 전달하려면, **상태 업데이트 이벤트 포함**을 선택하십시오.
5. 전달하려는 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
6. 전달에서 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오(예, FQXHMEM0214I,FQXHMEM0214I).

- **이벤트 코드별 일치**. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.
- **이벤트 범주별 제외**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 제외하려면 **모든 감사 이벤트 제외**를 선택하십시오.
  2. 모든 보증 이벤트를 제외하려면 **모든 보증 이벤트 제외**를 선택하십시오.
  3. 모든 상태 변경 이벤트를 제외하려면, **상태 변경 이벤트 제외**를 선택하십시오.
  4. 모든 상태 업데이트이벤트를 제외하려면, **상태 업데이트 이벤트 제외**를 선택하십시오.
  5. 제외할 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오.
- **이벤트 코드별 제외**. 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.

단계 12. 특정 이벤트 유형을 포함할지 여부를 선택합니다.

- **모든 감사 이벤트 포함**. 선택한 이벤트 클래스 및 심각도에 따라 감사 이벤트에 대한 알림을 전송합니다.
- **보증 이벤트 포함**. 보증에 관한 알림을 전송합니다.
- **상태 변경 이벤트 포함**. 상태 변경에 관한 알림을 전송합니다.
- **상태 업데이트 이벤트 포함**. 새 경고에 대한 알림을 보냈습니다.
- **게시판 이벤트 포함**. 새 게시판에 관한 알림을 전송합니다.

단계 13. 알림을 받을 이벤트 유형 및 심각도를 선택하십시오.

단계 14. 서비스 가능성을 기준으로 이벤트를 필터링할지 여부를 선택합니다.

단계 15. **스케줄러** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 16. **옵션:** 이 이벤트 전달자에 특정 이벤트를 전달하려는 시간 및 요일을 정의하십시오. 지정된 시간 슬롯 중에 발생하는 이벤트만 전달됩니다.

이벤트 전달자에 대한 스케줄을 만들지 않는 경우 이벤트는 24시간 연중무휴 전달됩니다.

1. **왼쪽으로 화면 이동** 아이콘(◀) 및 **오른쪽으로 화면 이동** 아이콘(▶) 및 **일**, **주** 및 **월** 버튼을 사용하여 스케줄을 시작하려는 요일과 시간을 찾으십시오.
2. 새 시간 기간 대화 상자를 열려면 시간 슬롯을 두 번 클릭하십시오.
3. 날짜, 시작 및 종료 시간 및 스케줄 반복 여부와 같은 필요한 정보를 지정하십시오.
4. 스케줄을 저장하고 대화 상자를 닫으려면 **만들기**를 클릭하십시오. 일정에 새 스케줄이 추가됩니다.

팁:
- 일정 항목을 캘린더의 다른 시간 슬롯으로 드래그하여 시간 슬롯을 변경할 수 있습니다.
- 일정 항목의 상단 또는 하단을 선택하고 캘린더의 새 시간에 끌어 기간을 변경할 수 있습니다.
- 일정 항목의 하단을 선택하고 캘린더의 새 시간에 끌어 종료 시간을 변경할 수 있습니다.
- 캘린더의 일정 항목을 두 번 클릭하고 **항목 편집**을 클릭하여 일정을 변경할 수 있습니다.
- **스케줄러 요약 표시**를 선택하여 모든 일정 항목에 대한 요약을 볼 수 있습니다. 요약에는 각 항목에 대한 시간 슬롯과 반복 가능한 항목이 포함됩니다.
- 항목을 선택하고 **항목 삭제**를 클릭하여 캘린더 또는 스케줄러 요약에서 일정 항목을 삭제할 수 있습니다.

단계 17. **만들기**를 클릭하십시오.

이벤트 전달자는 이벤트 전달 테이블에 나열되어 있습니다.

단계 18. 새 이벤트 전달자를 선택하고 **테스트 이벤트 생성**을 클릭한 후 이벤트가 적절한 Azure Log Analytics 서버에 올바로 전달되는지 확인하십시오.

완료한 후에

이벤트 전달 페이지에서 선택된 이벤트 전달자에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 전달자 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 전달자에 대한 세부 정보를 보십시오.
- **이름** 열에서 이벤트 전달자 이름을 클릭하여 이벤트 전달자 속성 및 필터 기준을 변경하십시오.
- **삭제** 아이콘()을 클릭하여 이벤트 전달자를 삭제합니다.
- 이벤트 전달을 보류하십시오(이벤트 전달 보류 참조).

SMTP를 사용하는 이메일 서비스에 대한 이벤트 전달 설정

Lenovo XClarity Administrator을 설정하여 SMTP를 사용해서 특정 이벤트를 이메일 서비스로 전달할 수 있습니다.

시작하기 전에

웹 기반 이메일 서비스(예, Gmail, Hotmail 또는 Yahoo)에 이메일을 전달하려면 SMTP 서버는 웹 메일 전달을 지원해야 합니다.

이벤트 전달자를 Gmail 웹 서비스로 설정하기 전에, Gmail SMTP 서비스에 이벤트 전달 설정Lenovo XClarity Administrator 온라인 설명서에서 Syslog, 원격 SNMP 관리자 또는 이메일에 이벤트 전달 설정의 내용을 참조하십시오.

이 작업 정보

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

참고: XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게

RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

절차

SMTP를 사용하는 이메일에 대한 이벤트 전달자를 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **이벤트 전달자** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘()을 클릭하십시오. 새 이벤트 전달자 대화 상자의 **일반** 탭이 표시됩니다.

단계 4. **이메일**를 이벤트 전달자 유형으로 선택하고 프로토콜 특정 정보를 입력하십시오.

- 이벤트 전달자에 대한 이름, 대상 호스트 및 옵션 설명을 입력하십시오.
- 이벤트 전달에 사용할 포트를 입력하십시오. 기본값은 25입니다.
- 요청에 대한 제한 시간(초)을 입력하십시오. 기본값은 30초입니다.
- 각 수신자에 대한 이메일 주소를 입력하십시오. 쉼표를 사용하여 여러 이메일 주소를 구분하십시오.

  장치에 지정된 지원 담당자에게 전자 메일을 보내려면, **지원 연락처 이메일 사용**을 선택하십시오(XClarity Administrator 온라인 설명서의 장치에 대한 지원 연락처 정의 참조).
- **옵션:** 이메일 발신자에 대한 이메일 주소를 입력하십시오(예, john@company.com).

  이메일 주소를 지정하지 않는 경우 발신자 주소는 기본적으로 LXCA.*<source_identifier>*@*<smtp_host>* 입니다.

  발신자 도메인만 지정하는 경우 발신자 주소의 형식은 *<LXCA_host_name>*@*<sender_domain>* 입니다(예: XClarity1@company.com).

  참고:

  - SMTP 서버를 이메일 전달에 호스트 이름이 필요하도록 설정하고 XClarity Administrator에 대한 호스트 이름을 설정하지 않는 경우 SMTP 서버가 전달된 이벤트를 거부할 수 있습니다. XClarity Administrator에 호스트 이름이 없는 경우 이벤트는 IP 주소와 함께 전달됩니다. IP 주소를 확보할 수 없는 경우 대신 "localhost"가 전송되며 이로 인해 SMTP 서버가 이벤트를 거부할 수 있습니다.
  - 발신자 도메인을 지정하는 경우 소스는 발신자 주소를 식별하지 않습니다. 대신 이벤트의 소스에 대한 정보는 시스템 이름, IP 주소, 유형/모델 및 일련 번호 등이 이메일의 본문에 포함됩니다.
  - SMTP 서버가 등록된 사용자가 전송한 이메일만 수락하는 경우 기본 발신자 주소(LXCA.*<source_identifier>*@*<smtp_host>*)가 거부됩니다. 이 경우 **발신 주소** 필드에 최소한 도메인 이름을 지정해야 합니다.
- **옵션:** SMTP 서버에 보안 연결을 설정하려면 다음 연결 유형을 선택하십시오.
  - SSL. 통신하는 동안 SSL 프로토콜을 사용하십시오.
  - STARTTLS. TLS를 사용하여 보안되지 않은 채널로 보안 통신을 설정하십시오.

  이러한 연결 유형 중 하나를 선택한 경우 LXCA는 트러스트 스토어에 SMTP 서버의 인증서 다운로드 및 가져오기를 시도합니다. 트러스트 스토어에 이 인증서 추가를 승인할 것인지 묻는 메시지가 표시됩니다.
- **옵션:** 인증이 필요한 경우 다음 인증 유형 중 하나를 선택하십시오.
  - **일반**. 지정된 사용자 ID 및 암호를 사용하여 지정된 SMTP 서버에 인증합니다.
  - NTLM. NT LAN Manager(NTLM) 프로토콜을 사용하여 지정된 사용자 ID, 암호 및 도메인 이름으로 지정된 SMTP 서버에 인증합니다.
  - OAUTH2. SASL(Simple Authentication and Security Layer) 프로토콜을 사용하여 지정된 사용자 이름 및 보안 토큰으로 지정된 SMTP 서버에 인증합니다. 일반적으로 사용자 이름은 이메일 주소입니다.

주의: 보안 토큰은 짧은 시간 후 만료됩니다. 보안 토큰을 새로 고칠 책임은 사용자에게 있습니다.

- **없음**. 인증이 사용되지 않습니다.

단계 5. **출력 형식**을 클릭하여 이메일 본문 및 이메일 제목의 형식에 전달할 이벤트 데이터의 출력 형식을 선택하십시오. 정보는 이벤트 전달자의 각 유형에 따라 다릅니다.

다음 예제 출력 형식은 이메일 수신자의 기본 형식입니다. 이중 대괄호 사이의 모든 단어는 이벤트가 전달될 때 실제 값으로 대체되는 변수입니다. 이메일 수신자가 사용할 수 있는 변수는 출력 형식 대화 상자에 나열되어 있습니다.

이메일 제목

```
[[DeviceName]]-[[EventMessage]]
```

이메일 본문

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint   : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name      : [[DeviceName]]\n
Product name     : [[DeviceProductName]]\n
Host name        : [[DeviceHostName]]\n
Machine Type     : [[DeviceMachineType]]\n
Machine Model    : [[DeviceMachineModel]]\n
Serial Number    : [[DeviceSerialNumber]]\n
DeviceHealthStatus  : [[DeviceHealthStatus]]\n
IPv4 addresses    : [[DeviceIPV4Addresses]]\n
IPv6 addresses    : [[DeviceIPV6Addresses]]\n
Chassis         : [[DeviceChassisName]]\n
DeviceBays       : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
 Event ID     : [[EventID]]\n
 Common Event ID : [[CommonEventID]]\n
 EventSeverity  : [[EventSeverity]]\n
 Event Class    : [[EventClass]]\n
 Sequence ID    : [[EventSequenceID]]\n
 Event Source ID : [[EventSourceUUID]]\n
 Component ID   : [[EventComponentUUID]]\n
 Serial Num     : [[EventSerialNumber]]\n
 MTM         : [[EventMachineTypeModel]]\n
 EventService   : [[EventService]]\n
 Console link   : [[ConsoleLink]]\n
 iOS link      : [[iOSLink]]\n
 Android link   : [[AndroidLink]]\n
 System Name    : [[DeviceFullPathName]]\n
```

기본값으로 재설정을 클릭하여 출력 형식을 기본 필드로 다시 변경하십시오.

단계 6. **제외된 이벤트 허용** 토글을 클릭하여 제외된 이벤트를 전달하도록 허용하거나 금지합니다.

단계 7. 이 이벤트 전달자에 대한 이벤트 전달을 활성화하려면 **이 전달자 사용**을 선택하십시오.

단계 8. **장치** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 9. 이 이벤트 전달자를 모니터링할 장치 및 그룹을 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID

가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

단계 10. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 11. 이 이벤트 전달자에 사용할 필터를 선택하십시오.

- **이벤트 범주별 일치**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
  2. 모든 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  3. 모든 상태 변경 이벤트를 전달하려면, **상태 변경 이벤트 포함**을 선택하십시오.
  4. 모든 상태 업데이트이벤트를 전달하려면, **상태 업데이트 이벤트 포함**을 선택하십시오.
  5. 전달하려는 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달에서 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오(예, FQXHMEM0214I,FQXHMEM0214I).
- **이벤트 코드별 일치**. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.
- **이벤트 범주별 제외**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 제외하려면 **모든 감사 이벤트 제외**를 선택하십시오.
  2. 모든 보증 이벤트를 제외하려면 **모든 보증 이벤트 제외**를 선택하십시오.
  3. 모든 상태 변경 이벤트를 제외하려면, **상태 변경 이벤트 제외**를 선택하십시오.
  4. 모든 상태 업데이트이벤트를 제외하려면, **상태 업데이트 이벤트 제외**를 선택하십시오.
  5. 제외할 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오.
- **이벤트 코드별 제외**. 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.

단계 12. 특정 이벤트 유형을 포함할지 여부를 선택합니다.

- **모든 감사 이벤트 포함**. 선택한 이벤트 클래스 및 심각도에 따라 감사 이벤트에 대한 알림을 전송합니다.
- **보증 이벤트 포함**. 보증에 관한 알림을 전송합니다.
- **상태 변경 이벤트 포함**. 상태 변경에 관한 알림을 전송합니다.
- **상태 업데이트 이벤트 포함**. 새 경고에 대한 알림을 보냈습니다.
- **게시판 이벤트 포함**. 새 게시판에 관한 알림을 전송합니다.

단계 13. 알림을 받을 이벤트 유형 및 심각도를 선택하십시오.

단계 14. 서비스 가능성을 기준으로 이벤트를 필터링할지 여부를 선택합니다.

단계 15. **스케줄러** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 16. **옵션:** 이 이벤트 전달자에 특정 이벤트를 전달하려는 시간 및 요일을 정의하십시오. 지정된 시간 슬롯 중에 발생하는 이벤트만 전달됩니다.

이벤트 전달자에 대한 스케줄을 만들지 않는 경우 이벤트는 24시간 연중무휴 전달됩니다.

1. **왼쪽으로 화면 이동** 아이콘(◀) 및 **오른쪽으로 화면 이동** 아이콘(▶) 및 **일**, **주** 및 **월** 버튼을 사용하여 스케줄을 시작하려는 요일과 시간을 찾으십시오.
2. 새 시간 기간 대화 상자를 열려면 시간 슬롯을 두 번 클릭하십시오.
3. 날짜, 시작 및 종료 시간 및 스케줄 반복 여부와 같은 필요한 정보를 지정하십시오.

4. 스케줄을 저장하고 대화 상자를 닫으려면 **만들기**를 클릭하십시오. 일정에 새 스케줄이 추가됩니다.

팁:
- 일정 항목을 캘린더의 다른 시간 슬롯으로 드래그하여 시간 슬롯을 변경할 수 있습니다.
- 일정 항목의 상단 또는 하단을 선택하고 캘린더의 새 시간에 끌어 기간을 변경할 수 있습니다.
- 일정 항목의 하단을 선택하고 캘린더의 새 시간에 끌어 종료 시간을 변경할 수 있습니다.
- 캘린더의 일정 항목을 두 번 클릭하고 **항목 편집**을 클릭하여 일정을 변경할 수 있습니다.
- **스케줄러 요약 표시**를 선택하여 모든 일정 항목에 대한 요약을 볼 수 있습니다. 요약에는 각 항목에 대한 시간 슬롯과 반복 가능한 항목이 포함됩니다.
- 항목을 선택하고 **항목 삭제**를 클릭하여 캘린더 또는 스케줄러 요약에서 일정 항목을 삭제할 수 있습니다.

단계 17. **만들기**를 클릭하십시오.

이벤트 전달자는 이벤트 전달 테이블에 나열되어 있습니다.

단계 18. 새 이벤트 전달자를 선택하고 **테스트 이벤트 생성**을 클릭한 후 이벤트가 적절한 이메일 서비스에 올바로 전달되는지 확인하십시오.

완료한 후에

이벤트 전달 페이지에서 선택된 이벤트 전달자에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 전달자 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 전달자에 대한 세부 정보를 보십시오.
- **이름** 열에서 이벤트 전달자 이름을 클릭하여 이벤트 전달자 속성 및 필터 기준을 변경하십시오.
- **삭제** 아이콘()을 클릭하여 이벤트 전달자를 삭제합니다.
- 이벤트 전달을 보류하십시오(이벤트 전달 보류 참조).

Gmail SMTP 서버 서비스에 이벤트 전달 설정

Lenovo XClarity Administrator를 모니터링되는 이벤트를 Gmail과 같은 웹 기반 이메일 서비스에 전달하도록 설정할 수 있습니다.

다음 구성 예제를 사용하여 Gmail SMTP 서비스를 사용하도록 이벤트 전달자를 설정하는 데 참조할 수 있습니다.

참고: Gmail은 대부분의 보안 통신에 OAUTH2 인증 방법을 사용하는 것을 권장합니다. 일반 인증을 사용하려는 경우 응용 프로그램이 최신 보안 표준을 사용하지 않고 사용자 계정을 사용하려고 시도했음을 표

시하는 이메일을 수신하게 됩니다. 이 이메일에는 이메일 계정을 이러한 유형의 응용 프로그램을 승인하도록 구성하는 것에 대한 지침이 포함됩니다.

Gmail SMTP 서버 구성에 대한 정보는 https://support.google.com/a/answer/176600?hl=en의 내용을 참조하십시오.

포트 465에 SSL을 사용하는 일반 인증

이 예제는 포트 465를 통해 SSL 프로토콜을 사용하여 Gmail SMTP 서버와 통신하고 유효한 Gmail 사용자 계정 및 암호를 사용하여 인증합니다.

매개변수	값
Host	smtp.gmail.com
포트	465
SSL	선택
STARTTLS	지우기
인증	일반
사용자	유효한 Gmail 이메일 주소
암호	Gmail 인증 암호
보내는 사람 주소	(옵션)

포트 587에 SSL을 사용하는 일반 인증

이 예제는 포트 587을 통해 TLS 프로토콜을 사용하여 Gmail SMTP 서버와 통신하고 유효한 Gmail 사용자 계정 및 암호를 사용하여 인증합니다.

매개변수	값
Host	smtp.gmail.com
포트	587
SSL	지우기
STARTTLS	선택
인증	일반
사용자	유효한 Gmail 이메일 주소
암호	Gmail 인증 암호
보내는 사람 주소	(옵션)

포트 587에 SSL을 사용하는 OAUTH2 인증

이 예제는 포트 587을 통해 TLS 프로토콜을 사용하여 Gmail SMTP 서버와 통신하고 유효한 Gmail 사용자 계정 및 보안 토큰을 사용하여 인증합니다.

다음 예제를 사용하여 보안 토큰을 확보하십시오.

1. Google Developers Console에서 프로젝트를 만들고 클라이언트 ID와 클라이언트 암호를 검색하십시오. 자세한 정보는 웹 사이트용 Google 로그인 웹 페이지 웹 사이트를 참조하십시오.
   a. 웹 브라우저에서 Google API 웹 페이지를 여십시오.
   b. 해당 웹 페이지의 메뉴에서 **프로젝트 선택 → 프로젝트 만들기**를 클릭하십시오. 새 프로젝트 대화 상자가 표시됩니다.

c. 이름을 입력하고 **예**를 선택하여 라이센스 계약에 동의하고 **만들기**를 클릭하십시오.
d. **개요** 탭에서 "gmail"을 검색할 검색 필드를 사용하십시오.
e. 검색 결과에서 GMAIL API를 클릭하십시오.
f. **사용**을 클릭하십시오.
g. **자격 증명** 탭을 클릭하십시오.
h. OAuth **동의 화면**을 클릭하십시오.
i. **사용자에게 표시되는 제품 이름** 필드에 이름을 입력하고 **저장**을 클릭하십시오.
j. **자격 증명 만들기** → OAuth **클라이언트** ID를 클릭하십시오.
k. **기타**를 선택하고 이름을 입력하십시오.
l. **만들기**를 클릭하십시오. OAuth 클라이언트 대화 상자가 클라이언트 ID 및 클라이언트 암호와 함께 표시됩니다.
m. 나중에 사용하도록 클라이언트 ID와 클라이언트 암호를 기록해 두십시오.
n. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

2. oauth2.py Python 스크립트를 사용하여 프로젝트를 만들 때 생성된 클라이언트 ID와 클라이언트 암호를 입력하여 보안 토큰을 생성 및 승인하십시오.

   참고: 이 단계를 완료하려면 Python 2.7이 필요합니다. Python 웹 사이트에서 Python 2.7을 다운로드하고 설치할 수 있습니다).

   a. 웹 브라우저에서 gmail-oauth2-tools 웹 페이지를 여십시오.
   b. **원시**를 클릭한 다음 컨텐츠를 로컬 시스템에 oauth2.py라는 파일 이름으로 저장하십시오.
   c. 다음 명령을 단자(Linux) 또는 명령 행(Windows)으로 실행하십시오.

   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
     --client_secret=<client_secret> --generate_oauth2_token
   ```

   예를 들어, 다음과 같습니다.

   ```
   py oauth2.py --user=jon@gmail.com
     --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
     --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```

   이 명령은 토큰을 승인하고 Google 웹 사이트에서 확인 코드를 검색하는 데 사용해야 하는 URL을 반환하는데, 다음 예와 같습니다.

   ```
   To authorize token, visit this url and follow the directions:

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
   google.com%2F

   Enter verification code:
   ```

   d. 웹 브라우저에서 이전 단계에서 반환된 URL을 여십시오.
   e. 이 서비스에 동의하려면 **허용**을 클릭하십시오. 확인 코드가 반환됩니다.
   f. `oauth2.py` 명령에 확인 코드를 입력하십시오.

   명령은 보안 토큰을 반환하고 토큰을 새로 고치는데, 다음 예와 같습니다.

   ```
   Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
   Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
   Access Token Expiration Seconds: 3600
   ```

중요: 보안 토큰은 일정 시간 후 만료됩니다. oauth2.py Python 스크립트를 사용하고 토큰을 새로 고쳐 새 보안 토큰을 생성할 수 있습니다. 새 보안 토큰을 생성하고 Lenovo XClarity Administrator에서 이벤트 포워더를 새 토큰으로 업데이트할 책임은 사용자에게 있습니다.

3. Lenovo XClarity Administrator 웹 인터페이스에서 다음 특성을 사용하여 이메일에 대해 이벤트 포워더를 설정하십시오.

매개변수	값
Host	smtp.gmail.com
포트	587
SSL	지우기
STARTTLS	선택
인증	OAUTH2
사용자	유효한 Gmail 이메일 주소
토큰	보안 토큰
보내는 사람 주소	(옵션)

FTP 서버에 대한 이벤트 전달 설정

Lenovo XClarity Administrator을 설정하여 FTP 서버로 특정 이벤트를 전달할 수 있습니다.

이 작업 정보

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

참고: XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게 RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

절차

FTP 서버에 대한 이벤트 전달자를 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **이벤트 전달자** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 이벤트 전달자 대화 상자의 **일반** 탭이 표시됩니다.

단계 4. FTP를 이벤트 전달자 유형으로 선택하고 프로토콜 특정 정보를 입력하십시오.

- 이벤트 전달자에 대한 이름, 대상 호스트 및 옵션 설명을 입력하십시오.
- 이벤트 전달에 사용할 포트를 입력하십시오. 기본값은 21입니다.
- 요청에 대한 제한 시간(초)을 입력하십시오. 기본값은 30초입니다.
- **옵션:** 파일 내용에서 제거할 문자의 순서를 지정하십시오.
- 전달된 이벤트가 들어 있는 파일에 사용할 파일 이름 형식을 입력하십시오. 기본 형식은 `event_[[EventSequenceID]].txt`입니다.

  참고: 각 파일에는 단일 이벤트에 대한 정보가 들어 있습니다.
- 파일을 업로드할 원격 FTP 서버의 경로를 입력하십시오.

- 문자 인코딩(UTF-8 또는 Big5)을 선택하십시오. 기본값은 UTF-8입니다.
- 인증 유형을 선택하십시오. 이는 다음 값 중 하나입니다.
  - **익명**. (기본값) 인증이 사용되지 않습니다.
  - **기본**. 지정된 사용자 ID 및 암호를 사용하여 FTP 서버에 인증합니다.

단계 5. **출력 형식**을 클릭하여 전달할 이벤트 데이터의 출력 형식을 선택하십시오. 정보는 이벤트 전달자의 각 유형에 따라 다릅니다.

다음 예제 출력 형식은 FTP 수신자의 기본 형식입니다. 이중 대괄호 사이의 모든 단어는 이벤트가 전달될 때 실제 값으로 대체되는 변수입니다. FTP 수신자가 사용할 수 있는 변수는 출력 형식 대화 상자에 나열되어 있습니다.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint   : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name      : [[DeviceName]]\n
Product name     : [[DeviceProductName]]\n
Host name        : [[DeviceHostName]]\n
Machine Type     : [[DeviceMachineType]]\n
Machine Model    : [[DeviceMachineModel]]\n
Serial Number    : [[DeviceSerialNumber]]\n
DeviceHealthStatus : [[DeviceHealthStatus]]\n
IPv4 addresses    : [[DeviceIPV4Addresses]]\n
IPv6 addresses    : [[DeviceIPV6Addresses]]\n
Chassis         : [[DeviceChassisName]]\n
DeviceBays       : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
 Event ID     : [[EventID]]\n
 Common Event ID : [[CommonEventID]]\n
 EventSeverity  : [[EventSeverity]]\n
 Event Class    : [[EventClass]]\n
 Sequence ID    : [[EventSequenceID]]\n
 Event Source ID : [[EventSourceUUID]]\n
 Component ID   : [[EventComponentUUID]]\n
 Serial Num     : [[EventSerialNumber]]\n
 MTM          : [[EventMachineTypeModel]]\n
 EventService   : [[EventService]]\n
 Console link   : [[ConsoleLink]]\n
 iOS link      : [[iOSLink]]\n
 Android link   : [[AndroidLink]]\n
 System Name    : [[DeviceFullPathName]]\n"
```

기본값으로 재설정을 클릭하여 출력 형식을 기본 필드로 다시 변경하십시오.

단계 6. **제외된 이벤트 허용** 토글을 클릭하여 제외된 이벤트를 전달하도록 허용하거나 금지합니다.

단계 7. 이 이벤트 전달자에 대한 이벤트 전달을 활성화하려면 **이 전달자 사용**을 선택하십시오.

단계 8. **장치** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 9. 이 이벤트 전달자를 모니터링할 장치 및 그룹을 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견

되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

단계 10. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 11. 이 이벤트 전달자에 사용할 필터를 선택하십시오.

- **이벤트 범주별 일치**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
  2. 모든 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  3. 모든 상태 변경 이벤트를 전달하려면, **상태 변경 이벤트 포함**을 선택하십시오.
  4. 모든 상태 업데이트이벤트를 전달하려면, **상태 업데이트 이벤트 포함**을 선택하십시오.
  5. 전달하려는 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달에서 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오(예, FQXHMEM0214I,FQXHMEM0214I).
- **이벤트 코드별 일치**. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.
- **이벤트 범주별 제외**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 제외하려면 **모든 감사 이벤트 제외**를 선택하십시오.
  2. 모든 보증 이벤트를 제외하려면 **모든 보증 이벤트 제외**를 선택하십시오.
  3. 모든 상태 변경 이벤트를 제외하려면, **상태 변경 이벤트 제외**를 선택하십시오.
  4. 모든 상태 업데이트이벤트를 제외하려면, **상태 업데이트 이벤트 제외**를 선택하십시오.
  5. 제외할 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오.
- **이벤트 코드별 제외**. 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.

단계 12. 특정 이벤트 유형을 포함할지 여부를 선택합니다.

- **모든 감사 이벤트 포함**. 선택한 이벤트 클래스 및 심각도에 따라 감사 이벤트에 대한 알림을 전송합니다.
- **보증 이벤트 포함**. 보증에 관한 알림을 전송합니다.
- **상태 변경 이벤트 포함**. 상태 변경에 관한 알림을 전송합니다.
- **상태 업데이트 이벤트 포함**. 새 경고에 대한 알림을 보냈습니다.
- **게시판 이벤트 포함**. 새 게시판에 관한 알림을 전송합니다.

단계 13. 알림을 받을 이벤트 유형 및 심각도를 선택하십시오.

단계 14. 서비스 가능성을 기준으로 이벤트를 필터링할지 여부를 선택합니다.

단계 15. **스케줄러** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 16. **옵션:** 이 이벤트 전달자에 특정 이벤트를 전달하려는 시간 및 요일을 정의하십시오. 지정된 시간 슬롯 중에 발생하는 이벤트만 전달됩니다.

이벤트 전달자에 대한 스케줄을 만들지 않는 경우 이벤트는 24시간 연중무휴 전달됩니다.

1. **왼쪽으로 화면 이동** 아이콘(◀) 및 **오른쪽으로 화면 이동** 아이콘(▶) 및 **일**, **주** 및 **월** 버튼을 사용하여 스케줄을 시작하려는 요일과 시간을 찾으십시오.
2. 새 시간 기간 대화 상자를 열려면 시간 슬롯을 두 번 클릭하십시오.
3. 날짜, 시작 및 종료 시간 및 스케줄 반복 여부와 같은 필요한 정보를 지정하십시오.

4. 스케줄을 저장하고 대화 상자를 닫으려면 **만들기**를 클릭하십시오. 일정에 새 스케줄이 추가됩니다.

팁:
- 일정 항목을 캘린더의 다른 시간 슬롯으로 드래그하여 시간 슬롯을 변경할 수 있습니다.
- 일정 항목의 상단 또는 하단을 선택하고 캘린더의 새 시간에 끌어 기간을 변경할 수 있습니다.
- 일정 항목의 하단을 선택하고 캘린더의 새 시간에 끌어 종료 시간을 변경할 수 있습니다.
- 캘린더의 일정 항목을 두 번 클릭하고 **항목 편집**을 클릭하여 일정을 변경할 수 있습니다.
- **스케줄러 요약 표시**를 선택하여 모든 일정 항목에 대한 요약을 볼 수 있습니다. 요약에는 각 항목에 대한 시간 슬롯과 반복 가능한 항목이 포함됩니다.
- 항목을 선택하고 **항목 삭제**를 클릭하여 캘린더 또는 스케줄러 요약에서 일정 항목을 삭제할 수 있습니다.

단계 17. **만들기**를 클릭하십시오.

이벤트 전달자는 이벤트 전달 테이블에 나열되어 있습니다.

단계 18. 새 이벤트 전달자를 선택하고 **테스트 이벤트 생성**을 클릭한 후 이벤트가 적절한 FTP 서버에 올바로 전달되는지 확인하십시오.

완료한 후에

이벤트 전달 페이지에서 선택된 이벤트 전달자에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 전달자 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 전달자에 대한 세부 정보를 보십시오.
- **이름** 열에서 이벤트 전달자 이름을 클릭하여 이벤트 전달자 속성 및 필터 기준을 변경하십시오.
- **삭제** 아이콘()을 클릭하여 이벤트 전달자를 삭제합니다.
- 이벤트 전달을 보류하십시오(이벤트 전달 보류 참조).

REST 웹 서비스에 대한 이벤트 전달 설정

Lenovo XClarity Administrator을 설정하여 REST 웹 서비스로 특정 이벤트를 전달할 수 있습니다.

이 작업 정보

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

참고: XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게 RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

절차

REST 웹 서비스에 대한 이벤트 전달자를 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **이벤트 전달자** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 이벤트 전달자 대화 상자의 **일반** 탭이 표시됩니다.

단계 4. REST를 이벤트 전달자 유형으로 선택하고 프로토콜 특정 정보를 입력하십시오.

- 전달자가 이벤트를 게시할 리소스 경로를 입력하십시오(예, /rest/test).
- 이벤트 전달에 사용할 프로토콜을 선택하십시오. 이는 다음 값 중 하나입니다.
  - HTTP
  - HTTPS
- REST 메서드를 선택하십시오. 이는 다음 값 중 하나입니다.
  - PUT
  - POST
- 요청에 대한 제한 시간(초)을 입력하십시오. 기본값은 30초입니다.
- **옵션:** 인증이 필요한 경우 다음 인증 유형 중 하나를 선택하십시오.
  - **기본**. 지정된 사용자 ID 및 암호를 사용하여 지정된 서버에 인증합니다.
  - **없음**. 인증이 사용되지 않습니다.

단계 5. **출력 형식**을 클릭하여 전달할 이벤트 데이터의 출력 형식을 선택하십시오. 정보는 이벤트 전달자의 각 유형에 따라 다릅니다.

다음 예제 출력 형식은 REST 웹 서비스 수신자의 기본 형식입니다. 이중 대괄호 사이의 모든 단어는 이벤트가 전달될 때 실제 값으로 대체되는 변수입니다. REST 웹 서비스 수신자가 사용할 수 있는 변수는 출력 형식 대화 상자에 나열되어 있습니다.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

기본값으로 재설정을 클릭하여 출력 형식을 기본 필드로 다시 변경하십시오.

단계 6. **제외된 이벤트 허용** 토글을 클릭하여 제외된 이벤트를 전달하도록 허용하거나 금지합니다.

단계 7. 이 이벤트 전달자에 대한 이벤트 전달을 활성화하려면 **이 전달자 사용**을 선택하십시오.

단계 8. **장치** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 9. 이 이벤트 전달자를 모니터링할 장치 및 그룹을 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

단계 10. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 11. 이 이벤트 전달자에 사용할 필터를 선택하십시오.

- **이벤트 범주별 일치**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
  2. 모든 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  3. 모든 상태 변경 이벤트를 전달하려면, **상태 변경 이벤트 포함**을 선택하십시오.
  4. 모든 상태 업데이트이벤트를 전달하려면, **상태 업데이트 이벤트 포함**을 선택하십시오.
  5. 전달하려는 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달에서 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오(예, FQXHMEM0214I,FQXHMEM0214I).
- **이벤트 코드별 일치**. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.
- **이벤트 범주별 제외**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 제외하려면 **모든 감사 이벤트 제외**를 선택하십시오.
  2. 모든 보증 이벤트를 제외하려면 **모든 보증 이벤트 제외**를 선택하십시오.
  3. 모든 상태 변경 이벤트를 제외하려면, **상태 변경 이벤트 제외**를 선택하십시오.
  4. 모든 상태 업데이트이벤트를 제외하려면, **상태 업데이트 이벤트 제외**를 선택하십시오.
  5. 제외할 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오.
- **이벤트 코드별 제외**. 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.

단계 12. 특정 이벤트 유형을 포함할지 여부를 선택합니다.

- **모든 감사 이벤트 포함**. 선택한 이벤트 클래스 및 심각도에 따라 감사 이벤트에 대한 알림을 전송합니다.
- **보증 이벤트 포함**. 보증에 관한 알림을 전송합니다.
- **상태 변경 이벤트 포함**. 상태 변경에 관한 알림을 전송합니다.
- **상태 업데이트 이벤트 포함**. 새 경고에 대한 알림을 보냈습니다.
- **게시판 이벤트 포함**. 새 게시판에 관한 알림을 전송합니다.

단계 13. 알림을 받을 이벤트 유형 및 심각도를 선택하십시오.

단계 14. 서비스 가능성을 기준으로 이벤트를 필터링할지 여부를 선택합니다.

단계 15. **스케줄러** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 16. **옵션:** 이 이벤트 전달자에 특정 이벤트를 전달하려는 시간 및 요일을 정의하십시오. 지정된 시간 슬롯 중에 발생하는 이벤트만 전달됩니다.

이벤트 전달자에 대한 스케줄을 만들지 않는 경우 이벤트는 24시간 연중무휴 전달됩니다.

1. **왼쪽으로 화면 이동** 아이콘(◀) 및 **오른쪽으로 화면 이동** 아이콘(▶) 및 **일**, **주** 및 **월** 버튼을 사용하여 스케줄을 시작하려는 요일과 시간을 찾으십시오.

2. 새 시간 기간 대화 상자를 열려면 시간 슬롯을 두 번 클릭하십시오.
3. 날짜, 시작 및 종료 시간 및 스케줄 반복 여부와 같은 필요한 정보를 지정하십시오.
4. 스케줄을 저장하고 대화 상자를 닫으려면 **만들기**를 클릭하십시오. 일정에 새 스케줄이 추가됩니다.

팁:
- 일정 항목을 캘린더의 다른 시간 슬롯으로 드래그하여 시간 슬롯을 변경할 수 있습니다.
- 일정 항목의 상단 또는 하단을 선택하고 캘린더의 새 시간에 끌어 기간을 변경할 수 있습니다.
- 일정 항목의 하단을 선택하고 캘린더의 새 시간에 끌어 종료 시간을 변경할 수 있습니다.
- 캘린더의 일정 항목을 두 번 클릭하고 **항목 편집**을 클릭하여 일정을 변경할 수 있습니다.
- **스케줄러 요약 표시**를 선택하여 모든 일정 항목에 대한 요약을 볼 수 있습니다. 요약에는 각 항목에 대한 시간 슬롯과 반복 가능한 항목이 포함됩니다.
- 항목을 선택하고 **항목 삭제**를 클릭하여 캘린더 또는 스케줄러 요약에서 일정 항목을 삭제할 수 있습니다.

단계 17. **만들기**를 클릭하십시오.

이벤트 전달자는 이벤트 전달 테이블에 나열되어 있습니다.

단계 18. 새 이벤트 전달자를 선택하고 **테스트 이벤트 생성**을 클릭한 후 이벤트가 적절한 REST 웹 서비스에 올바로 전달되는지 확인하십시오.

완료한 후에

이벤트 전달 페이지에서 선택된 이벤트 전달자에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 전달자 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 전달자에 대한 세부 정보를 보십시오.
- **이름** 열에서 이벤트 전달자 이름을 클릭하여 이벤트 전달자 속성 및 필터 기준을 변경하십시오.
- **삭제** 아이콘()을 클릭하여 이벤트 전달자를 삭제합니다.
- 이벤트 전달을 보류하십시오(이벤트 전달 보류 참조).

원격 SNMPv1 또는 SNMPv3 관리자에 대한 이벤트 전달 설정

Lenovo XClarity Administrator을 설정하여 원격 SNMPv1 또는 SNMPv3 관리자로 특정 이벤트를 전달할 수 있습니다.

이 작업 정보

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

참고: XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게 RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

XClarity Administrator MIB에 대한 정보는 lenovoMgrAlert.mib 파일의 내용을 참조하십시오.

절차

원격 SNMPv1 또는 SNMPv3 관리자에 대한 이벤트 전달자를 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **이벤트 전달자** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 이벤트 전달자 대화 상자의 **일반** 탭이 표시됩니다.

단계 4. SNMPv1 또는 SNMPv3을 이벤트 전달자 유형으로 선택하고, 프로토콜별 정보를 기입하십시오.

- 이벤트 전달자에 대한 이름 및 대상 호스트를 입력하십시오.
- 이벤트 전달에 사용할 포트를 입력하십시오. 기본값은 162입니다.
- **옵션:** 설명, 연락처 이름 및 위치와 같은 추가 정보를 입력하십시오.
- SNMP 버전을 선택하십시오. 이는 다음 값 중 하나입니다.
  - SNMPv1. 이 버전을 선택한 경우 커뮤니티 암호가 장치에 모든 SNMP 요청과 함께 전송됩니다.
  - SNMPv3. 이것은 기본 버전이며 보안 강화를 위해 권장됩니다. SNMPv3을 선택한 경우 선택적으로 사용자 ID, 인증 유형 및 암호 및 개인 정보 유형 및 암호를 지정하십시오.

    SNMPv3 트랩 수신기에 XClarity Administrator 인스턴스에 대한 엔진 ID가 필요한 경우 다음 단계를 수행하여 엔진 ID를 찾을 수 있습니다.

    1. 연결 매개 변수(사용자 이름, authProtocol, authPassword, privProtocol, privPassword)가 XClarity Administrator에 설정된 매개 변수와 일치해야 합니다.
    2. 선호 소프트웨어(예, snmpwalk)를 사용하여 XClarity Administrator 서버에서 다음 OID 중 하나를 사용하여 SNMP GET 요청을 수행하십시오.
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots: 1.3.6.1.6.3.10.2.1.2.0

       `snmpget` 명령의 경우 다음 구문을 사용하십시오. 전달자 인증 유형은 SHA이거나 공백(인증 없음)일 수 있습니다.

       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER_AUTH_PW> -x <FORWARDER_PRIVACY_TYPE> -X <FORWARDER_PRIVACY_PW> <LXCA_IP> 1.3.6.1.6.3.10.2.1.1.0
       ```

       예를 들어 XClarity Administrator IP 주소가 192.0.1.0, 인증 유형이 SHA, 개인 정보 유형이 AES인 경우 다음 명령은 engineID를 보여줍니다.

       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1 192.0.1.0 1.3
       ```

       다음 예시 응답이 반환됩니다. 이 예에서 engineID는 0x80001370017F00000134C27E12입니다.

       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```

- 요청에 대한 제한 시간(초)을 입력하십시오. 기본값은 30초입니다.
- **옵션:** 트랩 인증이 필요한 경우 사용자 ID 및 인증 암호를 입력하십시오. 트랩을 전달할 원격 SNMP 관리자에 동일한 사용자 ID 및 암호를 입력해야 합니다.

- 트랩 발신자를 확인하기 위해 원격 SNMP 관리자가 사용하는 인증 프로토콜을 선택하십시오. 이는 다음 값 중 하나입니다.
  - SHA. 지정된 사용자 ID, 암호 및 도메인 이름을 사용하여 지정된 SNMP 서버에 대한 인증에 SHA 프로토콜을 사용합니다.
  - **없음**. 인증이 사용되지 않습니다.
- 트랩 암호화가 필요한 경우 개인 정보 유형(암호화 프로토콜) 및 암호를 입력하십시오. 이는 다음 값 중 하나입니다. 트랩을 전달할 원격 SNMP 관리자에 동일한 프로토콜 및 암호를 입력해야 합니다.
  - AES
  - DES
  - **없음**

단계 5. **제외된 이벤트 허용** 토글을 클릭하여 제외된 이벤트를 전달하도록 허용하거나 금지합니다.

단계 6. 이 이벤트 전달자에 대한 이벤트 전달을 활성화하려면 **이 전달자 사용**을 선택하십시오.

단계 7. **장치** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 8. 이 이벤트 전달자를 모니터링할 장치 및 그룹을 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

단계 9. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 10. 이 이벤트 전달자에 사용할 필터를 선택하십시오.

- **이벤트 범주별 일치**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
  2. 모든 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  3. 모든 상태 변경 이벤트를 전달하려면, **상태 변경 이벤트 포함**을 선택하십시오.
  4. 모든 상태 업데이트이벤트를 전달하려면, **상태 업데이트 이벤트 포함**을 선택하십시오.
  5. 전달하려는 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달에서 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오(예, `FQXHMEM0214I,FQXHMEM0214I`).
- **이벤트 코드별 일치**. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.
- **이벤트 범주별 제외**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 제외하려면 **모든 감사 이벤트 제외**를 선택하십시오.
  2. 모든 보증 이벤트를 제외하려면 **모든 보증 이벤트 제외**를 선택하십시오.
  3. 모든 상태 변경 이벤트를 제외하려면, **상태 변경 이벤트 제외**를 선택하십시오.
  4. 모든 상태 업데이트이벤트를 제외하려면, **상태 업데이트 이벤트 제외**를 선택하십시오.
  5. 제외할 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오.
- **이벤트 코드별 제외**. 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.

단계 11. 특정 이벤트 유형을 포함할지 여부를 선택합니다.

- **모든 감사 이벤트 포함**. 선택한 이벤트 클래스 및 심각도에 따라 감사 이벤트에 대한 알림을 전송합니다.
- **보증 이벤트 포함**. 보증에 관한 알림을 전송합니다.
- **상태 변경 이벤트 포함**. 상태 변경에 관한 알림을 전송합니다.
- **상태 업데이트 이벤트 포함**. 새 경고에 대한 알림을 보냈습니다.
- **게시판 이벤트 포함**. 새 게시판에 관한 알림을 전송합니다.

단계 12. 알림을 받을 이벤트 유형 및 심각도를 선택하십시오.

단계 13. 서비스 가능성을 기준으로 이벤트를 필터링할지 여부를 선택합니다.

단계 14. **스케줄러** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 15. **옵션:** 이 이벤트 전달자에 특정 이벤트를 전달하려는 시간 및 요일을 정의하십시오. 지정된 시간 슬롯 중에 발생하는 이벤트만 전달됩니다.

이벤트 전달자에 대한 스케줄을 만들지 않는 경우 이벤트는 24시간 연중무휴 전달됩니다.

1. **왼쪽으로 화면 이동** 아이콘(◀) 및 **오른쪽으로 화면 이동** 아이콘(▶) 및 **일**, **주** 및 **월** 버튼을 사용하여 스케줄을 시작하려는 요일과 시간을 찾으십시오.
2. 새 시간 기간 대화 상자를 열려면 시간 슬롯을 두 번 클릭하십시오.
3. 날짜, 시작 및 종료 시간 및 스케줄 반복 여부와 같은 필요한 정보를 지정하십시오.
4. 스케줄을 저장하고 대화 상자를 닫으려면 **만들기**를 클릭하십시오. 일정에 새 스케줄이 추가됩니다.

팁:
- 일정 항목을 캘린더의 다른 시간 슬롯으로 드래그하여 시간 슬롯을 변경할 수 있습니다.
- 일정 항목의 상단 또는 하단을 선택하고 캘린더의 새 시간에 끌어 기간을 변경할 수 있습니다.
- 일정 항목의 하단을 선택하고 캘린더의 새 시간에 끌어 종료 시간을 변경할 수 있습니다.
- 캘린더의 일정 항목을 두 번 클릭하고 **항목 편집**을 클릭하여 일정을 변경할 수 있습니다.
- **스케줄러 요약 표시**를 선택하여 모든 일정 항목에 대한 요약을 볼 수 있습니다. 요약에는 각 항목에 대한 시간 슬롯과 반복 가능한 항목이 포함됩니다.
- 항목을 선택하고 **항목 삭제**를 클릭하여 캘린더 또는 스케줄러 요약에서 일정 항목을 삭제할 수 있습니다.

단계 16. **만들기**를 클릭하십시오.

이벤트 전달자는 이벤트 전달 테이블에 나열되어 있습니다.

단계 17. 새 이벤트 전달자를 선택하고 **테스트 이벤트 생성**을 클릭한 다음 이벤트가 적절한 원격 SNMP 관리자에 올바로 전달되는지 확인하십시오.

완료한 후에

이벤트 전달 페이지에서 선택된 이벤트 전달자에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 전달자 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 전달자에 대한 세부 정보를 보십시오.
- **이름** 열에서 이벤트 전달자 이름을 클릭하여 이벤트 전달자 속성 및 필터 기준을 변경하십시오.
- **삭제** 아이콘()을 클릭하여 이벤트 전달자를 삭제합니다.
- 이벤트 전달을 보류하십시오(이벤트 전달 보류 참조).
- **만들기** 아이콘()을 클릭한 후 새 이벤트 전달 대화 상자의 일반 탭에서 **MIB 파일 다운로드**를 클릭하여 SNMP 트랩에 대한 정보가 포함된 MIB 파일을 다운로드하십시오.

lenovoMgrAlert.mib 파일

이 관리 정보 기반(MIB) 파일은 XClarity Administrator 및 관리되는 장치에 의해 발생한 경고를 포함하여 Lenovo XClarity Administrator에서 생성하는 SNMP 트랩을 설명합니다. XClarity Administrator에서 전송된 SNMP 트랩을 의미 있게 렌더링할 수 있도록 모든 SNMP 트랩 관리자에서 이 MIB 파일을 컴파일할 수 있습니다.

메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하고 **만들기** 아이콘()을 클릭하고 이벤트 전달자 유형에 대해 SNMP를 선택한 다음 대화 상자 하단의 **MIB 파일 다운로드**를 클릭하여 웹 인터페이스에서 MIB 파일을 다운로드할 수 있습니다.

다음 오브젝트가 모든 발신 SNMP 트랩에 포함되어 있습니다. 일부 SNMP 트랩에는 추가 오브젝트가 포함되어 있을 수 있습니다. 모든 오브젝트는 MIB 파일에 설명되어 있습니다. 복구 정보는 트랩에 포함되지 않습니다.

참고: 이 목록은 XClarity Administrator의 릴리스마다 다를 수 있습니다.
- mgrTrapAppId. "Lenovo Event Manager"입니다.
- mgrTrapCommonEvtID. 일반 이벤트 ID
- mgrTrapDateTime. 이벤트가 발생한 현지 날짜 및 시간
- mgrTrapEventClass. 이벤트의 소스. 감사, 냉각, 전원, 디스크, 메모리, 프로세서, 시스템, 테스트, 어댑터, 확장, IOModule 또는 블레이드일 수 있습니다.
- mgrTrapEvtID. 이벤트의 고유 식별자
- mgrTrapFailFRUs. 장애가 발생한 FRU UUID를 쉼표로 구분한 목록(있는 경우)
- mgrTrapFailSNs. 장애가 발생한 FRU 일련 번호의 쉼표로 구분된 목록입니다(있는 경우).
- mgrTrapFullyQualifiedDomainName. 정규화된 도메인 이름: 호스트 이름 및 도메인 이름
- mgrTrapID. Trap ID
- mgrTrapMsgText. 메시지 텍스트(영어로만 제공)
- mgrTrapMsgID. 메시지 식별자
- mgrTrapMtm. 이벤트를 발생시킨 장치의 모델 유형 모델
- mgrTrapService. 서비스 가능성 표시기입니다. 000(알 수 없음), 100(없음), 200(서비스 센터) 또는 300(고객)일 수 있음
- mgrTrapSeverity. 심각도 표시기입니다. 정보, 경고, 경미, 주요 또는 위험일 수 있음
- mgrTrapSN. 이벤트를 발생시킨 장치의 일련 번호
- mgrTrapSrcIP. 발생한 이벤트를 수신한 장치의 IP 주소
- mgrTrapSrcLoc. 이벤트를 발생시킨 장치의 위치로, 영어로만 제공됨(예: Slot#xx)
- mgrTrapSrcName. 이벤트를 발생시킨 장치의 호스트 이름 또는 표시 이름
- mgrTrapSysContact. 사용자 구성 연락처 ID
- mgrTrapSysLocation. 사용자 구성 장치 위치 정보
- mgrTrapSystemName. 장치 이름, 구성 요소 이름 및 슬롯 위치
- mgrTrapTxtId. 트랩을 발생시킨 Lenovo Event Manager 서버의 호스트 이름 또는 IP 주소
- mgrTrapUserid. 이벤트와 연결된 사용자 ID(이벤트가 내부용이고 이벤트 클래스가 감사인 경우)
- mgrTrapUuid. 이벤트를 발생시킨 장치의 UUID

syslog에 대한 이벤트 전달 설정

Lenovo XClarity Administrator을 설정하여 시스템 로그로 특정 이벤트를 전달할 수 있습니다.

이 작업 정보

특정 수신자로 이벤트를 보낼 최대 20개의 이벤트 전달자를 만들어 활성화할 수 있습니다.

이벤트 전달자가 구성된 후 XClarity Administrator가 재부팅되면 이벤트가 올바로 전달되기 전에 관리 서버가 내부 데이터를 다시 생성할 때까지 잠시 기다려야 합니다.

참고: XClarity Administrator v1.2.0 이상의 경우 **스위치**가 새 이벤트 전달자 및 이벤트 전달자 변경 대화 상자의 **이벤트** 탭에 포함되어 있습니다. 이전 릴리스에서 1.2.0 이상으로 업그레이드한 경우 적절하게 RackSwitch 이벤트를 포함 또는 제외하도록 이벤트 수신자를 업데이트하십시오. 이는 모든 장치를 선택하기 위해 **모든 시스템** 확인란을 선택한 경우에도 필요합니다.

절차

syslog에 대한 이벤트 전달자를 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **이벤트 전달자** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 이벤트 전달자 대화 상자의 **일반** 탭이 표시됩니다.

단계 4. Syslog를 이벤트 전달자 유형으로 선택하고 프로토콜 특정 정보를 입력하십시오.

- 이벤트 전달자에 대한 이름, 대상 호스트 및 옵션 설명을 입력하십시오.
- 이벤트 전달에 사용할 포트를 입력하십시오. 기본값은 514입니다.
- 이벤트 전달에 사용할 프로토콜을 선택하십시오. 이는 다음 값 중 하나입니다.
  - UDP
  - TCP
- 요청에 대한 제한 시간(초)을 입력하십시오. 기본값은 30초입니다.
- syslog에서 타임스탬프의 형식을 선택할 수 있습니다(옵션). 이는 다음 값 중 하나입니다.
  - **현지 시간**. 기본 형식입니다. 예: `Fri Mar 31 05:57:18 EDT 2017`.
  - GMT **시간**. 날짜 및 시간의 국제 표준(ISO8601)입니다. 예: `2017-03-31T05:58:20-04:00`.

단계 5. **출력 형식**을 클릭하여 전달할 이벤트 데이터의 출력 형식을 선택하십시오. 정보는 이벤트 전달자의 각 유형에 따라 다릅니다.

다음 예제 출력 형식은 sylog 수신자의 기본 형식입니다. 이중 대괄호 사이의 모든 단어는 이벤트가 전달될 때 실제 값으로 대체되는 변수입니다. sylog 수신자가 사용할 수 있는 변수는 출력 형식 대화 상자에 나열되어 있습니다.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

기본값으로 재설정을 클릭하여 출력 형식을 기본 필드로 다시 변경하십시오.

단계 6. **제외된 이벤트 허용** 토글을 클릭하여 제외된 이벤트를 전달하도록 허용하거나 금지합니다.

단계 7. 이 이벤트 전달자에 대한 이벤트 전달을 활성화하려면 **이 전달자 사용**을 선택하십시오.

단계 8. **장치** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 9. 이 이벤트 전달자를 모니터링할 장치 및 그룹을 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

단계 10. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 11. 이 이벤트 전달자에 사용할 필터를 선택하십시오.

- **이벤트 범주별 일치**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
  2. 모든 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  3. 모든 상태 변경 이벤트를 전달하려면, **상태 변경 이벤트 포함**을 선택하십시오.
  4. 모든 상태 업데이트이벤트를 전달하려면, **상태 업데이트 이벤트 포함**을 선택하십시오.
  5. 전달하려는 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달에서 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오(예, FQXHMEM0214I,FQXHMEM0214I).
- **이벤트 코드별 일치**. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.
- **이벤트 범주별 제외**.
  1. 상태 수준에 관계없이 모든 감사 이벤트를 제외하려면 **모든 감사 이벤트 제외**를 선택하십시오.
  2. 모든 보증 이벤트를 제외하려면 **모든 보증 이벤트 제외**를 선택하십시오.
  3. 모든 상태 변경 이벤트를 제외하려면, **상태 변경 이벤트 제외**를 선택하십시오.
  4. 모든 상태 업데이트이벤트를 제외하려면, **상태 업데이트 이벤트 제외**를 선택하십시오.
  5. 제외할 이벤트 클래스 및 서비스 가능성 수준을 선택하십시오.
  6. 전달할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 ID를 구분하십시오.
- **이벤트 코드별 제외**. 제외할 하나 이상의 이벤트 ID를 입력하십시오. 쉼표를 사용하여 여러 ID를 구분하십시오.

단계 12. 특정 이벤트 유형을 포함할지 여부를 선택합니다.

- **모든 감사 이벤트 포함**. 선택한 이벤트 클래스 및 심각도에 따라 감사 이벤트에 대한 알림을 전송합니다.
- **보증 이벤트 포함**. 보증에 관한 알림을 전송합니다.
- **상태 변경 이벤트 포함**. 상태 변경에 관한 알림을 전송합니다.
- **상태 업데이트 이벤트 포함**. 새 경고에 대한 알림을 보냈습니다.
- **게시판 이벤트 포함**. 새 게시판에 관한 알림을 전송합니다.

단계 13. 알림을 받을 이벤트 유형 및 심각도를 선택하십시오.

단계 14. 서비스 가능성을 기준으로 이벤트를 필터링할지 여부를 선택합니다.

단계 15. **스케줄러** 탭을 표시하려면 **다음**을 클릭하십시오.

단계 16. **옵션:** 이 이벤트 전달자에 특정 이벤트를 전달하려는 시간 및 요일을 정의하십시오. 지정된 시간 슬롯 중에 발생하는 이벤트만 전달됩니다.

이벤트 전달자에 대한 스케줄을 만들지 않는 경우 이벤트는 24시간 연중무휴 전달됩니다.

1. **왼쪽으로 화면 이동** 아이콘(◀) 및 **오른쪽으로 화면 이동** 아이콘(▶) 및 **일**, **주** 및 **월** 버튼을 사용하여 스케줄을 시작하려는 요일과 시간을 찾으십시오.

2. 새 시간 기간 대화 상자를 열려면 시간 슬롯을 두 번 클릭하십시오.
3. 날짜, 시작 및 종료 시간 및 스케줄 반복 여부와 같은 필요한 정보를 지정하십시오.
4. 스케줄을 저장하고 대화 상자를 닫으려면 **만들기**를 클릭하십시오. 일정에 새 스케줄이 추가됩니다.

팁:
- 일정 항목을 캘린더의 다른 시간 슬롯으로 드래그하여 시간 슬롯을 변경할 수 있습니다.
- 일정 항목의 상단 또는 하단을 선택하고 캘린더의 새 시간에 끌어 기간을 변경할 수 있습니다.
- 일정 항목의 하단을 선택하고 캘린더의 새 시간에 끌어 종료 시간을 변경할 수 있습니다.
- 캘린더의 일정 항목을 두 번 클릭하고 **항목 편집**을 클릭하여 일정을 변경할 수 있습니다.
- **스케줄러 요약 표시**를 선택하여 모든 일정 항목에 대한 요약을 볼 수 있습니다. 요약에는 각 항목에 대한 시간 슬롯과 반복 가능한 항목이 포함됩니다.
- 항목을 선택하고 **항목 삭제**를 클릭하여 캘린더 또는 스케줄러 요약에서 일정 항목을 삭제할 수 있습니다.

단계 17. **만들기**를 클릭하십시오.

이벤트 전달자는 이벤트 전달 테이블에 나열되어 있습니다.

단계 18. 새 전달자를 선택하고 **테스트 이벤트 생성**을 클릭한 다음 이벤트가 적절한 syslog에 올바로 전달되는지 확인하십시오.

완료한 후에

이벤트 전달 페이지에서 선택된 이벤트 전달자에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 전달자 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 전달자에 대한 세부 정보를 보십시오.
- **이름** 열에서 이벤트 전달자 이름을 클릭하여 이벤트 전달자 속성 및 필터 기준을 변경하십시오.
- **삭제** 아이콘()을 클릭하여 이벤트 전달자를 삭제합니다.
- 이벤트 전달을 보류하십시오(이벤트 전달 보류 참조).

이벤트 전달 보류

이벤트 전달자를 사용 안 함으로 설정하여 이벤트 전달을 보류할 수 있습니다. 이벤트 전달을 보류하면 수신 이벤트 모니터링이 중지됩니다. 모니터링하는 동안 수신된 이벤트는 보류되고 전달되지 않습니다.

이 작업 정보

사용 안 함 상태는 지속적이지 않습니다. 관리 노드를 다시 시작하는 경우 모든 이벤트 전달자가 사용으로 설정됩니다.

절차

이벤트 전달을 사용 안 함으로 설정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. 보류하려는 각 이벤트 전달자에 대해 **상태** 열에서 **사용 안 함**을 선택하십시오.

모바일 장치에 이벤트 전달

Lenovo XClarity Administrator를 모바일 장치에 이벤트 알림을 푸시하도록 구성할 수 있습니다.

시작하기 전에

모바일 장치에 이벤트를 전달하려면 다음 요구사항을 충족해야 합니다.

- 유효한 DNS 서버가 Lenovo XClarity Administrator가 Apple 또는 Google 푸시 서버에 연결을 허용하도록 구성되어 있어야 합니다. 이는 **관리 → 네트워크 액세스 → 네트워크 액세스 편집** 을 클릭한 다음 **인터넷 설정** 탭을 클릭하여 구성할 수 있습니다(네트워크 액세스 구성 참조).
- 이벤트 관리에 필요한 모든 포트가 네트워크와 방화벽에서 열려 있어야 합니다. 포트 요구사항에 대한 정보는 Lenovo XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

이 작업 정보

Lenovo XClarity Mobile 앱이 모바일 장치에 설치된 경우 연결된 각 Lenovo XClarity Administrator 인스턴스가 해당 모바일 장치에 이벤트 알림을 푸시하도록 설정할 수 있습니다. 특정 인스턴스에 대해 푸시 알림을 사용으로 설정한 경우 해당 모바일 장치에 대해 Lenovo XClarity Administrator에 구독이 만들어집니다.

각 Lenovo XClarity Administrator 인스턴스에 대해 사전 정의된 또는 사용자 지정된 글로벌 이벤트 필터를 할당하여 모바일 장치에 푸시되는 이벤트를 정의할 수 있습니다. 사전 정의된 글로벌 이벤트 필터는 기본적으로 사용으로 설정됩니다. Lenovo XClarity Administrator는 필터 기준에 따라 수신 이벤트에 대한 모니터링을 시작합니다. 일치하는 것을 찾으면 모바일 장치에 이벤트가 전달됩니다.

Lenovo XClarity Mobile 및 지원되는 모바일 장치에 대한 자세한 정보는 Lenovo XClarity Mobile 앱 사용의 내용을 참조하십시오.

절차

해당 모바일 장치에 푸시 알림을 설정하려면 모바일 장치의 Lenovo XClarity Mobile 앱에서 다음 단계를 완료하십시오.

단계 1. 푸시 알림을 사용으로 설정하십시오.

- Lenovo XClarity Administrator 인스턴스에 대한 연결을 만들 때 푸시 알림을 사용으로 설정할 수 있습니다. 푸시 알림은 기본적으로 사용으로 설정되어 있습니다.
- 하나 이상의 이벤트 필터를 사용으로 설정하여 기존 연결에서 푸시 알림을 사용 설정할 수 있습니다.

단계 2. 모바일 장치에 어떤 이벤트를 전달할 것인지 지정하려면 글로벌 이벤트 필터를 할당하십시오.

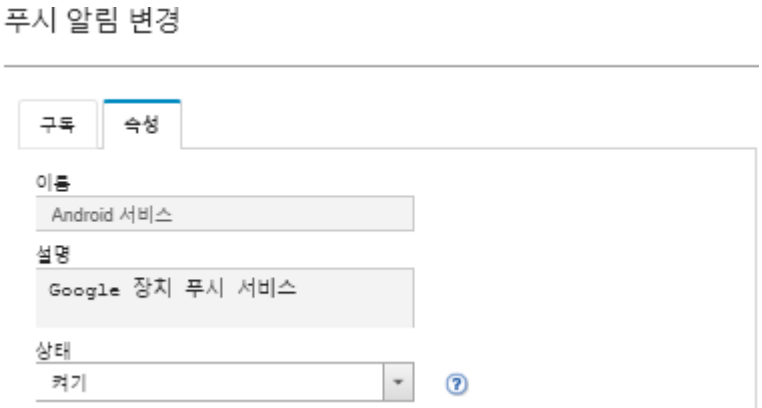
참고: Lenovo XClarity Mobile 앱에서만 구독에서 글로벌 필터를 추가 또는 제거할 수 있습니다. Lenovo XClarity Administrator 웹 인터페이스에서만 글로벌 필터를 만들 수 있습니다. 사용자 지정된 글로벌 이벤트 필터 만들기에 대한 정보는 모바일 장치 및 WebSocket에 대한 이벤트 필터 만들기의 내용을 참조하십시오.

1. **설정 → 푸시 알림**을 탭하십시오. Lenovo XClarity Administrator 연결 목록이 표시됩니다.
2. 푸시 필터 목록을 표시하려면 Lenovo XClarity Administrator 인스턴스를 탭하십시오.
3. Lenovo XClarity Administrator 인스턴스에 대해 모바일 장치에 푸시하려는 이벤트의 이벤트 필터를 사용으로 설정하십시오.
4. 이벤트 알림이 올바르 푸시되는지 확인하려면 **터치하여 테스트 푸시 알림 생성**을 탭하십시오.

결과

Lenovo XClarity Administrator 웹 인터페이스의 이벤트 전달 페이지에서 구독을 관리할 수 있습니다. 이벤트 전달 페이지를 표시하려면 **모니터링 → 이벤트 전달**을 클릭하십시오.

- 푸시 알림 변경 대화 상자를 표시하려면 **이름** 열의 푸시 알림 서비스(Google 또는 Apple)의 링크를 클릭하여 이벤트 전달 페이지의 **푸시 서비스** 탭에서 장치 알림 서비스 속성을 변경한 다음 **속성** 탭을 클릭할 수 있습니다.

- 구독을 사용 및 사용 안 함으로 설정할 수 있습니다.
  - 장치 알림 서비스 테이블에서 ON 또는 OFF 상태를 선택하여 이벤트 전달 페이지의 **푸시 서비스** 탭에서 특정 장치 알림 서비스에 대한 모든 구독을 사용 또는 사용 안 함으로 설정하십시오.
  - **설정 → 푸시 알림**을 탭한 다음 푸시 알림을 사용으로 설정하거나 사용으로 설정된 푸시 알림을 사용 안 함으로 설정하여 Lenovo XClarity Mobile 앱에서 특정 장치에 대한 모든 구독을 사용 또는 사용 안 함으로 설정하십시오.

  - **설정 → 푸시 알림**을 탭하고 Lenovo XClarity Administrator 연결을 탭하고 하나 이상의 이벤트 필터를 사용으로 설정하거나 모든 이벤트 필터를 사용 안 함으로 설정하여 Lenovo XClarity Mobile 앱에서 특정 구독을 사용 또는 사용 안 함으로 설정하십시오.
- 모바일 서비스를 선택하고 **테스트 이벤트 생성**을 클릭하여 이벤트 전달 페이지의 **푸시 서비스** 탭에서 특정 모바일 서비스에 대한 모든 구독에 대해 테스트 이벤트를 생성할 수 있습니다.
- 현재 구독 목록을 볼 수 있습니다. 이벤트 전달 페이지의 **푸시 서비스** 탭에서 **이름** 열에서 해당 장치 알림 서비스(Android 또는 iOS)의 링크를 클릭하여 푸시 알림 변경 대화 상자를 표시한 다음 **구독** 탭을 클릭하십시오. 장치 ID는 각 구독을 식별합니다.

  팁:

  - 장치 ID는 푸시 등록 ID의 처음 및 마지막 6개 숫자입니다. **설정 → 정보 → 푸시 등록 ID**를 탭하여 Lenovo XClarity Mobile 앱에서 푸시 등록 ID를 찾을 수 있습니다.
  - 다음 역할 중 하나를 가진 사용자로 로그인한 경우 모든 구독이 표시됩니다. 그렇지 않으면 로그인한 사용자에 대한 구독만 표시됩니다.
    - lxc-admin
    - lxc-supervisor
    - lxc-security-admin
    - lxc-sysmgr
- 구독에 대한 **이벤트 필터**의 **필터 목록**을 확장하여 푸시 알림 변경 대화 상자의 **구독** 탭에서 구독에 할당된 이벤트 필터 목록을 볼 수 있습니다.

- 구독을 클릭하여 푸시 알림 변경 대화 상자의 **구독** 탭에서 특정 구독에 대한 이벤트 필터를 만들고 **만들기** 아이콘( )을 클릭할 수 있습니다.

  참고: 이러한 이벤트 필터는 특정 구독에만 적용되고 다른 구독은 사용할 수 없습니다.

  또한 이벤트 필터를 선택하고 각각 **편집** 아이콘( ) 또는 **제거** 아이콘( )을 클릭하여 이벤트 필터를 편집 또는 제거할 수 있습니다.
- 푸시 알림 변경 대화 상자의 **구독** 탭에서 특정 구독에 대해 마지막으로 시도한 푸시의 상태를 확인할 수 있습니다. **타임스탬프** 열에는 마지막 푸시의 날짜 및 시간이 표시됩니다. **상태**는 푸시 알림이 푸시 서비스에 성공적으로 전달되었는지 표시합니다. 푸시 알림이 서비스에서 장치에 성공적으로 잔달되었는지에 대해 상태를 사용할 수 없습니다. 푸시 서비스를 전달하지 못한 경우 상태 열에 오류에 대한 추가 정보가 제공됩니다.
- 구독을 선택하고 **테스트 이벤트 생성**을 클릭하여 푸시 알림 변경 대화 상자의 **구독** 탭에서 특정 구독에 대한 테스트 이벤트를 생성할 수 있습니다.
- 구독을 선택하고 **제거** 아이콘( )을 클릭하여 푸시 알림 변경 대화 상자의 **구독** 탭에서 구독을 제거할 수 있습니다.

WebSocket 서비스에 이벤트 전달

Lenovo XClarity Administrator를 WebSocket 서비스에 이벤트 알림을 푸시하도록 구성할 수 있습니다.

이 작업 정보

WebSocket 구독은 Lenovo XClarity Administrator에 지속적으로 저장되지 않습니다. Lenovo XClarity Administrator가 재부팅되는 경우 WebSocket 구독자가 다시 구독해야 합니다.

절차

WebSocket 서비스에 이벤트 알림을 푸시하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.

단계 2. **푸시 서비스** 탭을 클릭하십시오.

단계 3. **이름** 열의 **WebSocket 서비스** 링크를 클릭하십시오. 푸시 알림 변경 대화 상자가 표시됩니다.

단계 4. **구독** 탭을 클릭하십시오.

단계 5. **만들기** 아이콘( )을 클릭하십시오.

단계 6. 대상 호스트의 IP 주소를 입력하십시오.

단계 7. **만들기**를 클릭하십시오.

단계 8. 새 구독을 선택하고 **테스트 이벤트 생성**을 클릭한 다음 이벤트가 WebSocket 서비스에 올바로 전달되었는지 확인하십시오.

결과

푸시 알림 변경 대화 상자의 **구독** 탭에서 선택된 WebSocket 구독에서 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘( )을 클릭하여 WebSocket 서비스 목록을 새로 고치십시오.
- 구독을 선택하고 **제거** 아이콘( )을 클릭하여 구독을 삭제하십시오.
- **상태** 열의 내용을 확인하여 특정 구독에 대해 마지막으로 시도한 푸시의 상태를 확인하십시오. 시도가 실패하는 경우 이 열에는 오류를 설명하는 메시지가 포함됩니다.

푸시 알림 변경 대화 상자의 **속성** 탭에서 다음 작업을 수행할 수 있습니다.

- 연결 유휴 시간, 최대 버퍼 크기, 최대 구독자 수 및 등록 제한시간 기간과 같은 WebSocket 서비스 속성을 변경하십시오.
- **기본값 복원**을 클릭하여 WebSocket 서비스를 기본 설정으로 재설정할 수 있습니다.
- **상태**를 꺼짐으로 설정하여 WebSocket 서비스에 대한 모든 구독에 이벤트 알림 푸시를 보류하십시오.

이벤트 전달 페이지의 **푸시 서비스** 탭에서 WebSocket 서비스를 선택하고 **테스트 이벤트 생성**을 클릭하여 모든 WebSocket 구독에 대한 테스트 이벤트를 생성할 수 있습니다.

모바일 장치 및 WebSocket에 대한 이벤트 필터 만들기

모바일 장치 및 WebSocket에 대한 하나 이상의 구독에 사용할 수 있는 글로벌 이벤트를 만들 수 있습니다. 또한 구독에 고유한 이벤트 필터를 만들 수 있습니다.

시작하기 전에

이벤트 필터를 만들려면 감독자 권한이 있어야 합니다.

최대 20개의 글로벌 이벤트 필터를 만들 수 있습니다.

이 작업 정보

다음 글로벌 이벤트 필터가 사전 정의되어 있습니다.

- **Match All Critical**. 이 필터는 모든 관리되는 장치 또는 XClarity Administrator에서 생성한 모든 중요 이벤트를 필터링합니다.
- **Match All Warning**. 이 필터는 모든 관리되는 장치 또는 XClarity Administrator에서 생성한 모든 경고 이벤트를 필터링합니다.

절차

글로벌 이벤트 필터를 만들려면 다음 단계를 완료하십시오.

- 구독이 사용할 수 있는 글로벌 이벤트 필터를 만드십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 이벤트 전달 페이지가 표시됩니다.
  2. **푸시 필터** 탭을 클릭하십시오.
  3. **만들기** 아이콘( )을 클릭하십시오. 새 푸시 필터 대화 상자의 **일반** 탭이 표시됩니다.
  4. 이 이벤트 필터에 대한 이름과 옵션 설명을 지정하십시오.
  5. **시스템** 탭을 표시하려면 **다음**을 클릭하십시오.
  6. 모니터할 장치를 선택하십시오.

     팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.
  7. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.
  8. 이벤트를 전달할 구성 요소 및 심각도를 선택하십시오.

     팁:
     - 모든 하드웨어 이벤트를 전달하려면 **모든 이벤트 일치**를 선택하십시오.
     - 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
     - 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
  9. **만들기**를 클릭하십시오.
- 특정 구독에 대한 이벤트 필터를 만드십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 이벤트 전달**을 클릭하십시오. 새 이벤트 전달 페이지가 표시됩니다.
  2. **푸시 필터** 탭을 클릭하십시오.
  3. 표의 이름 열에서 모바일 장치의 유형(Android 또는 iOS)에 대한 링크를 선택하십시오. 푸시 알림 변경 대화 상자가 표시됩니다.
  4. 활성 구독 목록을 표시하려면 **구독** 탭을 클릭하십시오.
  5. 구독을 선택하고 **만들기** 아이콘( )을 클릭하십시오. 새 이벤트 필터 대화 상자의 **일반** 탭이 표시됩니다.
  6. 이 이벤트 필터에 대한 이름과 옵션 설명을 지정하십시오.
  7. **시스템** 탭을 표시하려면 **다음**을 클릭하십시오.
  8. 모니터할 장치를 선택하십시오.

팁 모든 관리 장치(현재 또는 이후)의 이벤트를 전달하려면 **모든 시스템 일치** 선택란을 선택하십시오.**모든 시스템 일치** 선택란을 선택하지 않는 경우 선택된 장치는 UUID 열에 DUMMY-UUID가 없어야 합니다. 더미 UUID가 다시 시작 후 아직 복구되지 않았거나 관리 서버가 완전히 발견되지 않은 장치에 할당됩니다. 더미 UUID가 있는 장치를 선택하는 경우 장치가 완전히 발견되거나 더미 UUID가 실제 UUID로 변경되는 순간까지 이 장치에 이벤트 전달이 작동하지 않습니다.

9. **이벤트** 탭을 표시하려면 **다음**을 클릭하십시오.
10. 이벤트를 전달할 구성 요소 및 심각도를 선택하십시오.

    팁:
    - 모든 하드웨어 이벤트를 전달하려면 **모든 이벤트 일치**를 선택하십시오.
    - 감사 이벤트를 전달하려면 **모든 감사 이벤트 포함**을 선택하십시오.
    - 보증 이벤트를 전달하려면 **모든 보증 이벤트 포함**을 선택하십시오.
11. **만들기**를 클릭하십시오.

완료한 후에

이벤트 전달 페이지의 푸시 필터 탭에서 선택한 이벤트 필터에 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 이벤트 필터 목록을 새로 고치십시오.
- **이름** 열의 링크를 클릭하여 특정 이벤트 필터에 대한 세부 정보를 보십시오.
- **편집** 아이콘()을 클릭하여 이벤트 필터 속성 및 필터 기준을 변경하십시오.

삭제 아이콘()을 클릭하여 이벤트 필터를 삭제합니다.

작업 관련 작업

*작업*은 하나 이상의 장치에 대해 수행되는 더 긴 실행 작업입니다. 특정 작업이 한 번만(즉시 또는 나중에), 반복적으로 또는 특정 이벤트가 발생할 때 실행되도록 예약할 수 있습니다.

작업은 배경 화면에서 실행됩니다. 작업 로그에서 각 작업의 상태를 볼 수 있습니다.

작업 모니터링

Lenovo XClarity Administrator에서 시작하는 모든 작업에 대한 로그를 볼 수 있습니다. 작업 로그에는 실행 중이거나 완료되었거나 오류가 있는 작업이 포함됩니다.

이 작업 정보

*작업*은 하나 이상의 장치에 대해 수행되는 더 오래 실행 중인 작업입니다. 예를 들어 여러 개의 서버에 운영 체제를 배포하는 경우 각 서버 배포는 별도의 작업으로 나열됩니다.

작업은 배경 화면에서 실행됩니다. 작업 로그에서 각 작업의 상태를 볼 수 있습니다.

작업 로그에는 각 작업에 대한 정보가 들어 있습니다. 로그에는 최대 1,000개의 작업 또는 1GB가 포함될 수 있습니다. 최대 크기에 도달하면 성공적으로 완료된 가장 오래된 작업이 삭제됩니다. 로그에 성공적으로 완료된 작업이 없으면 경고와 함께 완료된 가장 오래된 작업이 삭제됩니다. 로그에 성공적으로 완료되거나 경고와 함께 완료된 작업이 없으면 오류와 함께 완료된 가장 오래된 작업이 삭제됩니다.

절차

다음 단계 중 하나를 완료하여 작업 로그를 표시하십시오.

- XClarity Administrator 제목 표시줄에서 **작업**을 클릭하여 실행 중이거나 완료되었거나 오류가 있는 작업의 요약을 표시합니다.

이 풀다운에서 다음 탭을 클릭할 수 있습니다.
- **오류**. 관련된 오류가 있는 모든 작업의 목록을 표시합니다.
- **경고**. 관련된 경고가 있는 모든 작업의 목록을 표시합니다.
- **실행 중**. 현재 진행 중인 모든 작업의 목록을 표시합니다.
- **완료됨**. 완료된 모든 작업의 목록을 표시합니다.

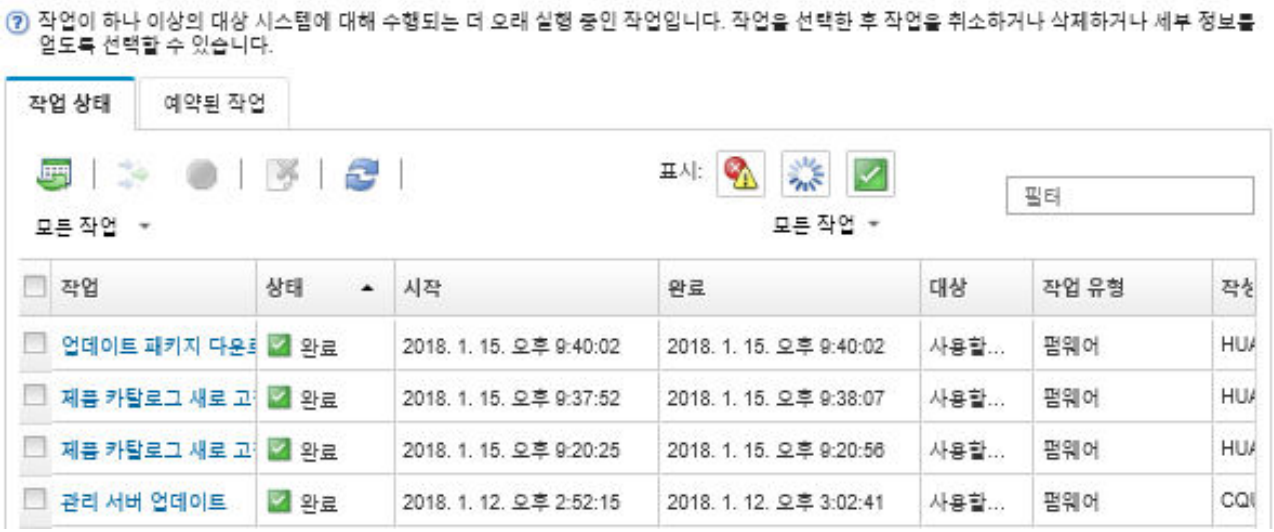
상태, 진행 상태 및 작업을 만든 사용자 등 작업에 대한 자세한 정보를 가져오려면 풀다운에서 작업 항목에 커서를 놓으십시오.

- XClarity Administrator 제목 표시줄에서 **작업**을 클릭하고 **모든 작업 보기** 링크를 클릭하여 작업 상태 페이지를 표시하십시오.
- XClarity Administrator 메뉴 표시줄에서 **모니터 → 작업**을 클릭한 후 **작업 상태** 탭을 클릭하여 작업 상태 페이지를 표시합니다.

완료한 후에

작업 페이지는 XClarity Administrator에 대한 모든 작업의 목록과 함께 표시됩니다.

작업



이 페이지에서 다음 작업을 수행할 수 있습니다.

- **예약된 작업** 탭을 클릭하여 작업 일정을 만듭니다(작업 스케줄링 참조).
- **작업** 열에서 작업 설명을 클릭하여 특정 작업에 대한 자세한 정보를 확인하십시오. 하위 작업 및 해당 대상 목록, 필요한 작업을 포함한 하위 작업의 요약 및 각 메시지의 심각도와 타임 스탬프를 포함한 로그 세부 정보가 있는 대화 상자가 표시됩니다. 하위 작업에 대한 로그를 숨기거나 표시하도록 선택할 수 있습니다.
- 예약된 작업의 경우 **작업** 열의 작업 설명에 있는 "이" 링크를 클릭하여 작업 일정에 대한 정보를 확인하십시오.
- 페이지당 표시된 작업의 수를 변경하십시오. 기본값은 10개의 작업입니다. 25개, 50개 또는 모든 작업을 표시할 수 있습니다.
- 표시된 작업의 목록을 압축하십시오.
  - **작업 유형**을 클릭하고 다음 옵션을 선택하여 특정 소스의 작업만 나열하십시오.
    - **모든 작업 유형**
    - **서비스**
    - **관리**
    - **구성**
    - **펌웨어**
    - Health
    - **전원**
    - **원격 액세스**
    - **시스템 ID**
    - OS **이미지**
    - OS **배포**
    - OS **프로필 내보내기**
    - **사용자 지정**
    - **인벤토리**
    - **알 수 없음**
  - **일정 유형**을 클릭하고 다음 옵션 중에서 선택하여 특정 일정 유형과 관련된 예약된 작업만 나열하십시오.
    - **모든 일정 유형**
    - **한 번**
    - **반복**

  - 트리거됨
  - **오류/경고 작업 숨기기** 아이콘()을 클릭하여 오류 또는 경고가 있는 작업을 숨기거나 표시하십시오.
  - **실행 중인 작업 숨기기** 아이콘()을 클릭하여 현재 실행 중인 작업을 숨기거나 표시하십시오.
  - **완료된 작업 숨기기** 아이콘()을 클릭하여 완료된 작업을 숨기거나 표시합니다.
  - **필터** 필드에 텍스트를 입력하여 특정 텍스트가 포함된 작업만 나열하십시오.
  - 페이지에 필터링이 적용된 경우 **모든 작업 표시** 아이콘()을 클릭하여 필터를 제거하십시오.
  - 열 표제를 클릭하여 작업을 열 기준으로 정렬하십시오.
- **CSV로 내보내기** 아이콘()을 클릭하여 작업 목록을 CSV 파일로 내보내십시오.

  참고: 내보낸 로그의 타임스탬프는 웹 브라우저에서 지정한 현지 시간을 사용합니다.
- 하나 이상의 실행 중인 작업 또는 하위 작업을 선택하고 **중지** 아이콘()을 클릭하여 실행 중인 작업 또는 하위 작업을 취소하십시오.

  참고: 작업을 취소하려면 몇 분 정도가 걸릴 수 있습니다.
- 하나 이상의 완료된 작업을 선택하고 **삭제** 아이콘()을 클릭하여 작업 로그에서 완료된 작업 또는 하위 작업을 삭제하십시오.
- 작업을 선택하고 **CSV로 내보내기**아이콘()을 클릭하여 특정 작업에 대한 정보를 내보내십시오.
- **새로 고침** 아이콘()을 클릭하여 작업 로그를 새로 고치십시오.

작업 스케줄링

Lenovo XClarity Administrator에서 일정을 만들어 특정 시간에 특정 작업을 실행할 수 있습니다.

이 작업 정보

다음 유형의 작업을 예약할 수 있습니다.
- 전원 끄기 및 재부팅과 같은 간단한 작업
- 특정 장치에 대한 서비스 데이터 수집
- Lenovo 웹 사이트에서 펌웨어 업데이트 및 OS 장치 드라이버 카탈로그 새로 고침
- Lenovo 웹 사이트에서 XClarity Administrator 업데이트 카탈로그 새로 고침
- Lenovo 웹 사이트에서 펌웨어 다운로드
- 관리되는 장치에서 펌웨어 및 OS 장치 드라이버 업데이트
- XClarity Administrator 데이터 및 설정 백업
- 스위치 구성 데이터 백업 및 복원

다음과 같이 실행할 작업을 예약할 수 있습니다.
- 한 번만(즉시 또는 나중에)
- 반복적으로
- 특정 이벤트 발생 시

절차

작업을 만들고 예약하려면 다음 단계를 완료하십시오.
- 펌웨어 업데이트 및 서비스 데이터 수집과 같은 복잡한 작업의 경우 현재 작업 페이지나 대화 상자에서 작업을 만드십시오.
  1. **일정**을 클릭하여 이 작업을 실행할 일정을 만드십시오. 새 작업 예약 대화 상자가 표시됩니다.
  2. 작업의 이름을 입력하십시오.

3. 다음과 같이 작업을 실행할 시기를 지정하십시오. 사용 가능한 옵션은 작업 유형에 따라 다릅니다. 일부 작업은 이벤트에 의해 반복되거나 트리거될 수 없습니다.
   - **한 번**. 이러한 작업은 한 번만 실행됩니다. 이 작업을 실행할 날짜와 시간을 지정하십시오.
   - **반복**. 이러한 작업은 두 번 이상 실행됩니다. 이 작업을 실행할 시기와 빈도를 지정하십시오.
   - **이벤트 발생 시 트리거됨**. 이러한 작업은 특정 이벤트가 발생할 때 실행됩니다.
     a. 이 작업을 실행할 날짜와 시간을 지정하고 **다음**을 클릭하십시오.
     b. 작업을 트리거할 이벤트를 선택하십시오.
4. **작업 만들기**를 클릭하십시오.

- 전원 켜기 및 재부팅과 같은 간단한 작업의 경우 작업 페이지에서 작업 일정을 만드십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **모니터** → **작업**을 클릭하고 **예약된 작업** 탭을 클릭하여 예약된 작업 페이지를 표시하십시오.
  2. **만들기** 아이콘( )을 클릭하여 새 작업 예약 대화 상자를 표시하십시오.
  3. 작업의 이름을 입력하십시오.
  4. 다음과 같이 작업을 실행할 시기를 지정하십시오.
     - **한 번**. 이러한 작업은 한 번만 실행됩니다.
       a. 이 작업을 실행할 날짜와 시간을 지정하고 **다음**을 클릭하십시오.
       b. 작업을 실행할 관리되는 장치를 선택하십시오.
     - **반복**. 이러한 작업은 두 번 이상 실행됩니다.
       a. 이 작업을 실행할 시기와 빈도를 지정하십시오.
       b. 작업을 실행할 관리되는 장치를 선택하십시오.
     - **이벤트 발생 시 트리거됨**. 이러한 작업은 특정 이벤트가 발생할 때 실행됩니다.
       a. 이 작업을 실행할 날짜와 시간을 지정하고 **다음**을 클릭하십시오.
       b. 작업을 실행할 관리되는 장치를 선택하고 **다음**을 클릭하십시오.
       c. 작업을 트리거할 이벤트를 선택하십시오.
  5. **만들기**를 클릭하십시오.

완료한 후에

예약된 작업 탭이 XClarity Administrator의 모든 작업 일정 목록과 함께 표시됩니다.

작업

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **작업** 열에서 링크를 클릭하여 특정 작업 일정에 대해 활성 상태인 작업과 완료된 작업에 대한 정보를 확인합니다.
  - **일정 유형**을 클릭하고 다음 옵션 중에서 선택하여 특정 일정 유형에 의해 표시되는 작업 일정 목록의 범위를 줄입니다.
    - **모든 일정 유형**
    - **한 번**
    - **반복**
    - **트리거됨**
  - 다음 아이콘 중 하나를 클릭하여 특정 상태에 있는 작업 일정만 숨기거나 표시합니다.
    - **활성** 아이콘()을 클릭하여 활성 상태인 모든 예약된 작업을 표시합니다.
    - **일시 중지됨** 아이콘()을 클릭하여 활성 상태가 아닌 모든 예약된 작업을 표시합니다.
    - **종료됨** 아이콘()을 클릭하여 이미 실행되었거나 다시 실행하도록 예약되지 않은 모든 예약된 작업을 표시합니다.
  - **필터** 필드에 텍스트를 입력하여 특정 텍스트가 포함된 예약된 작업만 나열합니다.
  - 열 표제를 클릭하여 예약된 작업을 열 기준으로 정렬합니다.
- **마지막 실행** 열을 보고 작업이 마지막으로 실행된 시기를 확인합니다. 해당 열의 "작업 상태" 링크를 클릭하여 마지막 실행 작업의 상태를 확인합니다.
- **다음 실행** 열을 보고 다음에 작업을 실행하도록 예약된 시기를 확인합니다. 해당 열의 "추가" 링크를 클릭하여 이후의 모든 날짜와 시간 목록을 확인합니다.
- **실행** 아이콘()을 클릭하여 일정과 관련된 작업을 즉시 실행합니다.

- **일시 중지** 아이콘( ) 또는 **활성화** 아이콘( )을클릭하여 작업 일정을 각각 사용 안 함 또는 사용으로 설정합니다.
- **복사** 아이콘( )을 클릭하여 작업 일정을 복사한 후 수정합니다.
- **편집** 아이콘( )을 클릭하여 작업 일정을 편집합니다.
- **삭제** 아이콘( )을 클릭하여 하나 이상의 선택된 작업 일정을 삭제합니다.
- 일정을 선택하고 CSV로 **내보내기**아이콘( )을 클릭하여 특정 작업 일정에 대한 정보를 내보내십시오.
- **모든 작업 → 새로 고침**을 클릭하여 작업 일정 목록을 새로 고칩니다.

작업에 해결 방법 및 주석 추가

성공 또는 오류 상태에 관계없이 완료된 작업에 해결 방법과 주석을 추가할 수 있습니다. 상위 작업 및 작업의 하위 작업에 대해 이를 수행할 수 있습니다.

절차

작업에 해결 방법과 주석을 추가하려면 다음 단계 중 하나를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **모니터 → 작업**을 클릭한 후 **작업 상태** 탭을 클릭하여 작업 상태 페이지를 표시합니다.

단계 2. **작업** 열에서 작업에 대한 링크를 클릭하여 작업 세부 정보를 표시합니다.

단계 3. **메모** 아이콘( )을 클릭하여 메모 대화 상자를 표시합니다.

이 대화 상자에서 작업에 추가된 모든 메모와 해결 방법에 대한 기록을 볼 수 있습니다. **모든 레코드 지우기**를 클릭하여 기록을 지울 수 있습니다.

단계 4. 다음 해결 방법 중 하나를 선택하십시오.
- **변경 없음**
- **조사 중**
- **해결됨**
- **중단됨**

단계 5. **메모** 필드에 설명을 추가하십시오.

단계 6. **적용**을 클릭하십시오.

작업 상태 페이지에서 해결 방법이 해당 작업의 **상태** 열에 표시됩니다.

작업 및 이벤트 간의 관계 보기

*플로우 다이어그램*은 사용자가 수동으로 시작하거나 Lenovo XClarity Administrator에서 자동으로 시작한 활동(작업 및 이벤트 포함) 간의 관계를 보여주는 그래픽 보기입니다. 플로우 다이어그램은 시작된 작업 및 생성된 이벤트의 순서, 생성된 시기 및 이벤트 생성 원인을 표시하여 문제를 식별하는 데 도움을 줍니다.

시작하기 전에

활동 플로우는 기본적으로 비활성화되어 있습니다. 활동에 대해 플로우가 생성되기 전에 활동 플로우를 사용으로 설정해야 합니다. 활동 흐름을 사용하는 경우, 발생하는 활동에 대해서만 흐름을 볼 수 있습니다.

주의: 활동 플로우는 XClarity Administrator에 의한 메모리 사용량을 증가시킵니다. XClarity Administrator에 의한 메모리 사용량이 이미 높은 경우 활동 플로우를 사용으로 설정하지 않는 것이 좋습니다.

이 작업 정보

다음 예는 플로우 다이어그램을 보여줍니다. 이벤트 순서는 왼쪽에서 오른쪽입니다. 플로우의 각 노드는 단일 활동을 나타내며 활동 설명, 날짜 및 상태를 포함합니다. 노드 제목 위에 커서를 올려 놓으면 활동에 대한 추가 정보를 볼 수 있습니다.

노드 사이의 선 스타일은 노드 간의 관계에 대한 확실성을 나타냅니다.
- 실선은 높은 확실성을 나타냅니다.
- 긴 점선은 중간 정도의 확실성을 나타냅니다.
- 짧은 점선은 낮은 확실성을 나타냅니다.

절차

특정 활동에 대한 플로우 다이어그램을 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 활동 플로우**를 클릭하여 활동 플로우 페이지를 표시하십시오.

단계 2. **활동 플로우 사용**을 선택하여 활동 플로우를 사용으로 설정하십시오.

단계 3. **활동** 섹션에서 작업 또는 이벤트를 선택하십시오.

특정 활동을 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 상태 유형, 활동 유형, 날짜를 선택하거나 사용자 정의 필터를 입력하거나 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하고 선택한 기준을 충족하는 활동만 나열할 수 있습니다.

단계 4. 플로우 **다이어그램 생성**을 클릭하여 플로우 **다이어그램** 섹션에서 플로우 다이어그램을 표시합니다.

완료한 후에

이 페이지에서 다음 작업을 수행할 수 있습니다.

- 커서를 활동 위에 놓으면 플로우 다이어그램의 각 활동에 대한 추가 정보를 볼 수 있습니다.
- **작업 → CSV로 내보내기**를 클릭하여 선택한 활동과 관련된 플로우를 CSV 파일로 내보냅니다.

제 4 장 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.

제 5 장 리소스 그룹 관리

Lenovo XClarity Administrator에서 리소스 그룹을 사용하여 집합적으로 보고 작업할 수 있는 관리되는 장치의 논리적 집합을 만들 수 있습니다.

자세히 알아보기: XClarity Administrator: 리소스 그룹

이 작업 정보

리소스 그룹에는 세 가지 유형이 있습니다.

- Static. 특정 장치의 사용자 지정된 그룹.
- **동적**. 규칙 기반 장치 그룹(예, 특정 유형의 모든 서버). 이 그룹에는 인벤토리 속성 세트를 기반으로 하는 동적 장치 목록이 있습니다.

리소스 그룹에서 작업을 수행할 수 없습니다. 그러나 그룹의 모든 장치를 선택하고 선택한 모든 장치에서 작업을 집합적으로 수행할 수 있습니다.

리소스 그룹의 장치 상태 보기

리소스 그룹에 있는 모든 관리되는 장치의 상태를 볼 수 있습니다.

이 작업 정보

다음 상태 아이콘은 리소스 그룹에 있는 모든 장치의 전반적인 상태를 나타내는 데 사용됩니다. 그룹의 전반적인 상태는 그룹에서 심각도가 가장 높은 장치로 표시됩니다.

- **위험** 아이콘( )
- **경고** 아이콘( )
- **일반** 아이콘( )

절차

리소스 그룹에 있는 장치의 상태를 보려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 대시보드 페이지에는 리소스 그룹을 포함하여 모든 관리되는 장치 및 기타 리소스에 대한 개요와 상태가 표시됩니다.

단계 2. XClarity Administrator 메뉴 표시줄에서 **하드웨어** → **리소스 그룹**을 클릭하십시오. 모든 리소스 그룹 페이지가 표시됩니다.

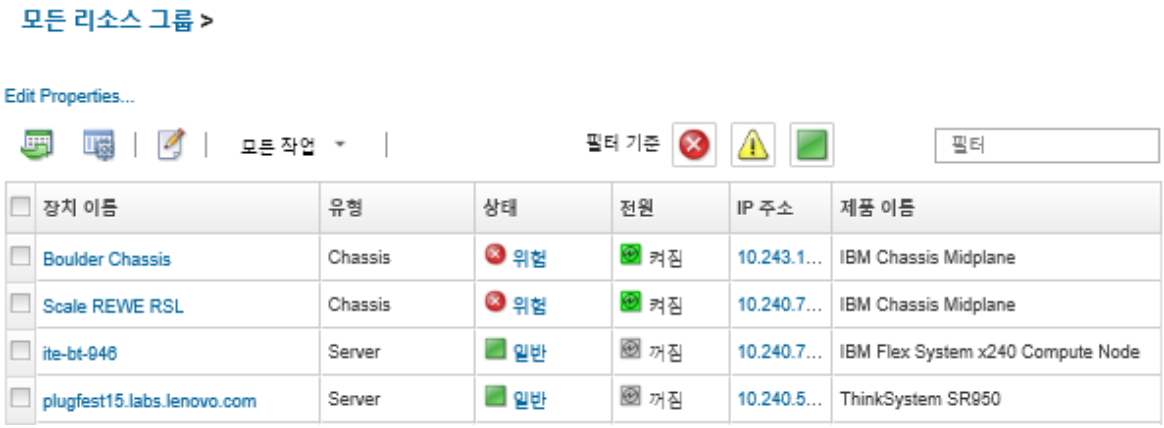
모든 리소스 그룹 페이지에 각 리소스 그룹이 나열됩니다. 여기에는 그룹 이름, 그룹에 있는 관리되는 장치 수, 그룹에서 심각도가 가장 높은 장치의 상태 등이 포함됩니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- 새 리소스 그룹을 만듭니다(동적 리소스 그룹 만들기 및 정적 리소스 그룹 만들기 참조).
- 그룹을 선택하고 **편집** 아이콘( )을 클릭하여 그룹 멤버십을 편집합니다.
- 그룹을 선택하고 **모든 작업** → **속성 편집**을 클릭하여 그룹 속성을 편집합니다.
- 그룹을 선택하고 **삭제** 아이콘( )을 클릭하여 리소스 그룹을 제거합니다.

  참고: 그룹을 제거하면 그룹 정의만 제거됩니다. 해당 그룹의 장치에는 영향을 주지 않습니다.
- **내보내기** 아이콘( )을 클릭하여 하나 이상의 리소스 그룹에 있는 모든 장치에 대한 자세한 정보를 CSV 파일로 내보냅니다.

단계 3. 모든 리소스 그룹 페이지의 **그룹** 열에서 이름을 클릭하여 해당 그룹의 장치 목록을 표시합니다.



이 페이지에서 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘( )을 클릭하여 정적 리소스 그룹에서 장치를 추가하거나 제거합니다.
- **장치 이름** 열에서 장치 이름을 클릭하여 리소스 그룹의 특정 장치에 대한 자세한 정보를 표시합니다.
- **내보내기** 아이콘( )을 클릭하여 하나 이상의 리소스 그룹에 있는 모든 장치에 대한 자세한 정보를 CSV 파일로 내보냅니다.

리소스 그룹의 멤버 보기

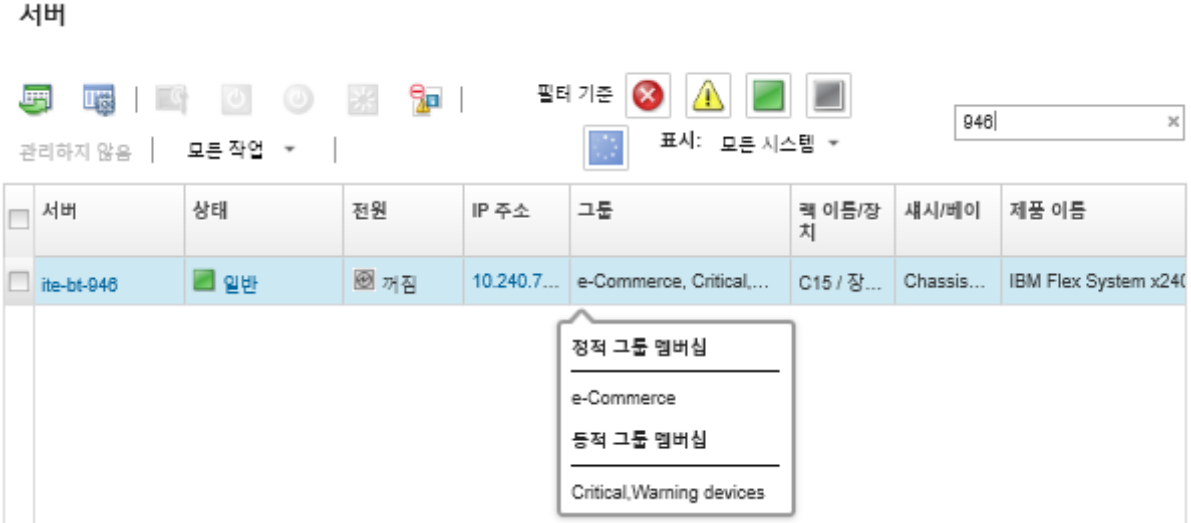
그룹 멤버를 포함하여 리소스 그룹에 대한 자세한 정보를 볼 수 있습니다.

절차

그룹 멤버십을 보려면 다음 단계를 완료하십시오.

- 장치가 멤버로 속한 모든 그룹을 보려면 다음을 수행하십시오.
  1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어**를 클릭하고 장치 유형을 클릭하여 모든 장치 페이지를 표시하십시오.

     그룹 열에 있는 그룹 목록 위로 마우스를 놓아 장치가 멤버로 속한 그룹을 나열하십시오.

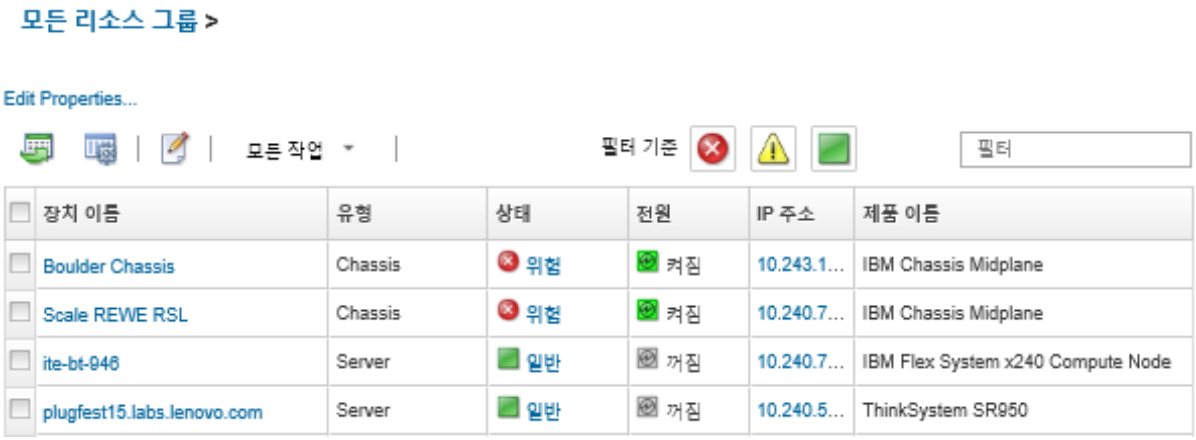


  2. 첫 번째 열의 장치 이름 링크를 클릭하십시오. 해당 장치의 요약 페이지가 표시되어 장치가 멤버로 속한 리소스 그룹 목록이 표시됩니다.

- 그룹 멤버를 확인하려면 다음을 수행하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 대시보드 페이지에는 랙을 포함하여 모든 관리 장치 및 기타 리소스에 대한 개요와 상태가 표시됩니다.
  2. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 그룹**을 클릭하십시오. 리소스 그룹 페이지가 표시됩니다.

     이 페이지에는 총 멤버 수와 그룹의 각 장치 유형의 멤버 수가 나열됩니다.

3. 모든 리소스 그룹 페이지의 그룹 열에서 이름을 클릭하여 리소스 그룹 세부 사항을 표시하십시오. 이 페이지는 리소스 그룹의 멤버로 속한 각 장치를 나열됩니다.



동적 리소스 그룹 만들기

일련의 기준에 따라 관리되는 장치의 동적 세트에 대한 리소스 그룹을 만들 수 있습니다.

이 작업 정보

각 장치 유형에 대한 다음 조건 중 하나 이상의 조건을 사용하여 동적 리소스 그룹을 만들 수 있습니다.

기준	섀시	밀집 섀시	서버	Flex System 스위치	Rack-Switch 스위치	스토리지 장치
추가 기능 카드 이름			✓(ThinkServer 제외)			
연락처	✓		✓		✓	✓
설명	✓	✓	✓		✓	✓
정규화된 도메인 이름	✓		✓			
호스트 이름	✓		✓	✓	✓	
IPv4 주소*	✓		✓	✓	✓	✓

기준	섀시	밀집 섀시	서버	Flex System 스위치	Rack-Switch 스위치	스토리지 장치
IPv6 주소	✓		✓	✓	✓	
위치	✓	✓	✓		✓	✓
시스템 유형	✓		✓	✓	✓	✓
모델	✓		✓	✓	✓	✓
전체 성능 상태	✓		✓	✓	✓	✓
프로세서 코어			✓			
제품 이름	✓		✓	✓	✓	✓
랙	✓	✓	✓		✓	✓
공간	✓	✓	✓		✓	✓
사용자 정의된 이름	✓	✓	✓	✓	✓	✓

참고: IPv4 주소의 경우 대시로 구분하거나 와일드카드로 별표 표시를 중간에 사용하여 단일 주소나 여러 개의 주소를 지정할 수 있습니다(예: 공백 없이 1.1.1.* 또는 1.1.1.1-1.1.1.255).

절차

동적 리소스 그룹을 만들고 채우려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 리소스 그룹**을 클릭하십시오. 모든 리소스 그룹 페이지가 표시됩니다.

단계 2. **만들기** 아이콘( )을 클릭하여 비어 있는 그룹을 만드십시오. 비어 있는 그룹 만들기 대화 상자가 표시됩니다.

단계 3. 기준 세트에 따라 장치를 그룹화할 **동적 그룹**을 선택하십시오.

단계 4. **만들기**를 클릭하십시오. 동적 그룹 편집 대화 상자가 표시됩니다.

단계 5. 이 동적 그룹에 대한 기준을 추가하십시오.

- 그룹 세트에 사용할 연산자를 선택하십시오. 이는 다음 값 중 하나입니다.
  - AND. 멤버가 지정된 모든 값을 충족해야 합니다.
  - OR. 멤버가 하나 이상의 지정된 값을 충족해야 합니다.
- **기준 만들기**를 클릭하여 새 기준을 세트에 추가하십시오.
- **기준 세트 만들기**를 클릭하여 기준 규칙 세브세트를 추가하십시오.

참고: 새로운 기준과 기준 세트는 항상 목록 맨 아래에 추가됩니다.

단계 6. **적용**을 클릭하여 그룹 기준을 저장하고 그룹을 만들거나 **미리 보기**를 클릭하여 그룹을 만들지 않고 현재 기준을 사용하는 그룹에 포함되는 장치를 볼 수 있습니다.

완료한 후에

- 모든 장치 페이지 및 장치 요약 페이지의 **그룹** 열에서 장치가 속한 리소스 그룹을 볼 수 있습니다.
- 리소스 그룹을 선택하고 **편집** 아이콘( )을 클릭하여 동적 그룹에 대한 기준을 수정할 수 있습니다.
- 모든 **작업 → 속성 편집**을 클릭하여 리소스 그룹 속성을 수정할 수 있습니다.

정적 리소스 그룹 만들기

사용자 지정된 관리되는 장치 세트가 포함된 리소스 그룹을 만들 수 있습니다.

절차

정적 리소스 그룹을 만들고 채우려면 다음 단계를 완료하십시오.

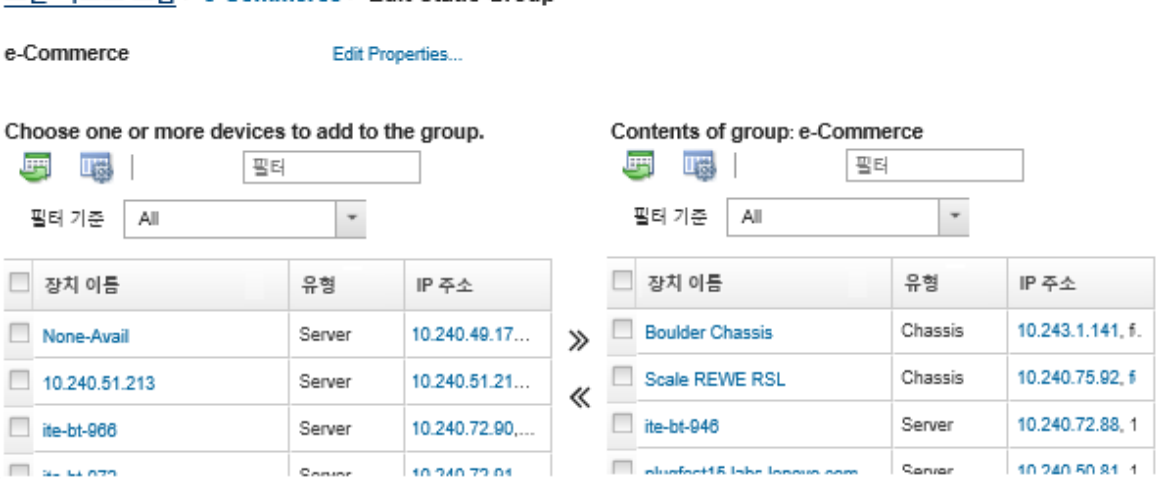
단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 리소스 그룹**을 클릭하십시오. 리소스 그룹 페이지가 표시됩니다.

단계 2. **만들기** 아이콘( )을 클릭하여 비어 있는 그룹을 만드십시오. 비어 있는 그룹 만들기 대화 상자가 표시됩니다.

단계 3. 그룹 이름과 선택적 설명을 지정하십시오.

단계 4. **정적 그룹**을 선택하여 명시적으로 정의된 장치 그룹을 만드십시오.

단계 5. **만들기**를 클릭하십시오. 정적 그룹 편집 페이지가 표시됩니다.



다.

단계 6. **그룹에 없는 모든 사용 가능한 장치** 목록에서 그룹에 추가할 장치를 선택하고 **추가** 아이콘(≫)을 클릭하여 선택한 장치를 **그룹 내용** 목록으로 이동하십시오.

참고:

- 열 머리글을 클릭하여 특정 장치를 더 쉽게 찾을 수 있도록 목록을 정렬할 수 있습니다. 또한 **필터 기준** 드롭 다운 목록에서 장치 유형을 선택하고 드롭 다운 목록에서 섀시를 선택하거나 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 선택한 기준을 충족하는 장치만 나열할 수 있습니다.
- 섀시를 그룹으로 이동하도록 선택하면, 섀시의 장치가 자동으로 그룹에 추가되지 않습니다. 모든 섀시 구성 요소를 그룹에 추가하려면, **표시** 드롭 다운 메뉴에서 **섀시 → *<chassis_name>*** 를 선택하여 지정된 섀시의 모든 구성 요소를 나열하고, 장치 이름 열 머리글 옆에 있는 확인란을 선택하여 모든 장치를 선택한 다음 **추가** 아이콘(≫)을 클릭하여 선택한 장치를 **그룹 내용** 목록으로 이동하십시오.

완료한 후에

- 모든 장치 페이지 및 장치 요약 페이지의 **그룹** 열에서 장치가 속한 리소스 그룹을 볼 수 있습니다.
- **모든 작업 → 그룹 → 그룹에 추가** 또는 **모든 작업 → 그룹 → 그룹에서 제거**를 클릭하여 모든 장치 페이지와 장치 세부 사항 페이지에서 정적 리소스 그룹의 장치를 추가하거나 제거할 수 있습니다.

  참고: 정적 리소스 그룹에서만 장치를 추가하고 제거할 수 있습니다. 동적 그룹에서는 제거할 수 없습니다.
- **모든 작업 → 속성 편집**을 클릭하여 리소스 그룹 속성을 수정할 수 있습니다.

리소스 그룹 제거

Lenovo XClarity Administrator에서 리소스 그룹을 제거할 수 있습니다.

이 작업 정보

그룹을 삭제하면 그룹 정의만 삭제됩니다. 해당 그룹의 장치에는 영향을 주지 않습니다.

절차

리소스 그룹을 제거하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 리소스 그룹**을 클릭하십시오. 모든 리소스 그룹 페이지가 표시됩니다.

모든 리소스 그룹 페이지에 각 리소스 그룹이 나열됩니다. 여기에는 그룹 이름, 그룹에 있는 관리되는 장치 수, 그룹에서 심각도가 가장 높은 장치의 상태 등이 포함됩니다.

단계 2. 제거할 리소스 그룹을 선택하십시오.

단계 3. **삭제** 아이콘(✖)을 클릭하십시오.

단계 4. **삭제**를 클릭하십시오.

리소스 그룹 속성 수정

특정 리소스 그룹에 대한 속성을 수정할 수 있습니다.

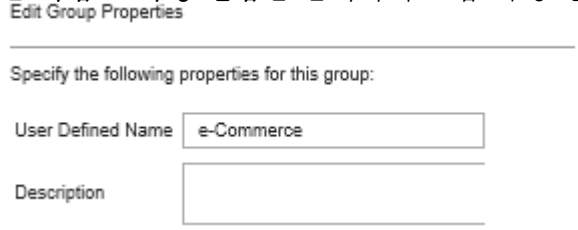
절차

리소스 그룹 속성을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 리소스 그룹**을 클릭하여 모든 리소스 그룹 페이지를 표시하십시오.

단계 2. 업데이트할 리소스 그룹을 선택하십시오.

단계 3. **모든 작업 → 속성 편집**을 클릭하여 그룹 속성 편집 대화 상자를 표시하십시오.



단계 4. 필요 시 다음 정보를 변경하십시오.
- 그룹 이름
- 설명

단계 5. **저장**을 클릭하십시오.

참고: 이러한 속성을 변경하는 경우 XClarity Administrator 웹 인터페이스에 변경 사항이 표시되기 전에 약간의 지연이 있을 수 있습니다.

제 6 장 랙 관리

Lenovo XClarity Administrator에 있는 랙을 사용하여 데이터 센터의 물리적 랙 설정을 반영하도록 관리 장치를 그룹화할 수 있습니다.

시작하기 전에

한 섀시에서 다른 섀시로 노드를 이동한 후, 5~10분 정도 기다린 후에 섀시를 포함하는 XClarity Administrator에서 랙을 편집하십시오.

장치를 랙 밖으로 옮기면, 랙 이름 및 가장 낮은 랙 장치 값이 장치 인벤토리에서 지워집니다. 실 및 위치 값은 지워지지 않습니다.

이 작업 정보

이 절차는 관리 장치와 필러를 사용하여 대화식으로 단일 랙을 작성하고 채우는 방법에 대해 설명합니다.

랙에 많은 장치를 추가하거나 많은 랙을 편집해야 하는 경우 스프레드시트를 사용하여 대량 가져오기를 수행하거나 PowerShell 스크립트를 구현하여 작업을 자동화하도록 고려해 보십시오. 대량 가져오기 사용에 대한 자세한 정보는 섀시 관리 및 서버 관리의 내용을 참조하십시오. PowerShell 스크립트에 대한 정보는 XClarity Administrator 온라인 설명서에서 PowerShell(LXCAPSTool) 툴킷의 내용을 참조하십시오.

XClarity Administrator는 관리 가능 장치에 정의된 랙 속성을 인식합니다. 장치를 관리하는 경우 XClarity Administrator는 해당 장치의 시스템 속성을 설정하고 랙 보기를 업데이트합니다. 랙이 XClarity Administrator에 없는 경우 새 랙이 작성되고 새 랙에 장치가 추가됩니다.

참고:

- 랙 보기에서는 System x3500 M5 서버, NeXtScale nx360 M5 서버, ThinkServer SD350 서버 및 타워 서버가 지원되지 않습니다.
- System x3850 X5 확장 가능 복합 시스템의 경우 각 노드(서버)를 개별적으로 랙에 추가해야 합니다.
- XClarity Administrator가 다시 시작되면 랙 보기에 데모 하드웨어가 표시되지 않습니다.

절차

랙을 만들고 채우려면, 다음 단계를 완료하십시오.

- 관리 장치가 있는 단일 랙을 만들고 채웁니다.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 ➞ 랙**을 클릭하십시오. 모든 랙 페이지가 표시됩니다.

     모든 랙 페이지에는 랙 이름, 랙에 있는 관리 장치 수 및 심각도가 최상인 장치의 상태와 함께 각 랙이 축소판 이미지로 표시됩니다.

     참고: 도구 모음에서 다음 아이콘을 클릭하여 심각도를 기준으로 랙을 필터링할 수 있습니다. **필터** 필드에 랙 이름을 입력하여 표시되는 랙을 상세하게 필터링할 수도 있습니다.
     - **위험 경고** 아이콘( )
     - **경고 경고** 아이콘( )
     - **일반 경고** 아이콘( )

2. **만들기** 아이콘( )을 클릭하여 비어 있는 랙을 작성하십시오. 비어 있는 랙 만들기 대화 상자가 표시됩니다.
3. 대화 상자에 랙 이름, 높이, 위치 및 룸을 입력하십시오.

   참고:

   - 랙 이름은 고유하지 않아도 됩니다. 위치나 공간이 다르거나 둘 다 다른 경우 동일한 이름으로 랙을 만들 수 있습니다.
   - 랙 이름에는 대소문자, 숫자 및 마침표(.), 대시(-) 및 밑줄(_)과 같은 특수 문자만 포함될 수 있습니다.
   - 위치는 최대 23자일 수 있습니다.
4. **만들기**를 클릭하십시오. 새 랙의 축소판 이미지가 모든 랙 페이지에 추가됩니다.
5. 랙의 축소판 이미지를 두 번 클릭하십시오. 비어 있는 랙 이미지와 해당 랙의 속성과 함께 랙 보기 페이지가 표시됩니다.

6. **랙 편집**을 클릭하여 랙 편집 페이지를 표시하십시오.

7. 적합한 모든 관리 장치와 필러를 그래픽 보기에 추가하십시오.

   참고: 온라인 상태의 관리되는 장치만 랙에 추가할 수 있습니다.

   - **섀시** 탭을 클릭하여 랙에 추가되지 않은 관리 섀시 목록을 보십시오. 랙에서 원하는 위치에 관리 섀시를 끌어다 놓아 섀시를 랙에 추가하십시오.
   - **서버 엔클로저** 탭을 클릭하여 랙에 추가되지 않은 관리 랙 서버 및 다중 노드 서버 엔클로저 목록을 보십시오. 랙 서버 또는 서버 엔클로저를 원하는 위치의 랙에 끌어다 놓아 랙 서버를 랙에 추가하십시오.
   - **RackSwitch** 탭을 클릭하여 랙에 추가되지 않은 관리 RackSwitch 스위치 목록을 보십시오. RackSwitch 스위치를 원하는 위치의 랙에 끌어다 놓아 스위치를 랙에 추가하십시오.
   - **스토리지** 탭을 클릭하여 여러 스토리지 장치 목록을 보십시오. 원하는 위치의 랙에 적합한 스토리지 장치를 끌어다 놓아 스토리지 장치를 랙에 추가하십시오.
   - **필러** 탭을 클릭하여 여러 필러 목록을 보십시오. 원하는 위치의 랙에 적합한 필러를 끌어다 놓아 필러를 랙에 추가하십시오.

     *필러*는 랙에 있으며 XClarity Administrator에서 관리 해제된 장치입니다. 다음 필러를 사용할 수 있습니다.
     - 일반 필러
     - 일반 랙 스위치
     - 스토리지 컨트롤러 및 엔클로저
     - 파트너 스토리지 컨트롤러 및 엔클로저(예, IBM, NetApp 및 EMC)

     - 랙에서 하나 이상의 장치를 추가하거나 제거하면 장치에 대한 위치, 룸, 랙 및 LRU(lowest rack unit) 속성이 업데이트됩니다.
     - **보기 기준** 드롭다운 목록을 사용하여 한 탭에서 장치 목록을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 필터와 장치를 상세하게 필터링할 수도 있습니다.
     - 오브젝트를 랙 외부로 끌어다 놓아 랙에서 관리 장치와 필러를 제거할 수 있습니다.

8. **저장**을 클릭하여 랙 구성을 저장하십시오.

   구성 프로세스를 완료하려면 몇 분 정도가 걸릴 수 있습니다. 구성 중에 랙과 위치 정보가 관리 장치의 CMM 또는 베이스보드 관리 컨트롤러에 푸시됩니다.

9. 필러를 클릭하고 **속성 편집**을 클릭하여 랙에 추가된 필러를 사용자 지정하십시오. 속성 편집 대화 상자에서 해당 장치에 대한 이름, LRU(lowest rack unit) 및 관리 사용자 인터페이스 실행에 사용할 URL를 지정할 수 있습니다.

   팁: 랙 구성이 저장되면 랙에서 필러를 클릭하고 URL **실행** 링크를 클릭하여 필러의 관리 사용자 인터페이스를 실행할 수 있습니다.

- 대량 가져오기 파일을 사용하여 랙을 만들고 채웁니다.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.
  2. **대량 가져오기**를 클릭하십시오. 대량 가져오기 마법사가 표시됩니다.

     일괄 가져오기

  3. 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.
  4. 템플릿 파일의 데이터 워크시트를 작성하고 파일을 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 랙을 정의하려면, 다음 필수 열을 완료하십시오.
     - (A열) 장치 유형에 대한 "랙"을 지정하십시오.
     - (V열) 랙 이름을 지정하십시오.
     - (X열) 랙 높이를 지정하십시오. 지원되는 랙 높이: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, 및 52U.

     다음 그림에는 정의되는 랙이 포함된 대량 가져오기 파일 예제가 표시되어 있습니다.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

참고: 동일한 대량 가져오기 파일을 사용하여 장치를 관리하고 해당 장치를 랙에 추가할 수 있습니다(Lenovo XClarity Administrator 온라인 설명서의 시스템 관리).

5. 대량 가져오기 마법사에서 처리를 위해 파일을 업로드할 CSV 파일의 이름을 입력하십시오. 파일을 쉽게 찾으려면 **찾아보기**를 클릭할 수 있습니다.
6. **업로드**를 클릭하여 파일을 업로드하고 유효성을 검사합니다.
7. **다음**을 클릭하여 관리할 랙 및 기타 장치 목록이 있는 입력 요약 페이지를 표시하고 관리할 랙 및 기타 장치의 요약을 검토하십시오.
8. **다음**을 클릭하여 장치 자격 증명 페이지를 표시하십시오. 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.
9. **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 "작업 모니터링" 154페이지의 내용을 참조하십시오.

완료한 후에

랙 번호 지정 순서 기본 설정을 변경할 수 있습니다(인벤토리 기본 설정 지정 참조).

랙의 장치 상태 보기

각 랙에 대해 랙에 있는 모든 관리 장치 상태를 볼 수 있습니다.

절차

랙에 있는 모든 장치 상태를 보려면 다음 작업 중 하나 이상을 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 대시보드 페이지에는 랙을 포함하여 모든 관리 장치 및 기타 리소스에 대한 개요와 상태가 표시됩니다.

단계 2. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 랙**을 클릭하십시오. 랙 페이지가 표시됩니다.

랙 페이지에는 랙 이름, 랙에 있는 관리 장치 수 및 심각도가 최상인 장치의 상태와 함께 각 랙이 축소판 이미지로 표시됩니다.

참고: 랙 이름, 랙에 있는 장치 수 또는 심각도별로 랙 목록을 정렬하여 특정 랙을 보다 쉽게 찾도록 할 수 있습니다. 정렬은 왼쪽에서 오른쪽, 위에서 아래로 정렬됩니다. 또한 도구 모음에서 다음 아이콘을 클릭하여 심각도 별로 랙을 필터링하거나 **필터** 필드를 사용하여 표시된 랙을 추가로 필터링합니다.

- **위험 경고 아이콘**( )
- **경고 경고 아이콘**( )
- **일반 경고 아이콘**( )

단계 3. 모든 랙 페이지에서 랙 이름을 클릭하거나 랙 축소판을 두 번 클릭하여 그래픽 보기와 해당 랙의 속성을 표시하십시오.

*랙 보기*는 섀시, 랙 서버, TOR(top-of-rack) 스위치 및 필러를 포함하여 랙에서 각 장치를 표시하는 앞면 랙의 그래픽 보기입니다. 각 장치의 상태 아이콘은 해당 장치의 현재 상태를 표시합니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **랙 편집**을 클릭하여 랙에서 장치를 추가하거나 제거하십시오.

  참고: 랙에서 구성 요소를 변경하는 경우 XClarity Administrator 인터페이스에 정보가 표시되기 전에 약간의 지연이 있을 수 있습니다.
- 장치 또는 필러를 클릭한 후 장치 요약 분할창에서 **속성 편집**을 클릭하여 장치와 필러 속성(관리 웹 인터페이스를 실행하기 위한 이름, 위치 및 URL 등)을 수정하십시오.
- 장치 또는 필러를 클릭하고 장치 요약 분할창에서 URL **실행** 링크를 클릭하여 장치 또는 필러에 대한 관리 컨트롤러 웹 인터페이스를 표시하십시오.

단계 4. 장치 또는 구성 요소에 대한 요약 또는 상세 상태를 표시하십시오.

a. 랙에서 장치나 구성 요소를 클릭하여 장치 또는 구성 요소의 상태와 상태 요약 및 속성을 표시하십시오.

b. 장치를 두 번 클릭하여 장치 세부 정보 페이지를 표시하십시오.

절차

랙 번호 지정 순서 기본 설정을 변경할 수 있습니다(인벤토리 기본 설정 지정 참조).

랙 제거

Lenovo XClarity Administrator에서 랙을 제거할 수 있습니다.

절차

랙을 제거하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 랙**을 클릭하십시오. 모든 랙 페이지가 표시됩니다.

모든 랙 페이지에는 랙 이름, 랙에 있는 관리 장치 수 및 심각도가 최상인 장치의 상태와 함께 각 랙이 축소판 이미지로 표시됩니다.

참고: 랙 이름, 랙에 있는 장치 수 또는 심각도별로 랙 목록을 정렬하여 특정 랙을 보다 쉽게 찾도록 할 수 있습니다. 정렬은 왼쪽에서 오른쪽, 위에서 아래로 정렬됩니다. 또한 도구 모음에서 다음 아이콘을 클릭하여 심각도 별로 랙을 필터링하거나 **필터** 필드를 사용하여 표시된 랙을 추가로 필터링합니다.

- **위험 경고 아이콘**( )
- **경고 경고 아이콘**( )
- **일반 경고 아이콘**( )

단계 2. 제거할 랙의 축소판을 선택하십시오.

단계 3. **제거** 아이콘( )을 클릭하십시오.

단계 4. **제거**를 클릭하십시오.

결과

랙의 축소판이 모든 랙 페이지에서 제거되고 랙에 있는 모든 장치를 랙 편집 페이지에 있는 다른 랙에 포함시킬 수 있습니다.

제 7 장 섀시 관리

Lenovo XClarity Administrator는 Flex System 섀시와 같은 다양한 유형의 시스템을 관리할 수 있습니다.

자세히 알아보기: XClarity Administrator: 검색

시작하기 전에

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

섀시를 관리하기 전에 다음 조건이 충족되는지 확인하십시오.

- 장치를 관리하기 전에 관리 고려사항을 검토하십시오. 정보는 XClarity Administrator 온라인 설명서에서 관리 고려사항의 내용을 참조하십시오.
- 관리하는 섀시에 대한 CMM과 통신하려면 특정 포트를 사용할 수 있어야 합니다. 섀시 관리를 시도하기 전에 이러한 포트를 사용할 수 있어야 합니다. 포트에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.
- XClarity Administrator를 사용하여 관리하려는 각 섀시에 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.
- CMM의 LDAP **사용자 동시 활성 세션 수** 설정은 섀시에 대해 0(영)으로 설정되어 있어야 합니다. **관리 모듈 관리 ➡ 사용자 계정**을 클릭하고 **전역 로그인 설정**을 클릭한 다음 **일반** 탭을 클릭하여 CMM 웹 인터페이스에서 이 설정을 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 Administrator에서 *다른* 서브넷에 있는 섀시를 검색하려면 다음 조건 중 하나가 충족되어야 합니다.
  - 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.
  - 엔드포인트 또는 네트워크에서 SLP를 사용하지 않는 경우 서비스 레코드(SRV 레코드)를 수동으로 XClarity Administrator의 도메인 이름 서버(DNS)에 추가하여 DNS 검색 방법을 대신 사용할 수 있습니다. 예를 들어 다음과 같습니다.
    ```
    _lxca._tcp.labs.lenovo.com    service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```
    그런 다음 **관리 모듈 관리 ➡ 네트워크 프로토콜**을 클릭하고 DNS 탭을 클릭한 후 DNS를 **사용하여 Lenovo XClarity Administrator 검색**을 선택하여 관리 웹 인터페이스에서 CMM에 DNS 검색 사용을 설정하십시오.

    참고:
    - DNS를 사용한 자동 검색을 지원하려면 CMM에서 날짜가 2017년 5월인 펌웨어 수준이 실행 중이어야 합니다.
    - 사용자 환경에 여러 XClarity Administrator 인스턴스가 있는 경우 섀시는 검색 요청에 처음 응답한 인스턴스에서만 검색됩니다. 섀시는 모든 인스턴스에서 검색되지 않습니다.

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.

주의: 3주보다 오래 실행되고 듀얼 CMM 구성을 사용하는 Flex 스택 릴리스 1.3.2.1 2PET12K ~ 2PET12Q를 실행하는 CMM을 관리하려는 경우 XClarity Administrator를 사용하여 펌웨어를 업데이트하기 전에 CMM를 가상으로 재배치해야 합니다.

중요: 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.

이 작업 정보

XClarity Administrator는 XClarity Administrator로 동일한 IP 서브넷에 있는 관리 가능한 시스템을 조사하여 환경에서 섀시를 자동으로 검색할 수 있습니다. 다른 서브넷에 있는 섀시를 검색하려면 IP 주소 또는 IP 주소 범위를 지정하거나 스프레드시트에서 정보를 가져오십시오.

섀시가 XClarity Administrator의 관리를 받은 후 XClarity Administrator는 각 관리 섀시를 주기적으로 폴링하여 인벤토리, 필수 제품 데이터 및 상태 등의 정보를 수집합니다. 각 관리 섀시를 보고 모니터링하고 관리 작업(예, 시스템 정보, 네트워크 설정 및 장애 조치 구성)을 수행할 수 있습니다. 보호 모드에 있는 섀시의 경우 관리 작업을 사용하지 않습니다.

섀시는 *XClarity Administrator 관리되는 인증*을 사용하여 관리됩니다.

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(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.

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 스토리지 장치를 관리하도록 하려면 먼저 초기 XClarity Administrator에서 장치를 관리 해제하고 이를 새 XClarity Administrator에서 관리하도록 설정하십시오. 관리 해제 프로세스 중에 오류가 발생하는 경우 새 XClarity Administrator에서 관리 중에 **강제 관리** 옵션을 선택할 수 있습니다.

참고: 관리 가능한 장치에 대한 네트워크를 검색하는 경우 XClarity Administrator는 장치 관리를 시도한 후까지 다른 관리자가 이미 장치를 관리하고 있는지 확인할 수 없습니다.

관리 프로세스 중에 XClarity Administrator는 다음 작업을 수행합니다.

- 제공된 자격 증명을 사용하여 섀시에 로그인합니다.
- CMM, 컴퓨팅 노드, 스토리지 장치 및 Flex 스위치 등 각 섀시의 모든 구성 요소에 대한 인벤토리를 수집합니다.

  참고: 일부 인벤토리 데이터는 관리 프로세스가 완료된 후 수집됩니다. 섀시는 모든 인벤토리 데이터가 수집될 때까지 보류 상태입니다. 해당 장치에 대해 모든 인벤토리 데이터를 수집하고 섀시가 더 이상 보류 상태에 있지 않을 때까지 관리 장치에서 특정 작업(예, 서버 패턴 배포)을 수행할 수 없습니다.
- 모든 관리 장치가 XClarity Administrator의 NTP 서버를 사용하도록 NTP 서버에 대한 설정을 구성합니다.
- 최근 편집한 펌웨어 준수 정책을 섀시에 할당합니다.
- Lenovo Flex 장치의 경우 수신 요청을 XClarity Administrator에서만 허용할 수 있도록 장치 방화벽 규칙을 선택적으로 구성할 수 있습니다.
- CMM과 보안 인증서를 교환하고 XClarity Administrator 신뢰 저장소에 CMM 보안 인증서를 복사하고 XClarity Administrator CA 보안 인증서를 CMM에 보냅니다. CMM은 CMM 신뢰 저장소에 인증서를 로드하고 컴퓨팅 노드 서비스 프로세서에 배포하여 해당 신뢰 저장소에 포함시킵니다.
- 관리되는 인증을 구성합니다. CMM LDAP 클라이언트의 설정은 XClarity Administrator를 인증 서버로 사용하도록 변경되고 CMM의 전역 로그인 설정은 **외부 인증 서버로만** 변경됩니다. 관리되는 인증에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.
- 복구 사용자 계정(RECOVERY_ID)을 만듭니다. RECOVERY_ID 계정에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.

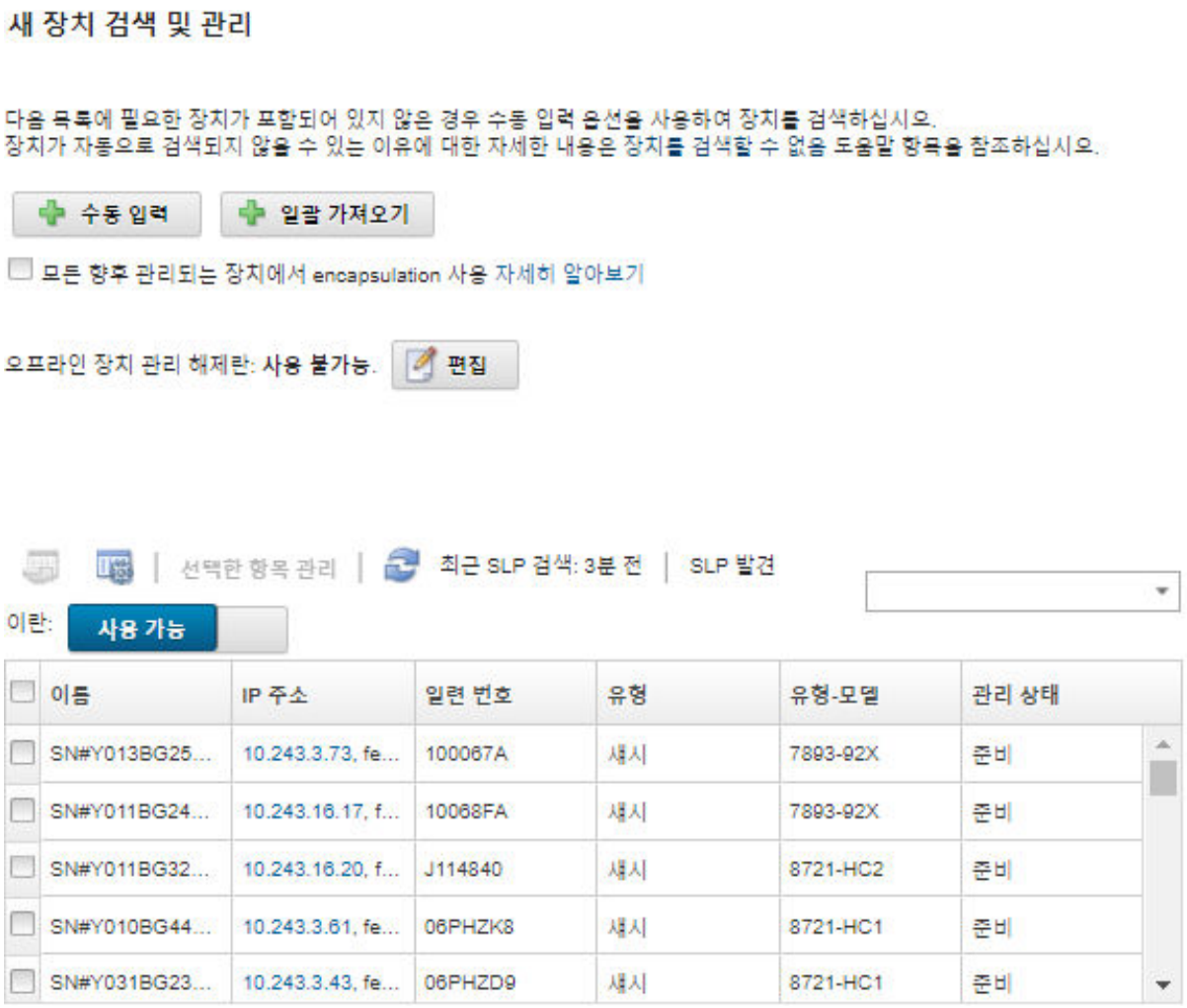
주의: 섀시를 관리하는 경우 XClarity Administrator는 동시 보안 TCP 명령 모드 연결의 최대 수를 15로 변경하고 동시 레거시 TCP 명령 모드 연결의 최대 수를 0으로 설정합니다. 이것은 CMM에 이미 설정되어 있을 수 있는 설정을 대체합니다.

참고: XClarity Administrator는 관리 프로세스 중에 보안 설정 또는 암호 설정(암호화 모드 및 보안 통신에 사용되는 모드)을 수정하지 않습니다. 섀시를 관리한 후 암호 설정을 수정할 수 있습니다 (관리 서버의 암호화 설정 구성 참조).

절차

XClarity Administrator를 사용하여 섀시를 검색 및 관리하려면 다음 절차 중 하나를 완료하십시오.

- 일괄 가져오기 파일을 사용하여 다수의 섀시 및 기타 장치를 검색하고 관리합니다 (Lenovo XClarity Administrator온라인 설명서의 시스템 관리 참조).
- XClarity Administrator와 동일한 IP 서브넷에 있는 섀시를 검색 및 관리합니다.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 새 장치 검색 및 관리 페이지가 표시됩니다.



관리할 섀시를 더 손쉽게 찾기 위해 표 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 필터와 섀시를 상세하게 필터링할 수도 있습니다. **열 사용자 지정** 아이콘( )을 클릭하여 표시되는 열과 기본 정렬 순서를 변경할 수 있습니다.

2. **새로 고침** 아이콘( )을 클릭하여 XClarity Administrator 도메인의 모든 관리 가능 장치를 검색하십시오. 검색에는 몇 분 정도 소요됩니다.
3. 수신 요청이 XClarity Administrator에서만 허용되도록 관리 프로세스 중에 모든 장치에서 방화벽 규칙을 변경하려면 **모든 미래 관리 장치에서 encapsulation 사용** 선택란을 클릭하십시오.

   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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.
4. 관리할 하나 이상의 섀시를 선택하십시오.
5. **선택 관리**을 클릭하십시오.
6. 이 장치에 대해 XClarity Administrator 관리되는 인증 또는 로컬 인증을 사용하도록 선택하십시오. 기본적으로 관리되는 인증이 선택됩니다. 로컬 인증을 사용하려면 **관리되는 인증**을 선택 취소하십시오.

   참고: 관리되는 인증 및 로컬 인증은 ThinkServer 및 System x M4 서버에서 지원되지 않습니다.

7. 장치에 사용할 자격 증명 유형을 선택하고 적절한 자격 증명을 지정하십시오.
   - **수동으로 입력된 자격 증명 사용**
     - CMM을 인증하기 위한 lxc-supervisor 권한을 가진 로컬 사용자 ID와 암호를 지정하십시오.
     - (옵션) 장치에서 암호가 현재 만료된 경우 CMM 사용자 계정의 새 암호를 지정하십시오.
   - **저장된 자격 증명 사용**

     이 관리되는 장치에 사용할 lxc-supervisor 권한이 있는 저장된 자격 증명을 선택하십시오. **저장된 자격 증명 관리**를 클릭하여 저장된 자격 증명을 추가할 수 있습니다.

     참고: 로컬 인증을 사용하도록 선택한 경우 장치를 관리할 저장된 자격 증명을 선택해야 합니다.

   팁: 감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우, 관리에 실패하거나 성공하더라도 장치의 기타 향후 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).

   일반 및 저장된 자격 증명에 대한 자세한 정보는 사용자 계정 관리 및 저장된 자격 증명 관리의 내용을 참조하십시오.
8. 관리되는 인증을 선택하는 경우 복구 암호를 지정하십시오.

   복구 계정(RECOVERY_ID)이 CMM에 만들어지고 모든 로컬 사용자 계정이 사용 안 함으로 설정됩니다. XClarity Administrator에 문제가 있고 어떤 이유에서 작동이 중지되면 일반 사용자 계정을 사용하여 CMM에 로그인할 수 *없습니다*. 그러나 RECOVERY_ID 계정을 사용하여 로그인할 수 있습니다.

   참고:
   - 관리되는 인증을 사용하도록 선택한 경우 복구 암호는 필수이며 로컬 인증을 사용하도록 선택한 경우에는 복구 암호가 허용되지 않습니다.
   - 로컬 복구 계정 또는 저장된 복구 자격 증명을 사용하도록 선택할 수 있습니다. 두 경우 모두 사용자 이름은 항상 RECOVERY_ID입니다.
   - 암호가 장치의 보안 및 암호 정책을 준수하는지 확인하십시오. 보안 및 암호 정책은 다를 수 있습니다.
   - 나중에 사용하도록 복구 암호를 기록해야 합니다.

   복구 ID에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.
9. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

   참고:
   - 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
   - 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.
10. **관리**를 클릭하십시오.

    이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 진행상황을 모니터링하십시오.

    프로세스가 완료되면 섀시의 장치 수와 섀시 상태를 표시하는 대화 상자가 표시됩니다.

    참고: 일부 인벤토리 데이터는 관리 프로세스가 완료된 후 수집됩니다. 섀시는 모든 인벤토리 데이터가 수집될 때까지 보류 상태입니다. 해당 장치에 대해 모든 인벤토리 데이터를 수집하고 섀시가 더 이상 보류 상태에 있지 않을 때까지 관리 장치에서 특정 작업(예, 서버 패턴 배포)을 수행할 수 없습니다.
11. 프로세스가 완료되면 **확인**을 클릭하십시오.

    장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

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.

12. 새 섀시인 경우 **섀시 구성 계속하기**를 클릭하여 전체 섀시(컴퓨팅 노드 및 Flex 스위치 포함)에 대한 관리 네트워크 설정의 유효성을 검증하고 변경하고 서버 패턴을 만들어 배포함으로써 컴퓨팅 노드 정보, 로컬 스토리지, I/O 어댑터, 부팅 대상 및 펌웨어 설정을 구성하십시오. 자세한 정보는 섀시에 대한 관리 IP 설정 수정 및 구성 패턴을 사용하여 서버 구성의 내용을 참조하십시오.

- IP 주소를 수동으로 지정하여 XClarity Administrator와 동일한 IP 서브넷에 있지 않은 섀시를 검색 및 관리하십시오.
  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.

     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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.
  3. **수동 입력**을 선택하십시오.
  4. 관리할 섀시의 네트워크 주소를 지정하십시오.
     - **단일 시스템**을 클릭하고 단일 IP 주소 도메인 이름 또는 완전한 도메인 이름(FQDN)을 입력하십시오.

       참고: FQDN을 지정하려면 네트워크 액세스 페이지에 올바른 도메인 이름이 지정되어 있어야 합니다(네트워크 액세스 구성 참조).
     - **다중 시스템**을 클릭하고 IP 주소의 범위를 입력하십시오. 다른 범위를 추가하려면 **추가** 아이콘(➕)을 클릭하십시오. 범위를 제거하려면 **제거** 아이콘(❌)을 클릭하십시오.
  5. **확인**을 누르십시오.
  6. 이 장치에 대해 XClarity Administrator 관리되는 인증 또는 로컬 인증을 사용하도록 선택하십시오. 기본적으로 관리되는 인증이 선택됩니다. 로컬 인증을 사용하려면 **관리되는 인증**을 선택 취소하십시오.

     참고: 관리되는 인증 및 로컬 인증은 ThinkServer 및 System x M4 서버에서 지원되지 않습니다.
  7. 장치에 사용할 자격 증명 유형을 선택하고 적절한 자격 증명을 지정하십시오.
     - **수동으로 입력된 자격 증명 사용**
       - CMM을 인증하기 위한 lxc-supervisor 권한을 가진 로컬 사용자 ID와 암호를 지정하십시오.

- (옵션) 장치에서 암호가 현재 만료된 경우 CMM 사용자 계정의 새 암호를 지정하십시오.

- **저장된 자격 증명 사용**

  이 관리되는 장치에 사용할 lxc-supervisor 권한이 있는 저장된 자격 증명을 선택하십시오. **저장된 자격 증명 관리**를 클릭하여 저장된 자격 증명을 추가할 수 있습니다.

  참고: 로컬 인증을 사용하도록 선택한 경우 장치를 관리할 저장된 자격 증명을 선택해야 합니다.

팁: 감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우, 관리에 실패하거나 성공하더라도 장치의 기타 향후 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).

일반 및 저장된 자격 증명에 대한 자세한 정보는 사용자 계정 관리 및 저장된 자격 증명 관리의 내용을 참조하십시오.

8. 관리되는 인증을 선택하는 경우 복구 암호를 지정하십시오.

   복구 계정(RECOVERY_ID)이 CMM에 만들어지고 모든 로컬 사용자 계정이 사용 안 함으로 설정됩니다. XClarity Administrator에 문제가 있고 어떤 이유에서 작동이 중지되면 일반 사용자 계정을 사용하여 CMM에 로그인할 수 *없습니다*. 그러나 RECOVERY_ID 계정을 사용하여 로그인할 수 있습니다.

   참고:

   - 관리되는 인증을 사용하도록 선택한 경우 복구 암호는 필수이며 로컬 인증을 사용하도록 선택한 경우에는 복구 암호가 허용되지 않습니다.
   - 로컬 복구 계정 또는 저장된 복구 자격 증명을 사용하도록 선택할 수 있습니다. 두 경우 모두 사용자 이름은 항상 RECOVERY_ID입니다.
   - 암호가 장치의 보안 및 암호 정책을 준수하는지 확인하십시오. 보안 및 암호 정책은 다를 수 있습니다.
   - 나중에 사용하도록 복구 암호를 기록해야 합니다.

   복구 ID에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.

9. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

   참고:

   - 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
   - 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

10. **관리**를 클릭하십시오.

    이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 진행상황을 모니터링하여 프로세스가 성공적으로 완료되는지 확인하십시오.

    프로세스가 완료되면 섀시의 장치 수와 섀시 상태를 표시하는 대화 상자가 표시됩니다.

    참고: 일부 인벤토리 데이터는 관리 프로세스가 완료된 후 수집됩니다. 섀시는 모든 인벤토리 데이터가 수집될 때까지 보류 상태입니다. 해당 장치에 대해 모든 인벤토리 데이터를 수집하고 섀시가 더 이상 보류 상태에 있지 않을 때까지 관리 장치에서 특정 작업(예, 서버 패턴 배포)을 수행할 수 없습니다.

11. 프로세스가 완료되면 **확인**을 클릭하십시오.

    장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

    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.

12. 새 섀시인 경우 **섀시 구성 계속하기**를 클릭하여 전체 섀시(컴퓨팅 노드 및 Flex 스위치 포함)에 대한 관리 네트워크 설정의 유효성을 검증하고 변경하고 서버 패턴을 만들어 배포함으로써 컴퓨팅 노드 정보, 로컬 스토리지, I/O 어댑터, 부팅 대상 및 펌웨어 설정을 구성하십시오. 자세한 정보는 섀시에 대한 관리 IP 설정 수정 및 구성 패턴을 사용하여 서버 구성의 내용을 참조하십시오.

완료한 후에

- 추가 장치를 검색 및 관리하십시오.
- 아직 운영 체제가 설치되지 않은 서버에 운영 체제 이미지를 배포하십시오. 자세한 정보는 베어메탈 서버에 운영 체제 설치의 내용을 참조하십시오.
- 현재 정책을 준수하지 않는 장치에 펌웨어를 업데이트하십시오(관리 장치에서 펌웨어 업데이트 참조).
- 물리적 환경을 반영하도록 새 관리되는 장치를 적절한 랙에 추가하십시오(랙 관리 참조).
- 하드웨어 상태 및 세부 정보를 모니터링하십시오(관리 서버의 상태 보기 참조).
- 이벤트 및 경고를 모니터링하십시오(이벤트 작업 및 경고 작업 참조).

관리 섀시의 상태 보기

Lenovo XClarity Administrator에서 관리되는 섀시 및 설치된 구성 요소의 요약 및 세부적인 상태를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

이 작업 정보

다음 상태 아이콘은 장치의 전반적인 상태를 나타내는 데 사용됩니다. 인증서가 일치하지 않으면 적용 가능한 각 장치의 상태에 "(신뢰할 수 없음)"이 추가됩니다. 예를 들어 경고(신뢰할 수 없음)이 표시됩니다. 연결 문제가 있거나 장치에 대한 연결을 신뢰할 수 없는 경우 적용 가능한 각 장치의 상태에 "(연결)"이 추가됩니다. 예를 들어 경고(연결)이 표시됩니다.

- () 위험
- () 경고
- () 보류 중
- () 정보
- () 정상
- () 오프라인
- () 알 수 없음

절차

다음 단계를 완료하여 관리되는 섀시에 대한 상태를 보십시오.

- **세부 정보** 링크를 클릭하거나 **작업 → 보기 → 세부 정보**를 클릭하여 섀시에 대한 자세한 정보를 봅니다.
- IP 주소 링크를 클릭하여 섀시의 CMM 웹 인터페이스를 실행하십시오(섀시에 대한 CMM 웹 인터페이스 실행 참조).
- **작업 → 인벤토리 → 속성 편집**을 클릭하여 정보(예, 지원 연락처, 위치 및 설명)를 수정합니다.
- **작업 → 인벤토리 → 관리 IP 주소 편집**을 클릭하여 컴퓨팅 노드 및 Flex 스위치 등 전체 섀시의 관리 IP 설정을 수정합니다.
- 섀시를 선택하고 **작업 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 하나 이상의 섀시에 대한 자세한 정보를 CSV 파일로 내보냅니다.

  참고: 한 번에 최대 60대의 장치에 대한 인벤토리 데이터를 내보낼 수 있습니다.

  팁: CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- 섀시를 선택하고 **작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 Lenovo XClarity Administrator 보안 인증서와 섀시 CMM의 보안 인증서 간에 발생할 수 있는 문제를 해결합니다.

관리 섀시의 세부 정보 보기

Lenovo XClarity Administrator에서 펌웨어 수준, IP 주소 및 UUID(범용 고유 식별자)를 비롯한 관리되는 섀시에 대한 자세한 정보를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

이 작업 정보

시스템 수준 공기 온도는 서버 앞면의 물리적 센서로 측정됩니다. 이 온도는 서버의 흡입구 공기 온도를 나타냅니다. 온도가 다른 시점에서 측정되면 XClarity Administrator와 CMM에서 보고되는 공기 온도가 다를 수 있음을 주의하십시오.

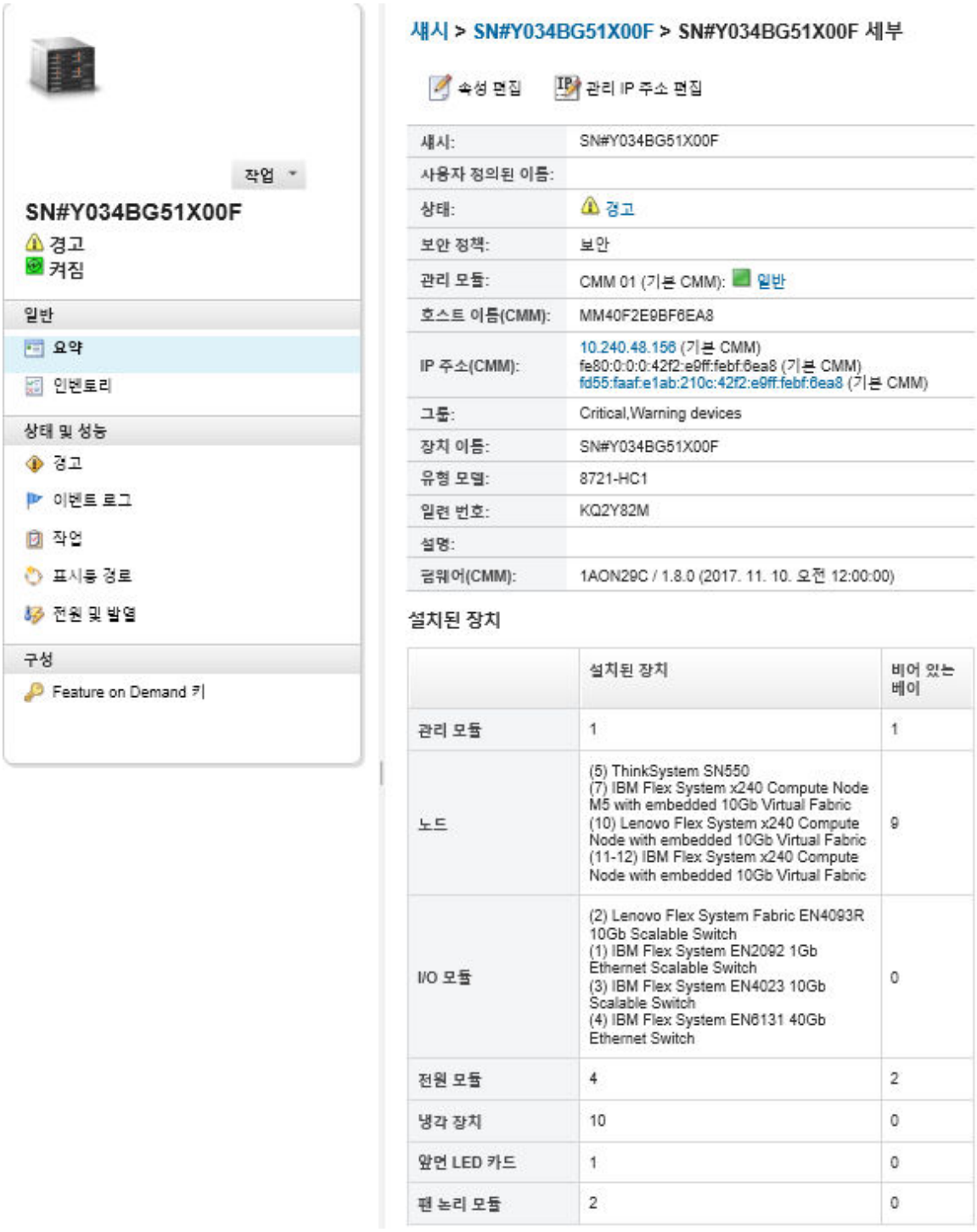
절차

다음 단계를 완료하여 관리되는 섀시에 대한 세부 정보를 보십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 섀시**를 클릭하십시오. 섀시 페이지가 모든 관리 섀시 표 보기와 함께 표시됩니다.

관리할 섀시를 더 손쉽게 찾기 위해 표 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 섀시 이름 또는 IP 주소)를 입력하여 표시되는 필터와 섀시를 상세하게 필터링할 수도 있습니다.

단계 2. **섀시** 열에서 섀시 이름을 클릭하십시오. 해당 섀시의 상태 요약 페이지가 표시되며, 여기에는 섀시에 설치된 구성 요소와 섀시 속성이 표시됩니다.



단계 3. 다음 작업 중 하나 이상을 완료합니다.

- **요약**을 클릭하여 시스템 정보와 설치된 구성 요소를 비롯한 섀시의 요약을 보십시오(관리 섀시의 상태 보기 참조).
- **인벤토리 세부 정보**를 클릭하여 다음과 같은 섀시 구성 요소에 대한 세부 정보를 보십시오.
  - 섀시의 모든 구성 요소에 대한 펌웨어 수준.

  - 호스트 이름, IPv4 주소, IPv6 주소 및 MAC 주소와 같은 CMM에 대한 세부 정보.
  - 이름, UUID(범용 고유 식별자) 및 위치 등 섀시 및 섀시에 설치된 CMM에 대한 자원 세부 정보.
- 이 섀시의 현재 경고 목록을 표시하려면 **경고**를 클릭하십시오(경고 작업 참조).
- 이 섀시의 이벤트 목록을 표시하려면 **이벤트 로그**를 클릭하십시오(이벤트 로그에서 이벤트 모니터링 참조).
- 섀시와 연결된 작업의 목록을 표시하려면 **작업**을 클릭하십시오(작업 모니터링 참조).
- 위치, 장애 및 정보 등 섀시 LED의 현재 상태를 표시하려면 Light Path를 클릭하십시오. 섀시의 앞면 패널을 보는 것과 동일합니다.
- 전원 및 통풍에 대한 세부 정보를 표시하려면 **전원 및 열**을 클릭하십시오.

  팁: 최신 전원 및 열 데이터를 수집하려면 웹 브라우저의 새로 고침 버튼을 사용하십시오. 데이터를 수집하려면 몇 분 정도가 걸릴 수 있습니다.
- Feature on Demand 키와 다른 에이전트 없는 정보를 주문하는 데 필요한 정보에 액세스하려면 Feature on Demand **키**를 클릭하십시오(Features on Demand 키 보기 참조).

완료한 후에

섀시에 대한 요약 및 세부 정보를 표시하는 것 외에도 다음 작업을 수행할 수 있습니다.

- **작업 → 보기 → 랙 보기에 표시** 또는 **작업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 섀시를 봅니다.
- IP **주소** 링크를 클릭하여 CMM 웹 인터페이스를 실행하십시오(섀시에 대한 CMM 웹 인터페이스 실행 참조).
- **속성 편집**을 클릭하여 정보(예, 지원 담당자, 위치 및 설명)를 수정하십시오(섀시에 대한 시스템 속성 수정 참조).
- **모든 작업 → 인벤토리 → 관리 IP 주소 편집**을 클릭하여 컴퓨팅 노드 및 Flex 스위치 등 전체 섀시의 관리 IP 설정을 수정하십시오(섀시에 대한 관리 IP 설정 수정 참조).
- **작업 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 섀시에 대한 자세한 정보를 CSV 파일로 내보내십시오.

  참고:
  - CSV 파일의 인벤토리 데이터에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 GET /chassis/*<UUID_list>*의 내용을 참조하십시오.
  - CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- 섀시를 관리 해제하십시오(섀시 관리 해제 참조).
- 섀시를 선택하고 **작업 → 보안 →** Encapsulation **사용** 또는 **작업 → 보안 →** Encapsulation **사용 안 함**을 클릭하여 수신 요청을 XClarity Administrator로만 제한하는 섀시의 방화벽 규칙 변경을 사용 또는 사용 안 함으로 설정합니다.

  글로벌 encapsulation 설정은 기본적으로 사용하지 않습니다. 사용하지 않는 경우 장치 encapsulation 모드를 "일반"으로 설정하고 방화 벽 규칙은 관리 프로세스의 일부로 변경되지 않습니다.

  글로벌 encapsulation 설정은 기본적으로 사용하지 않습니다. 사용하지 않는 경우 장치 encapsulation 모드를 "일반"으로 설정하고 방화 벽 규칙은 관리 프로세스의 일부로 변경되지 않습니다.

  글로벌 encapsulation 설정을 사용하고 장치가 encapsulation을 지원하는 경우 XClarity Administrator는 관리 프로세스 중에 장치와 통신하여 장치 encapsulation 모드를 "encapsulationLite"로 변경하고 장치의 방화벽 규칙을 변경하여 수신 요청을 XClarity Administrator로만 제한합니다.

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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.

- 섀시를 선택하고 **작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 XClarity Administrator 보안 인증서와 섀시 CMM의 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).

CMM 구성 데이터 백업 및 복원

Lenovo XClarity Administrator에는 CMM 구성 데이터에 대한 기본 제공 백업 및 복구 기능이 포함되어 있지 않습니다. 대신 관리되는 CMM에 사용할 수 있는 백업 기능을 사용하십시오.

관리 웹 인터페이스 또는 명령줄 인터페이스(CLI)를 사용하여 CMM을 백업하고 복원하십시오.

- CMM 구성 데이터 백업
  - 관리 웹 인터페이스에서 **관리 모듈 관리 → 구성 → 백업 구성**을 클릭하십시오. 자세한 정보는 Flex Systems 온라인 설명서의 웹 인터페이스를 통한 CMM 구성 저장의 내용을 참조하십시오.
  - CLI에서 `write` 명령을 사용하십시오. 자세한 정보는 Flex Systems 온라인 설명서의 CMM write 명령의 내용을 참조하십시오.
- CMM 구성 데이터 복원
  - 관리 웹 인터페이스에서 **관리 모듈 관리 → 구성 → 파일에서 구성 복원**을 클릭하십시오. 자세한 정보는 Flex Systems 온라인 설명서의 웹 인터페이스를 통한 CMM 구성 복원의 내용을 참조하십시오.
  - CLI에서 `read` 명령을 사용하십시오. 자세한 정보는 Flex Systems 온라인 설명서의 CMM read 명령의 내용을 참조하십시오.

참고: 팁: PureFlex 및 Flex System 백업 및 복원 모범 사례 안내서에서 섀시 구성 요소의 백업 및 복원에 대한 추가 정보를 찾을 수 있습니다.

섀시에 대한 CMM 웹 인터페이스 실행

Lenovo XClarity Administrator에서 특정 섀시에 대한 CMM 웹 인터페이스를 실행할 수 있습니다.

절차

CMM 웹 인터페이스를 실행하려면 다음 단계를 완료하십시오.

참고: Safari 웹 브라우저를 사용하여 XClarity Administrator에서 이 CMM 웹 인터페이스를 실행하는 것은 지원되지 않습니다.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 섀시**를 클릭하여 섀시 페이지를 표시하십시오.

관리할 섀시를 더 손쉽게 찾기 위해 표 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 섀시 이름 또는 IP 주소)를 입력하여 표시되는 필터와 섀시를 상세하게 필터링할 수도 있습니다.

단계 2. **섀시** 열의 섀시 링크를 클릭하십시오. 해당 섀시에 대한 상태 요약 페이지가 표시됩니다.

단계 3. **모든 작업 → 실행 → 관리 웹 인터페이스**를 클릭하십시오. CMM 웹 인터페이스가 시작됩니다.

팁: 또한 IP 주소를 클릭하여 CMM을 실행할 수 있습니다.

단계 4. XClarity Administrator 사용자 자격 증명을 사용하여 CMM 웹 인터페이스에 로그인하십시오.

섀시에 대한 시스템 속성 수정

특정 섀시에 대한 시스템 속성을 수정할 수 있습니다.

절차

시스템 속성을 수정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 섀시**를 클릭하여 섀시 페이지를 표시하십시오.

단계 2. 업데이트할 섀시를 선택하십시오.

단계 3. **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 편집 대화 상자를 표시하십시오.

단계 4. 필요 시 다음 정보를 변경하십시오.
- 서버 이름
- 지원 문의
- 설명

참고: 웹 인터페이스의 랙에서 장치를 추가하거나 제거할 때 XClarity Administrator에서 위치, 룸, 랙 및 하단 LRU(lowest rack unit) 속성을 업데이트합니다(랙 관리 참조).

단계 5. **저장**을 클릭하십시오.

참고: 이러한 속성을 변경하는 경우 XClarity Administrator 웹 인터페이스에 변경 사항이 표시되기 전에 약간의 지연이 있을 수 있습니다.

섀시에 대한 관리 IP 설정 수정

컴퓨팅 노드, 스토리지 장치 및 Flex 스위치 등 전체 섀시의 관리 IP 설정을 수정할 수 있습니다.

절차

관리 IP 설정을 수정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 섀시**를 클릭하여 섀시 페이지를 표시하십시오.

단계 2. 섀시를 선택하십시오.

단계 3. **모든 작업 → 인벤토리 → 관리 IP 주소 편집**을 클릭하여 섀시 및 구성 요소 IP 설정 페이지를 표시하십시오.

단계 4. 필요 시 다음 전역 설정을 변경하십시오.

- IPv4 주소 사용 또는 사용 안 함을 선택하십시오.

  IPv4 주소를 사용하는 경우, 다음 설정을 지정하십시오. IPv4 전역 설정은 IPv4 주소가 업데이트될 때 구성 요소에 적용됩니다.
  – (옵션) 정적으로 할당된 IP 주소를 사용하여 IP 주소를 가져옵니다.
  – 서브넷 마스크 및 게이트웨이 주소를 지정하십시오.
- IPv6 주소에 대한 다음 설정을 지정하십시오. IPv6 전역 설정은 IPv6 주소가 업데이트될 때 구성 요소에 적용됩니다.
  – (옵션) 정적으로 할당된 IP 주소를 사용하여 IP 주소를 가져옵니다.

    고정 IP 주소를 사용하는 경우, 상태 비저장 IP 주소 자동 구성 및 상태 저장 IP 주소 구성을 사용하도록 선택할 수도 있습니다.
  – 접두사 길이 및 게이트웨이 주소를 지정하십시오.
- DNS 서버 사용 또는 사용 안 함을 선택하십시오.

  DNS 서버를 사용하는 경우:
  – DNS 서버 검색 기본 설정을 선택하십시오.
  – DNS 검색 순서에 사용할 IP 주소를 입력하십시오.
  – 도메인 이름을 입력하십시오.

단계 5. 다음 CMM IP 설정을 변경하십시오.

- CMM의 호스트 이름 및 IP 주소를 입력하십시오.
- CMM IP 주소를 시작점으로 사용하여 컴퓨팅 노드, 스토리지 장치 및 Flex 스위치에 대한 IP 주소를 만들려면 **IP 주소 자동 생성**을 클릭하십시오.

단계 6. 섀시의 각 컴퓨팅 노드에 대한 호스트 이름 및 IP 주소를 입력하십시오.

단계 7. 섀시의 각 스토리지 장치에 대한 호스트 이름 및 IP 주소를 입력하십시오.

단계 8. 섀시의 각 Flex 스위치에 대한 IP 주소를 입력하십시오.

단계 9. **저장**을 클릭하십시오. 네트워크 설정의 요약이 포함된 대화 상자가 표시됩니다.

단계 10. **적용**을 클릭하십시오.

섀시의 모든 기존 구성 요소는 지정된 전역 설정으로 업데이트됩니다. 업데이트가 완료되면 대화 상자에 변경된 설정이 표시됩니다.

참고: 이 정보를 변경하는 경우 Lenovo XClarity Administrator 인터페이스에 정보가 표시되기 전에 약간의 지연이 있을 수 있습니다.

단계 11. **닫기**를 클릭하십시오.

CMM 장애 조치 구성

섀시에 두 번째 CMM을 설치하는 경우 두 번째 CMM은 기본적으로 자동으로 대기 CMM으로 구성됩니다. 기본 CMM이 실패하면 대기 CMM의 IP 주소는 기본 CMM에 사용된 것과 동일한 IP 주소로 변경되고 대기 CMM이 섀시 관리를 담당합니다. 하지만 섀시의 관리 컨트롤러 웹 인터페이스에서 보다 고급의 장애 조치 구성을 수행할 수 있습니다.

이 작업 정보

예를 들어 다음 사항을 선택할 수 있습니다.

- 대기 CMM에 대한 네트워크 인트페이스를 사용하지 않도록 설정하여 장애 조치를 방지합니다.
- 대기 CMM에 대한 네트워크 인터페이스를 사용하도록 설정하고 IP 주소가 장애 조치 중에 두 CMM 사이에서 스왑되도록 허용합니다.

- 대기 CMM에 대한 네트워크 인터페이스를 사용하도록 설정하고 IP 주소가 장애 조치 중에 두 CMM 사이에서 스왑되지 않도록 허용합니다.

CMM 고급 장애 조치 기능에 대한 자세한 정보는 CMM 온라인 설명서의 advfailover 명령의 내용을 참조하십시오.

절차

기본 및 대기 CMM에 대해 스왑 가능 IP 주소를 사용하도록 설정하려면 다음 단계를 완료하십시오.

단계 1. 섀시에 대한 관리 컨트롤러 웹 인터페이스에서 **관리 모듈 관리 → 네트워크 → 이더넷**을 클릭하여 이더넷 구성 페이지를 표시하십시오.

단계 2. 사용자의 시스템에 대해 IPv4 및 IPv6 중 하나를 선택하십시오.

단계 3. **IP 주소 구성**에서 고정 IP 주소 사용 옵션을 선택하십시오. 다른 프로토콜도 반복하십시오.

단계 4. **관리 모듈 관리 → 속성 → 고급 장애 조치**를 클릭하고 고급 장애 조치 옵션을 사용하십시오.

단계 5. **관리 모듈 IP 주소 스왑**을 선택하십시오.

단계 6. 테스트 시나리오를 수행하여 장애 조치가 제대로 작동하는지와 Lenovo XClarity Administrator가 기본 및 백업 CMM에 연결할 수 있는지 확인하십시오.

CMM 다시 시작

Lenovo XClarity Administrator에서 CMM(Chassis Management Module)을 다시 시작할 수 있습니다.

절차

섀시를 다시 시작하려면 다음 절차를 완료하십시오.

참고: CMM을 다시 시작하면 CMM에 대한 기존의 모든 네트워크 연결이 일시적으로 끊어집니다.

단계 1. XClarity Administrator 메뉴에서 **하드웨어 → 섀시**를 클릭하십시오. 섀시 페이지가 모든 관리 섀시 표 보기와 함께 표시됩니다.

단계 2. **섀시** 열에서 섀시 이름을 클릭하여 그래픽 섀시 보기를 표시하십시오.

단계 3. CMM 그래픽을 클릭하여 CMM 요약 페이지에 표시하십시오.

팁: 또한 **표 보기**를 클릭한 다음 **이름** 열에서 CMM 이름을 클릭하여 CMM 요약 페이지를 표시하십시오.

단계 4. **작업 → 전원 작업 → 다시 시작**을 클릭하십시오.

단계 5. **즉시 다시 시작**을 클릭하십시오.

이 작업은 완료하는 데 몇 분이 걸릴 수 있으며 결과를 보려면 페이지를 새로 고쳐야 할 수도 있습니다.

CMM 가상 재배치

섀시에서 Chassis Management Module(CMM)을 제거하고 다시 삽입하는 것을 시뮬레이션할 수 있습니다.

이 작업 정보

가상 재배치 중에는 기존의 모든 CMM 네트워크 연결이 끊어지고 CMM의 전원 상태가 변경됩니다.

주의: 가상 재배치를 수행하기 전에 CMM의 모든 사용자 데이터를 저장해야 합니다.

절차

다음 단계를 수행하여 CMM 가상 재배치를 하십시오.

단계 1. Lenovo XClarity Administrator 메뉴에서 **하드웨어 → 섀시**를 클릭하십시오. 섀시 페이지가 모든 관리 섀시 표 보기와 함께 표시됩니다.

단계 2. **섀시** 열에서 섀시 이름을 클릭하여 그래픽 섀시 보기를 표시하십시오.

단계 3. CMM 그래픽을 클릭하여 CMM 요약 페이지에 표시하십시오.

팁: 또한 **표 보기**를 클릭한 다음 **이름** 열에서 CMM 이름을 클릭하여 CMM 요약 페이지를 표시하십시오.

단계 4. **작업** → **서비스** → **가상 재배치**를 클릭하십시오.

단계 5. **가상 재배치**를 클릭하십시오.

섀시에 대해 만료되었거나 유효하지 않은 저장된 자격 증명 해결

저장된 자격 증명이 장치에서 만료되거나 작동 불능 상태가 되면 해당 장치의 상태가 "오프라인"으로 표시됩니다.

절차

섀시에 대해 만료되었거나 유효하지 않은 저장된 자격 증명을 해결하려면 다음을 수행하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어** → **섀시**를 클릭하십시오. 섀시 페이지가 모든 관리 섀시 표 보기와 함께 표시됩니다.

단계 2. **전원** 열 머리글을 클릭하여 테이블 맨 위에 있는 모든 오프라인 섀시를 그룹화합니다.

관리할 섀시를 더 손쉽게 찾기 위해 표 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 섀시 이름 또는 IP 주소)를 입력하여 표시되는 필터와 섀시를 상세하게 필터링할 수도 있습니다.

단계 3. 해결할 섀시를 선택하십시오.

단계 4. **모든 작업** → **보안** → **저장된 자격 증명 편집**을 클릭하십시오.

단계 5. 저장된 자격 증명의 암호를 변경하거나 관리되는 장치에 사용할 다른 저장된 자격 증명을 선택하십시오.

참고: 동일한 저장된 자격 증명을 사용하여 둘 이상의 장치를 관리하고 저장된 자격 증명의 암호를 변경하면 해당 암호 변경은 현재 저장된 자격 증명을 사용하는 모든 장치에 영향을 줍니다.

관리 서버 오류 후 CMM으로 관리 복구

섀시가 Lenovo XClarity Administrator에서 관리되고 XClarity Administrator에 오류가 발생한 경우 관리 노드가 복원되거나 교체될 때까지 CMM에 대한 관리 기능 및 로컬 사용자 계정을 복원할 수 있습니다.

절차

CMM에서 관리를 복원하려면 다음 절차 중 하나를 완료하십시오.

- 교체 XClarity Administrator 인스턴스가 오류가 있는 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 RECOVERY_ID 계정 및 암호와 **강제 관리** 옵션을 사용하여 장치를 다시 관리하십시오(섀시 관리 참조).
- 종이 클립을 사용하여 CMM의 핀 구멍을 10초 이상 눌러 CMM을 공장 출하 기본값으로 재설정하십시오. 중요 주의사항을 비롯한 CMM 재설정에 대한 자세한 정보는 Flex Systems 온라인 설명서의 CMM 재설정의 내용을 참조하십시오.
- 다음 단계를 사용하여 CMM 구성을 재설정하십시오.
  1. SSH 세션을 통해 섀시의 관리 명령줄 인터페이스를 열고 RECOVERY_ID 계정으로 로그인하십시오.

     참고: RECOVERY_ID 계정의 암호는 관리 도메인 페이지에서 관리 섀시를 선택했을 때 설정되었습니다. 중앙 계정 관리에 대한 자세한 정보는 섀시 관리의 내용을 참조하십시오.

     처음 RECOVERY_ID 계정으로 CMM에 로그인하는 경우 암호를 변경해야 합니다.
  2. 메시지가 표시되면 RECOVERY_ID 계정의 새 암호를 입력하십시오.
  3. 다음 단계 중 하나를 수행하여 CMM 구성을 복원하십시오.
     - 2015년 6월 이후의 CMM 펌웨어 릴리스를 실행하는 경우 다음 명령을 실행하십시오.
       `read -f unmanage -T mm[p]`
       자세한 정보는 CMM 온라인 설명서의 read 명령의 내용을 참조하십시오.
     - 2015년 6월 이전의 CMM 펌웨어 릴리스를 실행하는 경우 다음 명령을 표시된 순서대로 실행하십시오.
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

          fsmcm 명령은 XClarity Administrator 사용자 계정 관리를 사용 안 함으로 설정하고 로컬 CMM 사용자 계정을 사용하여 CMM 및 섀시에 설치된 모든 관리 프로세서에 인증할 수 있습니다.

          fsmcm -off 명령을 실행한 후 RECOVERY_ID 계정은 CMM 사용자 레지스트리에서 제거됩니다. fsmcm -off 명령을 실행하면 CMM CLI 세션이 종료됩니다. 이제 로컬 CMM 자격 증명을 사용하여 CMM 및 다른 섀시 구성 요소에 인증하고 로컬CMM 자격 증명을 사용하여 XClarity Administrator가 복원될 때까지 CMM 웹 인터페이스 또는 섀시의 CLI에 액세스할 수 있습니다.

자세한 정보는 CMM 온라인 설명서의 fsmcm 명령의 내용을 참조하십시오.

XClarity Administrator가 복원되거나 교체된 후 섀시를 다시 관리할 수 있습니다(섀시 관리 참조). 섀시에 대한 모든 정보(예, 네트워크 설정)는 유지됩니다.

섀시 관리 해제

Lenovo XClarity Administrator로 관리에서 섀시를 제거할 수 있습니다. 이 프로세스를 ***관리 해제***라고 합니다. 섀시를 관리 해제한 후 로컬 CMM 사용자 계정을 사용하여 섀시의 CMM에 로그인할 수 있습니다.

시작하기 전에

XClarity Administrator을(를) 사용하여 특정 기간 동안 오프라인 상태였던 장치를 자동으로 관리 해제할 수 있습니다. 기본적으로 이 기능은 사용 불가능하도록 설정되어 있습니다. 오프라인 장치 자동 관리 해제 기능을 사용하려면, XClarity Administrator 메뉴의 **하드웨어 → 새 장치 검색 및 관리**를 클릭한 다음, **오프라인 장치 관리 해제 기능을 사용할 수 없습니다** 옆의 **편집**을 클릭하십시오. 그러고 나서 **오프라인 장치 관리 해제 기능 사용**을 선택하고 시간 간격을 설정하십시오. 기본적으로 장치는 24시간 동안 오프라인 상태인 경우 관리 해제됩니다.

섀시를 관리 해제하기 전에 섀시에 설치된 장치에 대해 실행 중인 활성 작업이 없어야 합니다.

콜 홈이 XClarity Administrator에서 사용 설정된 경우 중복 문제 레코드가 작성되지 않도록 모든 관리되는 섀시와 서버에서 콜 홈이 사용 안 함으로 설정됩니다. XClarity Administrator를 사용한 장치 관리를 중단하려는 경우 나중에 개별 장치에 대해 콜 홈을 다시 사용 설정하는 대신 XClarity Administrator의 모든 관리되는 장치에서 콜 홈을 다시 사용 설정할 수 있습니다(XClarity Administrator 온라인 설명서에서 모든 관리 장치에서 콜 홈 다시 사용 가능하도록 설정 참조).

이 작업 정보

섀시를 관리 해제하면 XClarity Administrator가 다음 작업을 수행합니다.

- 중앙 집중식 사용자 관리에 사용되는 구성을 지웁니다.
- XClarity Administrator 보안 저장소에서 CMM 보안 인증서를 제거합니다.
- 장치에서 Encapsulation을 사용할 수 있는 경우 장치 방화벽 규칙을 장치를 관리하기 전의 설정으로 구성합니다.
- CMM에서 NTP 서버 액세스를 제거합니다.
- XClarity Administrator가 더 이상 해당 섀시에서 이벤트를 수신하지 않도록 XClarity Administrator 구성에서 CMM 구독을 제거합니다.

섀시를 관리 해제하면 XClarity Administrator는 섀시에 대한 특정 정보를 유지합니다. 해당 정보는 동일한 섀시를 다시 관리할 때 다시 적용됩니다.

섀시를 관리 해제하면 섀시 구성 요소에서 전송된 이벤트가 제거됩니다. 이벤트를 Syslog와 같은 외부 리포지토리에 전달하여 이러한 이벤트를 유지할 수 있습니다(이벤트 전달 참조).

팁: 초기 설정 중에 선택적으로 추가되는 모든 데모 장치는 섀시의 노드입니다. 데모 장치를 관리 해제하려면 **장치에 연결할 수 없는 경우에도 강제로 관리 해제** 옵션을 사용하여 섀시를 관리 해제하십시오.

절차

섀시를 관리 해제하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 섀시**를 클릭하여 섀시 페이지를 표시하십시오.

단계 2. 관리되는 섀시의 목록에서 하나 이상의 섀시를 선택하십시오.

단계 3. **섀시 관리 해제**를 클릭하십시오. 관리 해제 대화 상자가 표시됩니다.

단계 4. **옵션: 장치에 연결할 수 없는 경우에도 강제로 관리 해제**를 선택하십시오.

중요: 데모 하드웨어를 관리 해제하는 경우 이 옵션을 선택해야 합니다.

단계 5. **관리 해제**를 클릭하십시오.관리 해제 대화 상자에는 관리 해제 프로세스 각 단계의 진행상황이 표시됩니다.

단계 6. 관리 해제 프로세스가 완료되면 **확인**을 클릭하십시오.

완료한 후에

관리 해제 프로세스가 완료된 후 로컬 CMM 사용자 계정을 사용하여 CMM에 로그인할 수 있습니다. 로컬 CMM 사용자 계정에 대한 사용자 이름 또는 암호가 기억나지 않는 경우 CMM에 로그인하려면 CMM을 공장 출하 기본값으로 재설정하십시오. CMM을 공장 출하 기본값으로 재설정하는 것에 대한 정보는 CMM 제품 설명서의 Flex Systems 온라인 설명서의 CMM 재설정의 내용을 참조하십시오.

올바로 관리 해제되지 않은 섀시 복구

섀시가 올바로 관리 해제되지 않은 경우 다시 관리하려면 섀시를 복구해야 합니다.

절차

CMM에서 관리를 복원하려면 다음 절차 중 하나를 완료하십시오.

- 교체 XClarity Administrator 인스턴스가 오류가 있는 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 RECOVERY_ID 계정 및 암호와 **강제 관리** 옵션을 사용하여 장치를 다시 관리하십시오(섀시 관리 참조).
- 종이 클립을 사용하여 CMM의 핀 구멍을 10초 이상 눌러 CMM을 공장 출하 기본값으로 재설정하십시오. 중요 주의사항을 비롯한 CMM 재설정에 대한 자세한 정보는 Flex Systems 온라인 설명서의 CMM 재설정의 내용을 참조하십시오.
- 다음 단계를 사용하여 CMM 구성을 재설정하십시오.
  1. SSH 세션을 통해 섀시의 관리 명령줄 인터페이스를 열고 RECOVERY_ID 계정으로 로그인하십시오.

     참고: RECOVERY_ID 계정의 암호는 관리 도메인 페이지에서 관리 섀시를 선택했을 때 설정되었습니다. 중앙 계정 관리에 대한 자세한 정보는 섀시 관리의 내용을 참조하십시오.

     처음 RECOVERY_ID 계정으로 CMM에 로그인하는 경우 암호를 변경해야 합니다.
  2. 메시지가 표시되면 RECOVERY_ID 계정의 새 암호를 입력하십시오.
  3. 다음 단계 중 하나를 수행하여 CMM 구성을 복원하십시오.
     - 2015년 6월 이후의 CMM 펌웨어 릴리스를 실행하는 경우 다음 명령을 실행하십시오.
       `read -f unmanage -T mm[p]`
       자세한 정보는 CMM 온라인 설명서의 read 명령의 내용을 참조하십시오.
     - 2015년 6월 이전의 CMM 펌웨어 릴리스를 실행하는 경우 다음 명령을 표시된 순서대로 실행하십시오.
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

`fsmcm` 명령은 XClarity Administrator 사용자 계정 관리를 사용 안 함으로 설정하고 로컬 CMM 사용자 계정을 사용하여 CMM 및 섀시에 설치된 모든 관리 프로세서에 인증할 수 있습니다.

`fsmcm -off` 명령을 실행한 후 `RECOVERY_ID` 계정은 CMM 사용자 레지스트리에서 제거됩니다. `fsmcm -off` 명령을 실행하면 CMM CLI 세션이 종료됩니다. 이제 로컬 CMM 자격 증명을 사용하여 CMM 및 다른 섀시 구성 요소에 인증하고 로컬CMM 자격 증명을 사용하여 XClarity Administrator가 복원될 때까지 CMM 웹 인터페이스 또는 섀시의 CLI에 액세스할 수 있습니다.

자세한 정보는 CMM 온라인 설명서의 fsmcm 명령의 내용을 참조하십시오.

XClarity Administrator가 복원되거나 교체된 후 섀시를 다시 관리할 수 있습니다(섀시 관리 참조). 섀시에 대한 모든 정보(예, 네트워크 설정)는 유지됩니다.

제 8 장 서버 관리

Lenovo XClarity Administrator는 ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x® 및 ThinkServer® 서버를 포함하여 여러 유형의 시스템을 관리할 수 있습니다.

자세히 알아보기:  XClarity Administrator: 검색

시작하기 전에

참고: Flex 컴퓨팅 노드는 해당 노드가 포함된 섀시를 관리할 때 자동으로 검색되고 관리됩니다. Flex 컴퓨팅 노드를 섀시와 별도로 검색하고 관리할 수 없습니다.

서버를 관리하기 전에 다음 조건이 충족되는지 확인하십시오.

- 장치를 관리하기 전에 관리 고려사항을 검토하십시오. 정보는 XClarity Administrator 온라인 설명서에서 관리 고려사항의 내용을 참조하십시오.
- 특정 포트가 장치와 통신 가능해야 합니다. 섀시 관리를 시도하기 전에 필요한 모든 포트가 사용 가능해야 합니다. 포트에 대한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.
- XClarity Administrator를 사용하여 관리하려는 각 서버에 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.
- 장치에서 HTTPS를 통한 CIM이 사용 가능한지 확인하십시오.
  1. RECOVERY_ID 사용자 계정을 사용하여 서버의 관리 웹 인터페이스에 로그인하십시오.
  2. **IMM 관리 ➡ 보안**을 클릭하십시오.
  3. **HTTPS를 통한 CIM** 탭을 클릭하고 **HTTPS를 통한 CIM 사용**이 선택되었는지 확인하십시오.
- ThinkSystem SR635 및 SR655 서버:
  - 운영 체제가 설치되어 있어야 하며 XClarity Administrator가 해당 서버에 대한 인벤토리를 수집할 수 있도록 서버가 OS, 탑재된 부팅 가능한 미디어 또는 efishell로 한 번 이상 부팅되었는지 확인하십시오.
  - IPMI over LAN을 사용할 수 있어야 합니다. 이러한 서버에서는 IPMI over LAN가 기본적으로 비활성화되어 있으며, 서버를 관리하려면 수동으로 활성화해야 합니다. TSM을 사용하여 IPMI over LAN를 사용하려면, **설정 ➡ IPMI 구성**을 클릭하십시오. 서버를 다시 시작해 변경 사항을 활성화해야 할 수도 있습니다.
- 장치의 서버 인증서를 외부 인증 기관에서 서명한 경우 인증 기관 인증서 및 중간 인증서를 XClarity Administrator 신뢰 저장소로 가져와야 합니다(관리 장치에 사용자 지정된 서버 인증서 배포 참조).
- XClarity Administrator에서 *다른* 서브넷에 있는 서버를 검색하려면 다음 조건 중 하나가 충족되어야 합니다.
  - 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.
  - 엔드포인트 또는 네트워크에서 SLP를 사용하지 않는 경우 서비스 레코드(SRV 레코드)를 수동으로 XClarity Administrator의 도메인 이름 서버(DNS)에 추가하여 DNS 검색 방법을 대신 사용할 수 있습니다. 예를 들어 다음과 같습니다.
    ```
    _lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```

그런 다음 **IMM 관리 → 네트워크 프로토콜**을 클릭하고 DNS 탭을 클릭한 후 **DNS를 사용하여 Lenovo XClarity Administrator 검색**을 선택하여 관리 웹 인터페이스에서 베이스보드 관리 콘솔에 DNS 검색 사용을 설정하십시오.

참고:

- DNS를 사용한 자동 검색을 지원하려면 관리 컨트롤러에서 날짜가 2017년 5월 이상인 펌웨어 수준이 실행 중이어야 합니다.
- 사용자 환경에 여러 XClarity Administrator 인스턴스가 있는 경우 서버는 검색 요청에 처음 응답한 인스턴스에서만 검색됩니다. 서버는 모든 인스턴스에서 검색되지 않습니다.

- ThinkServer 서버를 검색하고 관리하려면 다음 요구사항이 충족되는지 확인하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치를 검색할 수 없음 및 장치를 관리할 수 없음의 내용을 참조하십시오.
  - XClarity Administrator가 서버를 자동으로 검색하도록 하려면 서버의 호스트 이름이 올바른 호스트 이름 또는 IP 주소를 사용하여 구성되어야 합니다.
  - 네트워크 구성은 XClarity Administrator와 서버 간에 SLP 트래픽을 허용해야 합니다.
  - 유니캐스트 SLP가 필요합니다.
  - XClarity Administrator가 ThinkServer 서버를 자동으로 검색하도록 하려면 멀티캐스트 SLP가 필요합니다. 또한 SLP는 ThinkServer System Manager(TSM)에서 사용으로 설정되어야 합니다.
  - ThinkServer 서버가 XClarity Administrator와 다른 네트워크에 있는 경우 XClarity Administrator가 해당 장치에 대한 이벤트를 검색할 수 있도록 네트워크가 포트 162를 통한 인바운드 UDP를 허용할 수 있게 구성되어야 합니다.
- ThinkAgile, ThinkSystem, Converged, Flex System의 경우. NeXtScale 및 System x 서버의 경우 서버에서 어댑터를 제거, 교체 및 구성하면 베이스보드 관리 컨트롤러와 XClarity Administrator 보고서(서버 전원 켜기 및 끄기)에서 새 어댑터 정보를 업데이트하기 위해 서버가 최소 한 번 이상 다시 시작됩니다.
- 서버에서 관리 작업을 수행하는 경우 BIOS/UEFI 설정 또는 실행 중인 운영 체제로 서버 전원이 켜지거나 꺼지는지 확인하십시오. **모든 작업 → 전원 작업 → BIOS/UEFI 설정으로 다시 시작**을 클릭하여 XClarity Administrator의 서버 페이지에서 BIOS/UEFI 설정을 부팅할 수 있습니다. 운영 체제 없이 서버 전원을 켜는 경우 운영 체제 검색 시 관리 컨트롤러가 서버를 계속해서 재설정합니다.
- 서버 UEFI 설정에서 모든 `UEFI_Ethernet_*` 및 `UEFI_Slot_*` 설정이 사용으로 설정되어야 합니다. 설정을 확인하려면, 서버를 다시 시작하고 `<F1> Setup` 프롬프트가 표시되면 `F1`을 눌러 Setup Utility를 시작하십시오. **System Settings → Devices and I/O Ports → Enable / Disable Adapter Option ROM Support**로 이동하여 **Enable / Disable UEFI Option ROM(s)** 섹션을 찾아 사용으로 설정되어 있는지 확인하십시오.

  참고: 지원되는 경우 베이스보드 관리 인터페이스에서 원격 콘솔 기능을 사용하여 설정을 원격으로 검토하고 수정할 수도 있습니다.
- System x3950 X6 서버는 각각의 고유한 베이스보드 관리 컨트롤러가 있는 두 개의 4U 엔클로저로 관리되어야 합니다.

이 작업 정보

XClarity Administrator는 XClarity Administrator와 동일한 IP 서브넷에 있는 관리 가능 장치를 프로브하여 사용자 환경에서 랙과 타워 서버를 자동으로 검색할 수 있습니다. 다른 서브넷에 있는 랙과 타워 서버를 검색하려면 IP 주소 또는 IP 주소 범위를 지정하거나 스프레드시트에서 정보를 가져오십시오.

중요: System x3850 및 x3950 X6 서버의 경우 확장 가능한 랙 환경에서 각 서버를 관리해야 합니다.

서버가 XClarity Administrator에서 관리되면 Lenovo XClarity Administrator는 관리되는 각 서버를 주기적으로 폴링하여 인벤토리, 필수 제품 데이터 및 상태와 같은 정보를 수집합니다. 관리되

는 서버를 보고 모니터하고, 관리 작업(예, 시스템 설정 구성, 운영 체제 이미지 배포 및 전원 켜기와 끄기)을 수행할 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(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.

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 스토리지 장치를 관리하도록 하려면 먼저 초기 XClarity Administrator에서 장치를 관리 해제하고 이를 새 XClarity Administrator에서 관리하도록 설정하십시오. 관리 해제 프로세스 중에 오류가 발생하는 경우 새 XClarity Administrator에서 관리 중에 **강제 관리** 옵션을 선택할 수 있습니다.

참고: 관리 가능한 장치에 대한 네트워크를 검색하는 경우 XClarity Administrator는 장치 관리를 시도한 후까지 다른 관리자가 이미 장치를 관리하고 있는지 확인할 수 없습니다.

참고: 관리 가능한 장치에 대한 네트워크를 검색하는 경우 XClarity Administrator는 ThinkServer 장치가 이미 관리되고 있는지 여부를 알 수 없으므로 관리되는 ThinkServer 장치가 관리 가능 장치 목록에 표시될 수 있습니다.

관리 프로세스 중에 XClarity Administrator는 다음 작업을 수행합니다.

- 제공된 자격 증명을 사용하여 서버에 로그인합니다.
- 각 서버의 인벤토리를 수집합니다.

  참고: 일부 인벤토리 데이터는 관리 프로세스가 완료된 후 수집됩니다. 해당 서버에 대해 모든 인벤토리 데이터를 수집하고 서버가 더 이상 보류 상태가 아닐 때까지 관리되는 서버에서 특정 작업(예, 서버 패턴 배포)을 수행할 수 없습니다.
- 모든 관리되는 장치가 XClarity Administrator에 구성된 동일한 NTP 서버 구성을 사용하도록 NTP 서버에 대한 설정을 구성합니다.
- (System x 및 NeXtScale 서버만 해당) 최근 편집한 펌웨어 준수 정책을 서버에 할당합니다.
- (Lenovo System x 및 NeXtScale 서버만 해당) XClarity Administrator로부터의 수신 요청만 승인하도록 장치 방화벽 규칙을 선택적으로 구성합니다.

- (System x 및 NeXtScale 서버만 해당) 관리 컨트롤러의 CIM 서버 인증서 및 LDAP 클라이언트 인증서를 XClarity Administrator 신뢰 저장소로 복사하고XClarity Administrator CA 보안 인증서 및 LDAP 신뢰할 수 있는 인증서를 관리 컨트롤러로 전송하여 보안 인증서를 관리 컨트롤러와 교환합니다. 관리 컨트롤러가 XClarity Administrator의 LDAP 및 CIM 서버에 대한 연결을 신뢰할 수 있도록 관리 컨트롤러는 인증서를 관리 컨트롤러 신뢰 저장소로 로드합니다.

  참고: CIM 서버 인증서나 LDAP 클라이언트 인증서가 없으면 관리 프로세스 중에 작성됩니다.
- 적용 가능한 경우 관리되는 인증을 구성합니다. 관리되는 인증에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.
- 적용 가능한 경우 복구 사용자 계정(RECOVERY_ID)을 만듭니다. RECOVERY_ID 계정에 관한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.

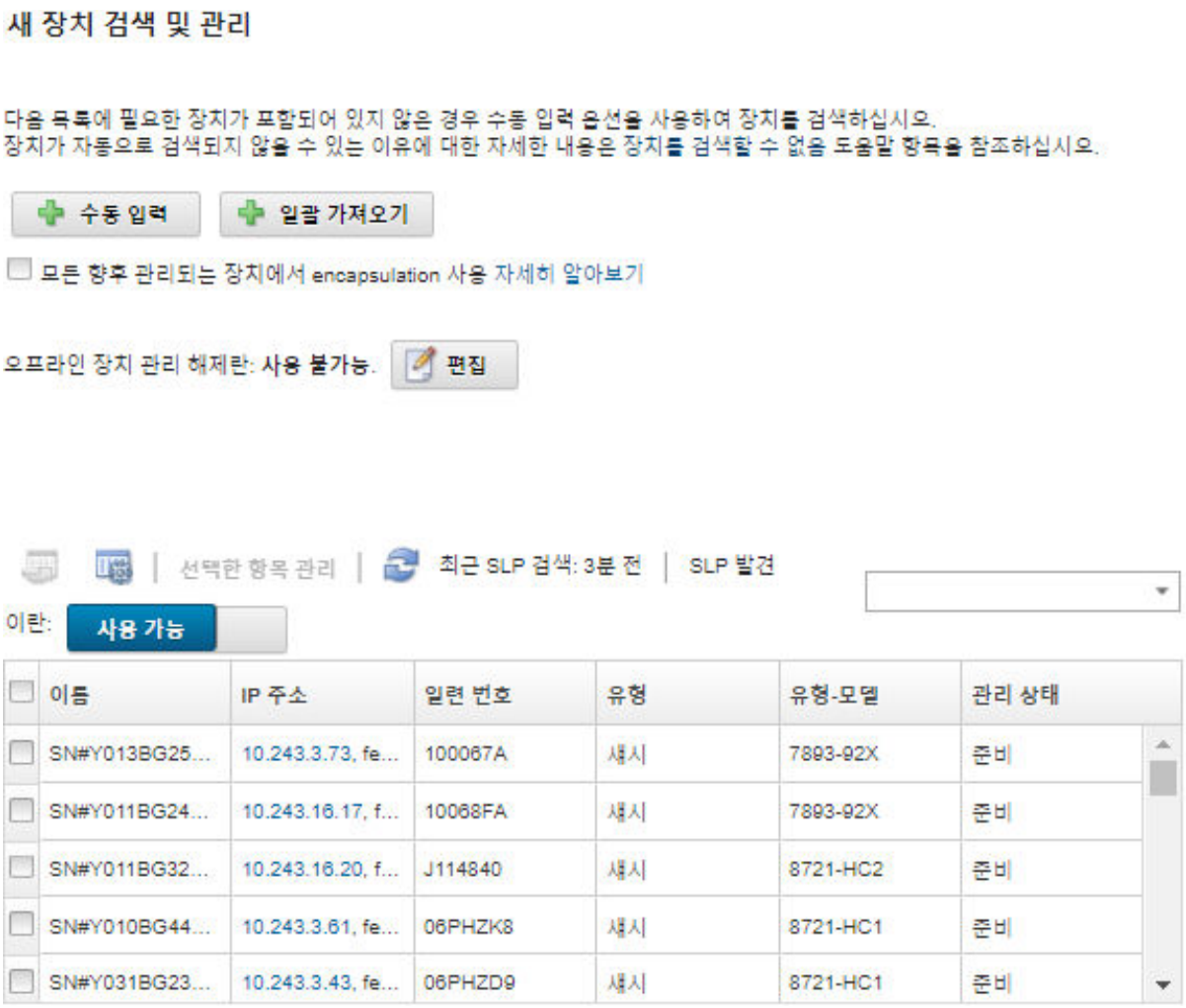
참고: XClarity Administrator는 관리 프로세스 중에 보안 설정 또는 암호 설정(암호화 모드 및 보안 통신에 사용되는 모드)을 수정하지 않습니다. 서버가 관리되면 암호화 설정을 수정할 수 있습니다 (관리 서버의 암호화 설정 구성 참조).

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.

절차

XClarity Administrator를 사용하여 랙 및 타워 서버를 관리하려면 다음 절차 중 하나를 완료하십시오.

- 일괄 가져오기 파일을 사용하여 다수의 타워 및 랙서버와 다른 장치를 검색하고 관리하십시오(XClarity Administrator 온라인 설명서의 시스템 관리 참조).
- XClarity Administrator와 동일한 IP 서브넷에 있는 랙 및 타워 서버를 검색하고 관리합니다.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 새 장치 검색 및 관리 페이지가 표시됩니다.



관리할 서버를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 필터와 서버를 상세하게 필터링할 수도 있습니다. **열 사용자 지정** 아이콘()을 클릭하여 표시되는 열과 기본 정렬 순서를 변경할 수 있습니다.

2. **새로 고침** 아이콘()을 클릭하여 XClarity Administrator 도메인의 모든 관리 가능 장치를 검색하십시오. 검색에는 몇 분 정도 소요됩니다.
3. 수신 요청이 XClarity Administrator에서만 허용되도록 관리 프로세스 중에 모든 장치에서 방화벽 규칙을 변경하려면 **모든 미래 관리 장치에서 encapsulation 사용** 선택란을 클릭하십시오.

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

   참고: 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.

   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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.
4. 관리할 하나 이상의 서버를 선택하십시오.
5. **선택 관리**을 클릭하십시오. 관리 대화 상자가 표시됩니다.

6. 이 장치에 대해 XClarity Administrator 관리되는 인증 또는 로컬 인증을 사용하도록 선택하십시오. 기본적으로 관리되는 인증이 선택됩니다. 로컬 인증을 사용하려면 **관리되는 인증**을 선택 취소하십시오.
7. 장치에 인증을 위해 사용할 자격 증명 유형을 선택하고 적절한 자격 증명을 지정하십시오.
   - **수동으로 입력된 자격 증명 사용**
     - 서버에 인증하기 위한 사용자 ID와 암호를 지정하십시오.
     - (옵션) 장치에서 암호가 현재 만료된 경우 지정된 사용자 이름에 대한 새 암호를 설정하십시오.

     참고: 수동으로 입력한 자격 증명을 사용하려면 XClarity Administrator 관리되는 인증을 선택해야 합니다.
   - **저장된 자격 증명 사용**

     이 관리되는 장치에 사용할 저장된 자격 증명을 선택하십시오. **새로 만들기**를 클릭하여 저장된 자격 증명을 새로 만들 수 있습니다.
   - **ID 관리 시스템 사용**

     이 관리되는 장치에 사용할 ID 관리 시스템을 선택합니다. 그런 다음 관리되는 서버의 IP 주소 또는 호스트 이름, 사용자 이름 및 원하는 경우 응용 프로그램 ID, 보관함, 폴더를 포함한 나머지 필드를 입력합니다.

     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.

   감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우, 관리에 실패하거나 성공하더라도 장치의 기타 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).

   일반 및 저장된 자격 증명에 대한 자세한 정보는 사용자 계정 관리 및 저장된 자격 증명 관리의 내용을 참조하십시오.
8. 관리되는 인증을 선택하는 경우 복구 암호를 지정하십시오.

   암호가 지정되면 복구 계정(RECOVERY_ID)이 서버에 생성되고 모든 로컬 사용자 계정이 사용 안 함으로 설정됩니다. XClarity Administrator에 문제가 있고 어떤 이유에서 작동이 중지되면 일반 사용자 계정을 사용하여 관리 컨트롤러에 로그인할 수 *없습니다*. 그러나 복구 계정을 사용하여 로그인할 수 있습니다.

   참고:
   - 관리되는 인증을 사용하도록 선택한 경우 복구 암호는 선택 사항이며 로컬 인증을 사용하도록 선택한 경우에는 복구 암호가 허용되지 않습니다.
   - 로컬 복구 계정 또는 저장된 복구 자격 증명을 사용하도록 선택할 수 있습니다. 두 경우 모두 사용자 이름은 항상 RECOVERY_ID입니다.
   - 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.

   복구 ID에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.
9. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

참고:

- 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
- 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

10. **관리**를 클릭하십시오.

    이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 진행상황을 모니터링하십시오.

11. 프로세스가 완료되면 **확인**을 클릭하십시오.

    장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

    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.

- IP 주소를 수동으로 지정하여 XClarity Administrator와 동일한 IP 서브넷에 있지 않은 랙 및 타워 서버를 검색하고 관리합니다.

  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.

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

     참고: 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.

     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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.
  3. **수동 입력**을 선택하십시오.
  4. 관리할 서버의 네트워크 주소를 지정하십시오.
     - **단일 시스템**을 클릭하고 단일 IP 주소 도메인 이름 또는 완전한 도메인 이름(FQDN)을 입력하십시오.

       참고: FQDN을 지정하려면 네트워크 액세스 페이지에 올바른 도메인 이름이 지정되어 있어야 합니다(네트워크 액세스 구성 참조).

- **다중 시스템**을 클릭하고 IP 주소의 범위를 입력하십시오. 다른 범위를 추가하려면 **추가** 아이콘(➕)을 클릭하십시오. 범위를 제거하려면 **제거** 아이콘(✖)을 클릭하십시오.

5. **확인**을 누르십시오. 관리 대화 상자가 표시됩니다.
6. 이 장치에 대해 XClarity Administrator 관리되는 인증 또는 로컬 인증을 사용하도록 선택하십시오. 기본적으로 관리되는 인증이 선택됩니다. 로컬 인증을 사용하려면 **관리되는 인증**을 선택 취소하십시오.
7. 장치에 인증을 위해 사용할 자격 증명 유형을 선택하고 적절한 자격 증명을 지정하십시오.
   - **수동으로 입력된 자격 증명 사용**
     - 서버에 인증하기 위한 사용자 ID와 암호를 지정하십시오.
     - (옵션) 장치에서 암호가 현재 만료된 경우 지정된 사용자 이름에 대한 새 암호를 설정하십시오.

     참고: 수동으로 입력한 자격 증명을 사용하려면 XClarity Administrator 관리되는 인증을 선택해야 합니다.
   - **저장된 자격 증명 사용**

     이 관리되는 장치에 사용할 저장된 자격 증명을 선택하십시오. **새로 만들기**를 클릭하여 저장된 자격 증명을 새로 만들 수 있습니다.
   - **ID 관리 시스템 사용**

     이 관리되는 장치에 사용할 ID 관리 시스템을 선택합니다. 그런 다음 관리되는 서버의 IP 주소 또는 호스트 이름, 사용자 이름 및 원하는 경우 응용 프로그램 ID, 보관함, 폴더를 포함한 나머지 필드를 입력합니다.

     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.

   감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우, 관리에 실패하거나 성공하더라도 장치의 기타 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).

   일반 및 저장된 자격 증명에 대한 자세한 정보는 사용자 계정 관리 및 저장된 자격 증명 관리의 내용을 참조하십시오.
8. 관리되는 인증을 선택하는 경우 복구 암호를 지정하십시오.

   암호가 지정되면 복구 계정(RECOVERY_ID)이 서버에 생성되고 모든 로컬 사용자 계정이 사용 안 함으로 설정됩니다. XClarity Administrator에 문제가 있고 어떤 이유에서 작동이 중지되면 일반 사용자 계정을 사용하여 관리 컨트롤러에 로그인할 수 *없습니다*. 그러나 복구 계정을 사용하여 로그인할 수 있습니다.

   참고:
   - 관리되는 인증을 사용하도록 선택한 경우 복구 암호는 선택 사항이며 로컬 인증을 사용하도록 선택한 경우에는 복구 암호가 허용되지 않습니다.
   - 로컬 복구 계정 또는 저장된 복구 자격 증명을 사용하도록 선택할 수 있습니다. 두 경우 모두 사용자 이름은 항상 RECOVERY_ID입니다.
   - 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.

복구 ID에 대한 자세한 정보는 인증 서버 관리의 내용을 참조하십시오.

9. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

   참고:

   - 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
   - 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

10. **관리**를 클릭하십시오.

    이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 진행상황을 모니터링하십시오.

11. 프로세스가 완료되면 **확인**을 클릭하십시오.

    장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

    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.

완료한 후에

- 추가 장치를 검색 및 관리하십시오.
- 서버 패턴을 작성하고 배포하여 시스템 정보, 로컬 스토리지, I/O 어댑터, 부팅 항목 및 펌웨어 설정을 구성하십시오(구성 패턴을 사용하여 서버 구성 참조).
- 설치된 운영 체제가 없는 서버에 운영 체제 이미지를 배포하십시오(베어메탈 서버에 운영 체제 설치 참조).
- 현재 정책을 준수하지 않는 장치에서 펌웨어를 업데이트하십시오(관리 장치에서 펌웨어 업데이트 참조).
- 물리적 환경을 반영하도록 장치를 적합한 랙에 추가하십시오(랙 관리 참조).
- 하드웨어 상태 및 세부 정보를 모니터링하십시오(관리 서버의 상태 보기 참조).
- 이벤트 및 경고를 모니터링하십시오(이벤트 작업 및 경고 작업 참조).
- XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하고 서버를 선택한 다음 **모든 작업 → 보안 → SEL 로그 지우기**를 클릭하여 서버의 SEL 로그를 지웁니다.이 작업은 ThinkSystem 및 ThinkAgile 서버에만 지원됩니다.
- 만료되었거나 유효하지 않은 저장된 자격 증명을 해결하십시오(저장된 자격 증명 관리 참조).
- XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하고 **활성 세션**을 클릭한 다음 SSO(Single sign-on)를 사용 또는 사용 중지하여 모든 관리되는 ThinkSystem 및 ThinkAgile 서버에 SSO(Single sign-on)를 사용 또는 사용 중지합니다.
- 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.

관리 서버의 상태 보기

Lenovo XClarity Administrator에서 관리되는 서버 및 설치된 구성 요소의 요약 및 세부 상태를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

이 작업 정보

다음 상태 아이콘은 장치의 전반적인 상태를 나타내는 데 사용됩니다. 인증서가 일치하지 않으면 적용 가능한 각 장치의 상태에 "(신뢰할 수 없음)"이 추가됩니다. 예를 들어 경고(신뢰할 수 없음)이 표시됩니다. 연결 문제가 있거나 장치에 대한 연결을 신뢰할 수 없는 경우 적용 가능한 각 장치의 상태에 "(연결)"이 추가됩니다. 예를 들어 경고(연결)이 표시됩니다.

- ( ) 위험
- ( ) 경고
- ( ) 보류 중
- ( ) 정보
- ( ) 정상
- ( ) 오프라인
- ( ) 알 수 없음

장치의 전원 상태는 다음 중 하나입니다.

- 켜짐
- 꺼짐
- 시스템 종료
- 대기
- 최대 절전
- 알 수 없음

절차

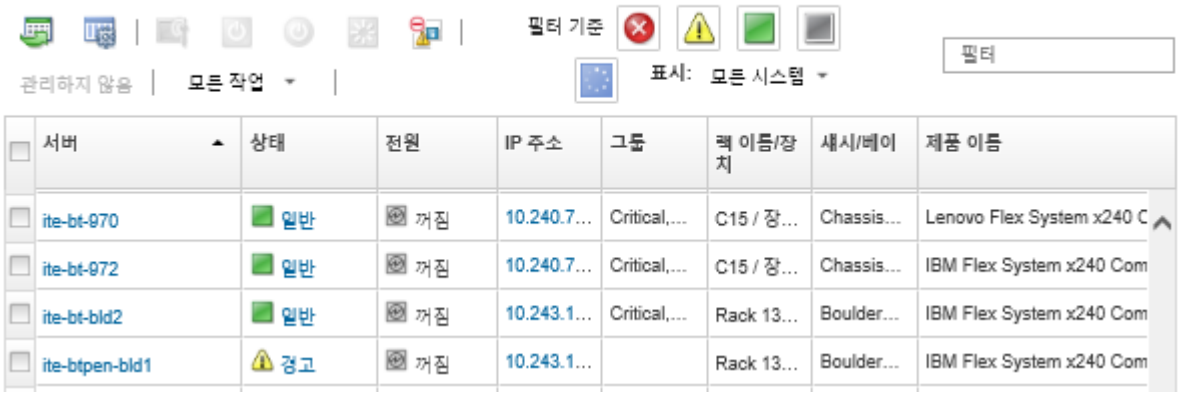
관리되는 서버의 상태를 보려면 다음 작업 중 하나 이상을 완료하십시오.

- XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 대시보드 페이지에는 모든 관리 장치 및 기타 리소스에 대한 개요와 상태가 표시됩니다.

- XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지가 모든 관리되는 서버(랙 및 타워 서버, 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

  특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭 다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하고 선택한 기준을 충족하는 서버만 나열하도록 상태 아이콘을 클릭하십시오.

  서버

  이 페이지에서 다음 작업을 수행할 수 있습니다.

  - 서버 및 그 구성 요소에 대한 자세한 정보를 보십시오(관리 서버의 세부 정보 보기 참조).
  - **모든 작업 → 보기 → 랙 보기에 표시** 또는 **모든 작업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 서버를 봅니다.
  - IP 주소 링크를 클릭하여 서버의 관리 컨트롤러 웹 인터페이스를 실행합니다(서버에 대한 관리 컨트롤러 인터페이스 실행 참조).
  - 서버를 원격으로 관리합니다(원격 제어를 사용하여 Converged, Flex System, NeXtScale 및 System x 서버 관리 참조).
  - 서버 전원을 켜고 끕니다(서버 전원 켜기 및 끄기 참조).

- 서버를 선택하고 **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 시스템 정보를 수정합니다.
- 서버를 선택하고 **모든 작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 인벤토리를 새로 고칩니다.
- 서버를 선택하고 **모든 작업 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 하나 이상의 서버에 대한 자세한 정보를 단일 CSV 파일로 내보냅니다.

  참고: 한 번에 최대 60대의 장치에 대한 인벤토리 데이터를 내보낼 수 있습니다.

  팁: CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- 서버를 관리 해제합니다(랙 또는 타워 서버 관리 해제 참조).
- **모든 작업 → 서비스 → 로컬 스토리지를 기본값으로 재설정**을 클릭하여 로컬 스토리지 어댑터를 기본 제조 설정으로 재설정합니다.
- 서버를 선택하고 **모든 작업 → 서비스 → 위치 LED 상태 전환**을 클릭한 후 상태를 선택하고 **적용**을 클릭하여 서버의 위치 LED 상태를 켜짐, 꺼짐 또는 깜박임으로 변경합니다.
  - ThinkSystem SR635 및 SR655 서버의 위치 LED 전환은 지원되지 않습니다.
  - ThinkServer 서버의 위치 LED는 켜짐 또는 꺼짐일 수 있습니다. 깜박임은 지원되지 않습니다.
- 서버를 가상으로 재배치합니다(가상으로 Flex System 섀시에서 서버 재배치 참조).
- **이벤트 제외** 아이콘()을 클릭하여 이벤트가 표시되는 모든 페이지에서 관심이 없는 이벤트를 제외합니다(이벤트 제외 참조).
- **모든 작업 → 서비스 → NMI 트리거**를 클릭하여 NMI(non-maskable interrupt)를 통해 서버를 다시 시작합니다.
- 서버를 선택하고 **모든 작업 → 보안 → Encapsulation 사용** 또는 **모든 작업 → 보안 → Encapsulation 사용 안 함**을 클릭하여 수신 요청을 XClarity Administrator로만 제한하는 서버의 방화벽 규칙 변경을 사용 또는 사용 안 함으로 설정합니다.글로벌 encapsulation 설정은 기본적으로 사용하지 않습니다. 사용하지 않는 경우 장치 encapsulation 모드를 "일반"으로 설정하고 방화 벽 규칙은 관리 프로세스의 일부로 변경되지 않습니다.

  글로벌 encapsulation 설정을 사용하고 장치가 encapsulation을 지원하는 경우 XClarity Administrator는 관리 프로세스 중에 장치와 통신하여 장치 encapsulation 모드를 "encapsulationLite"로 변경하고 장치의 방화벽 규칙을 변경하여 수신 요청을 XClarity Administrator로만 제한합니다.

  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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.
- (Converged, Flex System, NeXtScale 및 System x 및 ThinkSystem 서버만 해당) 서버를 선택하고 **모든 작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 XClarity Administrator 보안 인증서와 서버 베이스보드 관리 컨트롤러의 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).
- 그룹의 장치에 대해 만료되었거나 유효하지 않은 저장된 자격 증명을 해결하십시오(서버에 대해 만료되었거나 유효하지 않은 저장된 자격 증명 해결 참조).
- **모든 작업 → 그룹 → 그룹에 추가** 또는 **모든 작업 → 그룹 → 그룹에서 제거**를 클릭하여 정적 리소스 그룹에서 서버를 추가하거나 제거합니다.

관리 서버의 세부 정보 보기

Lenovo XClarity Administrator에서 펌웨어 수준, 서버 이름 및 UUID(범용 고유 식별자)를 비롯한 관리되는 서버에 대한 자세한 정보를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

이 작업 정보

CPU 사용은 집계된 C 상태 상주에 대한 측정치입니다. 이는 초당 사용량과 초당 최대 C0 상주량의 백분율로 측정됩니다.

메모리 사용은 집계된 모든 메모리 채널의 읽기/쓰기 볼륨의 측정치입니다. 이는 초당 사용량과 초당 사용 가능한 최대 메모리 대역폭의 백분율로 측정됩니다.

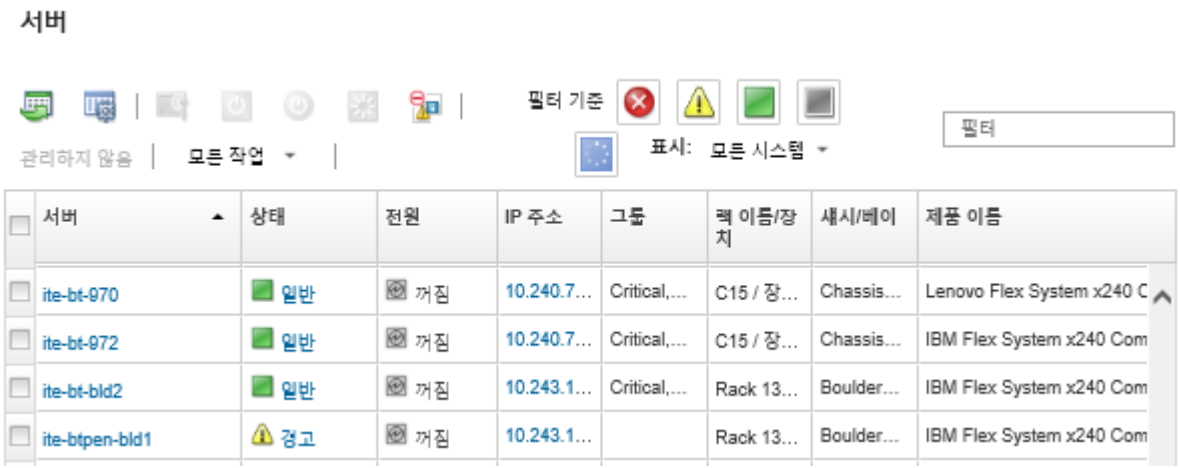
시스템 수준 공기 온도는 서버 앞면의 물리적 센서로 측정됩니다. 이 온도는 서버의 흡입구 공기 온도를 나타냅니다. 온도가 다른 시점에서 측정되면 XClarity Administrator와 CMM에서 보고되는 공기 온도가 다를 수 있음을 주의하십시오.

절차

관리되는 서버에 대한 세부 정보를 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지는 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 모든 **시스템** 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.



단계 2. **서버** 열에서 서버 링크를 클릭하십시오. 해당 서버의 상태 요약 페이지가 표시되며, 여기에는 해당 서버에 설치된 구성 요소 목록과 서버 속성이 표시됩니다.

참고: System x 및 NeXtScale 서버의 경우 LAN over USB 주소가 이 페이지에 나열됩니다. 그러나 XClarity Administrator에서 해당 주소를 변경할 수는 없습니다. 대신 서버의 베이스보드 관리 컨트롤러 인터페이스를 사용해야 합니다. 자세한 정보는 서버의 제품 설명서에서 "LAN over USB 인터페이스를 사용하여 IMM2 액세스"를 참조하십시오. BladeCenter 온라인 설명서에 서버의 제품 설명서가 있습니다.

단계 3. 다음 작업 중 하나 이상을 완료합니다.

- **요약**을 클릭하여 시스템 정보 및 설치된 구성 요소 등의 서버 요약 정보를 확인합니다(관리 서버의 상태 보기 참조).

- **인벤토리 세부 정보**를 클릭하여 다음과 같은 서버 구성 요소에 대한 세부 정보를 확인합니다.
  - 서버 및 관리 컨트롤러의 펌웨어 수준.
  - 관리 모듈 네트워크 세부 정보(예, 호스트 이름, IPv4 주소, IPv6 주소 및 MAC 주소).
  - 자산 세부 정보(예, 서버 이름, UUID(범용 고유 식별자) 및 위치).
  - 구성 요소 세부 정보(예, CPU, 메모리, 드라이브 및 확장 카드).

  참고:

  - 서버의 모든 IP 주소가 목록에 있습니다. 관리 컨트롤러 포트의 IP 주소가 목록 첫 번째에 있습니다. 관리 컨트롤러의 IP 주소가 사용 가능하다면, 이는 서버에 연결하는 데 사용됩니다.
  - 특정 어댑터에 데이터를 사용할 수 없는 경우 어댑터의 일부 필드(예, 제품 이름)가 비어 있을 수 있습니다.
  - 새 어댑터가 서버에 설치된 경우 인벤토리에서 어댑터를 표시하려면 이 서버를 다시 부팅해야 합니다.
  - 일부 추가 기능 카드의 경우 FoD(Feature on Demand) 정보가 장치 이름 아래에 표시됩니다.
  - 유형 열의 링크 위에 마우스를 올리면 Intel Optain DCPMM 메모리와 같은 특정 구성 요소에 대한 자세한 정보를 얻을 수 있습니다.
- **경고**를 클릭하여 이 서버의 현재 경고 목록을 표시합니다(경고 작업 참조).

  참고: ThinkSystem 또는 ThinkServer 서버의 SSD 수명과 같은 특정 값이 경고 또는 위험 수준을 초과할 때 경고와 이벤트를 발생시키는 임계값을 설정할 수 있습니다(경고 및 이벤트 생성을 위한 임계값 기본 설정 지정 참조).
- **이벤트 로그**를 클릭하여 이 서버의 이벤트 목록을 표시합니다(이벤트 로그에서 이벤트 모니터링 참조).
- **작업**을 클릭하여 이 서버와 연결된 작업 목록을 표시합니다(작업 모니터링 참조).
- Light Path를 클릭하여 서버 LED의 현재 상태(예, 위치, 장애 및 정보)를 표시합니다. 이는 서버의 앞면 패널을 보는 것과 동일합니다.
- **전원 및 열**을 클릭하여 전원 사용 및 공기 온도에 대한 세부 정보를 표시합니다.

  팁: 최신 전원 및 열 데이터를 수집하려면 웹 브라우저의 새로 고침 버튼을 사용하십시오. 데이터를 수집하려면 몇 분 정도가 걸릴 수 있습니다.
- 서버의 현재 구성 정보(로컬 스토리지, I/O 어댑터, SAN 부팅 설정, 펌웨어 설정 포함)와 구성 요소 및 할당된 구성 패턴을 보려면 **구성**을 클릭하십시오(구성 패턴을 사용하여 서버 구성 참조).
- Feature on Demand 키를 클릭하여 관리되는 서버에 현재 설치된 Feature on Demand 키 목록을 확인합니다(Features on Demand 키 보기 참조).

완료한 후에

서버에 대한 요약 및 자세한 정보를 표시하는 것 외에도 다음 작업을 수행할 수 있습니다.

- 요약 페이지에서 랙 또는 섀시 이름을 클릭하여 서버와 연결된 랙 또는 섀시를 봅니다.
- **모든 작업 → 보기 → 랙 보기에 표시** 또는 **모든 작업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 선택한 서버를 봅니다.
- **IP 주소** 링크를 클릭하여 선택한 서버의 관리 컨트롤러 웹 인터페이스를 실행합니다(서버에 대한 관리 컨트롤러 인터페이스 실행 참조).
- 서버에 원격으로 액세스합니다(원격 제어를 사용하여 Converged, Flex System, NeXtScale 및 System x 서버 관리 참조).
- 선택한 서버의 전원을 켜고 끕니다(서버 전원 켜기 및 끄기 참조).
- **속성 편집**을 클릭하여 선택한 서버의 시스템 정보를 수정합니다.

- **작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 선택한 서버의 인벤토리를 새로 고칩니다.
- **작업 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 서버에 대한 자세한 정보를 CSV 파일로 내보냅니다.

  참고:

  - CSV 파일의 인벤토리 데이터에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 GET /nodes/*<UUID_list>*의 내용을 참조하십시오.
  - CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- **작업 → 서비스 재설정 → 이벤트 제외**를 클릭하여 이벤트가 표시되는 모든 페이지에서 관심이 없는 이벤트를 제외합니다(이벤트 제외 참조).
- **작업 → 서비스 → NMI 트리거**를 클릭하여 NMI(non-maskable interrupt)를 통해 선택한 서버를 다시 시작합니다.
- **작업 → 서비스 → 위치 LED 상태 전환**을 클릭한 후 상태를 선택하고 **적용**을 클릭하여 선택한 서버의 위치 LED 상태를 켜짐, 꺼짐 또는 깜박임으로 변경합니다.

  참고:
  - ThinkSystem SR635 및 SR655 서버의 위치 LED 전환은 지원되지 않습니다.
  - ThinkServer 서버의 위치 LED는 켜짐 또는 꺼짐일 수 있습니다. 깜박임은 지원되지 않습니다.
- **모든 작업 → 보안 → SSO(Single sign-on) 사용** 또는 **모든 작업 → 보안 → SSO(Single sign-on) 사용 안 함**을 클릭하여 선택한 ThinkSystem 및 ThinkAgile 서버에 대해 SSO(Single sign-on)를 사용 중지하거나 사용합니다.

  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.

  참고: 인증에 CyberArk ID 관리 시스템을 사용하면 SSO(Single sign-on)가 자동으로 비활성화됩니다.
- **작업 → 보안 → Encapsulation 사용** 또는 **작업 → 보안 → Encapsulation 사용 안 함**을 클릭하여 수신 요청을 XClarity Administrator로만 제한하는 선택한 서버의 방화벽 규칙 변경을 사용하거나 사용 중지합니다. 글로벌 encapsulation 설정은 기본적으로 사용하지 않습니다. 사용하지 않는 경우 장치 encapsulation 모드를 "일반"으로 설정하고 방화 벽 규칙은 관리 프로세스의 일부로 변경되지 않습니다.

  글로벌 encapsulation 설정을 사용하고 장치가 encapsulation을 지원하는 경우 XClarity Administrator는 관리 프로세스 중에 장치와 통신하여 장치 encapsulation 모드를 "encapsulationLite"로 변경하고 장치의 방화벽 규칙을 변경하여 수신 요청을 XClarity Administrator로만 제한합니다.

  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 lenovoMgrAlert.mib 파일 및 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.
- (ThinkServer 이외의 서버만 해당) **작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 Lenovo XClarity Administrator 보안 인증서와 선택한 서버의 관리 컨트롤러 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).

서버 구성 데이터 백업 및 복원

Lenovo XClarity Administrator에는 서버 구성 데이터에 대한 기본 제공 백업 기능이 포함되어 있지 않습니다. 대신 관리되는 서버 사용할 수 있는 백업 기능을 사용하십시오.

- **Converged, Flex System, System x, ThinkSystem 및 NeXtScale 서버**
  - 서버 구성 데이터 백업

    관리 웹 인터페이스 또는 CLI를 사용하여 펌웨어를 백업하십시오.

    - IMM 웹 인터페이스에서 **IMM 관리 → IMM 구성**을 클릭하십시오.
    - CLI에서 `backup` 명령을 사용하십시오.

    IMM을 사용한 서버 백업에 대한 자세한 정보는 Integrated Management Module II 온라인 설명서의 내용을 참조하십시오.

    운영 체제에서 제공하는 도구를 사용하여 서버에서 실행되는 응용 프로그램을 백업하십시오. 자세한 정보는 운영 체제와 함께 제공된 설명서를 참조하십시오.

    Flex System 컴퓨팅 장치의 경우 컴퓨팅 노드에 설치된 옵션에 대한 설정을 백업해야 합니다. ASU(Advanced Settings Utility)를 사용하여 옵션 설정을 비롯한 모든 컴퓨팅 노드 설정을 백업할 수 있습니다. ASU에 대한 정보는 ASU(Advanced Settings Utility) 웹 사이트의 내용을 참조하십시오).
  - 서버 구성 데이터 복원

    관리 웹 인터페이스 또는 CLI를 사용하여 펌웨어를 복원하십시오. BMC를 통한 서버 복원에 대한 자세한 정보는 Integrated Management Module II 온라인 설명서의 내용을 참조하십시오.

    운영 시스템과 함께 제공되는 설명서와 서버에서 실행되는 모든 응용 프로그램을 사용하여 서버에 설치된 소프트웨어를 복원하십시오.

    - IMM 웹 인터페이스에서 **IMM 관리 → IMM 구성**을 클릭하십시오.
    - CLI에서 `restore` 명령을 사용하십시오.

  참고: 팁: PureFlex 및 Flex System 백업 및 복원 모범 사례 안내서에서 섀시 구성 요소의 백업 및 복원에 대한 추가 정보를 찾을 수 있습니다.
- **ThinkServer 서버**복원 절차는 각 ThinkServer 서버 유형에 따라 다릅니다. 장치 복원에 대한 정보는 서버와 함께 제공된 제품 설명서를 참조하십시오.

시스템 보호 사용

시스템 보호는 XCC2가 있는 ThinkSystem 서버의 하드웨어 인벤토리 편차를 모니터링합니다.

이 작업 정보

모니터링되는 인벤토리에는 프로세서, 메모리, PCI 어댑터, 드라이브, 시스템 보드 및 라이저가 포함됩니다. 펌웨어 수준 및 구성 설정의 변경은 감지되지 않습니다.

시스템 보호가 사용으로 설정되면 하드웨어 인벤토리의 스냅샷이 선택한 각 장치의 신뢰할 수 있는 참조로 사용됩니다. 장치가 재부팅되면 장치의 베이스보드 관리 컨트롤러가 현재 시스템 구성을 수집하고 이를 스냅샷과 비교합니다. 하나 이상의 구성 요소에서 편차가 감지되면 시스템 보호가 이벤트를 발생시킵니다. 프로세서나 메모리에서 편차가 감지될 경우에는 시스템 보호가 이벤트를 발생시키고 선택적으로 서버가 OS로 부팅되지 않도록 합니다.

절차

하나 이상의 XCC2가 있는 서버에서 시스템 보호를 사용으로 설정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴에서 **하드웨어 → 서버**를 클릭하십시오. 모든 관리되는 서버의 표 형식 보기와 함께 서버 페이지가 표시됩니다.

단계 2. 하나 이상의 XCC2가 있는 서버를 선택합니다.

단계 3. **모든 작업 → 보안 → 시스템 보호 사용**을 클릭하여 시스템 보호 사용 대화 상자를 표시합니다.

단계 4. 시스템 보호가 사용 설정되어 있고 인벤토리 변경이 감지되며 서버가 호환되지 않음 상태인 경우에 수행할 작업을 선택하십시오.

- **사용, 시스템 기본 동작 유지**. 현재 동작이 사용됩니다. . 기본 동작은 이벤트를 생성하는 것입니다.
- **사용, 비호환 시 OS 부팅 방지**. 이벤트가 발생됩니다. OS로 부팅하려고 하는 경우 시스템 보호가 프로세서나 메모리에 대한 구성 변경을 감지하면 경고가 표시됩니다. 이 경우 예상치 못한 변경이면 베이스보드 관리 컨트롤러에 로그인하라는 메시지가 표시됩니다. 그렇지 않으면 부팅 또는 종료 프로세스를 계속할 수 있습니다. 5분 이내에 응답하지 않으면 기본적으로 서버가 종료됩니다.
- **사용, 비호환 시 이벤트 생성**. 이벤트가 발생되지만 다른 작업은 수행되지 않습니다.

단계 5. **적용**을 클릭하십시오.

선택한 서버의 인벤토리 스냅샷을 생성하는 작업이 생성됩니다. 작업 로그에서 작업 진행상태를 모니터링할 수 있습니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오. 작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

완료한 후에

선택한 서버에서 시스템 보호를 사용 안 함으로 설정하려면 **모든 작업 → 보안 → 시스템 보호 사용 안 함**을 클릭한 다음 **적용**을 클릭합니다.

드라이브 데이터 안전하게 지우기

Lenovo XClarity Administrator은(는) 22B 이후 버전을 실행하는 일부 ThinkSystem 및 ThinkAgile 서버의 모든 드라이브에서 데이터를 안전하게 지울 수 있습니다. 이 작업은 전체 드라이브를 이진수 0, 이진수 1 또는 임의 데이터로 채워 각 드라이브를 영구적으로 다시 작성함으로써 드라이브에 저장되었던 데이터를 찾기 어렵게 합니다.

주의:

- 이 작업은 드라이브의 모든 데이터를 *영구적으로* 지우며 *되돌릴 수 없습니다*.
- 작업이 제출된 후에는 이 작업을 취소할 수 없습니다.

시작하기 전에

드라이브 데이터를 지우려면 lxc-supervisor 권한이 있어야 합니다.

삭제할 관리되는 서버에 설정된 UEFI 관리자 암호가 없어야 합니다. 어떤 서버에든 UEFI 관리자 암호가 설정되어 있으면 해당 서버의 드라이브는 지워지지 않습니다.

기본적으로 한 번에 최대 3개 서버에서 드라이브 데이터를 안전하게 지울 수 있습니다. **관리 → 인벤토리 기본 설정**을 클릭하고 **일괄적으로 삭제할 수 있는 최대 서버 수**를 원하는 값으로 설정하여 한 번에 허용되는 서버 수를 구성할 수 있습니다. 3 - 100개의 서버를 선택할 수 있습니다.

한 번에 하나의 보안 지우기 작업만 허용됩니다. 다른 보안 지우기 작업을 시작하려면 현재 작업이 완료될 때까지 기다려야 합니다.

용량이 매우 큰 드라이브는 지우는 데 몇 시간이 걸릴 수도 있습니다.

Marvell RAID 컨트롤러에 연결된 SATA SDD 볼륨은 안전하게 지울 수 없습니다. 대신 다음 권장 사항을 고려하십시오.

- 7mm SATA SSD의 경우 Broadcom RAID 컨트롤러에 연결하여 보안 지우기를 수행하십시오.
- M.2 SATA SSD의 경우 Marvell 비RAID 컨트롤러(예: ThinkSystem M.2 SATA/NVMe 2베이 사용 키트)에 연결하여 보안 지우기를 수행하십시오.

이 작업 정보

다음 드라이브의 데이터를 지울 수 있습니다.
- NVMe
- SAS
- SAS HBA
- SAS RAID
- SATA
- 외부 연결 스토리지 장치
  - Lenovo Storage D1212(MT 4587)
  - Lenovo Storage D1224(MT 4587)
  - Lenovo Storage D3284(MT 6413)

보안 지우기 작업은 감사 로그에 항목을 생성합니다. 이벤트 전달 기능을 사용하여 이 이벤트를 전달할 수 있습니다(syslog, 원격 SNMP 관리자, 이메일 또는 기타 이벤트 서비스에 이벤트 전달 참조).

보안 지우기 문제를 해결하려면 멈춘 드라이브의 드라이브 데이터를 안전하게 지울 수 없음 및 Marvel RAID에 연결된 경우 SATA SDD 볼륨을 안전하게 지울 수 없음의 내용을 참조하십시오.

절차

특정 관리되는 서버의 모든 드라이브를 안전하게 지우려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴에서 **하드웨어 → 서버**를 클릭하십시오. 모든 관리되는 서버의 표 형식 보기와 함께 서버 페이지가 표시됩니다.

단계 2. 서버를 선택하십시오.

단계 3. **모든 작업 → 서비스 → 드라이브 보안 지우기**(HDD/SDD)를 클릭합니다.

단계 4. 감독자 암호를 입력하여 선택한 서버의 모든 드라이브를 지울 것임을 확인하십시오.

단계 5. **지우기**를 클릭합니다.

3개가 넘는 서버에서 대량 드라이브 지우기를 수행하는 경우 사용자 ID와 암호를 입력하라는 메시지가 표시됩니다. XClarity Administrator에 로그인할 때 사용한 것과 동일한 사용자 자격 증명을 입력합니다.

이 작업을 수행하기 위한 작업이 생성됩니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하여 작업 페이지의 진행 상태를 모니터링할 수 있습니다. 작업이 성공적으로 완료되지 않은 경우에는 작업 링크를 클릭하여 작업에 대한 세부 정보를 볼 수 있습니다(작업 모니터링 참고).

원격 제어 사용

Lenovo XClarity Administrator 웹 인터페이스에서 로컬 콘솔에 있는 것처럼 관리되는 서버에 대한 원격 제어 세션을 열 수 있습니다. 원격 제어 세션을 사용하여 서버 전원 켜기 또는 끄기 및 논리적으로 로컬 또는 원격 드라이브 탑재와 같은 작업을 수행할 수 있습니다.

모든 장치에 대한 원격 제어 세션을 시작하려면 lxc-supervisor, lxc-admin, lxc-security-admin, lxc-fw-admin, lxc-os-admin, lxc-hw-admin, lxc-service-admin 또는 lxc-hw-manager 권한이 있어야 합니다.

원격 제어를 사용하여 ThinkSystem 또는 ThinkAgile 서버 관리

Lenovo XClarity Administrator 웹 인터페이스에서 로컬 콘솔에 있는 것처럼 관리되는 ThinkSystem 또는 ThinkAgile 서버에 대한 원격 제어 세션을 열 수 있습니다. 원격 제어 세션을 사용하여 전원 작업을 수행하고 로컬 또는 원격 드라이브를 논리적으로 탑재할 수 있습니다.

시작하기 전에

Encapsulation은 서버에서 사용 안 함으로 설정되어야 합니다.

서버에 대한 원격 제어 세션을 열려면 서버가 온라인 또는 일반 상태여야 합니다. 서버의 액세스 상태가 다른 경우 원격 제어 세션을 서버에 연결할 수 없습니다. 서버 상태 보기에 대한 자세한 정보는 관리 서버의 세부 정보 보기의 내용을 참조하십시오.

ThinkSystem SR635 및 SR655 서버에 대한 다음 고려 사항을 검토하십시오.
- 베이스보드 관리 컨트롤러 펌웨어 v2.94 이상이 필요합니다.
- 다중 사용자 모드만 지원됩니다. 단일 사용자 모드는 지원되지 않습니다.
- Internet Explorer 11은 지원되지 않습니다.
- 원격 제어 세션에서 서버의 전원을 켜거나 끌 수 없습니다.

이 작업 정보

XClarity Administrator에서 단일 ThinkSystem 또는 ThinkAgile 서버에 대한 원격 제어 세션을 실행할 수 있습니다.

원격 콘솔 및 미디어 기능 사용에 대한 자세한 정보는 ThinkSystem 또는 ThinkAgile 서버 설명서를 참조하십시오.

참고: ThinkSystem 및 ThinkAgile 서버의 경우 Java WebStart를 지원하는 JRE(Java Runtime Environment)가 필요하지 않습니다.

절차

특정 서버에 대한 원격 제어 세션을 열려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지가 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.

단계 2. 원격 제어 세션을 열려는 서버를 선택하십시오.

단계 3. **원격 제어** 아이콘()을 클릭하십시오.

단계 4. 웹 브라우저에서 보안 경고를 승인하십시오.

완료한 후에

원격 제어 세션이 제대로 열리지 않는 경우 XClarity Administrator 온라인 설명서에서 원격 제어 문제의 내용을 참조하십시오.

원격 제어를 사용하여 ThinkServer 및 NeXtScale sd350 M5 서버 관리

Lenovo XClarity Administrator 웹 인터페이스에서 로컬 콘솔에 있는 것처럼 관리되는 ThinkServer 및 NeXtScale sd350 M5 서버에 대한 원격 제어 세션을 열 수 있습니다. 원격 제어 세션을 사용하여 전원 및 재설정 작업을 수행하고, 서버에 로컬 또는 네트워크 드라이브를 논리적으로 탑재하고, 스크린 샷을 캡처하고, 비디오를 기록할 수 있습니다.

시작하기 전에

- 이러한 서버의 원격 제어를 이용하려면 Java WebStart를 지원하는 JRE(Java Runtime Environment)가 클라이언트 측에 설치되어 있어야 합니다. 오픈 소스 JDK의 사용이 권장됩니다. 공급업체의 JRE 또는 JDK를 사용하는 경우 상업적 사용에 적합한 라이센스가 있어야 합니다. 다음 JRE가 지원됩니다.
  - Oracle JRE 7(Oracle Java 다운로드 웹 사이트 참조)

    주의:
    - Java 7의 경우 TLSv1.2 이상을 지원해야 합니다(관리 서버의 암호화 설정 구성 참고).
    - Java 7에 대한 지원은 향후 중단됩니다.
  - Oracle JRE 8, 유료 라이센스 필요(Oracle Java 다운로드 웹 사이트 참조)
  - IcedTea-Web v1.8 플러그인이 있는 Adoptium OpenJDK 8(Adoptium OpenJDK 웹 사이트 참고)
  - Amazon Corretto 8(Amazon Corretto 8 다운로드 웹 사이트 참고)

  Java WebStart는 OpenJDK 또는 Coretto 설치 패키지에 포함되지 않으며 별도로 설치해야 합니다. IcedTea-Web 또는 OpenWebStart는 GNU GPLV2 라이센스로 사용할 수 있습니다(IcedTea-OpenJDK 다운로드 웹 사이트 및 OpenWebStart 웹 사이트 참고).
- 원격 제어를 사용하려면 ThinkServer 서버에 ThinkServer System Manager Premium Upgrade를 위한 Features on Demand 키가 설치되어 있어야 합니다. 서버에 설치되는 FoD 키에 대한 자세한 정보는 Features on Demand 키 보기 의 내용을 참조하십시오.

이 작업 정보

XClarity Administrator에서 단일 ThinkServer 서버에 대한 원격 제어 세션을 실행할 수 있습니다.

서버에 대한 원격 제어 세션을 열려면 서버가 온라인 또는 일반 상태여야 합니다. 서버의 액세스 상태가 다른 경우 원격 제어 세션을 서버에 연결할 수 없습니다. 서버 상태 보기에 대한 자세한 정보는 관리 서버의 세부 정보 보기의 내용을 참조하십시오.

ThinkServer 원격 콘솔 및 미디어 기능 사용에 대한 자세한 정보는 ThinkServer 서버 설명서를 참조하십시오.

절차

특정 서버에 대한 원격 제어 세션을 열려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지가 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.

단계 2. 원격 제어 세션을 열려는 서버를 선택하십시오.

단계 3. **원격 제어** 아이콘( )을 클릭하십시오.

단계 4. 웹 브라우저에서 보안 경고를 승인하십시오.

완료한 후에

원격 제어 세션이 제대로 열리지 않는 경우 XClarity Administrator 온라인 설명서에서 원격 제어 문제의 내용을 참조하십시오.

원격 제어를 사용하여 Converged, Flex System, NeXtScale 및 System x 서버 관리

Lenovo XClarity Administrator 웹 인터페이스에서 원격 제어 세션을 열어 로컬 콘솔에 있는 것처럼 Converged, Flex System, NeXtScale 및 System x 서버를 관리할 수 있습니다.

시작하기 전에

자세히 알아보기: XClarity Administrator: 원격 제어

- 이러한 서버의 원격 제어를 이용하려면 Java WebStart를 지원하는 JRE(Java Runtime Environment)가 클라이언트 측에 설치되어 있어야 합니다. 오픈 소스 JDK의 사용이 권장됩니다. 공급업체의 JRE 또는 JDK를 사용하는 경우 상업적 사용에 적합한 라이센스가 있어야 합니다. 다음 JRE가 지원됩니다.
  - Oracle JRE 7(Oracle Java 다운로드 웹 사이트 참조)

    주의:
    - Java 7의 경우 TLSv1.2 이상을 지원해야 합니다(관리 서버의 암호화 설정 구성 참고).
    - Java 7에 대한 지원은 향후 중단됩니다.
  - Oracle JRE 8, 유료 라이센스 필요(Oracle Java 다운로드 웹 사이트 참조)
  - IcedTea-Web v1.8 플러그인이 있는 Adoptium OpenJDK 8(Adoptium OpenJDK 웹 사이트 참고)
  - Amazon Corretto 8(Amazon Corretto 8 다운로드 웹 사이트 참고)

  Java WebStart는 OpenJDK 또는 Coretto 설치 패키지에 포함되지 않으며 별도로 설치해야 합니다. IcedTea-Web 또는 OpenWebStart는 GNU GPLV2 라이센스로 사용할 수 있습니다(IcedTea-OpenJDK 다운로드 웹 사이트 및 OpenWebStart 웹 사이트 참고).
- 다음 운영 체제(32비트 또는64비트)를 실행 중인 서버에서 원격 제어 세션을 실행할 수 있습니다.
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- 원격 제어를 사용하려면 원격 관리를 위한 Features on Demand 키가 Converged, NeXtScale 및 System x 서버에 설치되어야 합니다. FoD 키가 서버에서 감지되지 않으면 사용 가능한 모든 서버 목록을 표시할 때 원격 제어 세션에서 해당 서버에 대해 활성화 키 누락 메시지를 표시합니다. 원격지 상태가 서버 페이지에서 사용 가능, 사용 불가능 또는 서버에 설치되어 있지 않은지 여부를 판단할 수 있습니다(관리 서버의 상태 보기 참조). 서버에 설치된 FoD 키에 대한 자세한 정보는 Features on Demand 키 보기의 내용을 참조하십시오.
- 원격 제어 세션을 시작하는 데 사용되는 사용자 계정은 XClarity Administrator 인증 서버에 정의된 올바른 사용자 계정이어야 합니다. 또한 사용자 계정은 서버를 관리하고 서버에 액세스하는 데 충분한 사용자 권한을 가지고 있어야 합니다.
- 원격 제어 세션을 열기 전에 보안, 성능 및 키보드 고려사항을 검토하십시오. 이러한 고려사항에 대한 자세한 정보는 원격 제어 고려사항의 내용을 참조하십시오.
- 원격 제어 대화 상자는 로케일을 사용하여 로컬 시스템의 운영 체제에 대해 정의되는 언어 설정을 표시합니다.Windows에서 로컬 시스템을 실행하는 경우 로케일 설정 변경 방법에 대한 정보는 Java 웹 사이트의 내용을 참조하십시오. 표시 언어를 변경하려면 Windows 자국어 버전 사본을 설치하거나 Windows 웹 사이트에서 언어 팩을 설치하십시오.

이 작업 정보

Lenovo XClarity Administrator에서 여러 원격 제어 세션을 시작할 수 있습니다. 각 세션에서는 여러 서버를 관리할 수 있습니다.

서버에 대한 원격 제어 세션을 열려면 서버가 온라인 또는 일반 상태여야 합니다. 서버의 액세스 상태가 다른 경우 원격 제어 세션을 서버에 연결할 수 없습니다. 서버 상태 보기에 대한 자세한 정보는 관리 서버의 세부 정보 보기의 내용을 참조하십시오.

Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 원격 제어**를 클릭하여 대상이 지정되지 않은 원격 제어 세션을 열 수 있습니다. 그런 다음 웹 브라우저에서 보안 경고를 승인하십시오.

참고: Flex System x280, x480 및 x880 컴퓨팅 노드의 경우 기본 노드에 대해서만 원격 제어 세션을 시작할 수 있습니다. 다중 노드 시스템의 비기본 노드에 대해 원격 제어 세션을 시작하는 경우 원격 제어 대화 상자는 시작되지만 비디오가 표시되지 않습니다.

절차

특정 Converged, Flex System, NeXtScale 및 System x 서버에 대한 원격 제어 세션을 열려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지가 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.

단계 2. 원격 제어 세션을 열려는 서버를 선택하십시오.

단계 3. **원격 제어** 아이콘()을 클릭하십시오.

단계 4. 웹 브라우저에서 보안 경고를 승인하십시오.

단계 5. 선택적으로 원격 제어 아이콘을 데스크탑에 저장하도록 선택하십시오. 이 아이콘을 사용하여 XClarity Administrator 웹 인터페이스에 로그인하지 않고 원격 제어 세션을 실행할 수 있습니다.

단계 6. 프롬프트가 표시되면 다음 연결 모드 중 하나를 선택하십시오.

- **단일 사용자 모드**. 서버에서 독점 원격 제어 세션을 구축합니다. 서버에서 연결을 끊기 전에는 해당 서버에 대한 다른 모든 원격 제어 세션이 차단됩니다. 서버에 다른 원격 제어 세션이 구축되지 않은 경우에만 이 옵션이 사용 가능합니다.
- **다중 사용자 모드**. 동일한 서버에 여러 원격 제어 세션을 구축할 수 있습니다. XClarity Administrator에서는 단일 서버에 최대 6개까지의 동시 원격 제어 세션을 지원합니다.

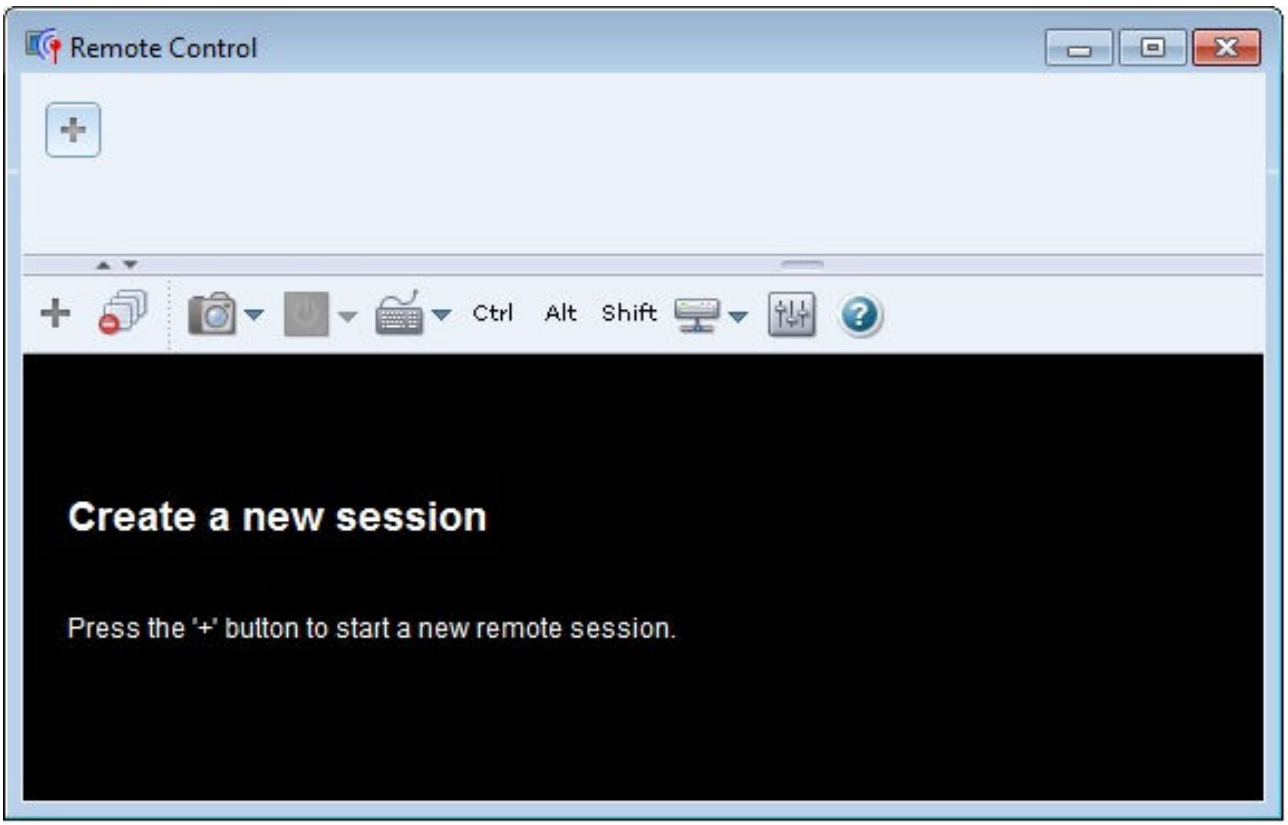
단계 7. 프롬프트가 표시되면 로컬 시스템에 원격 제어 세션에 대한 단축키를 저장할지 여부를 선택하십시오.

단축키를 저장하면 XClarity Administrator 웹 인터페이스에서 실행하지 않고도 이 단축키를 사용하여 특정 서버에 대한 원격 제어 세션을 열 수 있습니다. 그러나 XClarity Administrator 인증 서버를 사용하여 사용자 계정을 유효성 검증하려면 로컬 시스템에 XClarity Administrator에 대한 액세스 권한이 있어야 합니다.

단축키에는 서버를 수동으로 추가할 수 있는 비어 있는 원격 제어 세션을 여는 링크가 포함되어 있습니다.

결과

원격 제어 창이 표시됩니다.



축소판 영역에는 현재 원격 제어 세션을 통해 관리되는 모든 서버 세션의 축소판이 표시됩니다.

비디오 세션 영역에서 서버 콘솔을 표시하는 축소판을 클릭하여 여러 서버 세션을 표시하고 서버 세션 간을 이동할 수 있습니다. 축소판 영역에 맞는 것보다 더 많은 서버에 액세스하는 경우 추가 서버 축소판으로 화면 이동하려면 **오른쪽으로 화면 이동** 아이콘( )과 **왼쪽으로 화면 이동** 아이콘( )을 클릭하십시오. 모든 열린 서버 세션 목록을 보려면 **모든 세션** 아이콘( )을 클릭하십시오.

관리 중인 서버 목록에 새 서버를 추가하려면 축소판 영역에서 **서버 추가** 아이콘( )을 클릭하십시오. 서버 추가에 대한 자세한 정보는 원격 제어 세션에 서버 콘솔 추가의 내용을 참조하십시오. 축소판 영역이 표시되는지 여부와 축소판 페이지에서 축소판을 새로 고치는 빈도를 제어할 수 있습니다. 축소판 설정에 대한 자세한 정보는 원격 제어 기본 설정 지정의 내용을 참조하십시오.

완료한 후에

원격 제어 세션이 제대로 열리지 않는 경우 XClarity Administrator 온라인 설명서에서 원격 제어 문제의 내용을 참조하십시오.

원격 제어 대화 상자에서 다음 작업을 수행할 수 있습니다.

- 현재 원격 제어 세션에 다른 서버에 대한 세션을 추가합니다(원격 제어 세션에 서버 콘솔 추가 참조).
- **축소판 전환** 아이콘( )을 클릭하여 축소판 영역을 숨기거나 표시합니다.
- **화면** 아이콘( )을 클릭한 다음 **전체 화면 전환** 또는 **전체 화면 해제**를 클릭하여 원격 제어 세션을 창 또는 전체 화면으로 표시합니다.
- 원격 제어 세션에서 Ctrl, Alt 및 Shift 키를 사용합니다(Ctrl, Alt 및 Shift 키 사용 참조).
- 소프트키로 알려진 사용자 지정 키 시퀀스를 정의합니다(소프트 키 정의 참조).

- 현재 선택한 서버 세션를 화면 캡처하고, **화면** 아이콘()을 클릭한 후 **스크린샷**을 클릭하여 화면 캡처를 여러 형식으로 저장합니다.
- 선택한 서버에 원격 미디어(예, CD, DVD 또는 USB 장치, 디스크 이미지, 또는 CD(ISO) 이미지)를 탑재하거나 탑재한 장치를 다른 서버로 이동합니다(원격 미디어 마운팅 또는 이동 참조).
- 원격 미디어에서 서버로 이미지를 업로드합니다(서버에 이미지 업로드 참조).
- 원격 콘솔에서 서버 전원을 켜거나 끕니다(원격 제어 세션에서 서버 전원 켜기 및 끄기 참조).
- 원격 제어 기본 설정을 변경합니다(원격 제어 기본 설정 지정 참조).

원격 제어 고려사항

원격 제어 세션을 사용한 관리 서버 액세스와 관련된 보안, 성능 및 키보드 고려사항을 알고 있어야 합니다.

보안 고려사항

원격 제어 세션을 시작하는 데 사용되는 사용자 계정은 Lenovo XClarity Administrator 인증 서버에 정의된 올바른 사용자 계정이어야 합니다. 또한 사용자 계정은 서버를 관리하고 서버에 액세스하는 데 충분한 사용자 권한을 가지고 있어야 합니다.

기본적으로 서버에 다중 원격 제어 세션을 구축할 수 있습니다. 그러나 원격 제어 세션을 시작하는 경우 서버에 대한 독점 세션을 구축하는 단일 사용자 모드로 세션을 시작할 수 있는 옵션이 있습니다. 선택한 서버에서 연결을 끊기 전에는 해당 서버에 대한 다른 모든 원격 제어 세션이 차단됩니다.

참고: 현재 서버에 다른 원격 제어 세션이 구축되지 않은 경우에만 이 옵션이 사용 가능합니다.

FIPS(Federal Information Processing Standard) 140을 사용하려면 로컬 시스템에서 다음 단계를 완료하여 이를 수동으로 사용 설정해야 합니다.

1. 로컬 시스템에 설치되는 FIPS 140 인증 암호화 제공자의 제공자 이름을 찾으십시오.

   팁: FIPS 140 준수에 대한 자세한 정보는 SunJSSE용 FIPS 140 준수 모드 웹 사이트의 내용을 참조하십시오.
2. `$(java.home)/lib/security/java.security` 파일을 편집하십시오.
3. FIPS 140 인증 암호화 제공자의 제공자 이름을 추가하여 `com.sun.net.ssl.internal.ssl.Provider`가 포함된 행을 수정하십시오. 예를 들어 다음과 같이 변경하십시오.
   ```
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider
   ```
   다음으로 변경:
   ```
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS
   ```

성능 고려사항

원격 제어 세션이 느려지거나 응답이 없는 경우 선택한 서버에 대해 구축된 모든 비디오와 원격 미디어 세션을 닫아서 열린 서버 연결 수를 줄이십시오. 또한 다음 기본 설정을 변경하여 성능을 높일 수도 있습니다. 자세한 정보는 원격 제어 기본 설정 지정의 내용을 참조하십시오.

- KVM
  - 응용 프로그램에서 사용되는 비디오 대역폭 비율을 줄이십시오. 원격 제어 세션의 이미지 품질이 저하됩니다.
  - 응용 프로그램에서 새로 고치는 프레임 비율을 줄이십시오. 원격 제어 세션의 새로 고침 빈도가 줍니다.
- **축소판**
  - 축소판 새고 고침 간격 비율을 늘리십시오. 응용 프로그램이 더 느린 비율로 축소판을 새로 고칩니다.
  - 축소판 표시를 완전히 끄십시오.

원격 제어 세션 창의 크기와 활성 세션 수는 메모리 및 네트워크 대역폭과 같이 성능에 영향을 주는 워크스테이션 리소스에 영향을 미칠 수 있습니다. 원격 제어 세션은 32개의 열린 세션 소프트 한계를 사용합

니다. 32개보다 많은 세션이 열리면 성능이 심각하게 저하되고 원격 제어 세션이 응답하지 않을 수 있습니다. 네트워크 대역폭과 로컬 메모리 등의 리소스가 충분하지 않은 경우 32개보다 적은 세션이 열린 경우에도 성능 저하가 발생할 수 있습니다.

키보드 고려사항

원격 제어 세션은 다음 키보드 유형을 지원합니다.
- 벨기에어 105-키
- 브라질어
- 중국어
- 프랑스어 105-키
- 독일어 105-키
- 이탈리아어 105-키
- 일본어 109-키
- 한국어
- 포르투갈어
- 러시아어
- 스페인어 105-키
- 스위스어 105-키
- 영어(UK) 105-키
- 영어(US) 104-키

키보드 기본 설정에 대한 정보는 원격 제어 기본 설정 지정의 내용을 참조하십시오.

원격 제어 세션에 서버 콘솔 추가

현재 원격 제어 세션에 하나 이상의 서버 콘솔을 추가할 수 있습니다.

절차

현재 원격 제어 세션에 하나 이상의 서버 콘솔을 추가하려면 다음 단계를 완료하십시오.

단계 1. 원격 제어 창에서 **새 세션** 아이콘()을 클릭하십시오.

Lenovo XClarity Administrator에서 관리되고 사용자 계정이 관리 권한을 가진 사용 가능한 섀시 및 랙 서버 목록이 있는 대화 상자가 표시됩니다.

팁: 목록에 서버가 표시되지 않는 경우, 잠재적으로 문제를 해결하기 위한 절차는 XClarity Administrator 온라인 설명서에서 원격 제어 문제의 내용을 참조하십시오.

단계 2. 연결할 하나 이상의 서버를 선택하십시오.

유형 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 시스템 이름 또는 엔클로저 이름)를 입력하여 표시되는 서버를 필터링할 수 있습니다.

모두 선택을 선택하여 목록에 있는 모든 서버를 선택할 수 있습니다.

단계 3. **옵션: 단일 사용자 모드**를 선택하여 선택된 각 서버에 대한 독점 세션을 여십시오.

이 옵션을 선택하면 선택한 서버에서 연결을 끊기 전에는 선택한 서버에 대한 다른 모든 원격 제어 세션이 차단됩니다. 선택한 서버에 다른 원격 제어 세션이 구축되지 않은 경우에만 이 옵션이 사용 가능합니다.

이 옵션을 선택하지 않는 경우 기본적으로 다중 사용자 모드가 사용됩니다.

단계 4. **연결**을 클릭하십시오.

원격 제어 세션에서 서버 전원 켜기 및 끄기

원격 제어 세션에서 서버 전원을 켜고 끌 수 있습니다.

절차

서버 전원을 켜고 끄려면 다음 단계를 완료하십시오.

단계 1. 원격 제어 창에서 전원을 켜거나 끌 서버의 축소판을 클릭하십시오.

단계 2. **전원** 아이콘()을 클릭한 후 다음 전원 작업 중 하나를 클릭하십시오.

- **전원 켜기**
- **정상적으로 전원 끄기**
- **즉시 전원 끄기**
- **정상적으로 다시 시작**
- **즉시 다시 시작**
- NMI 트리거
- **시스템 설정으로 다시 시작** (Lenovo Converged, Flex System, NeXtScale 및 System x 서버만 해당)

팁: 현재 서버 전원이 켜져 있으면 **전원** 아이콘이 녹색입니다.

소프트 키 정의

현재 원격 제어 세션에 대해 *소프트 키*라는 사용자 지정 키 시퀀스를 정의할 수 있습니다.

시작하기 전에

현재 소프트 키 정의 목록을 표시하려면, **키보드** 아이콘()을 클릭하십시오.

소프트 키 정의는 원격 제어 세션이 시작된 시스템에 저장됩니다. 따라서 다른 시스템에서 원격 제어 세션을 실행한 경우 소프트 키를 다시 정의해야 합니다.

기본 설정 대화 상자의 **사용자 설정** 탭에서 사용자 설정(소프트 키 포함)을 내보내도록 선택할 수 있습니다. 자세한 정보는 사용자 설정 가져오기 및 내보내기의 내용을 참조하십시오.

참고: 다국어 키보드를 사용하고 AltGr(Alternate Graphics key)이 필요한 소프트 키를 정의하는 경우 원격 제어 응용 프로그램을 호출하는 데 사용하는 워크스테이션의 운영 체제는 원격으로 액세스하는 서버와 동일한 운영 체제 유형이어야 합니다. 예를 들어 서버에서 Linux가 실행 중인 경우 Linux를 실행하는 워크스테이션에서 원격 제어 세션을 호출해야 합니다.

절차

소프트 키를 추가하려면 다음 절차를 완료하십시오.

단계 1. 원격 제어 창에서 **키보드** 아이콘()을 클릭한 다음 **소프트 키 추가**를 클릭하십시오. 기본 설정 대화 상자에 **소프트 키 프로그래머** 탭이 표시됩니다.

단계 2. **새로 만들기**를 클릭하십시오.

단계 3. 정의할 키 시퀀스를 입력하십시오.

단계 4. **확인**을 누르십시오. 새 소프트 키가 소프트 키 목록에 추가됩니다.

Ctrl, Alt 및 Shift 키 사용

일부 운영 체제는 특정 키를 원격 서버에 전달하는 대신 인터셉트합니다. 고정 키 버튼을 사용하여 관리 중인 서버에 키스트로크를 직접 보낼 수 있습니다.

절차

Ctrl 또는 Alt 키 조합을 보내려면 도구 모음에서 Ctrl 또는 Alt를 클릭하고 비디오 세션 영역에 커서를 놓고 키보드에서 키를 누르십시오.

예를 들어 Ctrl+Alt+Del 키 조합을 보내려면 다음 단계를 완료하십시오.

1. 도구 모음에서 Ctrl을 클릭하십시오.
2. 도구 모음에서 Alt를 클릭하십시오.
3. 비디오 세션 영역 내의 아무 곳이나 마우스 왼쪽 단추로 클릭하십시오.
4. 키보드에서 Delete 키를 누르십시오.

참고: 마우스 캡처 모드를 사용으로 설정한 경우 비디오 세션 영역 밖으로 커서를 이동시키려면 왼쪽 Alt 키를 누르십시오. 마우스 캡처 모드는 기본적으로 사용 안 함으로 설정되지만 도구 모음 페이지에서 이를 사용으로 설정할 수 있습니다(원격 제어 기본 설정 지정 참조).

도구 모음에서 Ctrl, Alt 또는 Shift를 클릭하여 키를 활성화시키면 키보드 키를 누르거나 해당 버튼을 다시 클릭하기 전까지 키가 활성화된 상태 그대로 유지됩니다.

원격 미디어 마운팅 또는 이동

원격 미디어 기능을 사용하여 로컬 시스템에 있는 원격 미디어(예, CD, DVD 또는 USB 장치, 디스크 이미지, 또는 CD(ISO) 이미지)를 선택한 서버로 탑재할 수 있습니다. BMC(baseboard management-controller)에서 사용 가능한 로컬 스토리지에 이미지를 업로드할 수도 있습니다.

시작하기 전에

한 번에 한 사용자만 관리 컨트롤러에 있는 로컬 스토리지로 데이터를 탑재하고 업로드할 수 있습니다. 로컬 스토리지가 탑재되거나 로컬 스토리지에 데이터가 업로드되는 동안에는 다른 사용자가 관리 컨트롤러의 로컬 스토리지에 액세스할 수 없습니다.

Linux 운영 체제를 실행하는 서버에서는 둘 이상의 ISO 이미지 탑재가 지원되지 않습니다.

절차

원격 미디어를 탑재하거나 이동하려면 다음 단계를 완료하십시오.

단계 1. 원격 제어 창에서 **원격 미디어** 아이콘()을 클릭하십시오.

단계 2. 다음 작업 중 하나를 클릭하십시오.

- **원격 미디어 탑재**

  이 작업은 현재 선택한 서버에 로컬 미디어 리소스를 사용 가능하게 합니다. 단일 원격 제어 세션에서 미디어 리소스는 한 번에 한 서버에만 탑재될 수 있습니다.

  원격 미디어 탑재를 클릭하는 경우 다음 옵션이 사용 가능합니다.

  - **탑재할 이미지 선택**. 장치를 탑재 해제하거나 원격 제어 세션을 닫기 전까지 이 이미지를 현재 선택한 서버에 사용할 수 있습니다. 단일 서버에 다중 이미지를 탑재할 수 있으며 각 이미지를 다중 서버에 탑재할 수 있습니다.
  - **탑재할 드라이브(예, CD, DVD 또는 USB 장치) 선택**. 드라이브를 탑재 해제하거나 원격 제어 세션을 닫기 전까지 장치를 현재 선택한 서버에 사용할 수 있습니다. 단일 서버에 다중 장치를 탑재할 수 있지만 각 장치를 한 번에 한 서버에만 탑재할 수 있습니다.

    참고: 드라이브를 선택하는 경우 드라이브에서 미디어를 제거하기 전에 드라이브를 탑재 해제해야 합니다.
  - **IMM에 이미지 업로드**. 이 옵션을 사용하여 선택한 서버에 대한 관리 컨트롤러의 로컬 스토리지에 이미지를 저장하십시오. 원격 제어 세션을 종료하거나 서버를 다시 시작하는 경우에도 이미지는 관리 컨트롤러에 그대로 남아 있습니다.

    관리 컨트롤러에 약 50MB의 데이터를 저장할 수 있습니다.

    모든 이미지에 사용되는 총 공간이 50MB 이하인 다중 이미지를 제공되는 관리 컨트롤러에 업로드할 수 있습니다.

    관리 컨트롤러에 업로드되는 각 이미지는 자동으로 서버에 탑재됩니다. 관리 컨트롤러에 이미지를 업로드한 후에는 업로드한 이미지를 다른 서버의 관리 컨트롤러로 이동시

킬 수도 있습니다. 이미지를 이동하면 이전에 업로드한 이미지가 현재 서버에서 제거되고 선택한 서버로 업로드됩니다.

- **원격 미디어 이동**

  이 작업은 이전에 탑재한 미디어 리소스를 서버 간에 이동시킵니다.

  리소스를 서버에 사용 가능하게 하려면 다음 단계를 완료하십시오.

  1. 하나 이상의 리소스를 선택하십시오.
  2. **추가**를 클릭하여 **선택한 리소스** 목록으로 리소스를 이동하십시오.
  3. **탑재**를 클릭하여 서버에서 사용할 리소스를 탑재하십시오. 원격 제어 세션은 리소스에 대한 장치를 정의하고 해당 장치를 현재 선택한 서버의 탑재 지점에 매핑합니다. 탑재된 미디어를 쓰기 보호하는 옵션이 있습니다.

서버에 이미지 업로드

선택한 서버에 대한 BMC(baseboard management-controller)에서 사용 가능한 로컬 스토리지에 이미지를 업로드할 수 있습니다.

이 작업 정보

원격 제어 세션을 종료하거나 서버를 다시 시작하는 경우에도 이미지는 관리 컨트롤러에 그대로 남아 있습니다.

관리 컨트롤러에 약 50MB의 데이터를 저장할 수 있습니다.

모든 이미지에 사용되는 총 공간이 50MB 이하인 다중 이미지를 제공되는 관리 컨트롤러에 업로드할 수 있습니다.

관리 컨트롤러에 업로드되는 각 이미지는 자동으로 서버에 탑재됩니다. 관리 컨트롤러에 이미지를 업로드한 후에는 업로드한 이미지를 다른 서버의 관리 컨트롤러로 이동시킬 수도 있습니다. 이미지를 이동하면 이전에 업로드한 이미지가 현재 서버에서 제거되고 선택한 서버로 업로드됩니다.

절차

서버에 이미지를 업로드하려면 다음 단계를 완료하십시오.

단계 1. 원격 제어 창에서 **원격 미디어** 아이콘()을 클릭하십시오.

단계 2. **원격 미디어 탑재**를 클릭하십시오.

단계 3. IMM**에 이미지 업로드**를 클릭하십시오.

사용자 설정 가져오기 및 내보내기

현재 원격 제어 세션에 대한 사용자 설정을 가져오거나 내보내도록 선택할 수 있습니다.

이 작업 정보

사용자 설정을 내보내는 경우 현재 원격 제어 세션의 모든 사용자 설정이 로컬 시스템의 속성 파일에 저장됩니다. 이 속성 파일을 다른 시스템에 복사하고 해당 설정을 원격 제어 응용 프로그램으로 가져와서 설정을 사용할 수 있습니다.

절차

현재 원격 제어 세션에 대한 사용자 설정을 가져오거나 내보내려면 다음 단계를 완료하십시오.

단계 1. 원격 제어 창에서 **기본 설정** 아이콘()을 클릭하십시오.

단계 2. **사용자 설정** 탭을 클릭하십시오.

단계 3. 내보낸 파일에서 설정을 가져오려면 **가져오기**를 클릭하고 모든 현재 사용자 설정을 로컬 시스템의 속성 파일에 저장하려면 **내보내기**를 클릭하십시오.

원격 제어 기본 설정 지정

현재 원격 제어 세션에 대한 기본 설정을 수정할 수 있습니다.

절차

원격 제어 기본 설정을 수정하려면 다음 단계를 완료하십시오.

단계 1. 원격 제어 기본 설정을 수정하려면 **기본 설정** 아이콘()을 클릭하십시오. 모든 변경사항은 즉시 적용됩니다.

- KVM
  - **비디오 대역폭 비율**. 대역폭을 늘리면 원격 제어 세션의 모양 품질이 개선되지만 원격 제어 세션의 성능에 영향을 미칠 수 있습니다.
  - **새로 고침 프레임 비율**. 프레임 새로 고침 비율을 늘리면 원격 제어 세션을 업데이트하는 빈도가 증가되지만 원격 제어 세션의 성능에 영향을 미칠 수 있습니다.
  - **키보드 유형**. 원격 제어 세션에 사용하는 키보드 유형을 선택하십시오. 선택한 키보드 유형이 로컬 시스템의 키보드 설정과 일치하고 원격 호스트의 키보드 설정과 일치해야 합니다.

    참고: 다국어 키보드를 선택하고 AltGr(Alternate Graphics key)이 필요한 키 조합을 입력해야 하는 경우 원격 제어 세션을 호출하는 데 사용하는 워크스테이션의 운영 체제는 원격으로 액세스하는 서버와 동일한 운영 체제 유형이어야 합니다. 예를 들어 서버에서 Linux가 실행 중인 경우 Linux를 실행하는 워크스테이션에서 원격 제어 응용 프로그램을 호출해야 합니다.
  - **이미지를 창에 맞게 크기 조정**. 서버에서 받은 비디오 이미지를 비디오 세션 영역 크기에 맞게 조정하려면 이 옵션을 선택하십시오.
- **보안**
  - **단일 사용자 모드 연결 기본 설정**. 서버 연결 시 단일 사용자 모드 연결이 기본 선택인지 여부를 지정하십시오. 단일 사용자 모드에서 연결되는 경우 한 번에 한 사용자만 서버에 연결할 수 있습니다. 이 상자를 선택하지 않는 경우 다중 사용자 모드로 서버에 연결이 기본 기능이 됩니다.
  - **터널링 연결 필수(보안)**. 관리 노드를 통해 서버에 액세스하려면 이 옵션을 선택하십시오. 이 옵션을 사용하여 서버와 동일한 네트워크에 없는 클라이언트에서 서버에 액세스할 수 있습니다.

    참고: 원격 제어 응용 프로그램은 항상 원격 제어가 시작된 로컬 시스템에서 서버로 직접 연결하려고 시도합니다. 이 옵션을 선택하는 경우 클라이언트 워크스테이션이 서버에 직접 액세스할 수 없으면 원격 제어 응용 프로그램이 Lenovo XClarity Administrator를 통해 서버에 액세스합니다.
- **도구 모음**

  참고: 이 페이지의 모든 설정을 기본 설정으로 복원하려면 **기본값 복원**을 클릭하십시오.
  - **창에 도구 모음 고정**. 기본적으로 도구 모음은 원격 제어 세션 창의 위에 숨겨져 있으며 마우스 포인터가 위로 지나가는 경우에만 표시됩니다. 이 옵션을 선택하는 경우 도구 모음은 창에 고정되며 축소판 패널과 원격 제어 세션 창 사이에 항상 표시됩니다.
  - **키보드 버튼 표시**. 도구 모음에서 키보드 버튼 아이콘(CapsLock, NumLock 및 ScrollLock)을 표시할지 여부를 지정합니다.
  - **전원 제어 표시**. 도구 모음에서 전원 제어 옵션을 표시할지 여부를 지정합니다.
  - **고정 키 버튼 표시**. 도구 모음에서 고정 키 버튼 아이콘(Ctrl, Alt 및 Delete)을 표시할지 여부를 지정합니다.

- **로컬 마우스 포인터 숨기기**. 현재 비디오 세션 영역에 표시되는 서버 세션에 커서를 놓을 때 로컬 마우스 포인터를 표시할지 여부를 지정합니다.
- **마우스 캡처 모드 사용**. 기본적으로 마우스 캡처 모드는 사용 안 함으로 설정됩니다. 이는 비디오 세션 영역 안과 밖으로 커서를 자유롭게 이동시킬 수 있음을 의미합니다. 마우스 캡처 모드를 사용하는 경우 비디오 세션 영역 밖으로 커서를 이동하려면 먼저 왼쪽 Alt 키를 눌러야 합니다. 마우스 캡처 모드를 사용으로 설정하면 Ctrl+Alt 키를 사용하여 마우스 캡처 모드를 종료할지 여부를 지정할 수 있습니다. 기본값은 왼쪽 Alt 키 사용입니다.
- **도구 모음 백그라운드 투명도 지정**. 불투명 비율을 낮추면 도구 모음 백그라운드를 통해 더 많은 비디오 세션 영역이 표시됩니다.

  참고: 이 옵션은 도구 모음이 창에 고정되지 않은 경우에만 사용 가능합니다.

- **축소판**
  - **축소판 표시** 원격 제어 세션에 축소판 영역을 표시하려면 이 옵션을 선택하십시오.
  - **축소판 새로 고침 간격 지정**. 축소판 새로 고침 간격을 줄이면 서버 축소판이 업데이트되는 빈도가 증가됩니다.
- **일반**
  - **디버그 모드**. 원격 제어 응용 프로그램에 디버그 모드를 설정할지 여부를 지정합니다. 이 설정은 로그 파일에 로깅되는 이벤트 세분화를 판별합니다. 기본적으로 심각한 이벤트만 로깅됩니다. 로그 파일 위치에 대한 자세한 정보는 원격 제어 로그 및 추적 보기의 내용을 참조하십시오.
  - **시스템 모양 설정 상속**. 이 설정은 모양이 로컬 서버(Windows 실행)에서 구성된 색상 구성과 일치하도록 변경합니다. 이러한 설정을 적용하려면 원격 제어 응용 프로그램을 다시 시작해야 합니다.
  - **데스크탑 아이콘 만들기**. 이 설정은 시스템에서 원격 제어 응용 프로그램을 직접 시작할 수 있도록 로컬 시스템에 데스크탑 아이콘을 작성합니다. 시스템에서 관리 소프트웨어에 대한 액세스 권한을 가지고 있어야 합니다.
  - **관리 서버와 동기화**. 이 설정을 사용하면 원격 제어 응용 프로그램에 표시되는 서버 데이터가 관리 소프트웨어에서 표시되는 서버 데이터와 일치하게 됩니다.

원격 제어 로그 및 추적 보기

원격 제어 세션을 시작하면 로그 파일이 작성됩니다. 이러한 파일에 로그되는 이벤트 유형은 디버그 모드를 기반으로 합니다. 디버그 모드는 기본 설정 대화 상자의 **일반** 탭에서 설정됩니다. 이러한 로그 파일을 사용하여 문제를 해결할 수 있습니다.

절차

원격 제어 로그 파일이 다음 위치에 저장됩니다.

운영 체제	로그 디렉토리
Windows 7 및 8	%USERPROFILE%\lenovo\remoteaccess 예: C:\Users\win_user\lenovo\remoteaccess

진단 파일을 수집하고 Lenovo 지원로 파일을 보내는 데 대한 자세한 정보는 Lenovo XClarity Administrator 온라인 설명서에서 서비스 및 지원 작업의 내용을 참조하십시오.

관리되는 서버에서 운영 체제에 대한 액세스 관리

관리되는 서버에서 운영 체제에 대한 액세스를 관리할 수 있습니다.

시작하기 전에

Windows 드라이버 업데이트 페이지에서 장치 드라이버를 관리 및 배포하고 관리되는 서버에 대한 전원 작업을 수행하려면 lxc-os-admin, lxc-supervisor, lxc-admin 또는 lxc-hw-admin 권한이 있어야 합니다.

이 작업 정보

Lenovo XClarity Administrator가 관리되는 시스템에서 OS 장치 드라이버를 업데이트하려면, 먼저 OS IP 주소 및 호스트 운영 체제에 액세스할 수 있는 저장된 관리자 자격 증명 등 호스트 운영 체제에 액세스하는 데 필요한 정보를 제공해야 합니다. OS 장치 드라이버 업데이트에 대한 자세한 정보는 관리되는 서버에서 Windows 장치 드라이버 업데이트의 내용을 참조하십시오.

XClarity Administrator는 저장된 자격 증명을 사용하여 호스트 운영 체제에서 인증합니다. XClarity Administrator에서 저장된 자격 증명을 만드는 데 대한 자세한 정보는 저장된 자격 증명 관리의 내용을 참조하십시오.

팁: XClarity Administrator는 이 페이지에서 지정한 정보를 자동으로 유효성 검증하지 않습니다.

절차

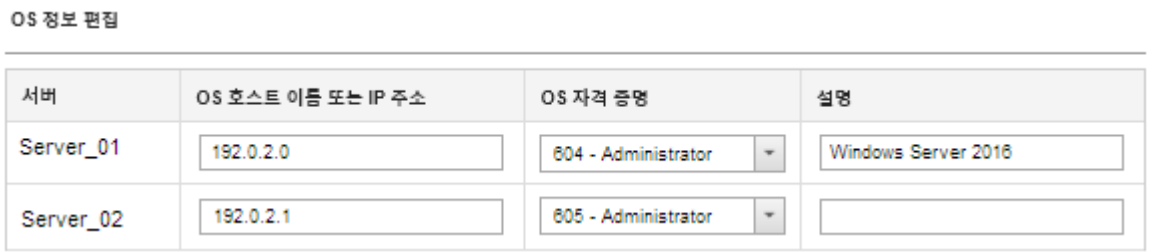
운영 체제 속성을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 액세스 관리**를 클릭하여 OS 액세스 관리 페이지를 표시하십시오.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.

단계 2. 업데이트할 서버를 선택하십시오.

단계 3. **OS 정보 편집** 아이콘()을 클릭하여 OS 정보 편집 대화 상자를 표시하십시오.



단계 4. 각 대상 서버에 대해 다음 정보를 지정하십시오.
- 호스트 운영 체제의 IP 주소 또는 호스트 이름
- (옵션) 호스트 운영 체제에 액세스하기 위한 저장된 자격 증명

- (옵션) 호스트 운영 체제에 대한 설명

단계 5. **저장**을 클릭하십시오.

완료한 후에

운영 체제 액세스를 관리하기 위해 다음 작업을 수행할 수 있습니다.

- 서버를 선택하고 OS **정보 제거** 아이콘()을 클릭하여 운영 체제 정보(IP 주소, 자격 증명 및 설명)을 지우십시오.
- **프로비저닝 → Windows 드라이버 업데이트: 적용**을 클릭하고 대상 서버를 선택한 다음 **인증 확인**을 클릭하여 Windows Server에서 인증을 테스트하십시오.
- 서버 이름 위로 마우스를 가져가면 특정 서버의 운영 체제에 대한 배포 정보를 볼 수 있습니다.

  참고: 배포 정보는 XClarity Administrator 인스턴스에서 성공적으로 배포한 운영 체제에만 있습니다. 배포 정보는 실패한 배포 및 다른 수단(다른 XClarity Administrator 인스턴스)에서 수행한 배포에는 없습니다.

Features on Demand 키 보기

관리 서버에 현재 설치된 Features on Demand 키 목록을 볼 수 있습니다.

이 작업 정보

Lenovo XClarity Administrator 웹 인터페이스에서 Features on Demand 키를 구매, 설치 또는 관리할 수 없습니다. Features on Demand 키 확보 및 설치에 대한 정보는 XClarity Administrator 온라인 설명서에서 Features on Demand의 내용을 참조하십시오.

절차

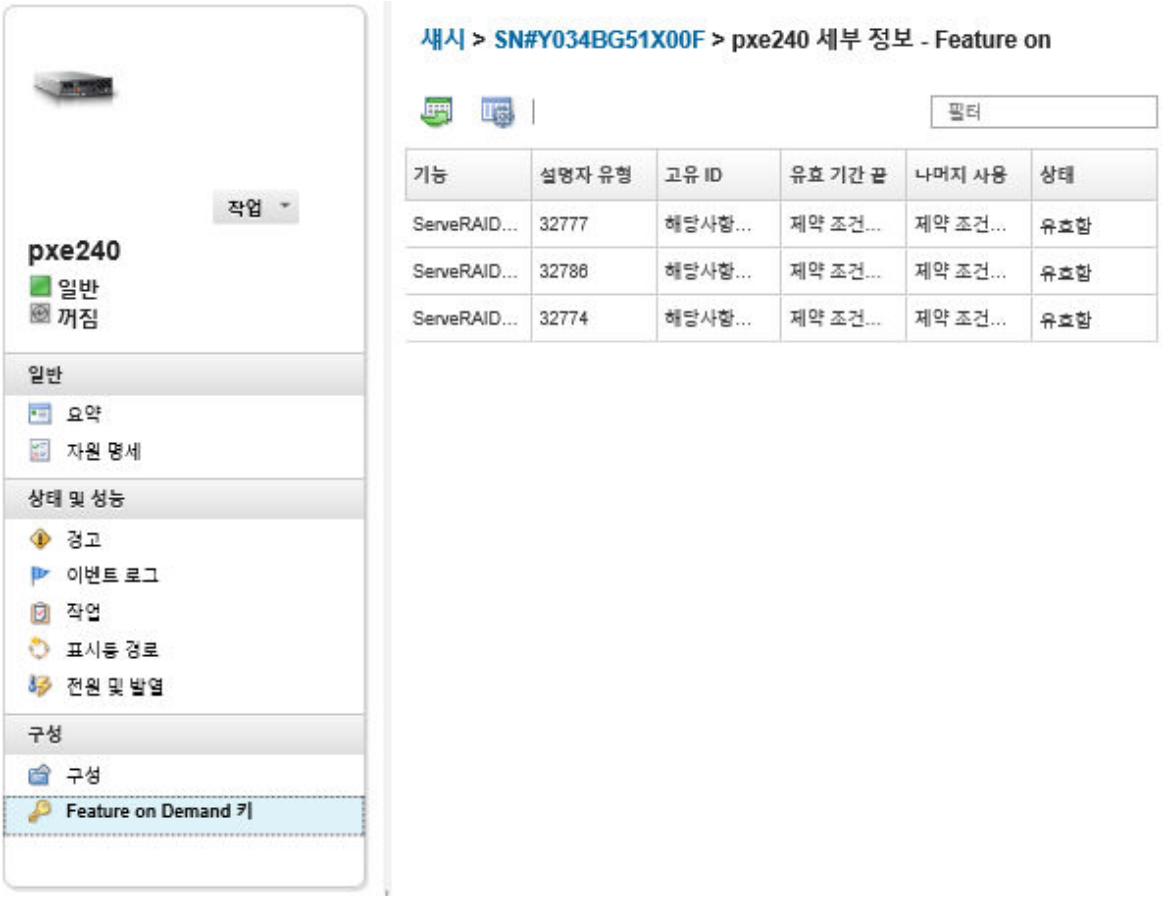
특정 관리 서버에 설치된 FoD 키 목록을 표시하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지가 모든 관리되는 서버(랙 및 타워 서버, 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

단계 2. **서버** 열에서 서버 이름을 클릭하십시오. 해당 서버의 상태 요약 페이지가 표시되며, 여기에는 해당 서버에 설치된 구성 요소 목록과 서버 속성이 표시됩니다.

단계 3. 왼쪽 탐색의 일반에서 **인벤토리 세부 정보**를 클릭하고 각 하드웨어 구성 요소 섹션을 확장하여 해당 구성 요소의 FoD 고유 ID를 보십시오.

단계 4. 왼쪽 탐색의 구성에서 **Features on Demand 키**를 클릭하여 서버에 설치된 모든 FoD 키에 대한 정보를 보십시오.



에너지 및 온도 관리

Converged, NeXtScale, System x 및 ThinkServer 서버의 소비 전력과 온도를 모니터링하고 관리하며, Lenovo XClarity Energy Manager를 사용하여 에너지 효율을 개선할 수 있습니다.

자세히 알아보기: Lenovo XClarity Energy Manager

이 작업 정보

XClarity Administrator는 다음을 포함하여 지원되는 서버의 소비 전력과 온도를 모니터링하고 관리하는 데 사용할 수 있는 독립 실행형 사용자 인터페이스입니다.

- 필요에 따라 에너지 소비를 모니터링하고, 전력 수요를 평가하고 서버에 전원을 재할당합니다.
- 서버의 온도와 냉각 용량을 모니터링합니다.
- 특정 이벤트가 발생하거나 임계값을 초과하는 경우 알림을 전송합니다.
- 정책을 사용하여 장치가 소비하는 에너지 크기를 제한합니다.
- 실시간 흡입구 온도를 모니터링하고, 대역 외 전력 데이터를 기반으로 하여 사용량이 적은 서버를 식별하고, 여러 서버 모델에 대한 전원 레인저를 측정하고, 리소스 사용 가능성을 기반으로 하여 서버가 새 워크로드를 수용하는 방법을 평가합니다.
- 비상 전원 이벤트(예, 데이터 센터 전원 장애) 중에는 서비스 시간을 연장하기 위해 소비 전력을 최소 수준으로 줄입니다.

XClarity Administrator 다운로드, 설치 및 사용에 대한 자세한 정보는 Lenovo XClarity Energy Manager 웹 사이트의 내용을 참조하십시오.

서버 전원 켜기 및 끄기

Lenovo XClarity Administrator에서 서버 전원을 켜고 끌 수 있습니다.

시작하기 전에

- RHEL(Red Hat® Enterprise Linux) v7 이상에서는 그래픽 모드에서 운영 체제를 다시 시작하면 기본적으로 서버가 일시 중단됩니다. XClarity Administrator에서 **정상적으로 다시 시작** 또는 **즉시 다시 시작** 작업을 수행하려면 먼저 전원 버튼의 동작을 변경하여 전원을 끄도록 운영 체제를 수동으로 구성해야 합니다. 지시사항은 Red Hat 데이터 마이그레이션 및 관리 안내서: 그래픽 대상 모드에서 전원 버튼을 누르면 동작 변경.의 내용을 참조하십시오.
- SUSE Linux Enterprise Server(SLES)의 경우 운영 체제를 종료하려면 SLES 세션에서 루트 암호를 입력해야 합니다. XClarity Administrator에서 **정상적으로 전원 끄기** 또는 **즉시 전원 끄기** 작업을 수행하려면 먼저 로컬 SLES 인터페이스를 사용하여 수동으로 서버 전원을 끄고 암호 입력 시 **인증 기억** 옵션을 선택하거나 보안 정책을 선택하여 필수 인증을 사용 안 함으로 설정할 수 있는지 여부를 확인해야 합니다.
- 이를 사용하는 경우 Wake-on-LAN 부팅 옵션은 서버 전원을 끄는 XClarity Administrator 작업을 방해할 수 있습니다. 예를 들어 사용자 네트워크의 Wake-on-LAN 클라이언트에서 "Wake on Magic 패킷" 명령을 실행하는 경우 펌웨어 업데이트를 방해합니다.
- 전원 작업 **시스템 설정으로 다시 시작**은 서버를 다시 시작하고 일반 운영 체제 부팅이 아닌 원격 제어 세션에서 BIOS/UEFI Startup 유틸리티를 엽니다.
- 전원 작업 **정상적으로 전원 끄기** 및 **즉시 전원 끄기**는 장치에 설치된 운영 체제 구성에 따라 다르며 운영 체제가 이를 지원하도록 구성된 경우에만 작동합니다.
- **모든 작업 → 서비스 → NMI 트리거**를 클릭하여 NMI(non-maskable interrupt)로 장치를 다시 시작할 수 있습니다.

절차

서버 전원을 켜거나 끄려면 다음 절차를 완료하십시오.

단계 1. XClarity Administrator 메뉴에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지는 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

단계 2. 서버를 선택하십시오.

단계 3. **모든 작업 → 전원 작업**을 클릭하고 다음 전원 작업 중 하나를 클릭하십시오.
- **전원 켜기**는 장치의 전원을 켭니다.
- **정상적으로 전원 끄기**는 운영 체제를 종료하고 장치의 전원을 끕니다.
- **즉시 전원 끄기**는 장치의 전원을 끕니다.
- **정상적으로 다시 시작**은 운영 체제를 종료하고 장치를 다시 시작합니다.
- **즉시 다시 시작**은 장치를 다시 시작합니다.
- **시스템 설정으로 다시 시작**은 장치를 BIOS/UEFI(F1) 설정으로 다시 시작합니다. 이는 제한 없이 지원되는 ThinkServer 이외의 서버에서 지원됩니다.
- **관리 컨트롤러 다시 시작**은 BMC를 다시 시작합니다.
- **즉시 다시 시작 및 PXE 네트워크 부팅 시도**는 서버를 즉시 다시 시작하고 서버를 PXE(Preboot Execution Environment) 네트워크로 부팅합니다. 이는 Lenovo Flex System, System x 및 ThinkSystem 서버에서만 지원됩니다.

  참고: PXE 부팅 관련 UEFI 설정은 서버에서 구성해야 합니다.

가상으로 Flex System 섀시에서 서버 재배치

NMI(non-maskable interrupt)로 서버를 다시 시작하여 Flex System 섀시에서 서버 제거 및 재삽입을 시뮬레이션할 수 있습니다.

이 작업 정보

가상 재배치 중에는 기존의 모든 서버 네트워크 연결이 끊어지고 서버의 전원 상태가 변경됩니다. 가상 재배치를 수행하기 전에 모든 사용자 데이터를 저장했는지 확인하십시오.

주의:

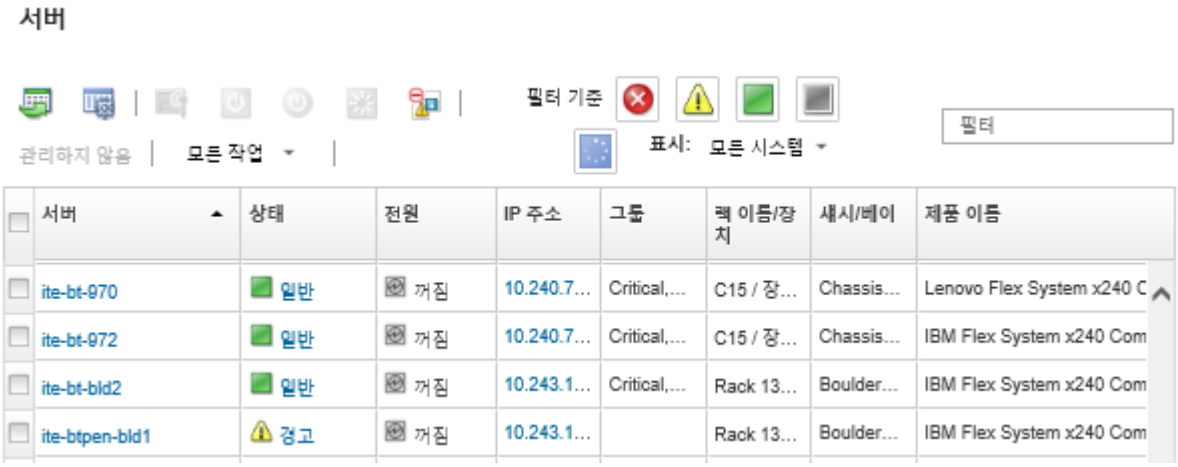
- Lenovo 지원에서 지시하지 않는 한 가상 재배치를 수행하지 마십시오.
- 가상 재배치를 수행하면 데이터 손실이 발생할 수 있습니다. 서버를 재배치하기 전에 사용자 데이터 보호에 필요한 작업을 수행하십시오.
- 가상 재배치를 수행하는 대신 서버 전원을 끌 것을 고려해 보십시오. 전원 작업에 대한 정보는 서버 전원 켜기 및 끄기의 내용을 참조하십시오.

절차

가상으로 Flex System 섀시의 서버를 재배치하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 모든 관리되는 서버의 표 형식 보기와 함께 서버 페이지가 표시됩니다.

재배치할 서버를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **모든 장치** 드롭 다운 목록에서 장치 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.



단계 2. 테이블에서 서버를 선택하십시오.

단계 3. **모든 작업 → 서비스 → 가상 재배치**를 클릭하십시오.

단계 4. **가상 재배치**를 클릭하십시오.

서버에 대한 관리 컨트롤러 인터페이스 실행

Lenovo XClarity Administrator에서 특정 서버에 대한 관리 컨트롤러 웹 인터페이스를 실행할 수 있습니다.

시작하기 전에

XClarity Administrator를 통해 ThinkSystem SR635 SR655 서버에 액세스하려면 사용자는 lxc-supervisor, lxc-sysmgr, lxc-admin, lxc-fw-admin 또는 lxc-os-admin 권한을 가지고 있어야 합니다(인증 서버 관리 참조).

SSO(Single sign-on)를 사용하는 경우 로그인을 하지 않고 XClarity Administrator에서 관리되는 서버의 관리 인터페이스를 시작할 수 있습니다. SSO는 ThinkSystem 및 ThinkAgile 서버(SR635

및 SR655 제외)에서 지원됩니다. ThinkSystem SR645 및 SR665 서버에는 XCC 펌웨어 21A 이상이 필요합니다.

XClarity Administrator에 로그인하지 않고 로컬 또는 외부 LDAP 사용자 계정을 사용하여 관리 컨트롤러에 직접 로그인하려면 `https://{XCC_IP_adderss}/#/login` URL을 사용하십시오.

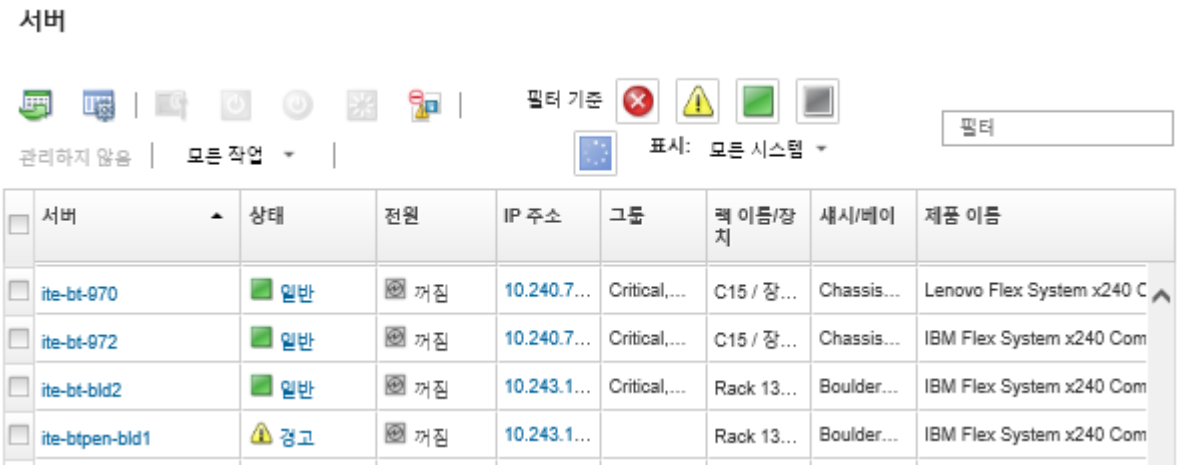
절차

서버의 관리 컨트롤러 인터페이스를 실행하려면 다음 단계를 완료하십시오.

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

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하여 서버 페이지를 표시하십시오.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.



단계 2. **서버** 열에서 서버 링크를 클릭하십시오. 해당 서버에 대한 상태 요약 페이지가 표시됩니다.

단계 3. **모든 작업 → 실행 → 관리 웹 인터페이스**를 클릭하십시오. 서버에 대한 관리 컨트롤러 웹 인터페이스가 시작됩니다.

팁: **IP 주소** 열에서 IP 주소를 클릭하여 관리 컨트롤러 인터페이스를 실행할 수도 있습니다.

단계 4. XClarity Administrator 사용자 자격 증명을 사용하여 관리 컨트롤러 인터페이스에 로그인하십시오.

완료한 후에

서버의 관리 컨트롤러 인터페이스 사용에 대한 자세한 정보는 Integrated Management Module II 온라인 설명서 및 XClarity Controller 온라인 설명서의 내용을 참조하십시오.

서버에 대한 시스템 속성 수정

특정 서버에 대한 시스템 속성을 수정할 수 있습니다.

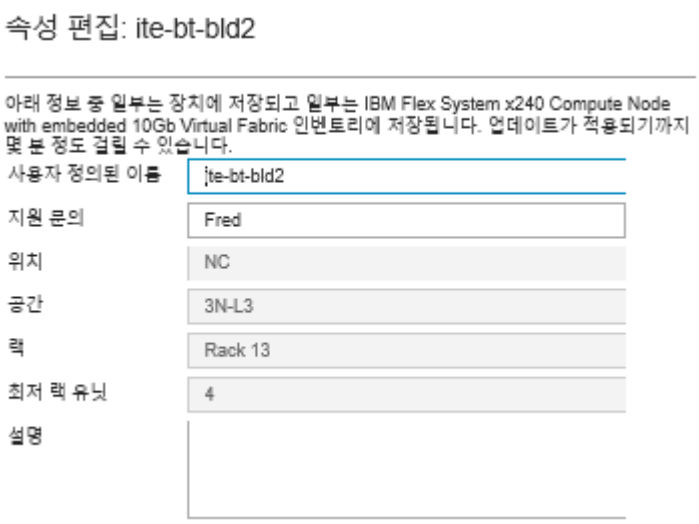
절차

시스템 속성을 수정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하여 서버 페이지를 표시하십시오.

단계 2. 업데이트할 서버를 선택하십시오.

단계 3. **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 편집 대화 상자를 표시하십시오.



단계 4. 필요 시 다음 정보를 변경하십시오.
- 서버에 대한 사용자 정의 이름
- 지원 문의
- 설명

참고: 웹 인터페이스의 랙에서 장치를 추가하거나 제거할 때 XClarity Administrator에서 위치, 룸, 랙 및 하단 LRU(lowest rack unit) 속성을 업데이트합니다(랙 관리 참조).

단계 5. **저장**을 클릭하십시오.

참고: 이러한 속성을 변경하는 경우 XClarity Administrator 웹 인터페이스에 변경 사항이 표시되기 전에 약간의 지연이 있을 수 있습니다.

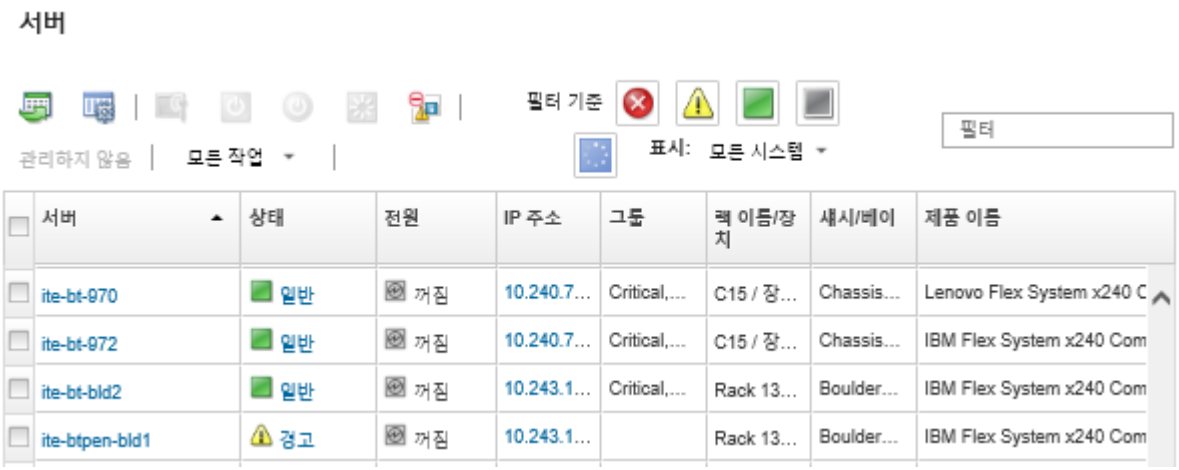
서버에 대해 만료되었거나 유효하지 않은 저장된 자격 증명 해결

저장된 자격 증명이 장치에서 만료되거나 작동 불능 상태가 되면 해당 장치의 상태가 "오프라인"으로 표시됩니다.

절차

서버에 대해 만료되었거나 유효하지 않은 저장된 자격 증명을 해결하려면 다음을 수행하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지는 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.



단계 2. **전원** 테이블 열 머리글을 클릭하여 테이블 맨 위에 있는 모든 오프라인 서버를 그룹화합니다.

또한 모든 시스템 드롭 다운 목록에서 시스템 유형을 선택하고 **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.

단계 3. 해결할 서버를 선택하십시오.

단계 4. **모든 작업 → 보안 → 저장된 자격 증명 편집**을 클릭하십시오.

단계 5. 저장된 자격 증명의 암호를 변경하거나 관리되는 장치에 사용할 다른 저장된 자격 증명을 선택하십시오.

참고: 동일한 저장된 자격 증명을 사용하여 둘 이상의 장치를 관리하고 저장된 자격 증명의 암호를 변경하면 해당 암호 변경은 현재 저장된 자격 증명을 사용하는 모든 장치에 영향을 줍니다.

서버 패턴을 배포한 후 장애가 발생한 서버 복구

서버 패턴을 배포한 후 서버에 오류가 발생한 경우 오류가 발생한 서버에서 프로필을 할당 해제한 다음 대기 서버에 프로필을 다시 할당하여 서버를 복구할 수 있습니다.

절차

Lenovo XClarity Administrator 관리되는 인증을 사용하는 오류가 발생한 서버를 복구하려면 다음 단계를 완료하십시오.

단계 1. 오류가 발생한 서버를 식별하십시오.

단계 2. 오류가 발생한 서버에서 서버 프로필을 할당 해제하십시오(서버 프로필 비활성화 참조).

주의: 프로필을 다시 할당하기 *전에* 오류가 발생한 서버 전원을 꺼서 할당된 가상 주소를 비활성화해야 합니다. 서버 프로필을 할당 해제하는 경우 서버 프로필 할당 해제 대화 상자에서 **서버 전원 끄기**를 선택하여 오류가 발생한 서버 전원을 끄십시오(서버 전원 켜기 및 끄기 참조).

단계 3. 대기 서버에 서버 프로필을 할당하십시오(서버 프로필 활성화 참조).

단계 4. 현재 전원이 꺼진 경우 대기 서버 전원을 켜거나 현재 전원이 켜진 경우 대기 서버를 다시 시작하여 프로필을 활성화하십시오(서버 전원 켜기 및 끄기 참조).

단계 5. 연결된 스위치의 VLAN 설정을 대기 서버로 마이그레이션하십시오.

단계 6. 오류가 발생한 서버 전원이 꺼져 있는지 확인하십시오.

단계 7. 오류가 발생한 서버를 교체하거나 수리하십시오. 서버를 수리하는 경우 다음 단계를 수행하여 새로 수리된 서버를 기본 설정으로 재설정해야 합니다.

a. 서버의 관리 웹 인터페이스를 사용하여 BMC를 공장 출하 기본값으로 재설정하십시오. BMC 재설정에 대한 정보는 관리 컨트롤러를 재설정하여 관리 서버 오류 후 ThinkSystem,

Converged, NeXtScale, 또는 System x M5 또는 M6 서버 관리 복구의 내용을 참조하십시오.

b. UEFI 메뉴를 사용하여 I/O 어댑터 가상 주소 등의 UEFI(Unified Extensible Firmware Interface) 정보를 지우십시오. 해당 정보는 UEFI 설명서를 참조하십시오.

서버 패턴 배포 후 부팅 설정 복구

하나 이상의 서버에 새 서버 패턴을 배포한 후 해당 서버가 시작되지 않는 경우 부팅 설정을 서버 패턴에 있는 기본 부팅 설정으로 덮어쓰는 문제가 발생할 수 있습니다. UEFI 모드로 설치된 운영 체제의 경우 부팅 구성을 복원하려면 기본 설정에 추가 구성 단계가 필요할 수 있습니다.

절차

원본 부팅 설정을 복원하려면 연결된 각 서버에 대해 다음 수동 복구 절차를 완료하십시오.

- Red Hat Enterprise Linux가 설치된 서버의 경우:
  1. 서버에 원격으로 액세스하는 경우 서버에 대한 원격 제어 세션을 구축하십시오(원격 제어를 사용하여 Converged, Flex System, NeXtScale 및 System x 서버 관리 참조).
  2. **도구 → 전원 → 켜기**를 클릭하여 서버를 다시 시작하십시오. 원격 제어 세션에 서버의 UEFI 스플래시 화면이 표시되는 경우 F1을 눌러 Setup Utility를 표시하십시오.
  3. Boot Manager를 선택하십시오.
  4. Add Boot Option을 선택하십시오.
  5. UEFI Full Path Option을 선택하십시오.
  6. 표시되는 목록에서 SAS가 포함된 항목을 선택하십시오.
  7. EFI를 선택하십시오.
  8. redhat을 선택하십시오.
  9. grub.efi를 선택하십시오.
  10. Input the Description 필드를 선택하십시오.
  11. Red Hat Enterprise Linux를 입력하십시오.
  12. Commit Changes를 선택하십시오.
  13. Red Hat Enterprise Linux를 부팅 순서의 첫 번째 옵션으로 만들고 부팅 순서에서 다른 모든 옵션을 제거하십시오.
  14. Escape를 누르고 Save changes then exit this menu를 선택하십시오.
  15. Escape를 누르고 Exit the Configuration Utility and Reboot를 선택하십시오. 컴퓨팅 노드를 다시 시작하십시오.
- Microsoft Windows Server 2008이 설치된 서버의 경우:
  1. 서버 전원을 켜고 프롬프트가 표시되면 F1을 눌러 설정을 시작하십시오.
  2. Boot Manager를 선택하십시오.
  3. Boot from File을 선택하십시오.
  4. Microsoft Windows Server 2008이 설치된 GPT(GUID Partition Tables) System Partition을 선택하십시오.
  5. EFI를 선택하십시오.
  6. Microsoft를 선택하십시오.
  7. Boot를 선택하십시오.
  8. bootmgfw.EFI를 선택하십시오.

참고: 자세한 정보는 RETAIN 팁 5079636의 내용을 참조하십시오.

관리 서버 오류 후 랙 또는 타워 서버 관리 복구

Lenovo XClarity Administrator에서 랙 또는 타워 서버를 관리하고 XClarity Administrator에 오류가 발생한 경우 XClarity Administrator가 복원되거나 교체될 때까지 관리 기능을 복원할 수 있습니다.

이 작업 정보

Flex System 서버에 대한 관리를 복구하려면, 관리 서버 오류 후 CMM으로 관리 복구의 내용을 참조하십시오.

강제 관리에 의해 관리 서버 오류 후 랙 또는 타워 서버 관리 복구

강제 관리 옵션으로 서버를 다시 관리하여 서버 관리를 복구할 수 있습니다.

절차

교체 Lenovo XClarity Administrator 인스턴스가 오류가 발생한 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 RECOVERY_ID 계정 및 암호와 **강제 관리** 옵션을 사용하여 장치를 다시 관리할 수 있습니다(서버 관리 참조).

관리 컨트롤러를 사용하여 제대로 관리 해제되지 않은 System x 또는 NeXtScale M4 서버 복구

베이스보드 관리 컨트롤러(BMC)를 사용하여 System x 또는 NeXtScale M4 서버 관리를 복구할 수 있습니다.

절차

Lenovo XClarity Administrator 관리되는 인증을 사용하는 서버의 서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator에서 서버를 관리하기 전에 작성된 사용자 계정과 암호를 사용하여 관리 컨트롤러 웹 인터페이스에 로그인하십시오.

단계 2. SNMP 트랩 설정을 지우십시오.

a. IMM **관리** ➡ **네트워크**를 클릭하십시오.

b. SNMP 탭을 클릭하십시오.

c. **커뮤니티** 탭을 클릭하십시오.

d. 이전 XClarity Administrator의 커뮤니티 항목을 찾으십시오. 예를 들어 다음과 같습니다.
   - **LXCA IP 주소:** 10.240.198.84
   - **LXCA 호스트:** LXCA_maqCBIt86d
   - **커뮤니티 2:**
   - **커뮤니티 이름:** LXCA_maqCBIt86d
   - **액세스 유형:** 트랩
   - **특정 호스트가 이 커뮤니티의 트랩을 수신하도록 허용:** 10.240.198.84

e. 커뮤니티 항목의 필드에서 값을 제거하십시오.

f. **적용**을 클릭하십시오.

단계 3. 사용자 계정을 지우십시오.

a. IMM **관리** ➡ **사용자**를 클릭하십시오.

b. **사용자 계정** 탭을 클릭하십시오.

c. 다음 접두사를 가진 사용자 계정을 포함하여 XClarity Administrator인 모든 사용자 계정을 삭제하십시오.
   - DISABLE_*

- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

완료한 후에

XClarity Administrator가 복원되거나 교체된 후 System x 또는 NeXtScale 서버를 다시 관리할 수 있습니다(서버 관리 참조). 서버에 대한 모든 정보(예, 네트워크 설정, 서버 정책 및 펌웨어 준수 정책)는 유지됩니다.

관리 컨트롤러를 재설정하여 관리 서버 오류 후 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 관리 복구

서버의 베이스보드 관리 컨트롤러를 공장 출하 기본값으로 재설정하여 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 관리를 복구할 수 있습니다.

절차

Lenovo XClarity Administrator 관리되는 인증을 사용하는 서버의 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. 장치에서 Encapsulation을 사용하는 경우 오류가 발생한 XClarity Administrator 가상 어플라이언스의 IP 주소를 사용하도록 구성된 시스템에서 대상 관리 컨트롤러에 연결하십시오.

단계 2. 관리 컨트롤러를 공장 출하 기본값으로 재설정하십시오.

a. XClarity Administrator에서 서버를 관리하기 전에 작성된 복구 사용자 계정과 암호를 사용하여 서버의 관리 컨트롤러 웹 인터페이스에 로그인하십시오.

b. IMM **관리 탭**을 클릭하십시오.

c. **공장 출하 기본값으로 IMM 다시 설정**을 클릭하십시오.

d. 재설정 작업을 확인하려면 **확인**을 클릭하십시오.

중요: BMC 구성이 완료되면 BMC가 다시 시작됩니다. 로컬 서버인 경우 TCP/IP 연결이 중단되며 연결을 복원하도록 네트워크 인터페이스를 다시 구성해야 합니다.

단계 3. 서버의 관리 컨트롤러 웹 인터페이스에 다시 로그온하십시오.

- BMC는 처음에 DHCP 서버의 IP 주소를 얻도록 구성되어 있습니다. 이 주소를 얻을 수 없는 경우 고정 IPv4 주소 192.168.70.125를 사용합니다.
- IMMBMC는 처음에 USERID 사용자 이름 및 PASSWORD(0 포함) 암호로 설정되어 있습니다. 이 기본 사용자 계정은 감독자 액세스 권한을 가지고 있습니다. 보안 강화를 위해 초기 구성 중에 이 사용자 이름과 암호를 변경하십시오.

단계 4. 연결을 복원하도록 네트워크 인터페이스를 다시 구성하십시오. 자세한 정보는 Integrated Management Module II 온라인 설명서의 내용을 참조하십시오.

완료한 후에

XClarity Administrator가 복원되거나 교체된 후 서버를 다시 관리할 수 있습니다(서버 관리 참조). 서버에 대한 모든 정보(예, 네트워크 설정, 서버 정책 및 펌웨어 준수 정책)는 유지됩니다.

구성 패턴을 사용하여 서버를 구성한 경우 이 구성을 적용할 서버에 할당된 서버 프로필을 비활성화한 후 다시 활성화할 수 있습니다(서버 프로필 작업 참조).

cimcli를 사용하여 관리 서버 오류 후 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 관리 복구

`cimcli` 유틸리티로 CIM 구독을 제거하여 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 관리를 복구할 수 있습니다.

시작하기 전에

대상 서버에 대한 네트워크 액세스 권한이 있는 시스템에 cimcli 유틸리티가 있는 OpenPegasus가 설치되어야 합니다. OpenPegasus 다운로드, 구성 및 컴파일에 대한 정보는 Linux용 OpenPegasus 릴리스 RPM 웹 사이트의 내용을 참조하십시오.

참고: Red Hat Enterprise Linux(RHEL) Server 7 이상의 경우 OpenPegasus 소스 및 2진 RPM이 Red Hat 분배의 일부로 포함되어 있습니다. `top-pegasus-test.x86_64` 패키지에 cimcli 유틸리티가 있습니다.

이 작업 정보

서버가 복원된 후 서버를 다시 관리할 수 있습니다. 서버에 대한 모든 정보(예, 네트워크 설정, 서버 정책 및 펌웨어 준수 정책)는 유지됩니다.

절차

Lenovo XClarity Administrator 관리되는 인증을 사용하고 OpenPegasus가 설치된 서버에서 서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. 장치에서 Encapsulation을 사용으로 설정하는 경우:

a. 오류가 발생한 XClarity Administrator 가상 어플라이언스의 IP 주소를 사용하여 구성된 시스템에서 대상 서버로 연결하십시오.

b. 장치에 대한 SSH 세션을 열고 다음 명령을 실행하여 Encapsulation을 사용 안 함으로 설정하는 경우:

```
encaps lite off
```

단계 2. 다음 명령을 실행하여 CIM_ListenerDestinationCIMXML, CIM_Indicationfilter 및 CIM_IndicationSubscription의 CIM 인스턴스를 판별하십시오.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_IndicationSubscription
```

여기서 *<IP_address>*, *<user_ID>*, *<password>*는 관리 컨트롤러의 IP 주소, 사용자 ID, 암호입니다. 예를 들어, 다음과 같습니다.

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
```

```
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

단계 3. 다음 명령을 실행하여 CIM_ListenerDestinationCIMXML, CIM_Indicationfilter 및 CIM_IndicationSubscription의 CIM 인스턴스를 한 번에 하나씩 삭제하십시오.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s di '<cim_instance>'
```

여기서 *<IP_address>*, *<user_ID>*, *<password>*는 관리 컨트롤러의 IP 주소, 사용자 ID, 암호이고 *<cim_instance>*는 이전 단계에서 각 CIM 인스턴스에 대해 리턴된 정보입니다(큰따옴표로 묶임). 예를 들어, 다음과 같습니다.

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

완료한 후에

Lenovo XClarity Administrator가 복원되거나 교체된 후 System x 또는 NeXtScale 서버를 다시 관리할 수 있습니다(서버 관리 참조). 서버에 대한 모든 정보(예, 네트워크 설정, 서버 정책 및 펌웨어 준수 정책)는 유지됩니다.

관리 컨트롤러 인터페이스를 사용하여 관리 서버 오류 후 ThinkServer 서버 관리 복구

관리 컨트롤러 인터페이스에서 ThinkServer 서버 관리를 복구할 수 있습니다.

절차

서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. 관리자로 서버의 관리 컨트롤러 웹 인터페이스에 로그인하십시오(서버에 대한 관리 컨트롤러 인터페이스 실행 참조).

단계 2. 기본 메뉴에서 사용자를 선택한 다음 접두사가 "LXCA_"인 모든 사용자 계정을 제거하여 Lenovo XClarity Administrator에서 작성한 IPMI 계정을 제거하십시오.

또는 계정 사용자 이름을 바꾸어 "LXCA_" 접두사를 제거할 수 있습니다.

단계 3. 기본 메뉴에서 PEF **관리**를 선택하여 SNMP 트랩 대상을 제거하고 LAN **대상** 탭을 클릭한 다음 XClarity Administrator 인스턴스의 IP 주소를 가리키는 항목을 제거하십시오.

단계 4. 기본 메뉴에서 NTP **설정**을 선택한 다음 날짜와 시간을 수동으로 구성하거나 올바른 NTP 서버 주소를 제공하여 올바른 NTP 설정을 가지고 있는지 확인하십시오.

랙 또는 타워 서버 관리 해제

Lenovo XClarity Administrator의 관리에서 랙 또는 타워 서버를 제거할 수 있습니다. 이 프로세스를 *관리 해제*라고 합니다.

시작하기 전에

XClarity Administrator을(를) 사용하여 특정 기간 동안 오프라인 상태였던 장치를 자동으로 관리 해제할 수 있습니다. 기본적으로 이 기능은 사용 불가능하도록 설정되어 있습니다. 오프라인 장치 자동 관리 해제 기능을 사용하려면, XClarity Administrator 메뉴의 **하드웨어 → 새 장치 검색 및 관리**를 클릭한 다음, **오프라인 장치 관리 해제 기능을 사용할 수 없습니다** 옆의 **편집**을 클릭하십시오. 그러고 나서 **오프라인 장치 관리 해제 기능 사용**을 선택하고 시간 간격을 설정하십시오. 기본적으로 장치는 24시간 동안 오프라인 상태인 경우 관리 해제됩니다.

랙 또는 타워 서버를 관리 해제하기 전에 서버에 대해 실행 중인 활성 작업이 없어야 합니다.

랙 또는 타워 서버에서 서버 패턴과 가상 주소를 제거하는 경우 서버를 관리 해제하기 전에 서버 프로필을 비활성화하십시오(서버 프로필 비활성화 참조).

콜 홈이 XClarity Administrator에서 사용 설정된 경우 중복 문제 레코드가 작성되지 않도록 모든 관리되는 섀시와 서버에서 콜 홈이 사용 안 함으로 설정됩니다. XClarity Administrator를 사용한 장치 관리를 중단하려는 경우 나중에 개별 장치에 대해 콜 홈을 다시 사용 설정하는 대신 XClarity Administrator의 모든 관리되는 장치에서 콜 홈을 다시 사용 설정할 수 있습니다(XClarity Administrator 온라인 설명서에서 모든 관리 장치에서 콜 홈 다시 사용 가능하도록 설정 참조).

이 작업 정보

랙 또는 타워 서버를 관리 해제하면 Lenovo XClarity Administrator가 다음 작업을 수행합니다.

- 중앙 집중식 사용자 관리에 사용되는 구성을 지웁니다.
- XClarity Administrator 신뢰 저장소에서 베이스보드 관리 컨트롤러 보안 인증서를 제거합니다.
- 장치에서 Encapsulation을 사용할 수 있는 경우 장치 방화벽 규칙을 장치를 관리하기 전의 설정으로 구성합니다.
- XClarity Administrator가 더 이상 랙 또는 타워 서버에서 이벤트를 수신하지 않도록 XClarity Administrator 구성에 대한 CIM 구독을 제거합니다.
- 콜 홈이 현재 XClarity Administrator에서 사용 설정된 경우 랙 또는 타워 서버에서 콜 홈을 사용 안 함으로 설정합니다.
- 랙 또는 타워 서버에서 보낸 이벤트를 무시합니다. 이벤트를 Syslog와 같은 외부 리포지토리에 전달하여 이러한 이벤트를 유지할 수 있습니다(이벤트 전달 참조).

랙 또는 타워 서버를 관리 해제해도 XClarity Administrator는 서버에 대한 특정 정보를 유지합니다. 해당 정보는 동일한 랙 또는 타워 서버를 다시 관리할 때 다시 적용됩니다.

중요: ThinkServer 서버를 관리 해제하고 다른 XClarity Administrator 인스턴스를 사용하여 해당 서버를 관리하는 경우 서버에 대한 정보가 유실됩니다.

팁: 초기 설정 중에 선택적으로 추가되는 모든 데모 장치는 섀시의 노드입니다. 데모 장치를 관리 해제하려면 **장치에 연결할 수 없는 경우에도 강제로 관리 해제** 옵션을 사용하여 섀시를 관리 해제하십시오.

절차

랙 또는 타워 서버를 관리 해제하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하여 서버 페이지를 표시하십시오.

단계 2. 관리 해제할 하나 이상의 랙 또는 타워 서버를 선택하십시오.

단계 3. **관리 해제**를 클릭하십시오. 관리 해제 대화 상자가 표시됩니다.

단계 4. **옵션: 장치에 연결할 수 없는 경우에도 강제로 관리 해제**를 선택하십시오.

중요: 데모 하드웨어를 관리 해제하는 경우 이 옵션을 선택해야 합니다.

단계 5. **관리 해제**를 클릭하십시오.관리 해제 대화 상자에는 관리 해제 프로세스 각 단계의 진행상황이 표시됩니다.

단계 6. 관리 해제 프로세스가 완료되면 **확인**을 클릭하십시오.

제대로 관리 해제되지 않은 랙 또는 타워 서버 복구

Converged, NeXtScale, System x 또는 ThinkServer 서버가 제대로 관리 해제되지 않은 경우 이를 다시 관리하려면 먼저 서버를 복구해야 합니다.

강제 관리로 제대로 관리 해제되지 않은 랙 또는 타워 서버 복구

강제 관리 옵션으로 서버를 다시 관리하여 서버 관리를 복구할 수 있습니다.

절차

교체 Lenovo XClarity Administrator 인스턴스가 오류가 발생한 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 RECOVERY_ID 계정 및 암호와 **강제 관리** 옵션을 사용하여 장치를 다시 관리할 수 있습니다(서버 관리 참조).

관리 컨트롤러를 사용하여 제대로 관리 해제되지 않은 System x 또는 NeXtScale M4 서버 복구

관리 컨트롤러를 사용하여 System x 또는 NeXtScale M4 서버 관리를 복구할 수 있습니다.

절차

서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator에서 서버를 관리하기 전에 작성된 사용자 계정과 암호를 사용하여 관리 컨트롤러 웹 인터페이스에 로그인하십시오.

단계 2. SNMP 트랩 설정을 지우십시오.

a. **IMM 관리 → 네트워크**를 클릭하십시오.

b. SNMP 탭을 클릭하십시오.

c. **커뮤니티** 탭을 클릭하십시오.

d. 이전 XClarity Administrator의 커뮤니티 항목을 찾으십시오. 예를 들어 다음과 같습니다.
- **LXCA IP 주소:** 10.240.198.84
- **LXCA 호스트:** LXCA_maqCBIt86d
- **커뮤니티 2:**
- **커뮤니티 이름:** LXCA_maqCBIt86d
- **액세스 유형:** 트랩
- **특정 호스트가 이 커뮤니티의 트랩을 수신하도록 허용:** 10.240.198.84

e. 커뮤니티 항목의 필드에서 값을 제거하십시오.

f. **적용**을 클릭하십시오.

단계 3. 사용자 계정을 지우십시오.

a. IMM **관리** → **사용자**를 클릭하십시오.

b. **사용자 계정** 탭을 클릭하십시오.

c. 다음 접두사를 가진 사용자 계정을 포함하여 XClarity Administrator인 모든 사용자 계정을 삭제하십시오.
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

단계 4. Lenovo XClarity Administrator를 사용하여 서버를 관리하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **하드웨어** → **새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.

b. **수동 입력**을 선택하십시오.

c. **단일 시스템**을 클릭하고 관리할 서버의 IP 주소를 입력한 후 **확인**을 클릭하십시오.

d. 서버에 인증하기 위한 사용자 ID와 암호를 지정하십시오.

e. **관리**를 클릭하십시오.

   이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 진행상황을 모니터링하여 프로세스가 성공적으로 완료되는지 확인하십시오.

f. 프로세스가 완료되면 **확인**을 클릭하십시오.

관리 컨트롤러를 공장 출하 기본값으로 재설정하여 제대로 관리 해제되지 않은 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 복구

서버의 베이스보드 관리 컨트롤러(BMC)를 공장 출하 기본값으로 재설정하여 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 관리를 복구할 수 있습니다.

절차

서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. 장치에서 Encapsulation을 사용하는 경우 오류가 발생한 XClarity Administrator 가상 어플라이언스의 IP 주소를 사용하도록 구성된 시스템에서 대상 관리 컨트롤러에 연결하십시오.

단계 2. 관리 컨트롤러를 공장 출하 기본값으로 재설정하십시오.

a. XClarity Administrator에서 서버를 관리하기 전에 작성된 복구 사용자 계정과 암호를 사용하여 서버의 관리 컨트롤러 웹 인터페이스에 로그인하십시오.

b. IMM **관리 탭**을 클릭하십시오.

c. **공장 출하 기본값으로 IMM 다시 설정**을 클릭하십시오.

d. 재설정 작업을 확인하려면 **확인**을 클릭하십시오.

중요: BMC 구성이 완료되면 BMC가 다시 시작됩니다. 로컬 서버인 경우 TCP/IP 연결이 중단되며 연결을 복원하도록 네트워크 인터페이스를 다시 구성해야 합니다.

단계 3. 서버의 관리 컨트롤러 웹 인터페이스에 다시 로그온하십시오.

- BMC는 처음에 DHCP 서버의 IP 주소를 얻도록 구성되어 있습니다. 이 주소를 얻을 수 없는 경우 고정 IPv4 주소 192.168.70.125를 사용합니다.
- IMMBMC는 처음에 USERID 사용자 이름 및 PASSWORD(0 포함) 암호로 설정되어 있습니다. 이 기본 사용자 계정은 감독자 액세스 권한을 가지고 있습니다. 보안 강화를 위해 초기 구성 중에 이 사용자 이름과 암호를 변경하십시오.

단계 4. 연결을 복원하도록 네트워크 인터페이스를 다시 구성하십시오. 자세한 정보는 Integrated Management Module II 온라인 설명서의 내용을 참조하십시오.

단계 5. Lenovo XClarity Administrator를 사용하여 서버를 관리하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.

b. **수동 입력**을 선택하십시오.

c. **단일 시스템**을 클릭하고 관리할 서버의 IP 주소를 입력한 후 **확인**을 클릭하십시오.

d. 서버에 인증하기 위한 사용자 ID와 암호를 지정하십시오.

e. **관리**를 클릭하십시오.

이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 진행상황을 모니터링하여 프로세스가 성공적으로 완료되는지 확인하십시오.

f. 프로세스가 완료되면 **확인**을 클릭하십시오.

단계 6. 구성 패턴을 사용하여 서버를 구성한 경우 서버에 할당된 서버 프로필을 다시 활성화하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 프로필**을 클릭하십시오. 구성 패턴: 서버 프로필 페이지가 표시됩니다.

b. 서버 프로필을 선택하고 **서버 프로필 비활성화** 아이콘()을 클릭하십시오.

c. ITE **전원 끄기**를 클릭하여 서버 전원을 끄십시오. 서버 전원을 다시 켜면 가상 주소 할당이 번인(burn-in) 기본값으로 되돌아갑니다.

d. **비활성화**를 클릭하십시오. 프로필 상태 열에서 프로필 상태가 "비활성"으로 변경됩니다. 참고: 프로필이 비활성화되어도 서버는 해당 식별 정보(예, 호스트 이름, IP 주소, 가상 MAC 주소)를 유지합니다.

e. 서버 프로필을 다시 선택하고 **서버 프로필 활성화** 아이콘()을 클릭하십시오.

f. **활성화**를 클릭하여 서버의 서버 프로필을 활성화하십시오. 프로필 상태 열에서 프로필 상태가 "활성"으로 변경됩니다.

단계 7. 서버에 준수 정책을 할당한 경우 준수 정책을 다시 할당하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 적용/활성화**를 클릭하십시오. 관리되는 장치 목록이 있는 펌웨어 업데이트: 적용/활성화 페이지가 표시됩니다.

b. **할당된 정책** 열의 드롭다운 메뉴에서 서버에 적합한 정책을 선택하십시오.

cimcli를 사용하여 제대로 관리 해제되지 않은 ThinkSystem, Converged, NeXtScale, 또는 System x M5 또는 M6 서버 복구

`cimcli`로 CIM 구독을 제거하여 ThinkSystem, Converged, NeXtScale 또는 System x 서버 관리를 복구할 수 있습니다.

시작하기 전에

대상 서버에 대한 네트워크 액세스 권한이 있는 시스템에 cimcli 유틸리티가 있는 OpenPegasus가 설치되어야 합니다. OpenPegasus 다운로드, 구성 및 컴파일에 대한 정보는 Linux용 OpenPegasus 릴리스 RPM 웹 사이트의 내용을 참조하십시오.

참고: Red Hat Enterprise Linux(RHEL) Server 7 이상의 경우 OpenPegasus 소스 및 2진 RPM이 Red Hat 분배의 일부로 포함되어 있습니다. `top-pegasus-test.x86_64` 패키지에 cimcli 유틸리티가 있습니다.

이 작업 정보

서버가 복원된 후 서버를 다시 관리할 수 있습니다. 서버에 대한 모든 정보(예, 네트워크 설정, 서버 정책 및 펌웨어 준수 정책)는 유지됩니다.

절차

Lenovo XClarity Administrator 관리되는 인증을 사용하고 OpenPegasus가 설치된 서버에서 서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. 장치에서 Encapsulation을 사용으로 설정하는 경우:

a. 오류가 발생한 XClarity Administrator 가상 어플라이언스의 IP 주소를 사용하여 구성된 시스템에서 대상 서버로 연결하십시오.

b. 장치에 대한 SSH 세션을 열고 다음 명령을 실행하여 Encapsulation을 사용 안 함으로 설정하는 경우:
```
encaps lite off
```

단계 2. 다음 명령을 실행하여 CIM_ListenerDestinationCIMXML, CIM_Indicationfilter 및 CIM_IndicationSubscription의 CIM 인스턴스를 판별하십시오.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_IndicationSubscription
```

여기서 *<IP_address>*, *<user_ID>*, *<password>*는 관리 컨트롤러의 IP 주소, 사용자 ID, 암호입니다. 예를 들어, 다음과 같습니다.

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

단계 3. 다음 명령을 실행하여 CIM_ListenerDestinationCIMXML, CIM_Indicationfilter 및 CIM_IndicationSubscription의 CIM 인스턴스를 한 번에 하나씩 삭제하십시오.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s di '<cim_instance>'
```

여기서 *<IP_address>*, *<user_ID>*, *<password>*는 관리 컨트롤러의 IP 주소, 사용자 ID, 암호이고 *<cim_instance>*는 이전 단계에서 각 CIM 인스턴스에 대해 리턴된 정보입니다(큰따옴표로 묶임). 예를 들어, 다음과 같습니다.

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
```

```
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

단계 4. Lenovo XClarity Administrator를 사용하여 서버를 관리하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.

b. **수동 입력**을 선택하십시오.

c. **단일 시스템**을 클릭하고 관리할 서버의 IP 주소를 입력한 후 **확인**을 클릭하십시오.

d. 서버에 인증하기 위한 사용자 ID와 암호를 지정하십시오.

e. **관리**를 클릭하십시오.

이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 진행상황을 모니터링하여 프로세스가 성공적으로 완료되는지 확인하십시오.

f. 프로세스가 완료되면 **확인**을 클릭하십시오.

관리 컨트롤러 인터페이스를 사용하여 제대로 관리 해제되지 않은 ThinkServer 서버 관리 복구

관리 컨트롤러 웹 인터페이스를 사용하여 ThinkServer 서버 관리를 복구할 수 있습니다.

절차

서버 관리를 복구하려면 다음 단계를 완료하십시오.

단계 1. 관리자로 서버의 관리 컨트롤러 웹 인터페이스에 로그인하십시오(서버에 대한 관리 컨트롤러 인터페이스 실행 참조).

단계 2. 기본 메뉴에서 사용자를 선택한 다음 접두사가 "LXCA_"인 모든 사용자 계정을 제거하여 Lenovo XClarity Administrator에서 작성한 IPMI 계정을 제거하십시오.

또는 계정 사용자 이름을 바꾸어 "LXCA_" 접두사를 제거할 수 있습니다.

단계 3. 기본 메뉴에서 PEF **관리**를 선택하여 SNMP 트랩 대상을 제거하고 LAN **대상** 탭을 클릭한 다음 XClarity Administrator 인스턴스의 IP 주소를 가리키는 항목을 제거하십시오.

단계 4. 기본 메뉴에서 NTP **설정**을 선택한 다음 날짜와 시간을 수동으로 구성하거나 올바른 NTP 서버 주소를 제공하여 올바른 NTP 설정을 가지고 있는지 확인하십시오.

제 9 장 저장 장치 관리

Lenovo XClarity Administrator은(는) Lenovo Storage, Flex System 스토리지 시스템 및 테이프 라이브러리 등 여러 유형의 스토리지 장치를 관리할 수 있습니다.

자세히 알아보기: XClarity Administrator: 검색

시작하기 전에

주의: 스토리지 장치를 관리하기 전에 스토리지 관리 고려사항의 내용을 검토하십시오.

참고: Flex System 스토리지 장치는 해당 장치가 포함된 섀시를 관리할 때 자동으로 검색되고 관리됩니다. Flex System 스토리지 장치를 섀시와 별도로 검색하고 관리할 수 없습니다.

특정 포트가 장치와 통신 가능해야 합니다. 스토리지 장치 관리를 시도하기 전에 필요한 모든 포트가 사용 가능해야 합니다. 포트에 대한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

XClarity Administrator를 사용하여 관리하려는 각 스토리지 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: 랙 스토리지 장치(ThinkSystem DE 시리즈 이외)를 검색하고 관리하기 전에, 다음 요구사항을 충족해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치를 검색할 수 없음 및 장치를 관리할 수 없음의 내용을 참조하십시오.

- 네트워크 구성은 XClarity Administrator와 랙 스토리지 장치 간에 SLP 트래픽을 허용해야 합니다.
- 유니캐스트 SLP가 필요합니다.
- XClarity Administrator가 Lenovo Storage 장치를 자동으로 검색하도록 하려면 멀티캐스트 SLP가 필요합니다. 또한 SLP는 랙 스토리지 장치에서 사용 가능해야 합니다.

이 작업 정보

XClarity Administrator는 XClarity Administrator와 동일한 IP 서브넷에 있는 관리 가능 장치를 프로브하여 사용자 환경에서 스토리지 장치를 자동으로 검색할 수 있습니다. 다른 서브넷에 있는 스토리지 장치를 검색하려면 IP 주소 또는 IP 주소 범위를 지정하거나 스프레드시트에서 정보를 가져오십시오.

스토리지 장치가 XClarity Administrator에서 관리되면 XClarity Administrator는 관리되는 각 스토리지 장치를 주기적으로 폴링하여 인벤토리, 필수 제품 데이터 및 상태와 같은 정보를 수집합니다. 관리되는 각 스토리지 장치를 보고 모니터할 수 있으며, 관리 작업(예, 시스템 설정 구성, 펌웨어 업데이트 및 전원 켜기와 끄기)을 수행할 수 있습니다.

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 스토리지 장치를 관리하도록 하려면 먼저 초기 XClarity Administrator에서 장치를 관리 해제하고 이를 새 XClarity Administrator에서 관리하도록 설정하십시오. 관리 해제 프로세스 중에 오류가 발생하는 경우 새 XClarity Administrator에서 관리 중에 **강제 관리** 옵션을 선택할 수 있습니다.

참고: 관리 가능한 장치에 대한 네트워크를 검색하는 경우 XClarity Administrator는 장치 관리를 시도한 후까지 다른 관리자가 이미 장치를 관리하고 있는지 확인할 수 없습니다.

절차

XClarity Administrator을(를) 사용하여 스토리지 장치를 관리하려면 다음 절차 중 하나를 완료하십시오.

- 일괄 가져오기 파일을 사용하여 다수의 스토리지 장치 및 다른 유형의 장치를 검색하고 관리하십시오(XClarity Administrator 온라인 설명서의 시스템 관리 참조).
- XClarity Administrator와 동일한 IP 서브넷에 있는 스토리지 장치를 검색하고 관리하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 새 장치 검색 및 관리 페이지가 표시됩니다.

  관리할 스토리지 장치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 필터와 스토리지 시스템을 상세하게 필터링할 수도 있습니다. **열 사용자 지정** 아이콘( )을 클릭하여 표시되는 열과 기본 정렬 순서를 변경할 수 있습니다.
  2. **새로 고침** 아이콘( )을 클릭하여 XClarity Administrator 도메인의 모든 관리 가능 장치를 검색하십시오. 검색에는 몇 분 정도 소요됩니다.
  3. 관리할 하나 이상의 스토리지 장치를 선택하십시오.
  4. **선택 관리**을 클릭하십시오. 관리 대화 상자가 표시됩니다.
  5. 스토리지 장치에 인증하기 위한 사용자 ID와 암호를 지정하십시오.

     팁: 감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우 관리에 실패하거나 성공하더라도 장치의 기타 향후 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).
  6. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

참고:

- 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
- 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

7. **관리**를 클릭하십시오.

   이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 진행상황을 모니터링하십시오.

8. 프로세스가 완료되면 **확인**을 클릭하십시오.

   장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

   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.

- 수동으로 IP 주소를 지정하여 XClarity Administrator와 동일한 IP 서브넷에 있지 않은 스토리지 장치를 검색하고 관리하십시오.

  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.
  2. **수동 입력**을 선택하십시오.
  3. 관리할 스토리지 장치의 네트워크 주소를 지정하십시오.
     - **단일 시스템**을 클릭하고 단일 IP 주소 도메인 이름 또는 완전한 도메인 이름(FQDN)을 입력하십시오.

       참고: FQDN을 지정하려면 네트워크 액세스 페이지에 올바른 도메인 이름이 지정되어 있어야 합니다(네트워크 액세스 구성 참조).
     - **다중 시스템**을 클릭하고 IP 주소의 범위를 입력하십시오. 다른 범위를 추가하려면 **추가** 아이콘(➕)을 클릭하십시오. 범위를 제거하려면 **제거** 아이콘(✖)을 클릭하십시오.
  4. **확인**을 누르십시오.
  5. 스토리지 장치에 인증하기 위한 사용자 ID와 암호를 지정하십시오.

     팁: 감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우 관리에 실패하거나 성공하더라도 장치의 기타 향후 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).
  6. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

     참고:

     - 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.

- 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

7. **관리**를 클릭하십시오.

   이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 진행상황을 모니터링하십시오.

8. 프로세스가 완료되면 **확인**을 클릭하십시오.

   장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

   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.

완료한 후에

- 추가 장치를 검색 및 관리하십시오.
- 현재 정책을 준수하지 않는 장치에서 펌웨어를 업데이트하십시오(관리 장치에서 펌웨어 업데이트 참조).
- 물리적 환경을 반영하도록 새 장치를 적합한 랙에 추가하십시오(랙 관리 참조).
- 하드웨어 상태 및 세부 정보를 모니터링하십시오(스토리지 장치의 상태 보기 참조).
- 이벤트 및 경고를 모니터링하십시오(이벤트 작업 및 경고 작업 참조).

스토리지 관리 고려사항

스토리지 장치를 관리하기 전에, 다음 관리 고려사항을 검토하십시오.

포트 요구사항에 대한 정보는 Lenovo XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

중요: 랙 스토리지 장치(ThinkSystem DE 시리즈 이외)를 검색하고 관리하기 전에, 다음 요구사항을 충족해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 장치를 검색할 수 없음 및 장치를 관리할 수 없음의 내용을 참조하십시오.

- 네트워크 구성은 XClarity Administrator와 랙 스토리지 장치 간에 SLP 트래픽을 허용해야 합니다.
- 유니캐스트 SLP가 필요합니다.
- XClarity Administrator가 Lenovo Storage 장치를 자동으로 검색하도록 하려면 멀티캐스트 SLP가 필요합니다. 또한 SLP는 랙 스토리지 장치에서 사용 가능해야 합니다.

Lenovo Storage 장치의 경우, 시스템 수준 공기 온도는 시스템의 미드플레인에 가까운 온도 센서로 측정되고 이는 공기 흐름이 드라이브를 통과한 후의 주변 온도를 반영합니다. 온도가 다른 시점에서 측정되면 XClarity Administrator와 관리 컨트롤러에서 보고되는 공기 온도가 다를 수 있음을 주의하십시오.

Lenovo DE 시리즈 스토리지 장치의 경우 초기 관리 중에 네트워크에서 두 관리 컨트롤러에 모두 연결할 수 있어야 합니다.

일부 저장 장치의 경우, SNMP 트랩은 영어로만 제공됩니다.

스토리지 장치의 상태 보기

Lenovo XClarity Administrator에서 관리되는 스토리지 장치의 요약 및 세부적인 상태를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

이 작업 정보

다음 상태 아이콘은 장치의 전반적인 상태를 나타내는 데 사용됩니다. 인증서가 일치하지 않으면 적용 가능한 각 장치의 상태에 "(신뢰할 수 없음)"이 추가됩니다. 예를 들어 경고(신뢰할 수 없음)이 표시됩니다. 연결 문제가 있거나 장치에 대한 연결을 신뢰할 수 없는 경우 적용 가능한 각 장치의 상태에 "(연결)"이 추가됩니다. 예를 들어 경고(연결)이 표시됩니다.

- ( ) 위험
- ( ) 경고
- ( ) 보류 중
- ( ) 정보
- ( ) 정상
- ( ) 오프라인
- ( ) 알 수 없음

절차

관리되는 스토리지 장치의 상태를 보려면 다음 작업 중 하나 이상을 완료하십시오.

- Lenovo XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 대시보드 페이지에는 모든 관리 스토리지 장치 및 기타 리소스에 대한 개요와 상태가 표시됩니다.

- Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스토리지 장치의 표 보기와 함께 스토리지 페이지가 표시됩니다.

  관리할 스토리지 장치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하고 상태 아이콘을 클릭하여 선택한 기준을 충족하는 스토리지 장치만 나열하십시오.

  이 페이지에서 다음 작업을 수행할 수 있습니다.

  - 스토리지 장치 및 해당 구성 요소에 대한 자세한 정보를 보십시오(스토리지 장치의 세부 정보 보기 참조).
  - **모든 작업 → 보기 → 랙 보기에 표시** 또는 **모든 작업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 스토리지 장치를 봅니다.
  - **IP 주소** 링크를 클릭하여 스토리지 장치의 관리 컨트롤러 웹 인터페이스를 실행합니다(스토리지 장치에 대한 관리 컨트롤러 인터페이스 실행 참조).
  - 스토리지 장치에서 스토리지 컨트롤러의 전원을 켜고 끕니다(스토리지 장치 전원 켜기 및 끄기 참조).
  - 스토리지 장치를 선택하고 **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 시스템 정보를 수정합니다.
  - 스토리지 장치를 선택하고 **모든 작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 인벤토리를 새로 고칩니다.

- 스토리지 장치를 선택하고 **모든 작업 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 하나 이상의 스토리지 장치에 대한 자세한 정보를 단일 CSV 파일로 내보냅니다.

  참고: 한 번에 최대 60대의 장치에 대한 인벤토리 데이터를 내보낼 수 있습니다.

  팁: CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- 스토리지 장치를 관리 해제하십시오(스토리지 장치 관리 해제 참조).
- (Flex System 스토리지 장치만 해당) 스토리지 장치에서 가상으로 스토리지 컨트롤러를 재배치합니다(Flex System 스토리지 장치에서 가상으로 스토리지 컨트롤러 재배치 참조).
- **이벤트 제외** 아이콘()을 클릭하여 이벤트가 표시되는 모든 페이지에서 관심이 없는 이벤트를 제외합니다. 이벤트 제외의 내용을 참조하십시오.
- 스토리지 장치를 선택하고 **모든 작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 스토리지 장치가 설치된 섀시에서 Lenovo XClarity Administrator 보안 인증서와 CMM 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).
- **모든 작업 → 그룹 → 그룹에 추가** 또는 **모든 작업 → 그룹 → 그룹에서 제거**를 클릭하여 정적 리소스 그룹에서 스토리지 장치를 추가하거나 제거합니다.

스토리지 장치의 세부 정보 보기

Lenovo XClarity Administrator에서 IP 주소, 제품 이름, 일련 번호 및 각 캐니스터의 세부 정보를 포함하여 관리되는 스토리지 장치에 대한 자세한 정보를 볼 수 있습니다.

이 작업 정보

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

Lenovo Storage 장치의 경우, 시스템 수준 공기 온도는 시스템의 미드플레인에 가까운 온도 센서로 측정되고 이는 공기 흐름이 드라이브를 통과한 후의 주변 온도를 반영합니다. 온도가 다른 시점에서 측정되면 XClarity Administrator와 관리 컨트롤러에서 보고되는 공기 온도가 다를 수 있음을 주의하십시오.

절차

특정 관리 스토리지 장치의 세부 정보를 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스토리지 장치의 표 보기와 함께 스토리지 페이지가 표시됩니다.

특정 스토리지 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 스토리지 장치를 상세하게 필터링할 수도 있습니다.

단계 2. **스토리지** 열에서 스토리지 장치 이름을 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스토리지 장치에 설치된 구성 요소 목록과 서버 속성이 표시됩니다.

단계 3. 스토리지 세부 정보를 보려면 다음 작업 중 하나 이상을 완료하십시오. 표시되는 데이터는 스토리지 장치 유형에 따라 다를 수 있습니다.

- **요약**을 클릭하여 시스템 정보 및 설치된 장치를 포함하여 서버 및 설치된 해당 구성 요소의 요약 정보를 확인합니다(스토리지 장치의 상태 보기 참조).
- **인벤토리 세부 정보**를 클릭하여 다음과 같은 스토리지 장치 구성 요소에 대한 세부 정보를 보십시오.
  - 스토리지 장치의 펌웨어 수준.
  - 관리 컨트롤러 네트워크의 세부 정보(예, 호스트 이름, IPv4 주소, IPv6 주소 및 MAC 주소).
  - 스토리지 장치의 자산 세부 정보.
  - 스토리지 장치의 각 캐니스터에 대한 세부 정보.

  팁: Flex System Storage Expansion Node 또는 Flex System PCIe Expansion Node 등의 확장 노드가 섀시에 설치되어 있고 스토리지 장치에 연결된 경우 확장 노드의 인벤토리 세부 정보도 표시됩니다.
- **경고**를 클릭하여 경고 목록에서 스토리지 장치와 관련된 경고를 표시합니다(경고 작업 참조).
- **이벤트 로그**를 클릭하여 이벤트 로그에서 스토리지 장치 스토리지 장치와 관련된 이벤트를 표시합니다(이벤트 작업 참조).

- **작업**을 클릭하여 스토리지 장치와 관련된 작업 목록을 표시합니다(작업 모니터링 참조).
- Light Path를 클릭하여 스토리지 장치에 있는 각 LED의 현재 상태를 표시합니다.
- **전원 및 열**을 클릭하여 스토리지 장치의 전원 및 열 특성을 표시합니다.

  팁: 최신 전원 및 열 데이터를 수집하려면 웹 브라우저의 새로 고침 버튼을 사용하십시오. 데이터를 수집하려면 몇 분 정도가 걸릴 수 있습니다.

완료한 후에

스토리지 장치에 대한 요약 및 자세한 정보를 표시하는 것 외에도 다음 작업을 수행할 수 있습니다.

- **작업 → 보기 → 랙 보기에 표시** 또는 **작업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 스토리지 장치를 봅니다.
- **동작 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 스토리지 장치에 대한 자세한 정보를 CSV 파일로 내보냅니다.

  참고:

  – CSV 파일의 인벤토리 데이터에 대한 자세한 정보는 Lenovo XClarity Administrator 온라인 설명서에서 GET /storage/*<UUID_list>* REST API의 내용을 참조하십시오.

  – CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- IP 주소 링크를 클릭하여 스토리지 장치의 관리 컨트롤러 웹 인터페이스를 실행합니다(스토리지 장치에 대한 관리 컨트롤러 인터페이스 실행 참조).
- 스토리지 장치에서 스토리지 컨트롤러의 전원을 켜고 끕니다(스토리지 장치 전원 켜기 및 끄기 참조).
- 스토리지 장치에서 가상으로 스토리지 컨트롤러를 재배치합니다(가상으로 Flex System 섀시에서 서버 재배치 참조).
- 스토리지 장치를 선택하고 **속성 편집**을 클릭하여 시스템 정보를 수정합니다.
- 스토리지 장치를 선택하고 **작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 인벤토리를 새로 고칩니다.
- **작업 → 서비스 재설정 → 이벤트 제외**를 클릭하여 이벤트가 표시되는 모든 페이지에서 관심이 없는 이벤트를 제외합니다(이벤트 제외 참조).
- 스토리지 장치를 선택하고 **작업 → 서비스 → 신뢰할 수 없는 인증서 해결**을 클릭하여 스토리지 장치가 설치된 섀시에서 XClarity Administrator 보안 인증서와 CMM 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).

스토리지 구성 데이터 백업 및 복원

Lenovo XClarity Administrator에는 스토리지 구성 데이터에 대한 기본 제공 백업 기능이 포함되어 있지 않습니다. 대신 관리되는 스토리지 장치에 사용할 수 있는 백업 기능을 사용하십시오.

장치 복구에 대한 정보는 스토리지 장치와 함께 제공된 제품 설명서를 참조하십시오.
- Lenovo Storage 장치의 경우 Lenovo Storage S2200/S3200 제품 설명서의 내용을 참조하십시오.
- Lenovo ThinkSystem 스토리지 장치의 경우 ThinkSystem Storage 제품 설명서의 내용을 참조하십시오.

스토리지 장치 전원 켜기 및 끄기

Lenovo XClarity Administrator에서 스토리지 장치 전원을 켜고 끌 수 있습니다.

이 작업 정보

Flex System 스토리지 장치의 경우 스토리지 컨트롤러 전원이 꺼지면 먼저 데이터가 내부 드라이브에 저장되고 스토리지 장치가 대기 상태가 됩니다. 대기 상태에서는 스토리지 장치에서 제공되는 볼륨에 더 이상 액세스할 수 없습니다.

ThinkSystem DM 시리즈 스토리지 장치의 전원을 켜려면, 관리에 사용되는 스토리지 장치 컨트롤러가 온라인 상태이고 해당 IP 주소가 외부 네트워크를 통해 전원이 꺼진 저장 장치 컨트롤러의 서비스 프로세서와 직접 통신할 수 있는지 확인하십시오.

절차

관리되는 스토리지 장치 전원을 켜고 끄려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스토리지 장치의 표 보기와 함께 스토리지 페이지가 표시됩니다.

특정 스토리지 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 스토리지 장치를 상세하게 필터링할 수도 있습니다.

단계 2. 전원을 켜거나 끌 스토리지 장치를 선택하십시오.

단계 3. **모든 작업**을 클릭하고 다음 전원 작업 중 하나를 클릭하십시오.
- **컨트롤러 A 전원 켜기**
- **컨트롤러 B 전원 켜기**
- **컨트롤러 A 전원 끄기**
- **컨트롤러 B 전원 끄기**
- **컨트롤러 A 다시 시작**
- **컨트롤러 B 다시 시작**

Flex System 스토리지 장치에서 가상으로 스토리지 컨트롤러 재배치

가상 재배치를 수행하여 스토리지 장치 베이에서 스토리지 컨트롤러(캐니스터) 제거 및 재삽입을 시뮬레이션할 수 있습니다.

이 작업 정보

가상 재배치 중에는 스토리지 장치에 대한 기존의 모든 네트워크 연결이 끊어지고 스토리지 장치의 전원 상태가 변경됩니다. 가상 재배치를 수행하기 전에 모든 사용자 데이터를 저장했는지 확인하십시오.

절차

스토리지 컨트롤러를 가상으로 재배치하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하십시오. 모든 스토리지 장치의 표 보기와 함께 스토리지 페이지가 표시됩니다.

특정 스토리지 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 스토리지 장치를 상세하게 필터링할 수도 있습니다.

단계 2. Flex System 스토리지 장치를 선택하십시오.

단계 3. **모든 작업 → 서비스**를 클릭한 다음 **컨트롤러 A 가상 재배치** 또는 **컨트롤러 B 가상 재배치**를 클릭하십시오.

단계 4. **가상 재배치**를 클릭하십시오.

스토리지 장치에 대한 관리 컨트롤러 인터페이스 실행

Lenovo XClarity Administrator에서 스토리지 장치가 설치된 섀시에 대해 관리 컨트롤러 웹 인터페이스를 실행할 수 있습니다.

절차

관리 컨트롤러 웹 인터페이스를 실행하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하십시오. 관리되는 모든 스토리지 장치의 표 보기와 함께 스토리지 페이지가 표시됩니다.

특정 스토리지 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예: 장치 이름 또는 IP 주소)를 입력하여 표시되는 스토리지 장치를 상세하게 필터링할 수도 있습니다.

단계 2. 스토리지 장치를 선택하십시오.

단계 3. **작업 → 실행 → 관리 웹 인터페이스**를 클릭하십시오. 관리 컨트롤러 웹 인터페이스가 시작됩니다.

단계 4. 관리 컨트롤러 인터페이스에 로그인하십시오.

참고: Flex System 스토리지 장치의 경우 XClarity Administrator 사용자 자격 증명을 사용하십시오.

스토리지 장치에 대한 시스템 속성 수정

특정 스토리지 장치에 대한 시스템 속성을 수정할 수 있습니다.

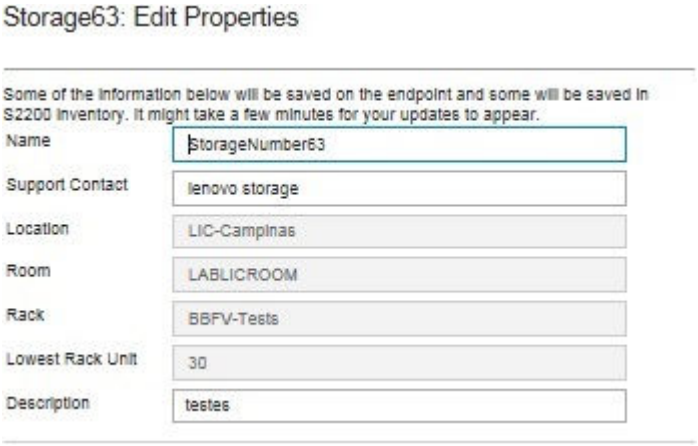
절차

시스템 속성을 수정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하여 스토리지 페이지를 표시하십시오.

단계 2. 업데이트할 스토리지 장치를 선택하십시오.

단계 3. **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 편집 대화 상자를 표시하십시오.



단계 4. 필요 시 다음 정보를 변경하십시오.
- 이름
- 지원 문의
- 설명

참고: XClarity Administrator는 랙에서 장치를 추가하거나 제거할 때 위치, 룸, 랙 및 LRU(lowest rack unit) 속성을 웹 인터페이스에서 업데이트합니다(랙 관리 참조).

단계 5. **저장**을 클릭하십시오.

참고: 이러한 속성을 변경하는 경우 XClarity Administrator 웹 인터페이스에 변경 사항이 표시되기 전에 약간의 지연이 있을 수 있습니다.

관리 서버 오류 후 랙 스토리지 장치 관리 복구

랙 스토리지 장치가 제대로 관리 해제되지 않은 경우 이를 다시 관리하려면 먼저 스토리지 장치를 복구해야 합니다. 이전에 Lenovo XClarity Administrator에서 설정한 스토리지 장치 구성의 특정 부분을 제거하여 관리를 복구할 수 있습니다.

절차

랙 스토리지 장치를 복구하려면 다음 단계 중 하나를 완료하십시오.

- 교체 XClarity Administrator 인스턴스가 오류가 발생한 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 **강제 관리** 옵션을 사용하여 장치를 다시 관리할 수 있습니다(저장 장치 관리 참조).
- 접두사가 "LXCA_"인 모든 사용자 계정을 제거하고, 스토리지 장치에서 접두사가 "SYSMGR_"이고 유형이 "SNMPv3"인 사용자 계정을 선택적으로 제거하십시오.

완료한 후에

XClarity Administrator가 복원되거나 교체된 후 스토리지 장치를 다시 관리할 수 있습니다(저장 장치 관리 참조). 스토리지 장치에 대한 모든 정보(예, 시스템 속성)는 유지됩니다.

관리 서버 장애 후 Lenovo ThinkSystem DE 시리즈 스토리지 장치로 관리 복구

Lenovo ThinkSystem DE 시리즈 랙 스토리지 장치가 제대로 관리 해제되지 않은 경우, 이를 다시 관리하려면 먼저 스토리지 장치를 복구해야 합니다. 이전에 Lenovo XClarity Administrator에서 설정한 스토리지 장치 구성의 특정 부분을 제거하여 관리를 복구할 수 있습니다.

절차

Lenovo ThinkSystem DE 시리즈 스토리지 장치를 복구하려면, 다음 단계 중 하나를 완료하십시오.

- 교체 XClarity Administrator 인스턴스가 오류가 발생한 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 **강제 관리** 옵션을 사용하여 장치를 다시 관리할 수 있습니다(저장 장치 관리 참조).
- 스토리지 장치 키-쌍 API에서 "LXCA_REMOTE_MANAGMENT_VERIFICATION" 키-쌍 레지스터를 제거하십시오.

완료한 후에

XClarity Administrator가 복원되거나 교체된 후 스토리지 장치를 다시 관리할 수 있습니다(저장 장치 관리 참조). 스토리지 장치에 대한 모든 정보(예, 시스템 속성)는 유지됩니다.

스토리지 장치 관리 해제

Lenovo XClarity Administrator(으)로 관리에서 스토리지 장치를 제거할 수 있습니다. 이 프로세스를 *관리 해제*라고 합니다.

시작하기 전에

스토리지 장치를 관리 해제하기 전에 스위치에 대해 실행 중인 활성 작업이 없는지 확인하십시오.

이 작업 정보

스토리지 장치를 관리 해제해도 XClarity Administrator는 스토리지 장치 대한 특정 정보를 유지합니다. 해당 정보는 동일한 스토리지 장치를 다시 관리할 때 다시 적용됩니다.

팁: 초기 설정 중에 선택적으로 추가되는 모든 데모 장치는 섀시의 노드입니다. 데모 장치를 관리 해제하려면 **장치에 연결할 수 없는 경우에도 강제로 관리 해제** 옵션을 사용하여 섀시를 관리 해제하십시오.

절차

스토리지 장치를 관리 해제하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스토리지**를 클릭하여 스토리지 페이지를 표시하십시오.

단계 2. 관리되는 스위치 목록에서 하나 이상의 관리되는 장치를 선택하십시오.

단계 3. **관리 해제**를 클릭하십시오. 관리 해제 대화 상자가 표시됩니다.

단계 4. **옵션: 장치에 연결할 수 없는 경우에도 강제로 관리 해제**를 선택하십시오.

중요: 데모 하드웨어를 관리 해제하는 경우 이 옵션을 선택해야 합니다.

단계 5. **관리 해제**를 클릭하십시오.관리 해제 대화 상자에는 관리 해제 프로세스 각 단계의 진행상황이 표시됩니다.

단계 6. 관리 해제 프로세스가 완료되면 **확인**을 클릭하십시오.

제대로 관리 해제되지 않은 랙 스토리지 장치 복구

Lenovo XClarity Administrator에서 랙 스토리지 장치를 관리하는 경우 및 XClarity Administrator에 오류가 발생하는 경우 관리 서버가 복원되거나 교체되기 전에는 관리 기능을 복구할 수 있습니다. 이전에 XClarity Administrator에서 설정한 스토리지 장치 구성의 특정 부분을 제거하여 시스템 관리를 복구할 수 있습니다.

절차

랙 스토리지 장치를 복구하려면 다음 단계 중 하나를 완료하십시오.

- 교체 XClarity Administrator 인스턴스가 오류가 발생한 XClarity Administrator와 동일한 IP 주소를 사용하는 경우 **강제 관리** 옵션을 사용하여 장치를 다시 관리할 수 있습니다(저장 장치 관리 참조).
- 접두사가 "LXCA_"인 모든 사용자 계정을 제거하고, 스토리지 장치에서 접두사가 "SYSMGR_"이고 유형이 "SNMPv3"인 사용자 계정을 선택적으로 제거하십시오.

완료한 후에

XClarity Administrator가 복원되거나 교체된 후 스토리지 장치를 다시 관리할 수 있습니다(저장 장치 관리 참조). 스토리지 장치에 대한 모든 정보(예, 시스템 속성)는 유지됩니다.

제 10 장 스위치 관리

Lenovo XClarity Administrator는 네트워크 스위치를 관리할 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 검색
- XClarity Administrator: 스위치 관리

시작하기 전에

주의: 스위치를 관리하기 전에 스위치 관리 고려사항을 검토하십시오. 정보는 스위치 관리 고려사항의 내용을 참조하십시오.

참고: Flex 스위치는 해당 노드가 포함된 섀시를 관리할 때 자동으로 검색되고 관리됩니다. Flex 스위치를 섀시와 별도로 검색하고 관리할 수 없습니다.

특정 포트가 스위치와 통신 가능해야 합니다. 스위치 관리를 시도하기 전에 필요한 모든 포트가 사용 가능해야 합니다. 포트에 대한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

XClarity Administrator를 사용하여 관리하려는 각 스위치에 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.

랙 스위치를 관리하려면 먼저 XClarity Administrator에 저장된 자격 증명을 만들어야 합니다. XClarity Administrator는 저장된 자격 증명만 사용하여 랙 스위치를 인증합니다. 저장된 자격 증명은 장치의 활성 사용자 계정과 일치해야 합니다. 관리 대화 상자 또는 저장된 자격 증명 페이지에서 저장된 자격 증명을 만들 수 있습니다. 자세한 정보는 저장된 자격 증명 관리의 내용을 참조하십시오.

루프백 인터페이스를 사용하는 관리는 모든 RackSwitch 장치에서 지원됩니다. 고정 경로를 추가하거나 라우팅 프로토콜을 통해 주소를 알리는 방법으로 XClarity Administrator가 루프백 인터페이스에 연결되어 있는지 확인하십시오. 관리 포트와 *어떤* 데이터 포트(루프백 포함) 사이에서도 라우팅을 수행 할 수 없습니다.

Lenovo ThinkSystem DB 시리즈 스위치의 경우:

- FOS 8.2.3 이상이 필요합니다.
- 스위치에서 다음 명령을 실행하여 스위치를 관리하기 *전에* 스위치의 인덱스 1에 SNMPv3 사용자를 구성해야 합니다. `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw`
- 스위치에 REST가 사용 설정되어 있는지 확인하십시오. REST를 사용하려면 다음 명령을 실행하십시오. `mgmtapp --enable rest`
- 허용되는 REST 세션 수가 10인지 확인합니다. REST 세션 수를 설정하려면 다음 명령을 실행하십시오. `mgmtapp --config -maxrestsession 10`
- Lenovo ThinkSystem DB 시리즈 스위치는 서비스 검색 프로토콜을 사용하여 검색할 수 없습니다. 이러한 스위치를 관리하려면 **수동 입력** 옵션을 사용하여 **장치 유형 식별을 위한 사용자 서비스 검색 프로토콜**을 지운 다음 **장치 유형** 목록에서 "Lenovo ThinkSystem DB 시리즈 스위치"를 선택합니다. 자세한 내용은 XClarity Administrator과(와) 동일한 IP 서브넷에 있지 않은 스위치 검색 및 관리에 대한 아래 절차를 참고하십시오.

NVIDIA 스위치의 경우:

- Cumulus 4.3 이상이 필요합니다.
- NVIDIA 스위치는 서비스 검색 프로토콜을 사용하여 검색할 수 없습니다. 이러한 스위치를 관리하려면 **수동 입력** 옵션을 사용하여 장치 유형 식별을 위한 사용자 서비스 검색 프로토콜을 지운 다음 **장치 유형** 목록에서 "NVIDIA 스위치"를 선택합니다. 자세한 내용은 XClarity Administrator와 동일한 IP 서브넷에 있지 않은 스위치 검색 및 관리에 대한 아래 절차를 참조하십시오.

이 작업 정보

XClarity Administrator는 XClarity Administrator와 동일한 IP 서브넷에 있는 관리 가능 장치를 프로브하여 사용자 환경에서 RackSwitch 스위치를 자동으로 검색할 수 있습니다. 다른 서브넷에 있는 스위치를 검색하려면 IP 주소 또는 IP 주소 범위를 지정하거나 스프레드시트에서 정보를 가져오십시오.

참고: 수동 자격 증명은 XClarity Administrator의 랙 스위치에는 지원되지 않습니다.

스위치가 XClarity Administrator에서 관리되면 XClarity Administrator는 관리되는 각 스위치를 주기적으로 폴링하여 인벤토리, 필수 제품 데이터 및 상태와 같은 정보를 수집합니다. 관리되는 각 스위치를 보고 모니터하고, 관리 작업(예, 관리 콘솔 실행과 전원 켜기 및 끄기)을 수행할 수 있습니다.

관리 프로세스 중에 인벤토리를 수집하는 동안 XClarity Administrator와 스위치의 통신 연결이 끊어진 경우(예, 전력 손실 또는 네트워크 장애로 인한 끊김, 또는 스위치가 오프라인인 경우) 관리는 성공적으로 완료되지만 일부 인벤토리 정보가 완전하지 않을 수 있습니다. 스위치가 온라인 상태가 되어 XClarity Administrator가 인벤토리 정보를 얻기 위해 스위치를 폴링할 때까지 기다리거나, 스위치를 선택한 후 **모든 작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 스위치 페이지에서 스위치에 대한 인벤토리를 수동으로 수집하십시오.

참고: 스위치를 스택할 수 있습니다. ***스택 스위치***는 단일 네트워크 스위치로 작동하는 스위치 그룹입니다. 스택에는 ***마스터 스위치***와 하나 이상의 ***멤버 스위치***가 포함됩니다. Flex 스위치의 경우 스택에서 각 스위치를 보고 모니터할 수 있으며 진단 데이터를 수집할 수 있습니다. 그러나 스택 스위치에서 관리 작업(예, 펌웨어 업데이트 및 서버 구성)을 수행할 수는 없습니다. 이러한 XClarity Administrator 관리 작업은 마스터 스위치를 비롯한 모든 스택 스위치에서 사용 불가능합니다. 마스터 스위치 CLI에서 스택 스위치의 펌웨어를 직접 업데이트할 수 있습니다. RackSwitch 스위치의 경우 마스터 스위치 정보만 보고 모니터링할 수 있습니다. 멤버 스위치는 XClarity Administrator에 의해 검색되지 않습니다.

관리 작업은 보호 모드인 Flex 스위치의 경우에도 사용 불가능합니다.

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 스토리지 장치를 관리하도록 하려면 먼저 초기 XClarity Administrator에서 장치를 관리 해제하고 이를 새 XClarity Administrator에서 관리하도록 설정하십시오. 관리 해제 프로세스 중에 오류가 발생하는 경우 새 XClarity Administrator에서 관리 중에 **강제 관리** 옵션을 선택할 수 있습니다.

참고: 관리 가능한 장치에 대한 네트워크를 검색하는 경우 XClarity Administrator는 장치 관리를 시도한 후까지 다른 관리자가 이미 장치를 관리하고 있는지 확인할 수 없습니다.

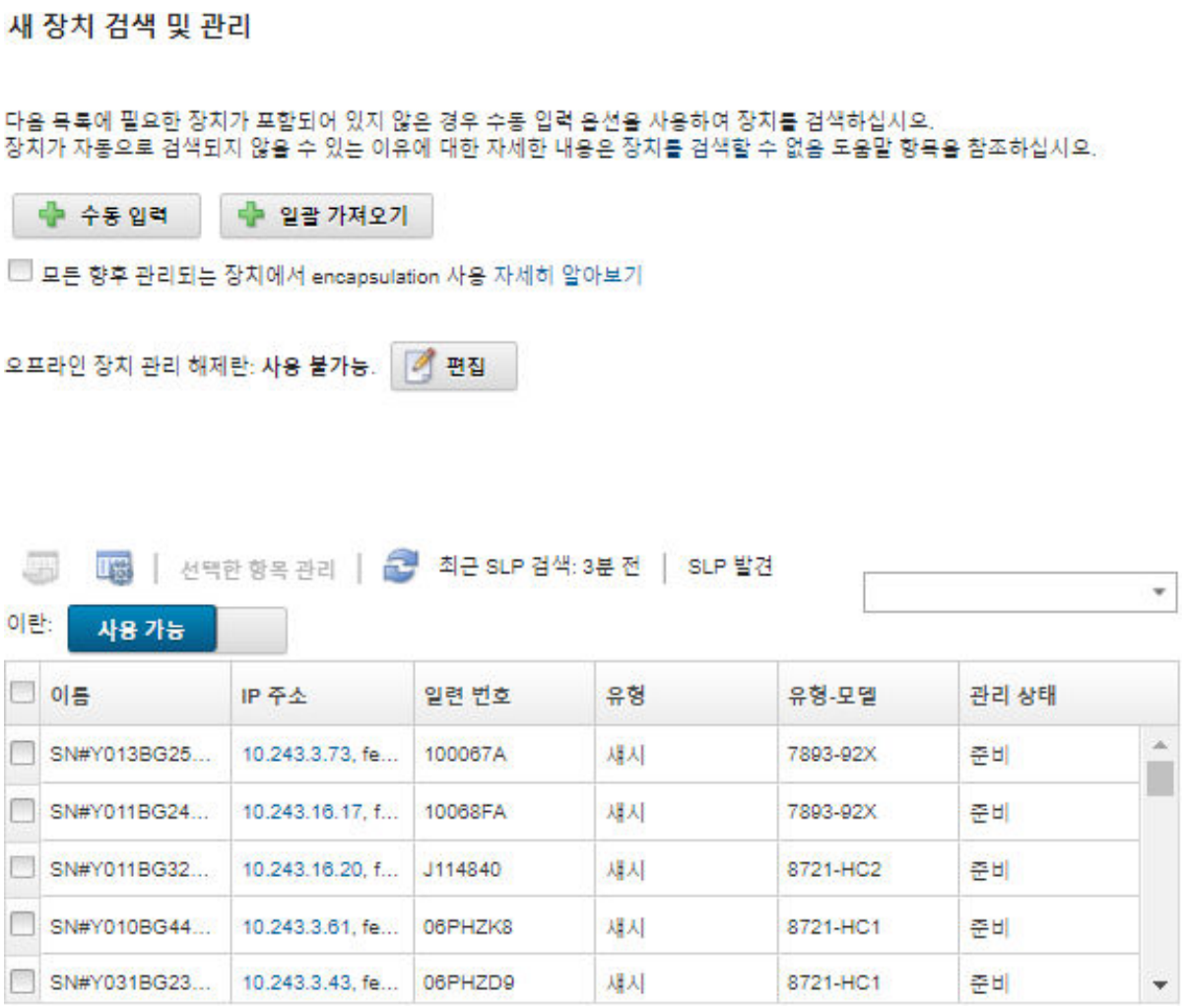
SSH를 사용하여 직접 또는 CMM을 통해 간접적으로 스위치를 관리하는 경우 스위치는 XClarity Administrator에서 관리되는 것으로 식별되고, 상호 작용을 위해 필요한 구성이 수행되고, 인벤토리가 수집됩니다.

절차

XClarity Administrator를 사용하여 RackSwitch 스위치를 관리하려면 다음 절차 중 하나를 완료하십시오.

- 일괄 가져오기 파일을 사용하여 다수의 스위치 및 기타 장치를 검색하고 관리하십시오(Lenovo XClarity Administrator 온라인 설명서의 시스템 관리 참조).

- XClarity Administrator와 동일한 IP 서브넷에 있는 RackSwitch 스위치를 검색하고 관리하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 새 장치 검색 및 관리 페이지가 표시됩니다.



     관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다. **열 사용자 지정** 아이콘( )을 클릭하여 표시되는 열과 기본 정렬 순서를 변경할 수 있습니다.
  2. **새로 고침** 아이콘( )을 클릭하여 XClarity Administrator 도메인의 모든 관리 가능 장치를 검색하십시오. 검색에는 몇 분 정도 소요됩니다.
  3. 관리할 스위치를 하나 이상 선택하십시오.
  4. **선택 관리**을 클릭하십시오.
  5. 스위치를 인증하기 위해 저장된 자격 증명을 지정해야 합니다.

     팁:

     - **저장된 자격 증명 관리**를 클릭하여 XClarity Administrator에서 저장된 자격 증명을 만들고 관리할 수 있습니다(저장된 자격 증명 관리 참조).
     - 감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우, 관리에 실패하거나 성공하더라도 장치의 기타 향후 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).

6. (ENOS를 실행하는 스위치만 해당) 설정된 경우 스위치에 권한 있는 실행 모드를 입력하는 데 사용되는 "사용" 암호를 지정하십시오.

   RackSwitch 스위치(ENOS 실행)를 관리하는 경우 스위치의 권한 있는 실행 모드에 대한 액세스가 필요합니다. 이는 스위치에 "enable" 명령을 실행할 때 XClarity Administrator에서 사용됩니다. 기본적으로 스위치에서 이 명령에 대한 암호가 설정되어 있지 않습니다. 그러나 스위치 관리자가 보안 강화를 위해 이 명령에 암호를 구성한 경우 스위치를 관리하려면 암호가 XClarity Administrator에 지정되어야 합니다.

7. 옵션: (ENOS를 실행하는 스위치만 해당) **고급**을 클릭한 다음 HTTPS **사용**을 선택하여 스위치에서 HTTPS를 사용할지 여부를 선택합니다. 기본적으로 사용으로 설정됩니다.

   참고:

   - CNOS를 실행하는 스위치의 경우 관리하기 전에 스위치에서 HTTPS를 사용하도록 설정해야 합니다(스위치 관리 고려사항 참조).
   - HTTPS를 사용하지 않도록 선택하면 스위치의 현재 설정이 사용됩니다.
   - 스위치가 관리 해제 상태인 경우, XClarity Administrator는 HTTPS를 원래 설정으로 복원합니다.

8. 옵션: **고급**을 클릭한 다음 **관리 서버에서 NTP 설정을 사용하도록 NTP 클라이언트 구성**을 선택하여 스위치의 NTP 구성을 Lenovo XClarity Administrator에 대해 정의된 NTP 구성 및 표준 시간대 설정으로 대체하도록 선택하십시오. 기본적으로 사용으로 설정됩니다.

   참고:

   - NTP 구성 및 표준 시간대를 대체하지 *않도록* 선택하면 로그 항목 및 이벤트의 타임스탬프가 관리되는 스위치 및 관리 서버 간에 동기화되지 않을 수 있습니다.
   - 스위치가 관리 해제 상태인 경우, XClarity Administrator는 NTP 구성 및 표준 시간대를 원래 설정으로 복원합니다.

9. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

   참고:

   - 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
   - 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

10. **관리**를 클릭하십시오.

    이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 작업 진행상황을 모니터링하십시오.

11. 프로세스가 완료되면 **확인**을 클릭하십시오.

    장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

    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.

- 수동으로 IP 주소를 지정하여 XClarity Administrator와 동일한 IP 서브넷에 있지 않은 RackSwitch 스위치를 검색하고 관리하십시오.
  1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 새 장치 검색 및 관리**를 클릭하십시오. 검색 및 관리 페이지가 표시됩니다.
  2. **수동 입력**을 선택하십시오.
  3. 관리할 스위치의 네트워크 주소를 지정하십시오.
     - **단일 시스템**을 클릭하고 단일 IP 주소 도메인 이름 또는 완전한 도메인 이름(FQDN)을 입력하십시오.

       참고: FQDN을 지정하려면 네트워크 액세스 페이지에 올바른 도메인 이름이 지정되어 있어야 합니다(네트워크 액세스 구성 참조).
     - **다중 시스템**을 클릭하고 IP 주소의 범위를 입력하십시오. 다른 범위를 추가하려면 **추가** 아이콘(➕)을 클릭하십시오. 범위를 제거하려면 **제거** 아이콘(❌)을 클릭하십시오.
  4. 서비스 검색 프로토콜을 사용하여 장치 유형을 검색할 수 없는 경우 사용자 서비스 검색 프로토콜을 지워서 장치 유형을 확인한 다음 드롭 다운 목록에서 관리할 장치 유형을 선택하십시오.

     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
  5. **확인**을 누르십시오.
  6. 스위치를 인증하기 위해 저장된 자격 증명을 지정해야 합니다.

     팁:
     - **저장된 자격 증명 관리**를 클릭하여 XClarity Administrator에서 저장된 자격 증명을 만들고 관리할 수 있습니다(저장된 자격 증명 관리 참조).
     - 감독자 또는 관리자 계정을 사용하여 장치를 관리하는 것이 좋습니다. 권한이 하위 수준인 계정을 사용하는 경우, 관리에 실패하거나 성공하더라도 장치의 기타 향후 XClarity Administrator 작업에 실패할 수 있습니다(특히 관리되는 인증 없이 장치가 관리되는 경우).
  7. (ENOS를 실행하는 스위치만 해당) 설정된 경우 스위치에 권한 있는 실행 모드를 입력하는 데 사용되는 "사용" 암호를 지정하십시오.

     RackSwitch 스위치(ENOS 실행)를 관리하는 경우 스위치의 권한 있는 실행 모드에 대한 액세스가 필요합니다. 이는 스위치에 "enable" 명령을 실행할 때 XClarity Administrator에서 사용됩니다. 기본적으로 스위치에서 이 명령에 대한 암호가 설정되어 있지 않습니다. 그러나 스위치 관리자가 보안 강화를 위해 이 명령에 암호를 구성한 경우 스위치를 관리하려면 암호가 XClarity Administrator에 지정되어야 합니다.
  8. 옵션: (ENOS를 실행하는 스위치만 해당) **고급**을 클릭한 다음 **HTTPS 사용**을 선택하여 스위치에서 HTTPS를 사용할지 여부를 선택합니다. 기본적으로 사용으로 설정됩니다.

     참고:
     - CNOS를 실행하는 스위치의 경우 관리하기 전에 스위치에서 HTTPS를 사용하도록 설정해야 합니다(스위치 관리 고려사항 참조).
     - HTTPS를 사용하지 않도록 선택하면 스위치의 현재 설정이 사용됩니다.

- 스위치가 관리 해제 상태인 경우, XClarity Administrator는 HTTPS를 원래 설정으로 복원합니다.

9. 옵션: **고급**을 클릭한 다음 **관리 서버에서 NTP 설정을 사용하도록 NTP 클라이언트 구성**을 선택하여 스위치의 NTP 구성을 Lenovo XClarity Administrator에 대해 정의된 NTP 구성 및 표준 시간대 설정으로 대체하도록 선택하십시오. 기본적으로 사용으로 설정됩니다.

   참고:

   - NTP 구성 및 표준 시간대를 대체하지 *않도록* 선택하면 로그 항목 및 이벤트의 타임스탬프가 관리되는 스위치 및 관리 서버 간에 동기화되지 않을 수 있습니다.
   - 스위치가 관리 해제 상태인 경우, XClarity Administrator는 NTP 구성 및 표준 시간대를 원래 설정으로 복원합니다.

10. **변경**을 클릭하여 장치에 할당할 역할 그룹을 변경하십시오.

    참고:

    - 현재 사용자에게 할당된 역할 그룹 목록에서 선택할 수 있습니다.
    - 역할 그룹을 변경하지 않으면, 기본 역할 그룹이 사용됩니다. 기본 역할 그룹에 대한 자세한 정보는 기본 권한 변경의 내용을 참조하십시오.

11. **관리**를 클릭하십시오.

    이 관리 프로세스의 진행상황을 표시하는 대화 상자가 표시됩니다. 프로세스가 성공적으로 완료되는지 확인하기 위해 작업 진행상황을 모니터링하십시오.

12. 프로세스가 완료되면 **확인**을 클릭하십시오.

    장치가 현재 XClarity Administrator에서 관리되고 있으며, 관리 장치를 정기적인 일정으로 자동으로 폴링하여 인벤토리와 같은 업데이트된 정보를 수집합니다.

    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.

완료한 후에

- 추가 장치를 검색 및 관리하십시오.
- 물리적 환경을 반영하도록 새 관리되는 장치를 적절한 랙에 추가하십시오(랙 관리 참조).
- 하드웨어 상태 및 세부 정보를 모니터링하십시오(스위치의 상태 보기 참조).
- 이벤트를 모니터링하십시오(이벤트 작업 참조).

스위치 관리 고려사항

스위치를 관리하기 전에 다음 관리 고려사항을 검토하십시오.

포트 요구사항에 대한 정보는 Lenovo XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

RackSwitch 장치는 데이터 포트 중 하나 또는 관리 포트를 사용하여 관리할 수 있습니다. CNOS를 실행하는 RackSwitch 장치는 "관리" 또는 "기본" VRF에 속하는 인터페이스에서만 관리할 수 있습니다.

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

XClarity 이벤트 및 SNMP 트랩 구성

ENOS를 실행하는 RackSwitch 장치(모든 버전)를 관리하는 경우, SNMP 트랩 소스는 관리에 사용되는 IP 주소가 있는 인터페이스로 설정됩니다.

CNOS v10.8.1 이상을 실행하는 RackSwitch 장치가 관리되는 경우 SNMP 트랩 소스 VRF가 선택되고 관리에 사용되는 포트와 일치하도록 변경됩니다.

v10.8.1 이전의 CNOS를 실행하는 RackSwitch 장치의 경우, XClarity Administrator에서 SNMP 트랩 소스는 관리에 사용되는 포트에 연결된 VRF여야 합니다. 기본값 "all"을 사용하면 관리 또는 데이터 포트를 사용할 수 있습니다. 스위치 구성에서 기본값을 사용하지 않으면 관리에 사용되는 포트와 일치하도록 스위치를 변경해야 합니다.

- 관리 포트가 관리에 사용되는 경우, SNMP 트랩 소스 VRF를 "all" 또는 "management"로 설정하십시오.
- 스위치가 데이터 포트 중 하나를 사용하여 관리하는 경우, SNMP 트랩 소스 VRF를 "all" 또는 "default"로 설정하십시오.

CNOS를 실행하는 RackSwitch 스위치

HTTPS는 관리를 위해 사용되어야 하며 SLP는 검색을 위해 사용되어야 합니다.

참고: HTTPS는 기본적으로 CNOS에서 사용으로 설정됩니다. restApi의 기본 구성을 변경한 경우(`feature restApi http` 명령 사용) `feature restApi` 명령을 사용하여 이를 다시 HTTPS로 변경할 수 있습니다. 현재 상태를 확인하려면 `display restApi server` 명령을 사용하십시오. 출력에는 현재 상태가 반영됩니다. 포트 번호 다음에 "(HTTP)"가 오는 경우 HTTPS가 *사용 안 함*으로 설정되어 있음을 나타냅니다. 그렇지 않으면 포트는 443이어야 합니다.

RackSwitch 장치가 관리되지 않는 경우, XClarity Administrator가 "기본" 옵션을 CNOS 펌웨어 버전에 따라 장치가 관리되기 전의 값으로 복원하지 못할 수도 있습니다.

ENOS를 실행하는 RackSwitch 스위치

- RackSwitch 스위치가 XClarity Administrator와 다른 네트워크에 있는 경우 XClarity Administrator가 이벤트를 수신하고 해당 장치를 관리할 수 있도록 네트워크가 포트 161 및 162를 통한 인바운드 UDP를 허용할 수 있게 구성되어야 합니다.
- SSH는 관리를 위해 사용되어야 하며 SLP는 검색을 위해 사용되어야 합니다. HTTPS는 옵션입니다. 그러나 스위치 웹 인터페이스를 실행하려면 사용으로 설정해야 합니다.
- 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.
  - `ip slp enable`
  - `ssh enable`
- RackSwitch 스위치가 관리되면 XClarity Administrator가 다음 구성 설정을 수정합니다. 관리되는 스위치에서 다음 설정을 변경하면 연결이 끊어져 관리 작업이 재대로 수행되지 않을 수 있습니다. RackSwitch 스위치가 관리되지 않는 경우, 구성 설정이 원래 값(관리 전)으로 복원됩니다.
  - snmp-server access 32

- snmp-server group 16
- snmp-server notify 16
- snmp-server target-parameters 16
- snmp-server target-address 16
- snmp-server trap-source *<IP interface>*
- snmp-server user 16
- snmp-server 버전 *<v3only or v1v2v3>*
- ntp enable
- ntp primary-server *<hostname or IP address>* MGT
- ntp secondary-server *<hostname or IP address>* MGT
- ntp interval 1500
- ntp offset 500
- access https enable

XClarity Administrator에서 스위치의 지원 연락처 정보, 이름 또는 위치 속성을 수정하여 다음 구성 설정을 수정할 수 있습니다. 랙에 스위치를 추가하면 위치가 수정됩니다.

- hostname "*<device_name>*"
- snmp-server location "Location:*<location>*,Room:*<room>*,Rack:*<rack>*,LRU:*<lru>*"
- snmp-server contact "*<contact_name>*"

스위치의 상태 보기

Lenovo XClarity Administrator에서 관리하는 모든 스위치의 상태를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

이 작업 정보

다음 상태 아이콘은 장치의 전반적인 상태를 나타내는 데 사용됩니다. 인증서가 일치하지 않으면 적용 가능한 각 장치의 상태에 "(신뢰할 수 없음)"이 추가됩니다. 예를 들어 경고(신뢰할 수 없음)이 표시됩니다. 연결 문제가 있거나 장치에 대한 연결을 신뢰할 수 없는 경우 적용 가능한 각 장치의 상태에 "(연결)"이 추가됩니다. 예를 들어 경고(연결)이 표시됩니다.

- (위험)
  - 하나 이상의 온도 센서가 오류 범위에 있습니다.
  - 다음과 같이 팬 모듈이나 팬이 제대로 작동하지 않습니다.
    - RackSwitch G8124-E: 하나 이상의 팬이 100RPM 이하로 작동 중입니다.
    - RackSwitch G8052: 팬 모듈이 세 개 미만인 경우 상태가 양호합니다. 해당 모듈의 팬이 500RPM을 초과하여 작동하는 경우 팬 모듈이 양호한 상태로 인식됩니다.
    - RackSwitch G8264, G8264CS, G8332, G8272: 팬 모듈이 네 개 미만인 경우 상태가 양호합니다. 해당 모듈의 팬이 500RPM을 초과하여 작동하는 경우 팬 모듈이 양호한 상태로 인식됩니다.
    - RackSwitch G8296: 팬 모듈이 세 개 미만인 경우 상태가 양호합니다. 해당 모듈의 팬이 480RPM을 초과하여 작동하는 경우 팬 모듈이 양호한 상태로 인식됩니다.
    - RackSwitch G7028, G7052: 팬 모듈이 세 개 미만인 경우 상태가 양호합니다. 해당 모듈의 팬이 500RPM을 초과하여 작동하는 경우 팬 모듈이 양호한 상태로 인식됩니다.
  - 한 전원 공급 장치가 꺼져 있습니다.
- (경고)
  - 하나 이상의 온도 센서가 경고 범위에 있습니다.
  - 플래시에 비상 덤프가 있습니다.
- (보류 중)
- (정보)
- (정상)

  - 모든 온도 센서가 정상 범위에 있습니다.
  - 모든 팬 모듈 또는 팬이 제대로 작동하지 않습니다.
  - 두 전원 공급 장치가 켜져 있습니다.
  - 플래시에 비상 덤프가 없습니다.
- () 오프라인
- () 알 수 없음

장치의 전원 상태는 다음 중 하나입니다.
- 켜짐
- 꺼짐
- 시스템 종료
- 대기
- 최대 절전
- 알 수 없음

절차

관리되는 스위치의 상태를 보려면 다음 작업 중 하나 이상을 완료하십시오.

- XClarity Administrator 메뉴 표시줄에서 **대시보드**를 클릭하십시오. 대시보드 페이지에는 모든 관리 스위치 및 기타 리소스에 대한 개요와 상태가 표시됩니다.

- XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

  관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하고 상태 아이콘을 클릭하여 선택한 기준을 충족하는 스위치만 나열하십시오.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- 스위치에 대한 자세한 정보를 봅니다(스위치의 세부 정보 보기 참조).
- **모든 작업 → 보기 → 랙 보기에 표시** 또는 **모든 작업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 Flex 스위치를 봅니다.
- **모든 작업 → 보기 → 랙 보기에 표시**를 클릭하여 그래픽 랙 보기로 RackSwitch 스위치를 봅니다.
- **IP 주소** 링크를 클릭하여 스위치의 관리 컨트롤러 웹 인터페이스를 실행합니다(스위치에 대한 관리 컨트롤러 인터페이스 실행 참조).
- 스위치 SSH 콘솔을 실행합니다(스위치의 원격 SSH 세션 실행 참조).
- 스위치 전원을 켜고 끕니다(스위치 전원 켜기 및 끄기 참조).
- (RackSwitch 스위치만 해당) 스위치를 선택하고 **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 시스템 정보를 수정합니다.
- 서버를 선택하고 **모든 작업 → 인벤토리 → 인벤토리 새로 고침**을 클릭하여 인벤토리를 새로 고칩니다.
- 스위치를 선택하고 **모든 작업 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 하나 이상의 스위치에 대한 자세한 정보를 단일 CSV 파일로 내보냅니다(이벤트 제외 참조).

  참고: 한 번에 최대 60대의 장치에 대한 인벤토리 데이터를 내보낼 수 있습니다.

  팁: CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- **이벤트 제외** 아이콘( )을 클릭하여 이벤트가 표시되는 모든 페이지에서 관심이 없는 이벤트를 제외합니다(이벤트 제외 참조).
- (Flex 스위치만 해당) 스위치를 선택하고 **모든 작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 스위치가 설치된 섀시에서 XClarity Administrator 보안 인증서와 CMM 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).
- **모든 작업 → 그룹 → 그룹에 추가** 또는 **모든 작업 → 그룹 → 그룹에서 제거**를 클릭하여 정적 리소스 그룹에서 스위치를 추가하거나 제거합니다.

스위치의 세부 정보 보기

Lenovo XClarity Administrator에서 펌웨어 수준 및 IP 주소 등 관리되는 스위치에 대한 자세한 정보를 볼 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 인벤토리
- XClarity Administrator: 모니터링

절차

XClarity Administrator에서 관리하는 특정 스위치의 세부 정보를 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 2. **스위치** 열에서 스위치를 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스위치에 설치된 구성 요소 목록과 속성이 표시됩니다.

단계 3. 자세한 인벤토리 정보를 보려면 다음 단계 중 하나 이상을 완료하십시오.

참고: 일부 세부 정보는 모든 스위치에서 사용 가능하지 않을 수 있습니다.

- **요약**을 클릭하여 시스템 정보와 펌웨어를 비롯한 스위치의 요약을 봅니다(스토리지 장치의 상태 보기 참조).
- **인벤토리 세부 정보**를 클릭하여 다음과 같은 스위치 구성 요소에 대한 세부 정보를 봅니다.
  - 스위치의 펌웨어 수준
  - 관리 컨트롤러 네트워크의 세부 정보(예, 호스트 이름, IPv4 주소, IPv6 주소 및 MAC 주소)
  - 스위치의 자산 세부 정보
- **I/O 연결**을 클릭하여 선택한 스위치에 대한 연결 세부 정보 및 스위치에 설치한 연관된 네트워크 어댑터를 표시합니다.
- **경고**를 클릭하여 경고 목록에서 스위치와 관련된 경고를 표시합니다(경고 작업 참조).
- **이벤트 로그**를 클릭하여 이벤트 로그에서 스위치와 관련된 이벤트를 표시합니다(이벤트 작업).
- **구성 파일**을 클릭하여 스위치 구성을 백업하고 복원하십시오(스위치 구성 데이터 백업 및 복원 참조).
- **배포 내역**을 클릭하여 스위치에 배포한 스위치 구성 템플릿에 대한 정보를 볼 수 있습니다(스위치 구성 배포 기록 보기 참조).
- **작업**을 클릭하여 스위치에 대한 구성 데이터 파일을 표시합니다(작업 모니터링 참조).
- **포트**를 클릭하여 관리되는 스위치에 있는 모든 포트의 상태와 구성을 표시하고 스위치 포트를 사용 또는 사용 안 함으로 설정합니다.

  참고: Flex 스위치의 경우 **새로 고침** 아이콘()을 클릭하여 현재 포트 데이터를 수집합니다. 데이터를 수집하려면 몇 분 정도가 걸릴 수 있습니다.
- Light Path를 클릭하여 스위치에 있는 각 LED의 현재 상태를 표시합니다.
- **전원 및 열**을 클릭하여 온도, 전원 공급 장치 및 팬에 대한 정보를 표시합니다.

  팁: 전원 및 열에 대한 최신 데이터를 수집하려면 웹 브라우저의 새로 고침 버튼을 사용하십시오. 데이터를 수집하려면 몇 분 정도가 걸릴 수 있습니다.

완료한 후에

스위치에 대한 요약 및 자세한 정보를 표시하는 것 외에도 다음 작업을 수행할 수 있습니다.

- **작업 → 보기 → 랙 보기에 표시** 또는 **박업 → 보기 → 섀시 보기에 표시**를 클릭하여 그래픽 랙 또는 섀시 보기로 Flex 스위치를 봅니다.
- **작업 → 보기 → 랙 보기에 표시**를 클릭하여 그래픽 랙 보기로 RackSwitch 스위치를 봅니다.
- IP 주소 링크를 클릭하여 스위치의 관리 컨트롤러 웹 인터페이스를 실행합니다(스위치에 대한 관리 컨트롤러 인터페이스 실행 참조).
- 스위치 SSH 콘솔을 실행합니다(스위치의 원격 SSH 세션 실행 참조).
- 스위치 전원을 켜고 끕니다(스위치 전원 켜기 및 끄기 참조).
- (RackSwitches만 해당) 스위치를 선택하고 **속성 편집**을 클릭하여 시스템 정보를 수정합니다.
- **동작 → 인벤토리 → 인벤토리 내보내기**를 클릭하여 스위치에 대한 자세한 정보를 CSV 파일로 내보냅니다.

  참고:
  - CSV 파일의 인벤토리 데이터에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 GET /switches/*<UUID_list>* REST API의 내용을 참조하십시오.
  - CSV 파일을 Microsoft Excel로 가져오는 경우, Excel은 숫자만 포함하는 텍스트 값을 숫자 값으로 취급합니다(예, UUID). 각 셀의 형식을 텍스트로 하여 이 오류를 수정합니다.
- **작업 → 서비스 재설정 → 이벤트 제외**를 클릭하여 이벤트가 표시되는 모든 페이지에서 관심이 없는 이벤트를 제외합니다(이벤트 제외 참조).

- 스위치를 선택하고 **작업 → 보안 → 신뢰할 수 없는 인증서 해결**을 클릭하여 Flex System 스위치가 설치된 섀시에 있는 RackSwtich 또는 CMM의 보안 인증서와 XClarity Administrator 보안 인증서 간에 발생할 수 있는 문제를 해결합니다(신뢰할 수 없는 서버 인증서 해결 참조).

스위치 전원 켜기 및 끄기

Lenovo XClarity Administrator에서 Flex System 또는 RackSwitch 스위치를 다시 시작하거나 전원을 켜고 끌 수 있습니다.

절차

관리되는 스위치 전원을 켜고 끄려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 2. 전원을 켜고 끄거나 다시 시작할 스위치를 선택하십시오.

단계 3. **모든 작업**을 클릭하고 다음 전원 작업 중 하나를 클릭하십시오.
- **전원 켜기**(Flex System 스위치만 해당)
- **전원 끄기**(Flex System 스위치만 해당)
- **다시 시작**. 현재 실행 중인 모든 작업이 완료되면 스위치가 다시 시작됩니다. 스위치가 다시 시작되는 동안 시작된 작업은 거부됩니다.

스위치 포트 사용 및 사용 안 함

RackSwitch 또는 Flex System 스위치에서 특정 포트를 사용 또는 사용 안 함으로 설정할 수 있습니다

절차

스위치 포트를 사용 또는 사용 안 함으로 설정하려면 다음 단계를 완료하십시오.

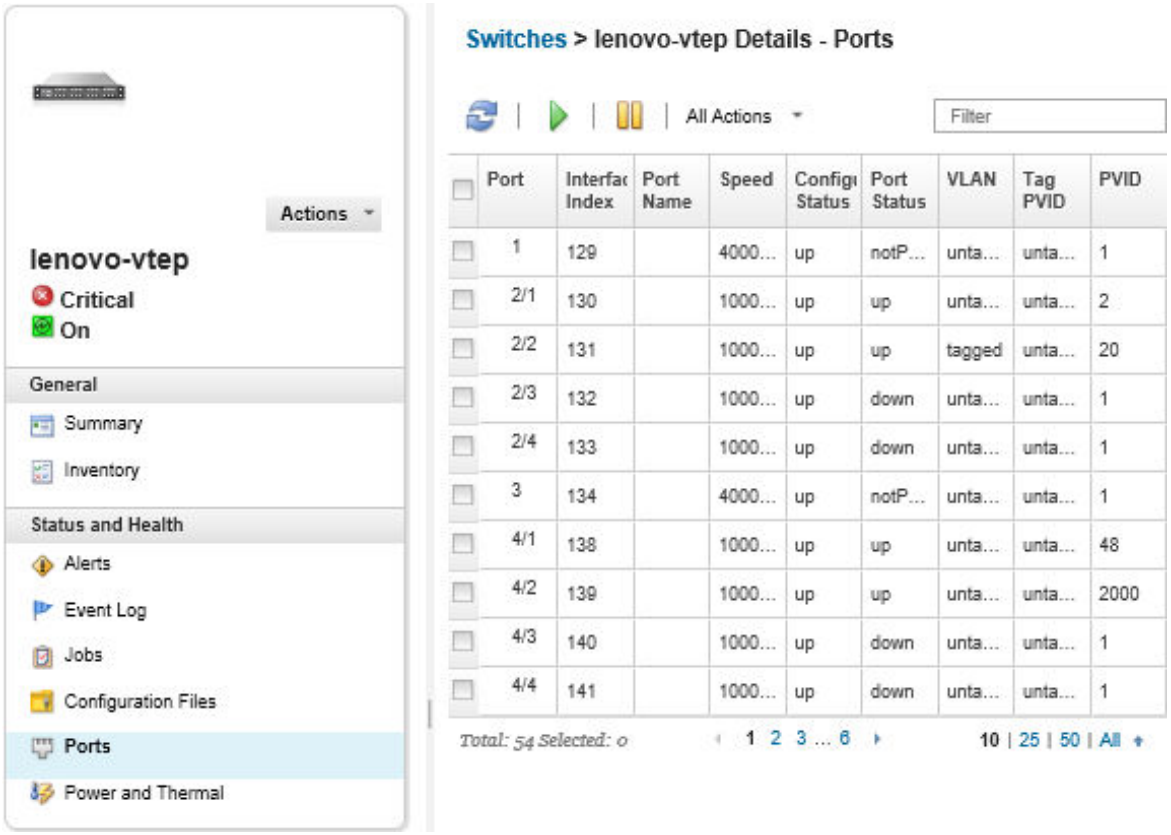
단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 2. **스위치** 열에서 스위치를 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스위치에 설치된 구성 요소 목록과 속성이 표시됩니다.

단계 3. 왼쪽 탐색에서 **포트**를 클릭하여 스위치에 있는 모든 포트의 상태와 구성을 표시합니다.

참고: Flex 스위치의 경우 **새로 고침** 아이콘()을 클릭하여 현재 포트 데이터를 수집합니다. 데이터를 수집하려면 몇 분 정도가 걸릴 수 있습니다.



단계 4. 포트를 선택하고 **사용** 아이콘() 또는 **사용 안 함** 아이콘()을 클릭하십시오.

스위치 구성 데이터 백업 및 복원

Lenovo XClarity Administrator를 사용하여 RackSwitch 및 Flex System 스위치의 구성 데이터를 백업하고 복원할 수 있습니다. 또한 스위치 구성 파일을 로컬 시스템으로 내보내고 스위치 구성 파일을 XClarity Administrator로 가져올 수도 있습니다.

스위치 구성 데이터 백업

Flex System 또는 RackSwitch 스위치의 구성 데이터를 백업할 수 있습니다. 스위치를 백업할 때 대상 스위치에서 스위치 구성 파일로 구성 데이터를 Lenovo XClarity Administrator로 가져옵니다.

절차

관리되는 스위치의 구성 데이터를 백업하려면 다음 단계를 완료하십시오.

- 단일 스위치의 경우:
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

     관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

  2. **스위치** 열에서 스위치를 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스위치에 설치된 구성 요소 목록과 속성이 표시됩니다.
  3. **구성**을 클릭하면 스위치의 구성 파일을 볼 수 있습니다.
  4. **구성 데이터 백업** 아이콘()을 클릭하여 스위치 구성을 백업하십시오.
  5. (옵션) 스위치 구성 파일의 이름을 지정하십시오.

     CNOS 장치의 경우 파일 이름은 영숫자와 밑줄(_), 하이픈(-) 및 마침표(.)와 같은 특수 문자를 포함할 수 있습니다. ENOS 스위치의 경우 파일 이름은 영숫자와 모든 특수 문자를 포함할 수 있습니다.

     파일 이름을 지정하지 않으면 다음 기본 이름이 사용됩니다.
     "*<switch_name>*_*<IP_address>*_*<timestamp>*.cfg."
  6. (옵션) 백업을 설명하는 주석을 추가하십시오.
  7. **백업**을 클릭하여 스위치 구성 데이터로 즉시 백업하거나, **일정**을 클릭하여 이 백업이 나중에 실행되도록 예약하십시오.

     백업 일정을 선택했다면, **덮어 쓰기**를 선택하여 각 작업 실행 시 동일한 파일에 스위치 구성 데이터를 백업하고 해당 내용을 덮어 씁니다. 파일을 덮어 쓰지 않기로 선택하는 경우, 후속 백업의 파일 이름에 고유 번호(예, MyBackup_33.cfg)가 추가됩니다.

     참고: 백업을 예약할 때, 예약된 각 작업에 대한 동적 파일 이름이나 의견을 선택할 수 없습니다.
- 다중 스위치의 경우:
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.
  2. 하나 이상의 스위치를 선택하십시오.
  3. **모든 작업 → 구성 → 구성 파일 백업**을 클릭하십시오.
  4. (옵션) 스위치 구성 파일의 이름을 지정하십시오.

CNOS 장치의 경우 파일 이름은 영숫자와 밑줄(_), 하이픈(-) 및 마침표(.)와 같은 특수 문자를 포함할 수 있습니다. ENOS 스위치의 경우 파일 이름은 영숫자와 모든 특수 문자를 포함할 수 있습니다.

파일 이름을 지정하지 않으면 다음 기본 이름이 사용됩니다.
"*<switch_name>_<IP_address>_<timestamp>*.cfg."

5. (옵션) 백업을 설명하는 주석을 추가하십시오.
6. **백업**을 클릭하여 스위치 구성 데이터로 즉시 백업하거나, **일정**을 클릭하여 이 백업이 나중에 실행되도록 예약하십시오.

   백업 일정을 선택했다면, **덮어 쓰기**를 선택하여 각 작업 실행 시 동일한 파일에 스위치 구성 데이터를 백업하고 해당 내용을 덮어 씁니다. 파일을 덮어 쓰지 않기로 선택하는 경우, 후속 백업의 파일 이름에 고유 번호(예, MyBackup_33.cfg)가 추가됩니다.

   참고: 백업을 예약할 때, 예약된 각 작업에 대한 동적 파일 이름이나 의견을 선택할 수 없습니다.

완료한 후에

백업 프로세스가 완료되면 스위치 구성 파일이 스위치 세부 정보 페이지의 **구성 파일**탭에 추가됩니다.

이 페이지에서 선택한 스위치 구성 파일에 다음 작업을 수행할 수 있습니다.

- 스위치 구성 파일을 선택하고 **구성 데이터 복원** 아이콘()을 클릭하여 스위치 구성을 복원하십시오.
- **삭제** 아이콘()을 클릭하여 XClarity Administrator에서 스위치 구성 파일을 삭제하십시오.
- 파일을 선택하고 **구성 파일 내보내기**아이콘()을 클릭하여 스위치 구성 파일을 로컬 시스템으로 내보내십시오.
- **구성 파일 가져오기**아이콘()을 클릭하여 스위치 구성 파일을 XClarity Administrator로 가져오십시오.

스위치 구성 데이터 복원

Flex System 또는 RackSwitch 스위치의 경우 Lenovo XClarity Administrator로 백업하거나 가져온 구성 데이터를 복원할 수 있습니다. 스위치 구성 파일이 XClarity Administrator에서 대상 스위치로 다운로드되고 구성이 자동으로 적용됩니다.

구성 파일은 특정 스위치와 연관됩니다. 연관된 스위치에서만 구성 파일을 복원할 수 있습니다. 한 스위치에 대해 백업된 구성 파일을 사용하여 다른 스위치의 구성을 복원할 수 없습니다.

절차

관리되는 스위치의 구성 데이터를 복원하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 2. **스위치** 열에서 스위치를 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스위치에 설치된 구성 요소 목록과 속성이 표시됩니다.

단계 3. **구성 파일**을 클릭하면 스위치의 구성 파일을 볼 수 있습니다.

단계 4. 스위치에서 복원하려고 하는 구성 파일을 선택한 다음 **구성 데이터 복원** 아이콘( )을 클릭하십시오. 복원 대화 상자가 표시됩니다.

단계 5. (CNOS를 실행하는 스위치 경우) 복원 작업이 완료된 후 스위치를 다시 시작할지 여부를 선택하십시오.

스위치를 자동으로 다시 시작하지 않기로 선택하는 경우, CNOS 스위치를 수동으로 다시 시작하여 복원된 구성 데이터를 활성화해야 합니다. 시간이 초과되어 저장 조작이 발생하면(예, 포트가 사용 또는 사용하지 않음으로 설정된 경우), 복원 조작이 중단되고 실행 중인 구성 데이터가 사용됩니다.

단계 6. **복원**을 클릭하여 스위치의 구성 데이터로 즉시 복원하거나, **일정**을 클릭하여 이 복원 작업이 나중에 실행되도록 예약하십시오.

참고: 되풀이 복원 작업을 예약할 때는 주의하십시오. 스위치가 이전 구성으로 재설정되면, 예약된 작업 페이지를 참조하십시오.

스위치 구성 파일 내보내기 및 가져오기

스위치 구성 파일을 로컬 시스템으로 내보내고 스위치 구성 파일을 Lenovo XClarity Administrator로 가져올 수 있습니다.

절차

관리되는 스위치의 구성 데이터를 백업하려면 다음 단계를 완료하십시오.

- 스위치 구성 파일 내보내기
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

     관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

  2. **스위치** 열에서 스위치를 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스위치에 설치된 구성 요소 목록과 속성이 표시됩니다.
  3. **구성**을 클릭하면 스위치의 구성 파일을 볼 수 있습니다.
  4. 내보낼 스위치 구성 파일을 선택하십시오.
  5. **구성 파일 내보내기**아이콘( )을 클릭하여 스위치 구성을 백업하십시오.
- 스위치 구성 파일 가져오기
  1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

     관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

2. **스위치** 열에서 스위치를 클릭하십시오. 요약 페이지가 표시되며, 여기에는 해당 스위치에 설치된 구성 요소 목록과 속성이 표시됩니다.
3. **구성**을 클릭하면 스위치의 구성 파일을 볼 수 있습니다.
4. **구성 파일 가져오기**아이콘( )을 클릭하여 스위치 구성을 백업하십시오.
5. 스위치 구성 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 부팅 파일을 찾으십시오.
6. **옵션:** 스위치 구성 파일에 대한 설명을 입력하십시오.
7. **가져오기**를 클릭하십시오.

   업로드가 완료되기 전에 파일이 업로드되는 웹 브라우저 또는 창을 닫는 경우 가져오기가 실패합니다.

스위치에 대한 관리 컨트롤러 인터페이스 실행

Lenovo XClarity Administrator에서 ENOS를 실행 중인 RackSwitch 또는 Flex System 스위치에 대한 관리 컨트롤러 웹 인터페이스를 실행할 수 있습니다.

절차

스위치의 관리 컨트롤러 인터페이스를 실행하려면 다음 단계를 완료하십시오.

참고: Safari 웹 브라우저를 통해 XClarity Administrator에서 관리 컨트롤러 웹 인터페이스를 실행하는 것은 지원되지 않습니다.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 2. 스위치를 선택하고 **모든 작업 → 실행 → 관리 웹 인터페이스**를 클릭하십시오. 스위치의 관리 컨트롤러 웹 인터페이스가 표시됩니다.

팁: IP 주소 열과 스위치 요약 및 스위치 세부 정보 페이지에서 IP 주소 링크를 클릭하여 관리 컨트롤러 인터페이스를 실행할 수도 있습니다.

단계 3. 관리 컨트롤러 인터페이스에 로그인하십시오.

팁: Flex 스위치의 경우 XClarity Administrator 사용자 자격 증명을 사용하십시오. XClarity Administrator 스위치의 경우 스위치 자격 증명을 사용하십시오.

스위치의 원격 SSH 세션 실행

Lenovo XClarity Administrator에서 관리 RackSwitch 또는 Flex 스위치에 대한 원격 SSH 세션을 실행할 수 있습니다. 원격 SSH 세션에서 명령줄 인터페이스를 사용하여 XClarity Administrator에서 제공되지 않는 관리 작업을 수행할 수 있습니다.

시작하기 전에

스위치에서 SSH를 사용하도록 구성되었는지 확인하십시오. RackSwitch 스위치의 경우 스위치가 XClarity Administrator에서 관리되면 SSH가 사용 가능합니다. Flex 스위치의 경우 일반적으로 SSH는 기본으로 사용으로 설정됩니다. 이를 사용하지 않는 경우 XClarity Administrator에서 스위치를 관리하기 전에 SSH를 사용으로 설정해야 합니다.

절차

관리되는 스위치의 원격 SSH 세션을 실행하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 섀시에 설치된 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 2. SSH 세션을 실행할 스위치를 선택하십시오.

단계 3. **모든 작업 → 실행 →** SSH 콘솔을 클릭하십시오.

단계 4. 필요한 경우 사용자 ID와 암호를 사용하여 스위치에 로그인하십시오.

스위치의 시스템 속성 수정

특정 Flex System 또는 RackSwitch 스위치에 대한 시스템 속성을 수정할 수 있습니다.

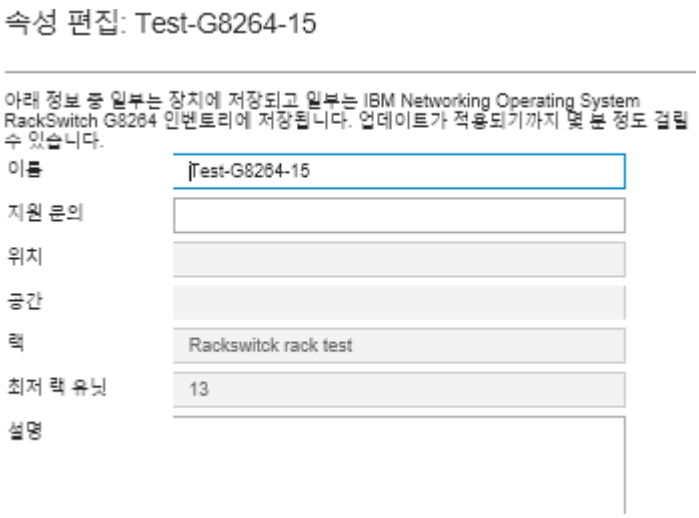
절차

시스템 속성을 수정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하여 스위치 페이지를 표시하십시오.

단계 2. 업데이트할 스위치를 선택하십시오.

단계 3. **모든 작업 → 인벤토리 → 속성 편집**을 클릭하여 편집 대화 상자를 표시하십시오.



단계 4. 필요 시 다음 정보를 변경하십시오.
- 스위치 이름
- 지원 문의
- 설명

참고: 웹 인터페이스의 랙에서 장치를 추가하거나 제거할 때 XClarity Administrator에서 위치, 룸, 랙 및 하단 LRU(lowest rack unit) 속성을 업데이트합니다(랙 관리 참조).

단계 5. **저장**을 클릭하십시오.

참고: 이러한 속성을 변경하는 경우 XClarity Administrator 웹 인터페이스에 변경 사항이 표시되기 전에 약간의 지연이 있을 수 있습니다.

스위치에 대해 만료되었거나 유효하지 않은 저장된 자격 증명 해결

저장된 자격 증명이 장치에서 만료되거나 작동 불능 상태가 되면 해당 장치의 상태가 "오프라인"으로 표시됩니다.

절차

스위치에 대한 만료되었거나 유효하지 않은 저장된 자격 증명을 해결하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하십시오. 관리되는 모든 스위치의 표 형식 보기와 함께 스위치 페이지가 표시됩니다.

단계 2. **전원** 열 머리글을 클릭하여 테이블 맨 위에 있는 모든 오프라인 스위치를 그룹화합니다.

관리할 스위치를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 시스템 이름 또는 IP 주소)를 입력하여 표시되는 스위치를 상세하게 필터링할 수도 있습니다.

단계 3. 해결할 스위치를 선택하십시오.

단계 4. **모든 작업 → 보안 → 저장된 자격 증명 편집**을 클릭하십시오.

단계 5. 저장된 자격 증명의 암호를 변경하거나 관리되는 장치에 사용할 다른 저장된 자격 증명을 선택하십시오.

참고: 동일한 저장된 자격 증명을 사용하여 둘 이상의 장치를 관리하고 저장된 자격 증명의 암호를 변경하면 해당 암호 변경은 현재 저장된 자격 증명을 사용하는 모든 장치에 영향을 줍니다.

관리 서버 오류 후 스위치로 관리 복구

관리 해제 중 연결 문제 또는 Lenovo XClarity Administrator 관리 오류 등으로 인해 제대로 관리 해제되지 않은 스위치의 관리를 복구할 수 있습니다.

절차

- **강제 관리** 옵션을 사용하여 스위치를 다시 관리하십시오(스위치 관리 참조).
- 제대로 관리 해제되지 않았으며 다시 관리하지 않을 스위치에서 XClarity Administrator 전용 구성을 영구적으로 제거하려면 다음 단계를 완료하십시오.
  - **강제 관리** 옵션을 사용하여 스위치를 다시 관리한 후(스위치 관리 참조) 스위치를 관리 해제하여 구성을 정리하십시오(스위치 관리 해제 참조).
  - (ENOS) 스위치 콘솔 포트 또는 SSH 또는 텔넷 세션을 사용하여 스위치에 로그인하고 지정된 순서 대로 다음 구성 명령을 실행하여 스위치 구성을 지우십시오.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

스위치 관리 해제

Lenovo XClarity Administrator에 의한 관리에서 스위치를 제거할 수 있습니다. 이 프로세스를 *관리 해제*라고 합니다.

시작하기 전에

XClarity Administrator을(를) 사용하여 특정 기간 동안 오프라인 상태였던 장치를 자동으로 관리 해제할 수 있습니다. 기본적으로 이 기능은 사용 불가능하도록 설정되어 있습니다. 오프라인 장치 자동 관리 해제 기능을 사용하려면, XClarity Administrator 메뉴의 **하드웨어 → 새 장치 검색 및 관리**를 클릭한 다음, **오프라인 장치 관리 해제 기능을 사용할 수 없습니다** 옆의 **편집**을 클릭하십시오. 그러고 나

서 **오프라인 장치 관리 해제 기능 사용**을 선택하고 시간 간격을 설정하십시오. 기본적으로 장치는 24시간 동안 오프라인 상태인 경우 관리 해제됩니다.

스위치를 관리 해제하기 전에 스위치에 대해 실행 중인 활성 작업이 없어야 합니다.

이 작업 정보

스위치를 관리 해제해도 XClarity Administrator는 스위치에 대한 특정 정보를 유지합니다. 해당 정보는 동일한 스위치를 다시 관리할 때 다시 적용됩니다.

팁: 초기 설정 중에 선택적으로 추가되는 모든 데모 장치는 섀시의 노드입니다. 데모 장치를 관리 해제하려면 **장치에 연결할 수 없는 경우에도 강제로 관리 해제** 옵션을 사용하여 섀시를 관리 해제하십시오.

절차

스위치를 관리 해제하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 스위치**를 클릭하여 스위치 페이지를 표시하십시오.

단계 2. 관리되는 스위치 목록에서 하나 이상의 스위치를 선택하십시오.

단계 3. **스위치 관리 해제**를 클릭하십시오. 관리 해제 대화 상자가 표시됩니다.

단계 4. **옵션: 장치에 연결할 수 없는 경우에도 강제로 관리 해제**를 선택하십시오.

중요: 데모 하드웨어를 관리 해제하는 경우 이 옵션을 선택해야 합니다.

단계 5. **관리 해제**를 클릭하십시오.관리 해제 대화 상자에는 관리 해제 프로세스 각 단계의 진행상황이 표시됩니다.

단계 6. 관리 해제 프로세스가 완료되면 **확인**을 클릭하십시오.

제대로 관리 해제되지 않은 스위치 복구

스위치가 Lenovo XClarity Administrator에서 관리 중인 경우 및 XClarity Administrator에 오류가 발생하는 경우 관리 서버가 복원되거나 교체될 때까지 관리 기능을 복구할 수 있습니다.

절차

- **강제 관리** 옵션을 사용하여 스위치를 다시 관리하십시오(스위치 관리 참조).
- 제대로 관리 해제되지 않았으며 다시 관리하지 않을 스위치에서 XClarity Administrator 전용 구성을 영구적으로 제거하려면 다음 단계를 완료하십시오.
  - **강제 관리** 옵션을 사용하여 스위치를 다시 관리한 후(스위치 관리 참조) 스위치를 관리 해제하여 구성을 정리하십시오(스위치 관리 해제 참조).
  - (ENOS) 스위치 콘솔 포트 또는 SSH 또는 텔넷 세션을 사용하여 스위치에 로그인하고 지정된 순서 대로 다음 구성 명령을 실행하여 스위치 구성을 지우십시오.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

제 11 장 구성 패턴을 사용하여 서버 구성

서버 패턴은 정의된 단일 구성 설정 세트에서 여러 서버(랙 및 타워 서버와 컴퓨팅 노드)를 신속하게 프로비저닝하고 사전 프로비저닝하는 데 사용됩니다.

자세히 알아보기:

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

시작하기 전에

90일 무료 평가판이 만료된 후에도 XClarity Administrator을(를) 사용하여 무료로 하드웨어를 관리하고 모니터할 수 있습니다. 그러나 계속해서 서버 구성 기능을 사용하려면 XClarity Administrator 고급 기능을 지원하는 각 관리되는 서버에 대해 전체 기능 사용 라이센스를 구입해야 합니다. Lenovo XClarity Pro은(는) 서비스 및 지원에 대한 자격과 전체 기능 사용 라이센스를 제공합니다. Lenovo XClarity Pro 구입에 대한 자세한 정보는 Lenovo 담당자 또는 공인 비즈니스 파트너에게 문의하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 전체 기능 사용 라이센스 설치의 내용을 참조하십시오.

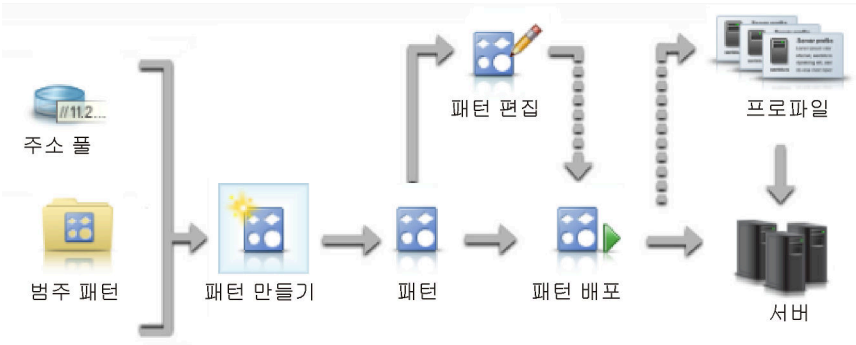
특정 서버와 장치의 구성 지원에 대한 중요한 정보는 구성 고려사항의 내용을 검토하십시오.

이 작업 정보

XClarity Administrator에서 서버 패턴을 사용하여 관리되는 서버의 로컬 스토리지, I/O 어댑터, 부팅 순서 및 기타 베이스보드 관리 컨트롤러 및 UEFI(Unified Extensible Firmware Interface) 설정을 구성할 수 있습니다. 또한 서버 패턴은 I/O 주소 가상화를 위한 지원을 통합하기 때문에 패브릭을 중단하지 않고 서버 패브릭 연결을 가상화하거나 서버의 용도를 변경할 수 있습니다. 또한 Fibre Channel 주소를 가상화(미리 구성)하여 새 하드웨어를 받기 전에 SAN 구역 변경 요청을 초기화할 수도 있습니다.

절차

다음 그림은 관리되는 서버를 구성하는 워크플로우를 설명합니다. 실선 화살표는 사용자가 수행하는 작업을 표시합니다. 점선 화살표는 XClarity Administrator에서 자동으로 수행되는 작업을 표시합니다.



단계 1. **주소 풀 만들기** *주소 풀*은 정의된 주소 범위 세트입니다. 개별 서버에 서버 패턴이 배포될 때 Lenovo XClarity Administrator는 주소 풀을 사용하여 해당 서버에 IP와 I/O 주소를 할당합니다.

주소 풀 만들기에 대한 자세한 정보는 주소 풀 정의의 내용을 참조하십시오.

단계 2. **범주 패턴 만들기**

*범주 패턴*은 관련 펌웨어 설정을 함께 그룹화하고 여러 서버 패턴에서 재사용될 수 있습니다. 다음 펌웨어 범주에 대한 패턴을 작성할 수 있습니다.

- 시스템 정보
- 관리 인터페이스
- 장치 및 I/O 포트
- FC 부팅 대상
- I/O 어댑터 포트

범주 패턴에 대한 자세한 정보는 서버 패턴 작업의 내용을 참조하십시오.

단계 3. **서버 패턴 만들기**

*서버 패턴*은 로컬 스토리지 구성, I/O 어댑터 구성, 부팅 설정, 기타 베이스보드 관리 컨트롤러 및 UEFI 펌웨어 설정 등의 사전 OS 서버 구성을 표시합니다. 서버 패턴은 한 번에 여러 서버를 빠르게 구성하기 위한 전체 패턴으로 사용됩니다.

데이터 센터에서 사용되는 여러 구성을 표시하는 여러 서버 패턴을 정의할 수 있습니다.

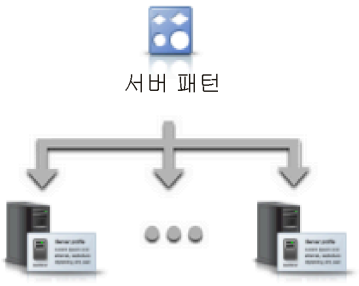
서버 패턴을 정의하는 경우 필요에 따라 범주 패턴과 주소 풀을 선택하여 특정 서버 그룹에 대해 원하는 구성을 생성하십시오. 범주 패턴은 여러 서버 패턴에서 재사용될 수 있는 관련 구성 설정을 함께 그룹화합니다.

Converged, Flex System, NeXtScale 및 System x 서버에 대해 서버 패턴을 처음부터 새로 작성하여 하드웨어가 도착하기 전에 원하는 구성을 정의할 수 있습니다, 또는 기존 관리되는 서버에서 서버 패턴을 작성할 수 있습니다. 기존 서버에서 서버 패턴을 작성하는 경우 XClarity Administrator는 선택한 서버에서 범주 패턴을 얻습니다.

서버 패턴 만들기에 대한 자세한 정보는 서버 패턴 만들기의 내용을 참조하십시오.

단계 4. **서버 패턴 배포**

예를 들어 하나 이상의 개별 서버 또는 서버 그룹에 서버 패턴을 배포할 수 있습니다. 예를 들어 서버 패턴을 섀시에 배포할 수 있으므로 해당 서버에 있는 모든 컴퓨팅 노드가 동일하게 구성됩니다. 배포 중에 XClarity Administrator는 서버 패턴을 배포할 각 서버에 대해 서버 프로필을 작성합니다. 각 *서버 프로필*은 단일 서버에 대한 특정 구성을 나타냅니다. 이는 서버 패턴으로부터 설정을 상속받으며 서버 특정 정보(예, 할당된 IP 주소 및 MAC 주소)를 포함하기도 합니다. 서버 프로필은 서버 패턴으로부터 설정을 상속받기 때문에 서버 프로필에서 변경사항이 자동으로 업데이트됩니다. 이러한 방식으로 공통 구성을 한 위치에서 유지보수할 수 있습니다.



참고: 구성 패턴을 사용하지 않고 설정을 변경하거나 펌웨어 중에 펌웨어 문제나 잘못된 설정과 같은 문제가 발생한 경우 서버의 설정이 서버 프로필을 준수하지 못할 수 있습니다. 구성 패턴: 서버 프로필 페이지에서 각 서버의 준수 상태를 판별할 수 있습니다.

다음에 서버 패턴을 배포할 수 있습니다.

- **기존 서버**. 각 서버에 대해 서버 프로필이 작성됩니다. 연결된 서버가 다시 부팅되면 서버 프로필이 활성화됩니다.

- **기존 섀시의 비어 있는 베이**. 비어 있는 각각의 베이에 대해 서버 프로필이 작성됩니다. 컴퓨팅 노드가 물리적으로 설치되면 비어 있는 베이와 연결된 서버 프로필이 활성화될 수 있습니다.
- **가지고 있지 않은 섀시의 자리 표시자**. 하드웨어가 도착하기 전에 서버 패턴의 대상으로 작동하도록 ***자리 표시자 섀시***를 정의하여 아직 가지고 있지 않은 섀시에 컴퓨팅 노드를 사전 프로비저닝할 수 있습니다. 자리 표시자 섀시는 비어 있는 각각의 컴퓨팅 노드 베이에 대해 작성된 모든 서버 프로필을 번들로 만듭니다. 따라서 하드웨어가 도착하면 자리 표시자 섀시를 새 섀시에 배포하여 서버 프로필을 새 섀시의 모든 컴퓨팅 노드에 할당할 수 있습니다. 연결된 컴퓨팅 노드가 다시 부팅되면 각 서버 프로필이 활성화됩니다.

참고: 여러 서버에 서버 패턴을 배포할 수 있지만 여러 패턴을 단일 서버에 배포할 수는 없습니다.

서버 패턴 배포에 대한 자세한 정보는 서버에 서버 패턴 배포 및 자리 표시자 섀시 배포의 내용을 참조하십시오.

단계 5. **서버 패턴 편집**

서버 패턴을 사용하여 단일 위치에서 공통 구성을 제어합니다. 더 이상 서버에서 설정을 직접 업데이트하지 않습니다. 대신 범주 패턴과 서버 패턴을 업데이트하면 모든 연결된 프로필과 해당 서버에 변경사항이 자동으로 배포됩니다.

서버 패턴 편집에 대한 자세한 정보는 서버 패턴 수정의 내용을 참조하십시오.

구성 고려사항

Lenovo XClarity Administrator를 통해 서버 구성을 시작하기 전에 다음 중요 고려사항을 검토하십시오.

- 서버 프로필에 이전 펌웨어 수준이 포함되어 있고 펌웨어를 이후 수준으로 업데이트하는 경우 XClarity Administrator는 저장된 프로필 설정을 서버 설정과 비교하여 '호환되지 않음'을 보고합니다. 비호환 이유를 확인하려면 '호환되지 않음' 상태 위로 커서를 이동하십시오.

  장치를 선택한 다음 **모든 작업 ➙ 준수**를 클릭하면 프로필을 다시 배포하지 않고도 수동으로 '호환되지 않음' 상태의 장치를 '호환'으로 변경할 수 있습니다.
- 서버의 펌웨어(예: UEFI, BMC 또는 I/O 컨트롤러)를 업그레이드하면 일부 구성이 변경될 수 있습니다(예: 새 항목 추가, 기존 항목 삭제, 항목의 동작 또는 값 범위를 변경하는 경우). 그 결과 서버 프로필이 비준수 상태가 되거나 이전 펌웨어 수준을 사용하여 생성된 경우에는 서버 패턴이 적용되지 않을 수도 있습니다. 이 경우에는 업데이트된 펌웨어를 기반으로 새로운 패턴을 학습하도록 하거나 실패한 패턴을 편집하여 특정 항목의 구성을 제외한 다음 서버에 해당 패턴을 적용하는 것이 좋습니다.
- QLogic 8200 2포트 10GbE SFP+ VFA 어댑터에 iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName 및 IPv6LinkLocalAddress 설정에 대한 잘못된 값이 있습니다. 서버의 구성 패턴을 학습하기 전에 시스템 설정에서 이러한 값을 수동으로 수정하거나 학습된 구성 패턴의 값을 수정해야 합니다.
- 임베디드 RAID 어댑터가 있는 Flex System x240 및 x440 계산 노드의 경우 RAID 구성 정의를 정의하는 서버 패턴은 기존 RAID 구성이 없는 하나 이상의 서버에만 배포할 수 있습니다. 기존 RAID 구성이 있는 서버에 서버 패턴을 배포하는 경우 기존 배열과 볼륨을 덮어쓰지 않습니다. 서버 패턴에 정의된 RAID 구성을 적용하려면 먼저 서버에서 기존 RAID 구성을 지우고(스토리지 어댑터를 기본값으로 재설정 참조), 서버를 선택한 후 **추가 ➙ 서버 프로필 배포**를 클릭하여 서버 프로필을 다시 배포해야 합니다.
- Flex System x220, Flex System x222 및 ThinkSystem 서버의 온보드 스토리지 컨트롤러는 소프트웨어 기반 RAID를 지원합니다. 그러나 구성 패턴을 사용하는 소프트웨어 RAID의 구성은 지원되지 않습니다.
- 구성 패턴을 사용하여 RAID를 구성할 때 서버의 전원이 꺼져 있으면 서버 프로필을 활성화하기 전에 서버가 자동으로 BIOS/UEFI Setup으로 부팅됩니다.
- ThinkServer 서버의 경우 구성 패턴이 지원되지 않습니다.

- 특정 I/O 장치는 서버 패턴을 사용하여 구성될 수 없습니다. 자세한 정보는 XClarity Administrator 지원 – 호환성 웹 페이지의 내용을 참조하십시오.
- Flex 스위치 EN4093R, CN4093, SI4093 또는 SI4091에서 고급 기능(예, SPAR, Easy Connect 및 스택)을 사용하는 경우 내부 포트에 네트워크 구성을 제대로 적용할 수 없습니다.
- 기본적으로 Flex 스위치 SI4093은 공장 출하 시 SPAR이 사용 설정된 상태로 제공됩니다. 이러한 스위치에서 포트 패턴을 사용하여 내부 포트에 네트워크 설정을 배포하려면 SPAR에서 스위치 내부 포트를 수동으로 제거하거나 스위치에서 SPAR 구성을 수동으로 제거해야 합니다.
- 구성 패턴을 사용하여 Converged 및 ThinkAgile 어플라이언스를 구성하려면 XClarity Administrator를 사용하지 *않도록* 권장합니다.
- 사용 가능한 모든 포트와 설정이 패턴에 포함되도록 기존 서버에서 구성 패턴을 생성하기 전에 설치된 어댑터에서 사용 가능한 모든 포트가 사용 설정되어 있는지 확인하십시오. 그런 다음 필요에 따라 패턴에 정의된 적절한 설정을 사용하여 포트를 사용 안 함으로 설정할 수 있습니다. 패턴이 작성될 때 포트를 사용할 수 없는 경우, 패턴이 올바르게 작성되지 않고 배포되지 않을 수 있습니다.

주소 풀 정의

*주소 풀*은 정의된 주소 범위 세트입니다. 개별 서버에 서버 패턴이 배포될 때 Lenovo XClarity Administrator는 주소 풀을 사용하여 해당 서버에 IP와 I/O 주소를 할당합니다.

이 작업 정보

XClarity Administrator는 IP 및 I/O 주소 풀을 지원합니다.

IP 주소 풀
*IP 주소 풀*은 서버의 베이스보드 관리 컨트롤러 네트워크 인터페이스 구성 시 사용할 IP 주소 범위를 정의합니다. 필요에 따라 미리 정의된 주소 풀을 사용하거나 사용자 지정할 수 있으며, 새 풀을 작성할 수도 있습니다. 서버 패턴을 작성할 때 배포 중에 사용할 IP 주소 풀을 선택할 수 있습니다. 서버 패턴이 배포되는 경우 IP 주소는 선택한 풀에서 할당되어 개별 관리 컨트롤러에 할당됩니다.

참고: 관리 컨트롤러 네트워크 구성에 만족하는 경우 이 옵션을 사용하지 마십시오.

주의:

- 데이터 센터의 기존 I/O 주소와 충돌하지 않는 IP 주소 하위 범위를 선택해야 합니다.
- 지정된 범위의 IP 주소가 서브 네트워크의 일부이고 XClarity Administrator에서 도달 가능한지 확인하십시오.
- 주소 충돌을 방지하려면 지정된 범위의 IP 주소가 각 XClarity Administrator 도메인과 기존 IP 관리 도구에 고유해야 합니다.

전체 주소 풀 범위는 지정된 라우팅 접두사 길이 및 게이트웨이나 초기 범위에서 파생됩니다. 특정 라우팅 접두사 길이를 기반으로 하여 다른 크기의 풀을 작성할 수 있지만 전체 풀 범위가 XClarity Administrator 도메인에서 고유해야 합니다. 그런 다음 전체 풀 범위에서 범위를 만듭니다.

별도의 호스트(예, 운영 체제 유형, 워크로드 유형 및 비즈니스 유형)에 주소 범위를 사용할 수 있습니다. 주소 범위를 조직 네트워크 규칙에 묶을 수도 있습니다.

이더넷 주소 풀
*이더넷 주소 풀*은 서버 구성 시 네트워크 어댑터에 할당할 수 있는 고유한 MAC 주소의 컬렉션입니다. 필요에 따라 미리 정의된 주소 풀을 사용하거나 사용자 지정할 수 있으며, 새 풀을 작성할 수도 있습니다. 서버 패턴을 작성할 때 배포 중에 사용할 이더넷 주소 풀을 선택할 수 있습니다. 서버 패턴이 배포되는 경우 주소는 선택한 풀에서 할당되어 개별 어댑터 포트에 할당됩니다.

다음 미리 정의된 MAC 주소 풀을 사용할 수 있습니다.
- Lenovo MAC 주소 풀

이 풀의 MAC 주소 범위 목록에 대해서는 이더넷 주소(MAC) 풀의 내용을 참조하십시오.

Fibre Channel 주소 풀

*Fibre Channel 주소 풀*은 서버 구성 시 Fibre Channel 어댑터에 할당할 수 있는 고유한 WWNN 및 WWPN 주소의 컬렉션입니다. 필요에 따라 미리 정의된 주소 풀을 사용하거나 사용자 지정할 수 있으며, 새 풀을 작성할 수도 있습니다. 서버 패턴을 작성할 때 배포 중에 사용할 Fibre Channel 주소 풀을 선택할 수 있습니다. 서버 패턴이 배포되는 경우 주소는 선택한 풀에서 할당되어 개별 어댑터 포트에 할당됩니다.

다음 미리 정의된 Fibre Channel 주소 풀을 사용할 수 있습니다.
- Lenovo WWN 주소
- Brocade WWN 주소
- Emulex WWN 주소
- QLogic WWN 주소

이러한 풀의 WWN 주소 범위 목록에 대해서는 Fibre Channel 주소(WWN) 풀의 내용을 참조하십시오.

주소 풀의 주소 범위는 XClarity Administrator 도메인에서 고유해야 합니다. XClarity Administrator는 정의된 범위와 할당된 주소가 해당 관리 도메인에서 고유한지 확인합니다.

중요: 다중 XClarity Administrator 인스턴스가 있는 대형 환경에서는 주소가 중복되지 않도록 각 XClarity Administrator에 고유한 주소 범위를 사용해야 합니다.

I/O 어댑터 가상 주소 지정에 이더넷과 Fibre Channel 주소 풀을 사용하여 조직에서 고유한 I/O 주소를 할당합니다. 컴퓨팅 노드에 대한 서버 패턴을 작성하는 경우 장치와 I/O 어댑터 구성의 일부로 가상 주소 지정을 사용할 수 있습니다. 가상 주소 지정을 사용하는 경우 주소 충돌을 방지하기 위해 이더넷과 Fibre Channel 주소 풀에서 주소가 할당됩니다.

제한사항: 가상 주소 지정은 Flex System 컴퓨팅 노드에만 지원됩니다. 독립 실행형 랙 및 타워 서버는 지원되지 않습니다.

서버 패턴 작성에 대한 정보는 서버 패턴 만들기의 내용을 참조하십시오.

IP 주소 풀 만들기

*IP 주소 풀*은 서버의 베이스보드 관리 컨트롤러 네트워크 인터페이스 구성 시 사용할 IP 주소 범위를 정의합니다. 연결된 서버 패턴이 배포되는 경우 IP 주소는 지정된 풀에서 할당되어 개별 서버에 할당됩니다.

이 작업 정보

새 IP 주소 풀 대화 상자에 있는 전체 네트워크 정보 테이블의 데이터는 지정된 서브넷 마스크 및 게이트웨이 또는 초기 범위에서 파생됩니다. 특정 서브넷 마스크를 기반으로 하여 다른 크기의 풀을 작성할 수 있지만 전체 풀 범위가 관리 도메인에서 고유해야 합니다. 그런 다음 전체 풀 범위에서 범위를 만듭니다. 모든 범위는 동일한 서브넷 마스크의 일부여야 하며 전체 네트워크 정보 테이블에 표시된 한계로 제한됩니다.

풀과 범위에는 Lenovo XClarity Administrator 범위가 있습니다. 다중 XClarity Administrator 인스턴스가 있는 환경에서는 주소가 기존 IP 관리 도구와 충돌하지 않도록 각 XClarity Administrator에 고유한 풀과 범위를 작성하십시오. 범위를 별도의 호스트(예, 운영 체제 유형, 워크로드 유형 및 비즈니스 기능)에 사용하여 조직 네트워크 규칙을 지키도록 강제할 수도 있습니다.

절차

IP 주소 풀을 작성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 주소 풀**을 클릭하십시오. 구성 패턴: 주소 풀 페이지가 표시됩니다.

단계 2. **IP 주소 풀** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 IP 주소 풀 마법사 대화 상자가 표시됩니다.

단계 4. 다음 정보를 입력하십시오.

- 주소 풀의 이름과 설명을 입력하십시오.
- IPv4 또는 IPv6 주소 사용을 선택하십시오.
- 서브넷 마스크(IPv4의 경우) 또는 라우팅 접두사 길이(IPv6의 경우)를 선택하십시오.
- 게이트웨이 주소를 지정하십시오.지정된 서브넷 마스크와 게이트웨이 또는 초기 범위에서 네트워크 정보 값이 파생되어 테이블에 입력됩니다.
- 하나 이상의 주소 범위를 추가하십시오.
  1. 주소 범위를 추가하려면 **범위 추가**를 클릭하십시오. 새 IP 주소 범위 추가 대화 상자가 표시됩니다.
  2. 범위 이름, 첫 번째 주소 및 범위 크기를 입력하십시오.마지막 주소는 자동으로 계산됩니다.
  3. **확인**을 누르십시오.범위가 **IP 풀 주소 범위 정의** 테이블에 추가되고 요약 섹션의 필드가 자동으로 업데이트됩니다.

  편집 아이콘( )을 클릭하여 범위를 편집하거나 **제거** 아이콘( )을 클릭하여 범위를 제거할 수 있습니다.

단계 5. **만들기**를 클릭하십시오.

완료한 후에

새 IP 주소 풀이 IP 주소 풀 페이지의 테이블에 나열됩니다.

이 페이지에서 선택한 주소 풀에 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘( )을 클릭하여 주소 풀을 수정합니다.
- **이름 바꾸기** 아이콘을 클릭하여 주소 풀의 이름을 바꿉니다.
- **삭제** 아이콘( )을 클릭하여 주소 풀을 삭제합니다.
- **풀 이름** 열에서 풀 이름을 클릭하면 가상 주소, 설치된 어댑터 포트 및 예약된 가상 주소 간의 맵핑을 포함하여 주소 풀에 대한 세부 정보가 표시됩니다.

이더넷 주소 풀 만들기

*이더넷 주소 풀*은 네트워크 어댑터에 할당할 수 있는 고유한 MAC(media access control) 주소의 컬렉션입니다. 필요에 따라 미리 정의된 주소 풀을 사용하거나 사용자 지정할 수 있으며, 새 주소 풀을 작성할 수도 있습니다. 서버 패턴을 작성하는 경우 이더넷 어댑터에 가상 주소 지정을 사용하면 패턴 배포 시 사용할 이더넷 주소 풀을 선택할 수 있습니다. 연결된 서버 패턴이 배포되는 경우 MAC 주소는 선택한 주소 풀에서 할당되어 서버의 개별 네트워크 어댑터에 할당됩니다.

절차

이더넷 주소 풀을 작성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 주소 풀**을 클릭하십시오. 구성 패턴: 주소 풀 페이지가 표시됩니다.

단계 2. **이더넷 주소 풀** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘()을 클릭하십시오. 새 이더넷(MAC) 주소 풀 대화 상자가 표시됩니다.

단계 4. 주소 풀의 이름과 설명을 입력하십시오.

단계 5. 하나 이상의 주소 범위를 추가하십시오.

a. 주소 범위를 추가하려면 **범위 추가**를 클릭하십시오. 이더넷(MAC) 주소 범위 대화 상자가 표시됩니다.

b. 범위 이름, 첫 번째 MAC 주소 및 범위 크기를 입력하십시오.

마지막 MAC 주소는 자동으로 계산됩니다.

c. **추가**를 클릭하십시오.

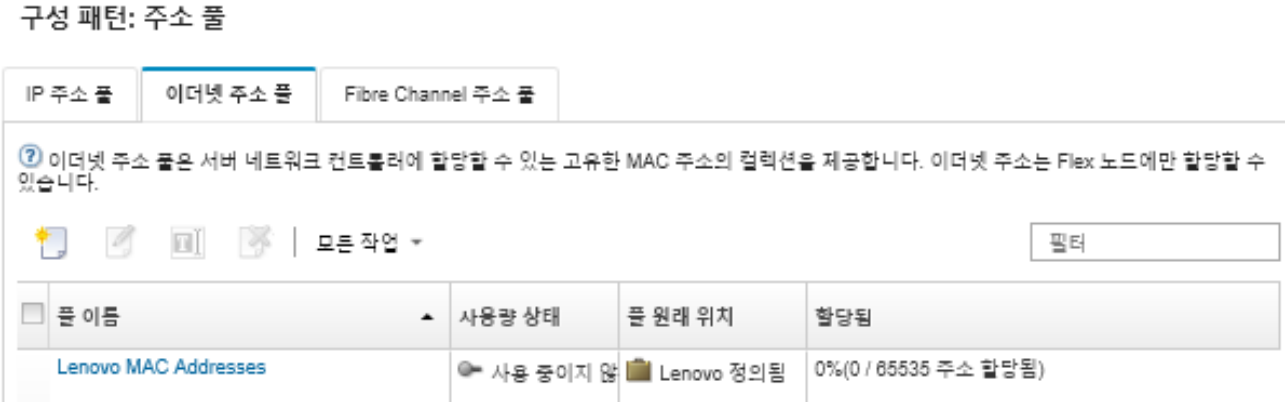
범위가 **이더넷(MAC) 풀 주소 범위 정의** 테이블에 추가되고 요약 섹션의 필드가 자동으로 업데이트됩니다.

편집 아이콘()을 클릭하여 범위를 편집하거나 **제거** 아이콘()을 클릭하여 범위를 제거할 수 있습니다.

단계 6. **저장**을 클릭하십시오.

완료한 후에

새 이더넷 주소 풀이 이더넷 주소 풀 페이지에 나열됩니다.



이 페이지에서 선택한 주소 풀에 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘()을 클릭하여 주소 풀을 수정합니다.
- **이름 바꾸기** 아이콘을 클릭하여 주소 풀의 이름을 바꿉니다.
- **삭제** 아이콘()을 클릭하여 주소 풀을 삭제합니다.
- **풀 이름** 열에서 풀 이름을 클릭하면 가상 주소, 설치된 어댑터 포트 및 예약된 가상 주소 간의 맵핑을 포함하여 주소 풀에 대한 세부 정보가 표시됩니다.

이더넷 주소(MAC) 풀

이더넷 주소 풀은 네트워크 어댑터에 할당할 수 있는 고유한 MAC(media access control) 주소의 컬렉션입니다. 서버 패턴에서 미리 정의된 다음 주소 풀을 사용할 수 있습니다.

표 3. Lenovo MAC 주소 풀

미리 정의된 범위	시작 주소	종료 주소
범위 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
범위 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
범위 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
범위 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
범위 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
범위 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
범위 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
범위 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
범위 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Fibre Channel 주소 풀 만들기

*Fibre Channel 주소 풀*은 Fibre Channel 어댑터에 할당할 수 있는 고유한 WWNN(World Wide Node Name) 및 WWPN(World Wide Port Name) 주소의 컬렉션입니다. 필요에 따라 미리 정의된 주소 풀을 사용하거나 사용자 지정할 수 있으며, 새 풀을 작성할 수도 있습니다. 서버 패턴을 작성하는 경우 이더넷 어댑터에 가상 주소 지정을 사용하면 패턴 배포 시 사용할 Fibre Channel 주소 풀을 선택할 수 있습니다. 연결된 서버 패턴이 배포되면 풀에서 WWNN 및 WWPN 주소가 할당되어 개별 서버에 할당됩니다.

절차

Fibre Channel 주소 풀을 작성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 주소 풀**을 클릭하십시오. 구성 패턴: 주소 풀 페이지가 표시됩니다.

단계 2. **Fibre Channel 주소 풀** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘()을 클릭하십시오. Fibre Channel 주소 풀 대화 상자가 표시됩니다.

단계 4. 주소 풀의 이름과 설명을 입력하십시오.

단계 5. 하나 이상의 주소 범위를 추가하십시오.

a. 주소 범위를 추가하려면 **범위 추가**를 클릭하십시오. Fibre Channel(WWN) 주소 범위 대화 상자가 표시됩니다.

b. 범위 이름, 범위 크기 및 각 패브릭의 첫 번째 주소를 입력하십시오.

마지막 주소는 자동으로 계산됩니다.

c. **추가**를 클릭하십시오.

범위가 **Fibre Channel 풀 주소 범위 정의** 테이블에 추가되고 요약 섹션의 필드가 자동으로 업데이트됩니다.

편집 아이콘()을 클릭하여 범위를 편집하거나 **제거** 아이콘()을 클릭하여 범위를 제거할 수 있습니다.

단계 6. **저장**을 클릭하십시오.

완료한 후에

새 Fibre Channel 주소 풀이 Fibre Channel 주소 풀 테이블에 나열됩니다.

이 페이지에서 선택한 주소 풀에 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘( )을 클릭하여 주소 풀을 수정합니다.
- **삭제** 아이콘( )을 클릭하여 주소 풀을 삭제합니다.
- **풀 이름** 열에서 풀 이름을 클릭하면 가상 주소, 설치된 어댑터 포트 및 예약된 가상 주소 간의 맵핑을 포함하여 주소 풀에 대한 세부 정보가 표시됩니다.

Fibre Channel 주소(WWN) 풀

Fibre Channel 주소 풀은 Fibre Channel 어댑터에 할당할 수 있는 고유한 WWNN(World Wide Node Name) 및 WWPN(World Wide Port Name) 주소의 컬렉션입니다. 서버 패턴에서 미리 정의된 다음 주소 풀을 사용할 수 있습니다.

표 4 "Brocade WWN 주소 풀" 303페이지은 BrocadeWWN(World Wide Name) 주소 풀을 나열합니다. 각 Brocade 범위에는 1,864,135개의 주소가 있습니다.

표 5 "Emulex WWN 주소 풀" 304페이지은 EmulexWWN 주소 풀을 나열합니다. 각 Emulex 범위에는 1,864,135개의 주소가 있습니다.

표 6 "Lenovo WWN 주소 풀" 305페이지은 LenovoWWN 주소 풀을 나열합니다. 각 Lenovo WWN 범위에는 116,508개의 주소가 있습니다.

표 7 "QLogic WWN 주소 풀" 306페이지은 QLogicWWN 주소 풀을 나열합니다. 각 QLogic WWN 범위에는 116,508개의 주소가 있습니다.

표 4. Brocade WWN 주소 풀

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 시작 주소	WWPN 종료 주소
Fabric A				
범위 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C-:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C-:71:C6
범위 2	2B:FA:00:05:1E:1C-:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C-:71:C7	2B:FC:00:05:1E:38:E3:8D
범위 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54

표 4. Brocade WWN 주소 풀 (계속)

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 시작 주소	WWPN 종료 주소
범위 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
범위 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E-:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E-:38:E2
범위 6	2B:FA:00:05:1E:8E-:38:E3	2B:FA:00:05:1E:AA-:AA:A9	2B:FC:00:05:1E:8E-:38:E3	2B:FC:00:05:1E:AA-:AA:A9
범위 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA-:AA:AA	2B:FC:00:05:1E:C7:1C:70
범위 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
범위 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF-:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF-:FF:FE
Fabric B				
범위 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C-:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C-:71:C6
범위 2	2B:FB:00:05:1E:1C-:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C-:71:C7	2B:FD:00:05:1E:38:E3:8D
범위 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54
범위 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
범위 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E-:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E-:38:E2
범위 6	2B:FB:00:05:1E:8E-:38:E3	2B:FB:00:05:1E:AA-:AA:A9	2B:FD:00:05:1E:8E-:38:E3	2B:FD:00:05:1E:AA-:AA:A9
범위 7	2B:FB:00:05:1E:AA-:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA-:AA:AA	2B:FD:00:05:1E:C7:1C:70
범위 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
범위 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF-:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF-:FF:FE

표 5. Emulex WWN 주소 풀

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 시작 주소	WWPN 종료 주소
Fabric A				
범위 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C-:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C-:71:C6
범위 2	2F:FE:00:00:C9:1C-:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C-:71:C7	2F:FC:00:00:C9:38:E3:8D
범위 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
범위 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B

표 5. Emulex WWN 주소 풀 (계속)

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 시작 주소	WWPN 종료 주소
범위 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E-:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E-:38:E2
범위 6	2F:FE:00:00:C9:8E-:38:E3	2F:FE:00:00:C9:AA-:AA:A9	2F:FC:00:00:C9:8E-:38:E3	2F:FC:00:00:C9:AA-:AA:A9
범위 7	2F:FE:00:00:C9:AA-:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA-:AA:AA	2F:FC:00:00:C9:C7:1C:70
범위 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
범위 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF-:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF-:FF:FE
Fabric B				
범위 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C-:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C-:71:C6
범위 2	2F:FF:00:00:C9:1C-:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C-:71:C7	2F:FD:00:00:C9:38:E3:8D
범위 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
범위 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
범위 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E-:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E-:38:E2
범위 6	2F:FF:00:00:C9:8E-:38:E3	2F:FF:00:00:C9:AA-:AA:A9	2F:FD:00:00:C9:8E-:38:E3	2F:FD:00:00:C9:AA-:AA:A9
범위 7	2F:FF:00:00:C9:AA-:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA-:AA:AA	2F:FD:00:00:C9:C7:1C:70
범위 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
범위 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF-:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF-:FF:FE

표 6. Lenovo WWN 주소 풀

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 시작 주소	WWPN 종료 주소
Fabric A				
범위 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C-7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C-7:1B
범위 2	20:80:00:50:76:01:C-7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C-7:1C	21:80:00:50:76:03:8E:37
범위 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
범위 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
범위 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E-3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E-3:8B

표 6. Lenovo WWN 주소 풀 (계속)

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 시작 주소	WWPN 종료 주소
범위 6	20:80:00:50:76:08:E-3:8C	20:80:00:50:76:0A-:AA:A7	21:80:00:50:76:08:E-3:8C	21:80:00:50:76:0A-:AA:A7
범위 7	20:80:00:50:76:0A-:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A-:AA:A8	21:80:00:50:76:0C:71:C3
범위 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
범위 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:F-F:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:F-F:FB
Fabric B				
범위 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C-7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C-7:1B
범위 2	20:81:00:50:76:21:C-7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C-7:1C	21:81:00:50:76:23:8E:37
범위 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
범위 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
범위 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E-3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E-3:8B
범위 6	20:81:00:50:76:28:E-3:8C	20:81:00:50:76:2A-:AA:A7	21:81:00:50:76:28:E-3:8C	21:81:00:50:76:2A-:AA:A7
범위 7	20:81:00:50:76:2A-:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A-:AA:A8	21:81:00:50:76:2C:71:C3
범위 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
범위 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:F-F:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:F-F:FB

표 7. QLogic WWN 주소 풀

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 종료 주소	WWPN 종료 주소
Fabric A				
범위 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
범위 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
범위 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
범위 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
범위 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
범위 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A-:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A-:AA:A7

표 7. QLogic WWN 주소 풀 (계속)

미리 정의된 범위	WWNN 시작 주소	WWNN 종료 주소	WWPN 종료 주소	WWPN 종료 주소
범위 7	20:80:00:E0:8B:0A-:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A-:AA:A8	21:80:00:E0:8B:0C:71:C3
범위 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
범위 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F-:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F-:FF:FB
Fabric B				
범위 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
범위 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37
범위 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53
범위 4	20:81:00:E0:8B:25:55:54	20:81:00:E0:8B:27:1C:6F	21:81:00:E0:8B:25:55:54	21:81:00:E0:8B:27:1C:6F
범위 5	20:81:00:E0:8B:27:1C:70	20:81:00:E0:8B:28:E3:8B	21:81:00:E0:8B:27:1C:70	21:81:00:E0:8B:28:E3:8B
범위 6	20:81:00:E0:8B:28:E3:8C	20:81:00:E0:8B:2A-:AA:A7	21:81:00:E0:8B:28:E3:8C	21:81:00:E0:8B:2A-:AA:A7
범위 7	20:81:00:E0:8B:2A-:AA:A8	20:81:00:E0:8B:2C:71:C3	21:81:00:E0:8B:2A-:AA:A8	21:81:00:E0:8B:2C:71:C3
범위 8	20:81:00:E0:8B:2C:71:C4	20:81:00:E0:8B:2E:38:DF	21:81:00:E0:8B:2C:71:C4	21:81:00:E0:8B:2E:38:DF
범위 9	20:81:00:E0:8B:2E:38:E0	20:81:00:E0:8B:2F-:FF:FB	21:81:00:E0:8B:2E:38:E0	21:81:00:E0:8B:2F-:FF:FB

서버 패턴 작업

*서버 패턴*은 로컬 스토리지 구성, I/O 어댑터, SAN 부팅, 기타 베이스보드 관리 컨트롤러 및 UEFI 펌웨어 설정 등의 사전 OS 서버 구성을 표시합니다. 또한 서버 패턴은 I/O 주소 가상화를 위한 지원을 통합하기 때문에 중단하지 않고 서버 패브릭 연결을 가상화하거나 서버의 용도를 변경할 수 있습니다. 서버 패턴은 한 번에 여러 서버를 빠르게 구성하기 위한 전체 패턴으로 사용됩니다.

이 작업 정보

데이터 센터에서 사용되는 여러 구성을 표시하는 여러 서버 패턴을 정의할 수 있습니다.

서버 패턴을 정의하는 경우 필요에 따라 범주 패턴과 주소 풀을 선택하거나 작성하여 특정 서버 그룹에 대해 원하는 구성을 생성하십시오. *범주 패턴*은 여러 서버 패턴에서 재사용될 수 있는 특정 펌웨어 설정을 정의합니다. 주소 풀을 사용하여 서버 패턴 배포 시 개별 서버에 주소를 할당하는 데 사용할 주소 범위를 정의할 수 있습니다. IP 주소 풀, 이더넷 주소(MAC) 풀 및 Fibre Channel 주소(WWN) 풀이 있습니다.

여러 서버에 서버 패턴을 배포하는 경우 여러 개의 서버 프로필이 자동으로 생성됩니다(각 서버당 하나의 프로필). 각 프로필은 상위 서버 패턴의 설정을 상속받으므로 단일 위치에서 공통 구성을 제어할 수 있습니다.

하드웨어가 도착하기 전에 원하는 구성을 정의하여 새 서버 패턴을 처음부터 새로 작성할 수 있습니다. 또는 기존 서버에서 서버 패턴을 작성한 다음 해당 패턴을 사용하여 나머지 서버를 프로비저닝할 수 있습니

다. 기본 서버에서 서버 패턴을 작성하는 경우 확장된 범주 패턴을 가져와서 서버의 현재 설정에서 동적으로 작성됩니다. 범주 설정을 변경하는 경우 서버 패턴에서 범주 설정을 직접 편집할 수 있습니다.

주의: 새 서버 패턴을 처음부터 새로 작성하는 경우 서버의 부팅 설정을 정의해야 합니다. 서버에 서버 패턴을 배포하는 경우 서버의 기존 부팅 순서를 서버 패턴에 있는 기본 부팅 순서로 덮어씁니다. 해당 서버에 서버 패턴을 배포한 후 서버가 시작되지 않는 경우 원래 부팅 설정을 새 서버 패턴에 있는 기본 부팅 순서 설정으로 덮어쓰는 문제가 발생할 수 있습니다. 서버의 원래 부팅 설정을 복원하려면 서버 패턴 배포 후 부팅 설정 복구의 내용을 참조하십시오.

중요: 서버 패턴을 작성할 때 각 유형의 서버에 대한 서버 패턴을 작성해야 합니다. 예를 들어 모든 Flex System x240 컴퓨팅 노드에 대한 서버 패턴을 작성하고 모든 Flex System x440 컴퓨팅 노드에 대해서는 다른 서버 패턴을 작성하십시오. 한 서버 유형에 대해 작성된 서버 패턴을 다른 서버 유형에 배포하지 마십시오.

중요: 관리 노드가 실패하면 서버 패턴이 유실될 수 있습니다. 서버 패턴을 작성하거나 수정한 후에는 항상 관리 소프트웨어를 백업하십시오(Lenovo XClarity Administrator 백업 참조).

네트워크 장치에 대한 설정

일부 Flex System 네트워크 장치는 다른 장치보다 서버 패턴에 더 많은 구성 옵션을 제공합니다.

서버 패턴을 모든 네트워크 장치에 적용할 수 있지만 일부 서버 패턴 기능은 특정 네트워크 어댑터로 제한됩니다. 또한 이더넷 네트워크 어댑터에 대한 일부 고급 설정(예, 어댑터 및 포트 호환성 기본 설정)은 현재 지원되지 않습니다.

서버 패턴은 지원되는 네트워크 어댑터에 대한 기존 구성 데이터 및 설정을 가져와서 패턴 배포를 통해 구성 설정을 변경할 수 있습니다.

범주 패턴

펌웨어 설정은 관련 설정을 그룹화하는 범주로 구성됩니다. 각 범주에 대해 공통 펌웨어 설정이 포함되고 여러 서버 패턴에서 재사용될 수 있는 ***범주 패턴***을 작성할 수 있습니다. 베이스보드 관리 컨트롤러 및 UEFI에서 직접 구성할 수 있는 대부분의 펌웨어 설정은 범주 패턴을 통해서도 구성할 수 있습니다. 사용 가능한 펌웨어 설정은 서버 유형, Flex System 환경 및 서버 패턴 범위에 따라 다릅니다.

범주 패턴을 서버 패턴과 별도로 작성할 수 있습니다.

범주 패턴을 미리 정의하거나, 기존 서버에서 가져오거나, 사용자 정의할 수 있습니다.

- **확장된 범주 패턴**

  확장된 범주 패턴은 특정 관리되는 서버에서 가져와서 동적으로 작성한 일부 I/O 어댑터 포트, 고급 UEFI(Unified Extensible Firmware Interface) 및 베이스보드 관리 컨트롤러(BMC) 설정에 대한 패턴입니다. Lenovo XClarity Administrator는 기존 서버에서 서버 패턴을 작성할 때 이러한 패턴을 작성합니다. 확장된 범주 패턴을 수동으로 작성할 수는 없지만 패턴이 작성된 후에는 패턴을 편집할 수 있습니다.

  다음 확장된 UEFI 패턴은 특정 환경에 대해 서버를 최적화하기 위해 XClarity Administrator에 의해 미리 정의됩니다.
  - **ESXi 설치 옵션**
  - **효율성 – 성능 우선**
  - **효율성 – 전력 우선**
  - **최대 성능**
  - **최소 전력**

- **사용자 정의된 범주 패턴**

  사용자 정의된 범주 패턴은 시스템 정보, 관리 인터페이스, 장치 및 I/O 포트, Fibre Channel 부팅 대상 및 I/O 어댑터 포트 등 사용자가 작성할 수 있는 패턴입니다. 다음 범주 패턴을 작성할 수 있습니다.

- **시스템 정보**. 이 설정에는 자동으로 생성된 시스템 이름, 위치, 접속자가 포함됩니다.
- **관리 인터페이스**. 이 설정에는 관리 인터페이스에 대해 자동으로 생성된 호스트 이름, IP 주소, 도메인 이름 공간(DNS), 인터페이스 속도 및 포트 할당이 포함됩니다.서버 패턴에서는 Duplex 설정이 지원되지 않습니다.
- **장치 및 I/O 포트**. 이 설정에는 콘솔 리디렉션 및 COM 포트가 포함됩니다. 서버 패턴을 사용하여 콘솔 리디렉션 영역에서 SOL(serial over LAN)을 사용으로 설정할 수 있습니다. 그러나 SOL(serial over LAN)을 사용하는 경우 서버 패턴에서 지원되는 직렬 포트 액세스 모드 설정만 **전용**입니다. 직렬 포트 액세스 모드의 **공유** 및 **사전 부팅** IPMI 설정은 서버 패턴에서 사용할 수 없습니다.

  중요: 기존 서버에서 서버 패턴을 작성하고 해당 서버의 직렬 포트 액세스 모드 설정이 **공유** 또는 **사전 부팅**인 경우 서버에서 가져온 장치 및 I/O 포트 패턴의 직렬 포트 액세스 모드 설정은 **전용**입니다.
- Fibre Channel **부팅 대상**. 이 설정에는 특정 기본 및 보조 Fibre Channel WWN 부팅 대상이 포함됩니다.
- **포트**. 이 설정에는 패브릭 상호 연결을 구성하기 위한 I/O 어댑터와 포트가 포함됩니다.

서버 패턴 만들기

서버 패턴을 작성할 때 특정 유형의 서버에 대한 구성 특성을 정의합니다. 기본 설정으로 새 서버 패턴을 처음부터 새로 만들거나 기존 서버의 설정을 사용하여 서버 패턴을 만들 수 있습니다.

이 작업 정보

서버 패턴을 작성하기 전에 다음 제안을 고려하십시오.

- 처음으로 서버 패턴을 작성하는 경우 이를 기존 서버에서 작성할 것을 고려해 보십시오. 기존 서버에서 서버 패턴을 작성하는 경우 Lenovo XClarity Administrator는 일부 I/O 어댑터 포트, UEFI 및 베이스보드 관리 컨트롤러 설정에 대해 확장된 범주 패턴을 가져와서 작성합니다. 그러면 이러한 범주 패턴을 나중에 작성할 서버 패턴에 사용할 수 있습니다. 범주 패턴에 대한 자세한 정보는 펌웨어 설정 정의의 내용을 참조하십시오.
- 동일한 하드웨어 옵션을 가지고 동일한 방식으로 구성하려는 서버 그룹을 식별하십시오. 서버 패턴을 사용하여 여러 서버에 동일한 구성 설정을 적용함으로써 한 위치에서 공통 구성을 제어할 수 있습니다.
- 서버 패턴(예, 로컬 스토리지, 네트워크 어댑터, 부트 설정, 관리 컨트롤러 설정, UEFI 설정)에 대해 사용자 지정하려는 구성 측면을 식별하십시오.
- 구성 패턴을 사용하여 로컬 사용자 계정을 관리하거나 LDAP 서버를 구성할 수 없습니다.

중요: 관리 노드가 실패하면 서버 패턴이 유실될 수 있습니다. 서버 패턴을 작성하거나 수정한 후에는 항상 관리 소프트웨어를 백업하십시오(Lenovo XClarity Administrator 백업 참조).

절차

서버 패턴을 작성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.

단계 2. **서버 패턴** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 서버 패턴 마법사가 표시됩니다.

단계 4. 서버 패턴을 작성하려면 다음 작업 중 하나를 수행하십시오.

- 기존 서버의 설정을 사용하려면 **기존 서버에서 새 패턴 만들기**를 클릭하십시오. 그런 다음 표시된 목록에서 새 패턴을 기반으로 하는 관리되는 서버를 선택하십시오.

  기존 서버에서 서버 패턴을 작성하는 경우 XClarity Administrator는 지정된 관리되는 서버의 설정(예, 확장된 포트, UEFI 및 관리 컨트롤러 설정)을 가져와서 해당 설정에 대한 범주 패턴을 동적으로 작성합니다. 서버가 새 제품인 경우 Lenovo XClarity Administrator는 제조 시 설정을 학습합니다. XClarity Administrator에서 서버를 관리하는 경우 XClarity

Administrator는 사용자 정의 설정을 사용합니다. 이 패턴을 배포할 서버에 특정하게 설정을 사용자 지정할 수 있습니다.

- 기본 설정을 사용하려면 **새 패턴 처음부터 새로 만들기**를 클릭하십시오. 그런 다음 **폼 팩터** 필드에서 서버 유형을 선택하십시오.

참고: 나머지 탭에 표시되는 옵션은 패턴을 작성할 서버 유형에 따라 다를 수 있습니다.

단계 5. 패턴 이름과 설명을 입력하십시오.

단계 6. **사용자 지정** 토글을 선택한 후 이름 지정 스키마(예, 사용자 지정 텍스트, 서버 이름 및 증가 번호)에 포함할 하나 이상의 요소와 순서를 선택하여 서버 프로필 이름을 사용자 지정하십시오.

단계 7. **다음**을 클릭하십시오.

단계 8. 서버에 패턴을 배포할 때 적용할 로컬 스토리지 구성을 선택하고 **다음**을 클릭하십시오.

로컬 스토리지 설정에 대한 정보는 로컬 저장 장치 정의의 내용을 참조하십시오.

단계 9. **옵션:** I/O 어댑터 주소 지정을 수정하고 이 패턴으로 구성될 하드웨어와 일치하도록 추가 I/O 어댑터를 정의한 후 **다음**을 클릭하십시오.

I/O 어댑터 설정에 대한 정보는 I/O 어댑터 정의의 내용을 참조하십시오.

단계 10. 이 패턴을 서버에 배포할 때 적용할 부팅 순서를 정의하고 **다음**을 클릭하십시오.

SAN 부팅 대상 설정에 대한 정보는 부팅 옵션 정의의 내용을 참조하십시오.

단계 11. 기존 범주 패턴에서 펌웨어 설정을 선택하십시오.

만들기 아이콘( )을 클릭하여 새 범주 패턴을 작성할 수 있습니다.

펌웨어 설정에 대한 정보는 펌웨어 설정 정의의 내용을 참조하십시오.

단계 12. 패턴을 저장하려면 **저장**을 클릭하고 하나 이상의 서버에 패턴을 즉시 배포하려면 **저장 및 배포**를 클릭하십시오.

서버 패턴 배포에 대한 정보는 서버에 서버 패턴 배포의 내용을 참조하십시오.

완료한 후에

저장 및 배포를 클릭하면 서버 패턴 배포 페이지가 표시됩니다. 이 페이지에서 서버 패턴을 특정 서버에 배포할 수 있습니다.

저장을 클릭하면 서버 패턴과 모든 범주 패턴이 서버 패턴 페이지에 저장됩니다.

이 페이지에서 선택한 서버 패턴에 다음 동작을 수행할 수 있습니다.
- **이름** 열에서 패턴 이름을 클릭하여 패턴에 대한 세부 정보를 봅니다.
- 패턴을 배포합니다(서버에 서버 패턴 배포 참조).
- **복사** 아이콘( )을 클릭하여 패턴을 복사합니다.
- 패턴을 편집합니다(서버 패턴 수정 참조).
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- 서버 패턴을 내보내고 가져옵니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

로컬 저장 장치 정의

이 패턴을 배포할 때 대상 서버에 적용할 로컬 스토리지 구성을 정의할 수 있습니다.

이 작업 정보

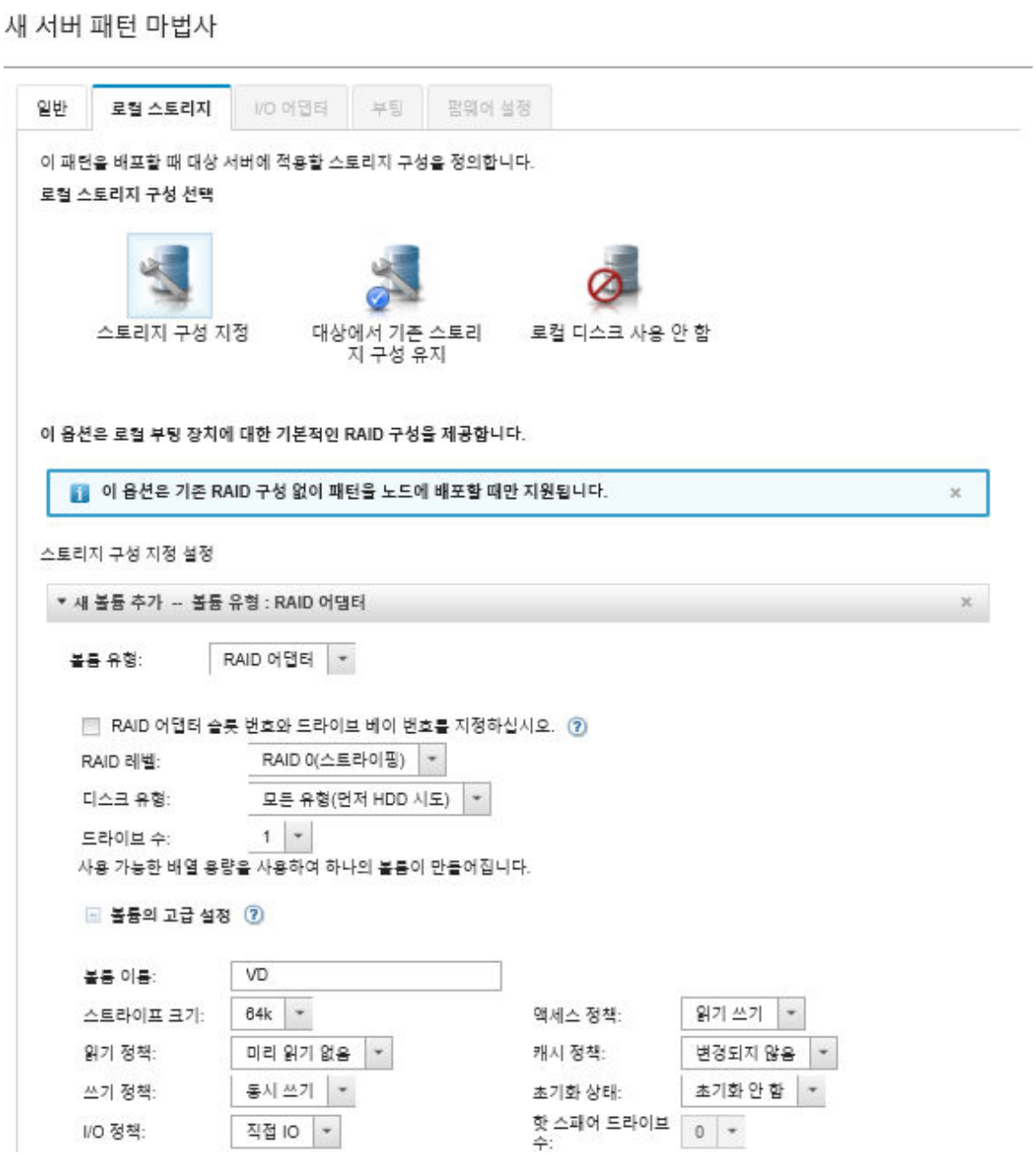
참고:

- Flex System x220, Flex System x222 및 ThinkSystem 서버의 온보드 스토리지 컨트롤러는 소프트웨어 기반 RAID를 지원합니다. 그러나 구성 패턴을 사용하는 소프트웨어 RAID의 구성은 지원되지 않습니다.
- 구성 패턴을 사용하여 RAID를 구성할 때 서버의 전원이 꺼져 있으면 서버 프로필을 활성화하기 전에 서버가 자동으로 BIOS/UEFI Setup으로 부팅됩니다.

절차

로컬 스토리지 구성을 정의하려면 다음 단계를 완료하십시오.

단계 1. 새 서버 패턴 마법사에서 **로컬 스토리지** 탭을 클릭하십시오.



단계 2. 로컬 스토리지 설정을 정의하려면 다음 옵션 중 하나를 선택하십시오.

- **스토리지 구성 지정**. (RAID 구성을 종료하지 않고 장치만) 기본 RAID 설정은 배포 중에 로컬 부트 장치에 구성됩니다

  스토리지 옵션에 따라 스토리지 구성을 지정하십시오. **추가**를 클릭하여 추가 저장 공간을 추가할 수 있습니다. (➕) 아이콘을 클릭하여 추가 볼륨 유형을 추가할 수 있습니다.

  – **RAID 어댑터**. RAID 수준, 특성 및 서버에 설치되는 드라이브 수를 선택하십시오. RAID 0, 1, 5가 지원됩니다. 또한 스트라이프 크기, 정책 및 핫 스페어 드라이브 수와 같은 고급 볼륨 설정을 선택할 수 있습니다.

    XCC 버전 2.1 이상이 지원되는 ThinkSystem 서버(ThinkSystem SR950에는 XCC 버전 1.4 이상 필요), 사용 가능한 어레이 용량을 사용하여 단일 볼륨을 작성하도록 RAID 어댑터 슬롯 번호 및 드라이브 베이 번호를 지정할 수도 있습니다. 이 경우 RAID 레벨 0, 1, 5, 6, 10, 50, 60 및 00이 지원됩니다. 또한 스트라이프 크기, 정책 및 핫 스페어 드라이브와 같은 고급 볼륨 설정을 선택할 수 있습니다.

참고: 대상 서버에서 지정된 유형의 사용 가능한 드라이브가 충분한지 확인하고 서버 인벤토리 세부 정보 페이지의 **드라이브** 섹션에 설명된 대로 드라이브의 RAID 상태가 Unconfigured Good인지 확인하십시오(관리 서버의 세부 정보 보기 참조).

- **Lenovo SD 미디어 어댑터**. 볼륨을 만들고 볼륨 크기를 지정할 위치를 선택하십시오. 또한 미디어 유형 및 액세스 정책과 같은 고급 볼륨 설정을 지정할 수 있습니다.
- **ThinkSystem M.2(미러링 포함)**. PCI 슬롯, RAID 레벨, 볼륨 이름, 및 스프라이프 크기를 선택하여, 이용 가능한 어레이 용량을 사용하는 단일 볼륨을 생성하십시오.
  - Mirroring 저장소 어댑터가 있는 ThinkSystem M.2 여러 개를 각각 다른 PCI 슬롯에 정의할 수 있습니다.
  - ThinkSystem Edge Server의 경우 특정 PCI 슬롯 번호를 지정해야 합니다. M.2 RAID 어댑터가 하나만 설치된 다른 ThinkSystem 서버의 경우, First Matched(기본값)를 선택하거나 특정 PCI 슬롯 번호를 지정할 수 있습니다.
- **Intel Optane DC 영구 메모리**. 영구 메모리 유형, 남은 용량의 백분율에 대한 경고 임계값 및 메모리로 사용할 총 용량의 백분율을 선택하십시오. (남은 메모리는 영구 스토리지로 사용됩니다.)

  주의:
  - Intel Optane DC 영구 메모리 DIMM을 구성하려면 보안을 사용 안 함으로 설정하고 네임스페이스를 생성하지 않아야 합니다.
  - 서버에 있는 모든 Intel Optane DC 영구 메모리 DIMM의 보안 상태가 "사용 안 함"인 경우에만 보안 사용이 지원됩니다.
  - 보안 사용 안 함 및 보안 지우기는 보안 상태가 "잠금"이고 암호가 서버의 모든 Intel Optane DC 영구 메모리 DIMM에 대해 동일한 경우에만 지원됩니다.
  - Intel Optane DC PMEM 보안 상태는 XClarity Administrator 인벤토리에 포함되지 않습니다. UEFI에서 보안 상태를 수동으로 확인할 수 있습니다.

- **대상에서 기존 스토리지 구성 유지**. 배포 중에는 기존 스토리지 구성이 변경되지 않습니다. 대상 서버에 이미 있는 스토리지 구성을 사용하려면 이 옵션을 선택하십시오.
- **로컬 디스크 사용 안 함**. (Flex System x240 계산 노드 경우) 온보드 스토리지 컨트롤러 및 스토리지 옵션 ROM(UEFI 및 Legacy 모두)을 사용 안 함으로 설정할 수 있습니다. 로컬 디스크 드라이브를 사용 안 함으로 설정하면 SAM에서 부팅할 때 전체 부팅 시간이 줄어듭니다.

I/O 어댑터 정의

이 패턴을 배포할 때 대상 서버에 적용할 I/O 포트 설정 및 주소 지정 모드를 정의할 수 있습니다.

이 작업 정보

I/O 어댑터 주소를 가상화하거나 다시 할당하는 경우 가상 I/O 어댑터 주소 지정을 사용하도록 이 패턴을 구성할 수 있습니다.

기존 서버에서 패턴을 만드는 경우 일부 어댑터 정보가 자동으로 설정될 수 있습니다. 이 패턴을 배포할 때 서버에 있을 것으로 예상되는 하드웨어와 일치하도록 추가 I/O 어댑터 패턴을 정의할 수 있습니다. I/O 어댑터 패턴을 정의하여 지원되는 어댑터에 대한 어댑터 포트 설정을 구성할 수 있습니다. 가상 I/O 어댑터 주소를 사용하는 경우 추가하는 Fibre Channel 어댑터에 대한 SAN 부팅 대상을 정의할 수도 있습니다(부팅 옵션 정의 참조).

절차

I/O 어댑터 설정을 정의하려면 다음 단계를 완료하십시오.

단계 1. 새 서버 패턴 마법사에서 **I/O 어댑터** 탭을 클릭하십시오.

참고: **고급 설정**을 클릭하여 I/O 어댑터에 대한 추가 정보를 표시할 수 있습니다.

단계 2. Flex System 섀시의 서버에 대한 서버 패턴을 작성하는 경우 I/O 어댑터 주소 지정 모드 유형을 선택하십시오.

- **번인(burn-in)**. 공장 출하 시 어댑터와 함께 제공되는 기존 WWN(World Wide Name) 및 MAC(Media Access Control) 주소를 사용하십시오.
- **가상**. LAN 및 SAN 연결 관리를 단순화하려면 가상 I/O 어댑터 주소 지정을 사용하십시오. I/O 주소를 가상화하면 가상화된 Fibre WWN 및 이더넷 MAC 주소로 번인(burn-in) 하드웨어 주소를 다시 할당합니다. SAN 멤버십을 미리 구성하여 배포 속도를 높이고 하드웨어 교체 시 SAN 구역 지정 및 LAN 마스킹 할당 재구성 필요를 제거함으로써 장애 조치를 용이하게 할 수 있습니다.

  가상 주소 지정을 사용하는 경우 정의된 어댑터와 상관 없이 기본적으로 이더넷과 Fibre Channel 주소가 둘 다 할당됩니다. 이더넷 및 Fibre Channel 주소를 할당하는 소스 풀을 선택할 수 있습니다.

  주소 모드 옆에 있는 **편집** 아이콘( )을 클릭하여 가상 주소 설정을 편집할 수도 있습니다.

  제한사항: 가상 주소 지정은 Flex System 섀시의 서버에만 지원됩니다. 랙 및 타워 서버는 지원되지 않습니다.

단계 3. Flex System 섀시의 서버에 대한 서버 패턴을 작성하는 경우 다음 확장 옵션 중 하나를 선택하십시오. 테이블의 행은 선택한 항목을 기반으로 하여 변경됩니다.
- 확장 불가능 Flex system
- 2 노드 확장 가능 Flex system
- 4 노드 확장 가능 Flex system

단계 4. 패턴을 배포할 서버에 설치되어 있을 것으로 예상되는 I/O 어댑터 패턴을 선택하십시오. 어댑터를 추가하려면 다음을 수행하십시오.

a. I/O 어댑터 1 또는 LOM 추가 대화 상자를 표시하려면 테이블에서 **I/O 어댑터 추가** 링크를 클릭하십시오.

b. 어댑터의 PCI 슬롯을 선택하십시오.

c. 테이블에서 어댑터 유형을 선택하십시오.

  참고: 기본적으로 테이블에는 관리되는 서버에 현재 설치된 I/O 어댑터만 나열됩니다. 지원되는 모든 I/O 어댑터를 나열하려면 **지원되는 모든 어댑터**를 클릭하십시오.

d. 패턴이 배포될 때 포트 그룹의 모든 포트에 할당될 초기 포트 패턴을 선택하십시오.

*포트 패턴*을 사용하여 서버에서 가져온 포트 설정을 수정할 수 있습니다. 어댑터가 처음 추가되면 이러한 초기 포트 패턴이 할당됩니다. 어댑터가 추가된 후 I/O 어댑터 페이지에서 개별 포트에 다른 패턴을 할당할 수 있습니다.

만들기 아이콘( )을 클릭하여 포트 패턴을 작성할 수 있습니다. **편집** 아이콘( )을 클릭하여 기존 패턴을 기반으로 하여 포트 패턴을 작성할 수 있습니다.

포트 패턴에 대한 자세한 정보는 포트 설정 정의의 내용을 참조하십시오.

e. **추가**를 클릭하여 I/O 어댑터 페이지의 테이블에 포트 패턴을 추가하십시오.

부팅 옵션 정의

이 패턴을 배포할 때 대상 서버에 적용할 부팅 순서를 정의할 수 있습니다.

절차

부팅 옵션 패턴을 작성하려면 다음 단계를 완료하십시오.

단계 1. 새 서버 패턴 마법사에서 **부팅** 탭을 클릭하십시오.

단계 2. 다음 시스템 부팅 모드 중 하나를 선택하십시오.

- **UEFI Only Boot**. UEFI(Unified Extensible Firmware Interface)를 지원하는 서버를 구성하려면 이 옵션을 선택하십시오. UEFI 사용 운영 체제를 부팅하는 경우 이 옵션은 레거시 옵션 ROM을 사용 안 함으로 설정하여 부팅 시간을 단축시킬 수 있습니다.

  Thinksystem 서버에서 패턴을 학습하는 경우, **기본 부팅 순서** 탭을 클릭하여 부팅 순서를 지정할 수 있습니다. 패턴을 배치할 서버에 지정된 부팅 순서를 유지하거나 부팅 옵션을 적용 할 순서를 지정하도록 부팅 순서를 구성할 수 있습니다. 그러나 장치 그룹에서 부팅 장치의 부팅 우선 순위(부팅 옵션)는 지원되지 않습니다.

- **UEFI First, Then Legacy**. 우선 UEFI를 사용하여 부팅하도록 서버를 구성하려면 이 옵션을 선택하십시오. 문제가 있으면 서버가 레거시 모드로 부팅합니다.

  Thinksystem 서버에서 패턴을 학습하는 경우, **기본 부팅 순서** 탭을 클릭하여 부팅 순서를 지정할 수 있습니다. 패턴을 배치할 서버에 지정된 부팅 순서를 유지하거나 부팅 옵션을 적용 할 순서를 지정하도록 부팅 순서를 구성할 수 있습니다. 그러나 장치 그룹에서 부팅 장치의 부팅 우선 순위(부팅 옵션)는 지원되지 않습니다.

- **Legacy Only Boot**. 레거시(BIOS) 펌웨어가 필요한 운영 체제를 부팅하도록 서버를 구성하는 경우 이 옵션을 선택하십시오. 비UEFI 사용 운영 체제를 부팅하는 경우에만 이 옵션을 선택하십시오.

  팁: Legacy Only Boot 모드(부팅 시간이 훨씬 빠름)를 선택하는 경우 FoD(Features on Demand) 키를 활성화할 수 없습니다.

  이 옵션을 선택한 경우 다음을 지정할 수 있습니다.

- **기본 부팅 순서**. 패턴을 배포할 서버에 지정된 부팅 순서를 유지하도록 선택하십시오. 또한 Legacy Only Boot 순서를 구성하여 부팅 옵션이 적용되는 순서를 지정하도록 선택할 수도 있습니다.
- **WoL(Wake on LAN) 부팅 순서**. 패턴을 배포할 서버에 지정된 현재 WoL 부팅 순서를 유지하도록 선택하십시오. 또한 Legacy Only Boot 순서를 구성하여 WoL 부팅 옵션이 적용될 순서를 지정하도록 선택할 수도 있습니다.

• **기존 부팅 모드 유지**. 대상 서버에서 기존 설정을 유지하려면 이 옵션을 선택하십시오. 패턴을 배포할 때 부팅 순서가 변경되지 않습니다.

단계 3. SAN **부팅** 탭을 선택하여 부팅 대상 패턴을 선택하고 부팅 장치 대상을 지정하십시오.

참고: I/O 어댑터를 정의할 때 Fibre Channel 어댑터를 정의하고 가상 주소 지정을 사용하도록 설정한 경우 Fibre Channel 어댑터에 대한 SAN 기본 및 보조 부팅 대상을 설정할 수 있습니다. 스토리지 대상에 대한 여러 WWPN(worldwide port name) 및 LUN(logical unit number) ID를 지정할 수 있습니다.

펌웨어 설정 정의

이 패턴을 배포할 때 대상 서버에 적용할 베이스보드 관리 컨트롤러 및 UEFI 펌웨어 설정을 지정할 수 있습니다.

이 작업 정보

펌웨어 설정은 관련 설정을 그룹화하는 범주로 구성됩니다. 각 범주에 대해 공통 펌웨어 설정이 포함되고 여러 서버 패턴에서 재사용될 수 있는 *범주 패턴*을 작성할 수 있습니다. 베이스보드 관리 컨트롤러 및 UEFI에서 직접 구성할 수 있는 대부분의 펌웨어 설정은 범주 패턴을 통해서도 구성할 수 있습니다. 사용 가능한 펌웨어 설정은 서버 유형, Flex System 환경 및 서버 패턴 범위에 따라 다릅니다.

범주 패턴을 미리 정의하거나, 사용자 정의하거나, 기존 서버에서 가져올 수 있습니다.

- *확장된 범주 패턴*은 특정 관리되는 서버에서 가져와서 동적으로 작성한 일부 I/O 어댑터 포트, 고급 UEFI(Unified Extensible Firmware Interface) 및 베이스보드 관리 컨트롤러(BMC) 설정에 대한 패턴입니다. Lenovo XClarity Administrator는 기존 서버에서 서버 패턴을 작성할 때 이러한 패턴을 작성합니다. 확장된 범주 패턴을 수동으로 작성할 수는 없지만 패턴이 작성된 후에는 패턴을 편집할 수 있습니다.
- *사용자 정의된 범주 패턴*은 시스템 정보, 관리 인터페이스, 장치 및 I/O 포트, Fibre Channel 부팅 대상 및 I/O 어댑터 포트 등 사용자가 작성할 수 있는 패턴입니다.

절차

펌웨어 설정을 정의하려면 다음 단계를 완료하십시오.

단계 1. 새 서버 패턴 마법사에서 **펌웨어 설정** 탭을 클릭하십시오.

단계 2. 정의하려는 설정이 포함된 범주 패턴 유형을 선택하십시오.

- **시스템 정보**. 이 범주 패턴을 사용하여 자동 시스템 이름 생성, 접속자 이름 및 위치를 정의하십시오. 시스템 정보 패턴에 대한 자세한 정보는 시스템 정보 설정 정의의 내용을 참조하십시오.
- **관리 인터페이스**. 이 범주 패턴을 사용하여 자동 호스트 이름 생성, 관리 IP 주소 할당, 도메인 이름 시스템(DNS) 설정 및 인터넷 속도 설정을 정의합니다. 관리 인터페이스 패턴에 대한 자세한 정보는 관리 인터페이스 설정 정의의 내용을 참조하십시오.
- **장치 및 I/O 포트**. 이 범주 패턴을 사용하여 콘솔 리디렉션 및 COM 포트, PCIe 속도, 온보드 장치, 어댑터 옵션 ROM 및 옵션 ROM 실행 순서를 정의합니다. 장치 및 I/O 포트 패턴에 대한 자세한 정보는 장치 및 I/O 포트 설정 정의의 내용을 참조하십시오.
- **확장된** BMC. 이 범주 패턴을 사용하여 다른 베이스보드 관리 컨트롤러 설정을 정의합니다. 확장된 관리 컨트롤러 패턴은 기존 서버에서 서버 패턴을 작성할 때 자동으로 작성됩니다. 확장된 관리 컨트롤러 패턴은 수동으로 작성할 수 없습니다. 관리 인터페이스 패턴에 대한 자세한 정보는 확장된 관리 컨트롤러 설정 정의의 내용을 참조하십시오.
- **확장된** UEFI. 이 범주 패턴을 사용하여 다른 UEFI(Unified Extensible Firmware Interface) 설정을 정의합니다. 확장된 UEFI 패턴은 기존 서버에서 서버 패턴을 작성할 때 자동으로 작성됩니다. 확장된 UEFI 패턴은 수동으로 작성할 수 없습니다. 관리 인터페이스 패턴에 대한 자세한 정보는 확장 UEFI 설정 정의의 내용을 참조하십시오.

단계 3. 해당 범주 패턴 유형 옆에 있는 **만들기** 아이콘( )을 클릭하여 새 범주 패턴을 작성하십시오.

드롭다운 목록에서 특정 패턴을 선택하고 해당 범주 패턴 유형 옆에 있는 **편집** 아이콘( )을 클릭하여 기존 범주 패턴을 편집할 수도 있습니다. 패턴을 편집하고 **다른 이름으로 저장**을 클릭하여 패턴을 새 이름으로 저장함으로써 기존 범주 패턴을 복사할 수도 있습니다.

시스템 정보 설정 정의

시스템 정보 패턴을 작성하여 시스템 이름, 접속자 및 위치 정보를 정의할 수 있습니다.

절차

시스템 정보 패턴을 작성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **시스템 정보 패턴** 수직 탭을 클릭한 다음 **만들기** 아이콘( )을 클릭하십시오.

팁: 시스템 정보 섹션 옆에 있는 **만들기** 아이콘을 클릭하여 새 서버 패턴 마법사의 펌웨어 설정 페이지에서 새 시스템 정보 패턴을 작성할 수도 있습니다.

단계 4. 새 시스템 정보 패턴 대화 상자에서 다음 정보를 지정하십시오.

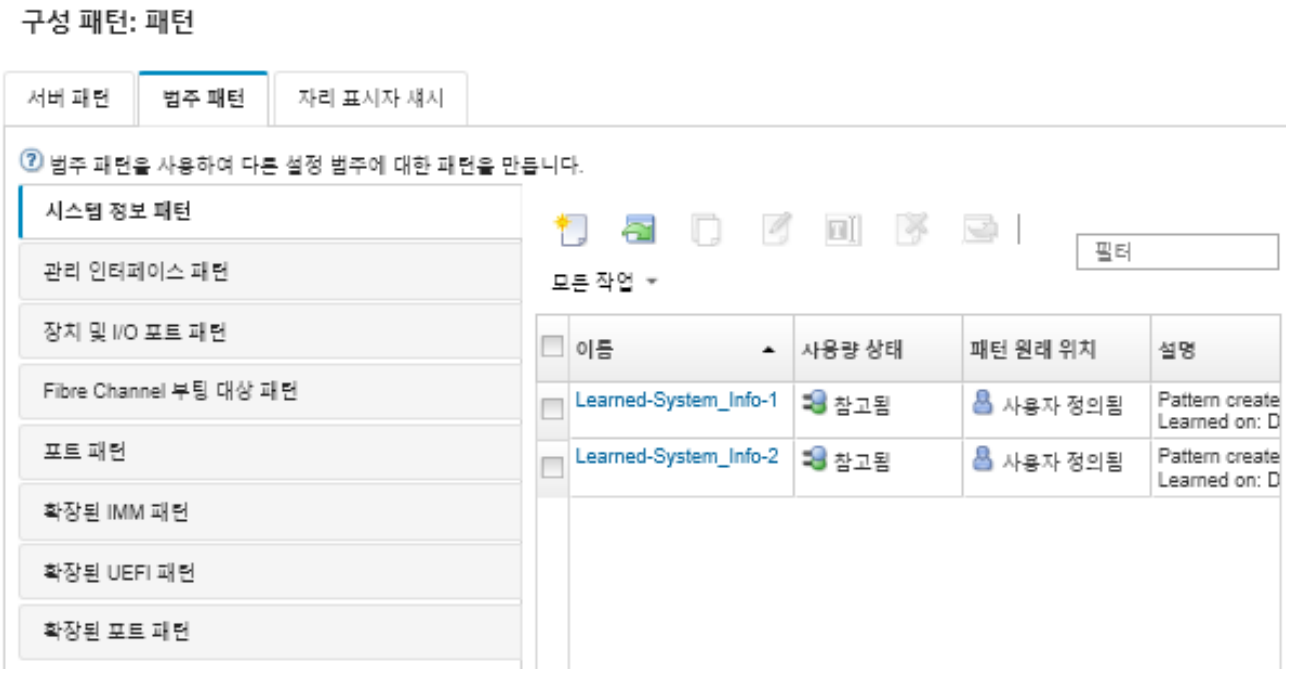
- 패턴의 이름과 설명을 입력하십시오.
- 시스템 이름을 자동으로 생성할지 여부를 선택하십시오. **사용자 지정**을 클릭한 경우 패턴을 배포할 때 이름이 생성되는 방법을 지정할 수 있습니다. **사용 안 함**을 클릭하면 패턴을 배포할 때 각 서버에서 시스템 이름이 변경되지 않고 그대로 유지됩니다. 대부분의 장치에서 이름은 베이스보드 관리 컨트롤러에 의해 256자의 영문자로 제한됩니다. 자동으로 생성되는 이름은 256자에서 잘립니다.
- 이 서버에 접속할 사용자와 서버 위치를 지정하십시오.

  참고: SNMP를 사용하는 경우 접속자와 시스템 위치를 반드시 지정해야 합니다.

단계 5. **만들기**를 클릭하십시오.

결과

새 패턴은 구성 패턴: 범주 패턴 페이지의 **시스템 정보 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **편집** 아이콘( )을 클릭하여 현재 패턴 설정을 수정합니다.
- **복사** 아이콘( )을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

관리 인터페이스 설정 정의

관리 인터페이스 패턴을 작성하여 관리 인터페이스에 대한 호스트 이름, IP 주소, 도메인 이름 시스템(DNS), 인터페이스 속도 및 포트 할당을 정의할 수 있습니다.

절차

관리 인터페이스 패턴을 작성하려면 다음 단계를 완료하십시오.

참고: 서버 패턴에서는 Duplex 설정이 지원되지 않습니다.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **관리 인터페이스 패턴** 수직 탭을 클릭한 다음 **만들기** 아이콘( )을 클릭하십시오.

팁: 관리 인터페이스 선택 항목 옆에 있는 **만들기** 아이콘( )을 클릭하여 새 서버 패턴 마법사의 펌웨어 설정 페이지에서 새 관리 인터페이스 패턴을 작성할 수도 있습니다.

단계 4. 새 관리 인터페이스 패턴 대화 상자에서 다음 정보를 지정하십시오.

- 패턴의 이름과 설명을 입력하십시오.
- **호스트 이름** 탭을 클릭하고 호스트 이름을 자동으로 생성하도록 선택하십시오. **사용자 지정**을 클릭한 경우 패턴을 배포할 때 이름이 생성되는 방법을 지정할 수 있습니다. **사용 안 함**을 클릭하면 패턴을 배포할 때 각 서버에서 호스트 이름이 변경되지 않고 그대로 유지됩니다.

  호스트 이름은 베이스보드 관리 컨트롤러에 의해 63자의 영문자로 제한됩니다. 자동으로 생성되는 이름은 63자에서 잘립니다.
- **관리 IP 주소** 탭을 클릭하고 IPv4 및 IPv6 주소 설정을 구성하십시오.

  IPv4 주소의 경우 다음 옵션 중 하나를 선택할 수 있습니다.
  - **DHCP 서버에서 동적 IP 주소를 얻으십시오.**
  - **DHCP에 의한 첫 번째**. 실패하는 경우 주소 풀에서 고정 IP 주소를 얻으십시오.
  - **주소 풀에서 고정 IP 주소를 얻으십시오.**

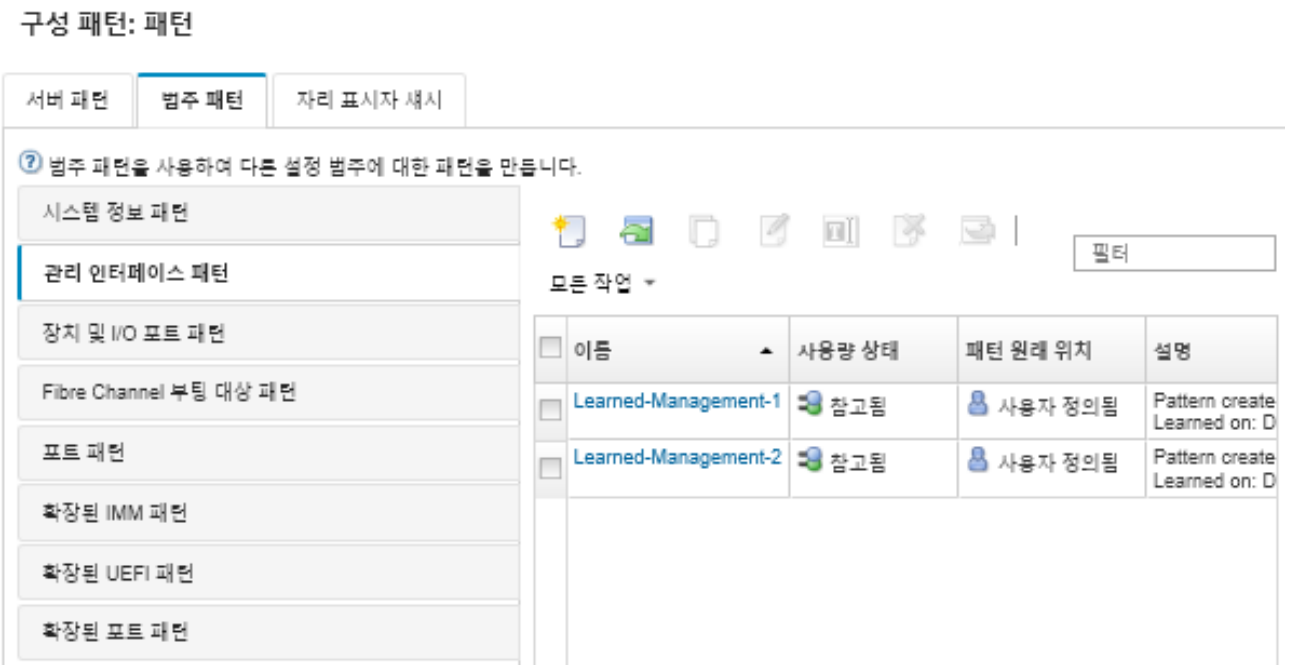
  IPv6 주소의 경우 다음을 선택할 수 있습니다.
  - **상태 비저장 주소 자동 구성을 사용합니다.**
  - **DHCP 서버에서 동적 IP 주소를 얻으십시오.**
  - **주소 풀에서 고정 IP 주소를 얻으십시오.**

  도메인 이름 시스템(DNS) 탭에서 동적 도메인 이름 서비스(DDNS)를 사용 또는 사용 안 함으로 선택하십시오. DDNS를 사용하는 경우 다음 옵션 중 하나를 선택할 수 있습니다.
  - DHCP 서버에서 도메인 이름을 얻습니다.
  - 도메인 이름을 지정합니다.
- **인터페이스 설정** 탭을 클릭하고 최대 전송 단위(MTU)를 지정하십시오. 기본값은 1500입니다.
- **포트 할당** 탭을 클릭하고 다음 포트에 사용할 번호를 지정하십시오.
  - HTTP
  - HTTPS
  - 텔넷 CLI
  - SSH CLI
  - SNMP 에이전트
  - SNMP 트랩
  - 원격 제어 콘솔
  - HTTP를 통한 CIM
  - HTTPS를 통한 CIM

단계 5. **만들기**를 클릭하십시오.

결과

새 패턴은 구성 패턴: 범주 패턴 페이지의 **관리 인터페이스 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **편집** 아이콘()을 클릭하여 현재 패턴 설정을 수정합니다.
- **복사** 아이콘()을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘()을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘()을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

장치 및 I/O 포트 설정 정의

장치 및 I/O 포트 패턴을 작성하여 콘솔 리디렉션을 사용 설정하고 COM 1 포트 특성을 사용 설정 및 정의할 수 있습니다.

절차

장치 및 I/O 포트 패턴을 작성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **장치 및 I/O 포트 패턴** 수직 탭을 클릭한 다음 **만들기** 아이콘()을 클릭하십시오.

팁: 장치 및 I/O 포트 선택 항목 옆에 있는 **만들기** 아이콘()을 클릭하여 새 서버 패턴 마법사의 펌웨어 설정 페이지에서 장치 및 I/O 포트 패턴을 작성할 수도 있습니다.

단계 4. 새 장치 및 I/O 포트 패턴 대화 상자에서 다음 정보를 지정하십시오.

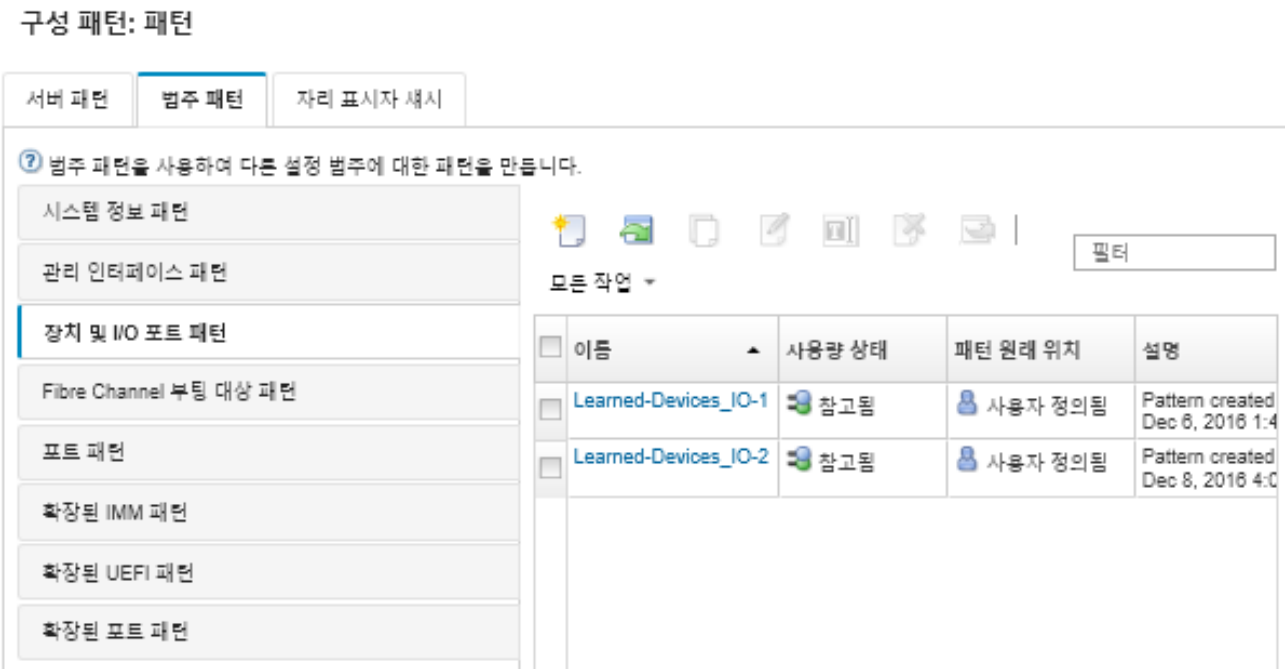
- 패턴의 이름과 설명을 입력하십시오.
- 콘솔 리디렉션 사용 또는 사용 안 함을 선택하십시오. 콘솔 리디렉션을 사용하는 경우 다음을 사용 또는 사용 안 함으로 선택할 수 있습니다.
  - Serial over LAN.
  - **서비스 프로세서 리디렉션**. 서비스 프로세서 리디렉션을 사용하는 경우 레거시 옵션 직렬 데이터 포트에 COM 포트 1 또는 2를 사용하도록 선택할 수도 있습니다. 사용 안 함으로 설정된 경우 항상 COM 포트 1이 사용됩니다.다음 CLI 모드 중 하나를 선택할 수도 있습니다.
    - 사용 안 함

  - 사용자 정의 키스트로크 시퀀스에 사용
  - EMS 호환 키 입력 순서 사용
- COM 포트 1과 2를 사용 또는 사용 안 함으로 선택하십시오. COM 포트를 사용으로 선택한 경우 다음 설정을 지정하십시오.
  - 전송 속도
  - 데이터 비트
  - 패리티
  - 정지 비트
  - 텍스트 열거
  - 부팅 후 활성
  - 흐름 제어

단계 5. **만들기**를 클릭하십시오.

결과

새 패턴은 구성 패턴: 범주 패턴 페이지의 **장치 및 I/O 포트 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **편집** 아이콘( )을 클릭하여 현재 패턴 설정을 수정합니다.
- **복사** 아이콘( )을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

Fibre Channel 부팅 대상 설정 정의

Fibre Channel 부팅 대상 패턴을 작성하여 로컬 디스크 드라이브 대신 SAN(storage area network) 장치에서 부팅할 서버를 구성할 수 있습니다.

절차

Fibre Channel 부팅 대상 패턴을 작성하려면 다음 단계를 완료하십시오.

제한사항: Fibre Channel 부팅 대상은 Flex 컴퓨팅 노드에만 지원됩니다. 독립 실행형 랙 및 타워 서버는 지원되지 않습니다.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **Fibre Channel 부팅 대상 패턴** 수직 탭을 클릭한 다음 **만들기** 아이콘( )을 클릭하십시오.

단계 4. 새 Fibre Channel 부팅 대상 패턴 대화 상자에서 다음 정보를 지정하십시오.

- 패턴의 이름과 설명을 입력하십시오.
- 기본 부팅 대상으로 사용할 하나 이상의 WWPN 주소와 LUN ID를 지정하십시오. 보조 부팅 대상으로 사용할 하나 이상의 WWPN 주소와 LUN ID를 선택적으로 지정할 수도 있습니다.

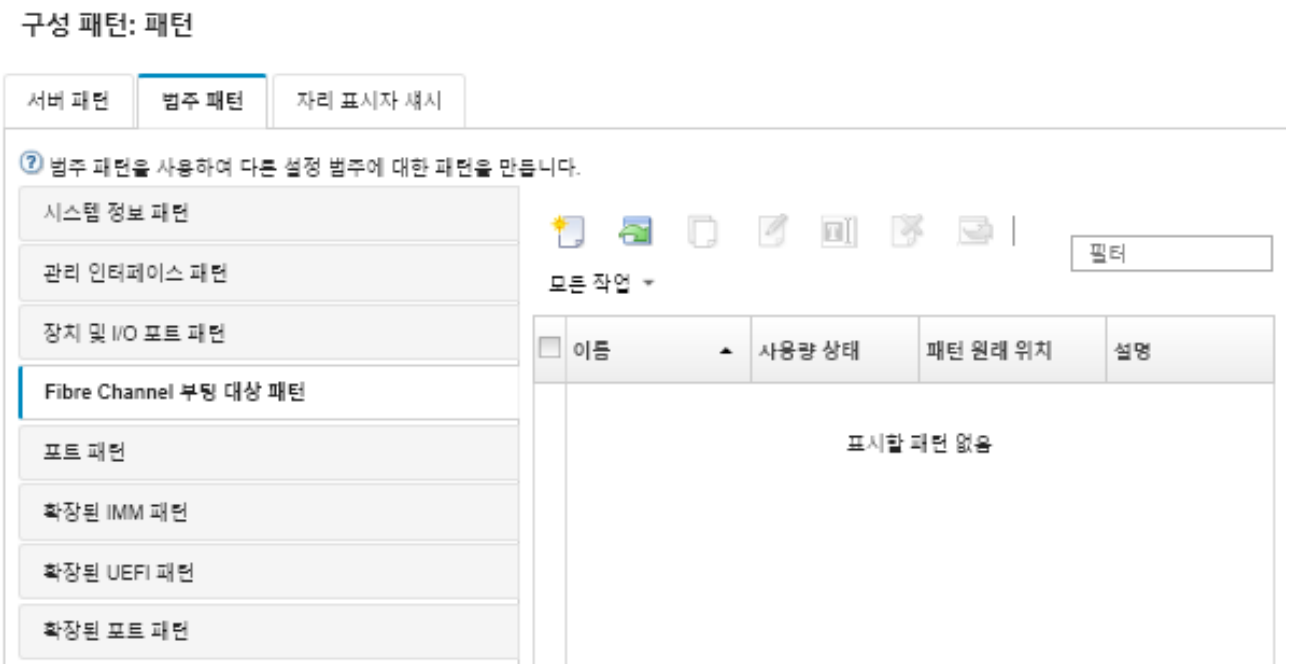
  예를 들어 스토리지 기본 경로를 기본 대상으로 추가하고 스토리지 보조 경로를 보조 대상으로 추가할 수 있습니다. 다른 서버 패턴에 있는 다른 대상 그룹을 사용하여 여러 호스트로부터의 동시 부팅 요청에서 스토리지 로드 밸런스를 맞출 수 있습니다.

  팁: WWPN에 `00:00:00:00:00:00:00:00`을 지정하는 경우 XClarity Administrator는 처음 검색된 대상에서 부팅을 시도합니다.

단계 5. **만들기**를 클릭하십시오.

결과

새 패턴은 구성 패턴: 범주 패턴 페이지의 **Fibre Channel 부팅 대상 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **편집** 아이콘( )을 클릭하여 현재 패턴 설정을 수정합니다.
- **복사** 아이콘( )을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

포트 설정 정의

포트 패턴을 작성하여 특정 I/O 어댑터에 대한 일반적인 포트 설정을 정의할 수 있습니다.

이 작업 정보

포트 패턴의 네트워크 설정을 사용하여 스위치 내부 포트를 구성할 수 있습니다. 그러나 VLAN ID, 전역 UFP 모드, 전역 CEE 모드 및 전역 FIPs와 같은 스위치 전역 설정을 구성하는 데는 포트 패턴을 사용할 수 없습니다. 포트 패턴을 배포하기 전에 배포하려는 내부 포트 설정과 호환되는 다음 규칙을 사용하여 전역 설정을 수동으로 구성해야 합니다. PVID 태깅을 구성하는 데는 포트 패턴을 사용할 수도 없습니다. 전역 설정과 내부 포트 설정 간의 호환성 검사를 판별하고 해당 스위치에 대한 설정 구성 방법을 보려면 스위치와 함께 제공되는 설명서를 참조하십시오.

- PFC가 구성된 경우 globalCEEState가 "켜기"인지 확인하십시오.
- vport가 "FCoE" 모드로 설정된 경우 globalCEEState가 "켜기"인지 확인하십시오.
- FIPs가 구성된 경우 globalCEEState가 "켜기"이고 globalFIPsState가 "켜기"인지 확인하십시오.
- 스위치 내부 포트 모드가 "UFP" 모드로 설정된 경우 globalUFPMode가 "사용"인지 확인하십시오.
- 특정 VLAN에 포트를 추가하기 전에 VLAN ID가 작성되었는지 확인하십시오.

절차

I/O 어댑터 포트 패턴을 작성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **포트 패턴** 수직 탭을 클릭한 다음 **만들기** 아이콘( )을 클릭하십시오.

팁: 초기 포트 패턴 선택 항목 옆에 있는 **만들기** 아이콘( )을 클릭하여 I/O 어댑터 추가 페이지에서 새 패턴을 작성할 수 있습니다.

단계 4. 새 포트 패턴 대화 상자에서 다음 정보를 지정하십시오.

- 패턴의 이름과 설명을 입력하십시오.
- 다음 어댑터 및 포트 호환성 설정을 지정하십시오. 어댑터 및 포트에 패턴 할당 시 패턴 설정은 대상 어댑터 또는 포트와의 호환성을 기준으로 필터링됩니다.
  - 대상 어댑터 유형
  - 대상 포트 작동 가능 모드. 예:
    - pNIC 모드
    - vNIC 가상 패브릭 모드
    - vNIC 스위치 독립 모드
    - vNIC 통합 패브릭 포로토콜 모드

    이러한 설정은 NIC 가상화를 사용 가능하게 합니다. 자세한 정보는 Flex System Fabric 솔루션의 NIC 가상화의 내용을 참조하십시오.
  - 다음을 포함한 대상 포트 프로토콜
    - 이더넷만
    - 이더넷 및 FCoE
    - 이더넷 및 iSCSI
  - 포트 확장 설정 패턴(서버에서 가져온 추가 포트 설정을 구성하는 데 사용됨)
- 대상 포트 작동 가능 모드를 pNIC 모드로 설정한 경우 해당 설정을 Flex 스위치 내부 포트에 적용하도록 선택하십시오(적용 가능한 경우). 이를 선택한 경우 추가 VLAN 및 고급 설정을 구성할 수 있습니다.
  - 대상 포트 프로토콜을 지정하십시오.

- 대상 포트 프로토콜을 **이더넷 및 FCoE**로 설정한 경우 우선순위 2 ID를 선택적으로 선택하고 지정하십시오.

- 대상 포트 작동 가능 모드를 vNIC **가상 패브릭 모드**로 설정한 경우 각 기능에 대한 유형과 VLAN 태그를 포함하여 물리적 기능 설정을 구성하십시오.
- 대상 포트 작동 가능 모드를 vNIC **스위치 독립 모드**로 설정한 경우, 각 사용 기능에 대한 유형, 최소 대역폭 및 VLAN 태그를 지정하십시오. 또한 해당되는 경우 해당 설정을 Flex 스위치 내부 포트에 적용하도록 선택할 수 있습니다. 이를 선택한 경우 추가 스위치 내부 포트 및 고급 설정을 구성할 수 있습니다.
  - 기본 LAN을 지정하십시오(운영 체제에서 태그 지정되지 않은 패킷을 보낼 때 운영 체제에서만 사용됨).
  - 쉼표로 구분된 VLAN 목록을 지정하십시오.
  - 수동 제어를 구성하고 트리거를 지정하도록 선택하십시오.
  - 다음을 포함하여 플로우 제어 유형을 구성하도록 선택하십시오.
    - 기존 흐름 제어 유지
    - 우선 순위 기반 흐름 제어
    - 링크 레벨 흐름 제어

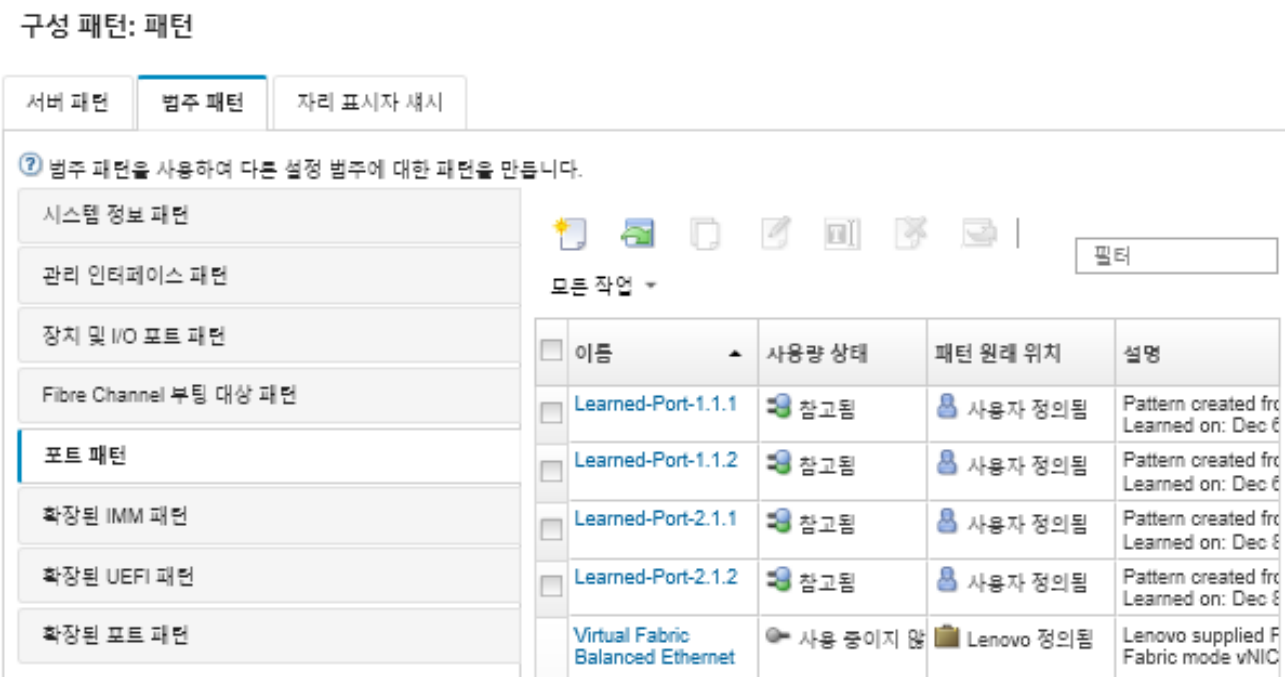
    해당 플로우 제어 유형에 대한 자세한 정보는 Flex 스위치와 함께 제공되는 설명서를 참조하십시오.
- 대상 포트 작동 가능 모드를 vNIC **통합 패브릭 프로토콜 모드**로 설정한 경우 해당 설정을 Flex 스위치 내부 포트에 적용하도록 선택하십시오(적용 가능한 경우). 이를 선택한 경우 추가 UFP 기능 및 고급 설정을 구성할 수 있습니다.
  - QoS 모드(대역폭 또는 우선 순위)를 지정하십시오.
  - 기본 VLAN ID 태깅을 사용하도록 선택하고 사용으로 설정된 각 기능에 대한 모드, 최소 대역폭 및 VLAN 태그를 지정하십시오.
  - 레이어 2 실패를 구성하고 각 기능에 대한 트리거 수를 지정하도록 선택하십시오.
  - 대역폭 QoS 모드의 경우, 흐름 제어 유형(우선 순위 기반, 링크 수준 또는 기존 흐름 제어)을 지정하십시오.
  - 대역폭 QoS 모드의 경우, iSCSI를 선택하면 우선순위 4가 사용으로 설정되는지 여부를 선택하십시오.

참고: 장애 조치 트리거를 정의할 때 전역 장애 조치가 "켜기"인지 확인하십시오.

단계 5. **만들기**를 클릭하십시오.

결과

새 패턴은 구성 패턴: 범주 패턴 페이지의 **포트 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **편집** 아이콘()을 클릭하여 현재 패턴 설정을 수정합니다.
- **복사** 아이콘()을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘()을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘()을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

확장된 관리 컨트롤러 설정 정의

확장된 베이스보드 관리 컨트롤러 설정은 특정 관리되는 서버에서 가져와서 동적으로 작성됩니다. 기존 서버에서 서버 패턴을 작성하는 경우 Lenovo XClarity Administrator는 이러한 패턴을 작성합니다. 확장된 관리 컨트롤러 패턴을 수동으로 작성할 수는 없지만 이미 작성된 패턴을 복사하고 수정할 수는 있습니다.

시작하기 전에

참고: IMM 온도 설정이 UEFI 작동 모드 설정과 충돌할 수 있습니다. 충돌이 발생하면 장치가 재부팅될 때 UEFI 설정이 IMM 설정을 겹쳐쓰고 확장된 베이스보드 관리 컨트롤러 패턴에서 정의한 열 설정이 준수 조건을 벗어납니다. 비준수 문제를 해결하려면 확장된 베이스보드 관리 컨트롤러 패턴에서 설정을 제거하거나 현재 UEFI 작동 모드 설정과 충돌하지 않는 설정을 선택하십시오.

절차

확장된 관리 컨트롤러 패턴을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **확장된 BMC 패턴** 수직 탭을 클릭하십시오.

단계 4. 수정할 패턴을 선택하고 **편집** 아이콘()을 클릭하십시오.

단계 5. 적합한 필드를 수정하십시오.

포함/제외 설정을 클릭하여 범주 패턴에 포함시킬 설정을 선택할 수 있습니다.

- DNS 설정을 구성하려면 **네트워크 설정 인터페이스 → DNS 구성**을 클릭하십시오. DNS를 사용하도록 설정하고 IP 프로토콜을 선택하고 최대 3개의 IPv4 또는 IPv6 주소를 지정하고 XClarity Administrator IP 주소 검색을 사용하도록 설정할 수 있습니다.

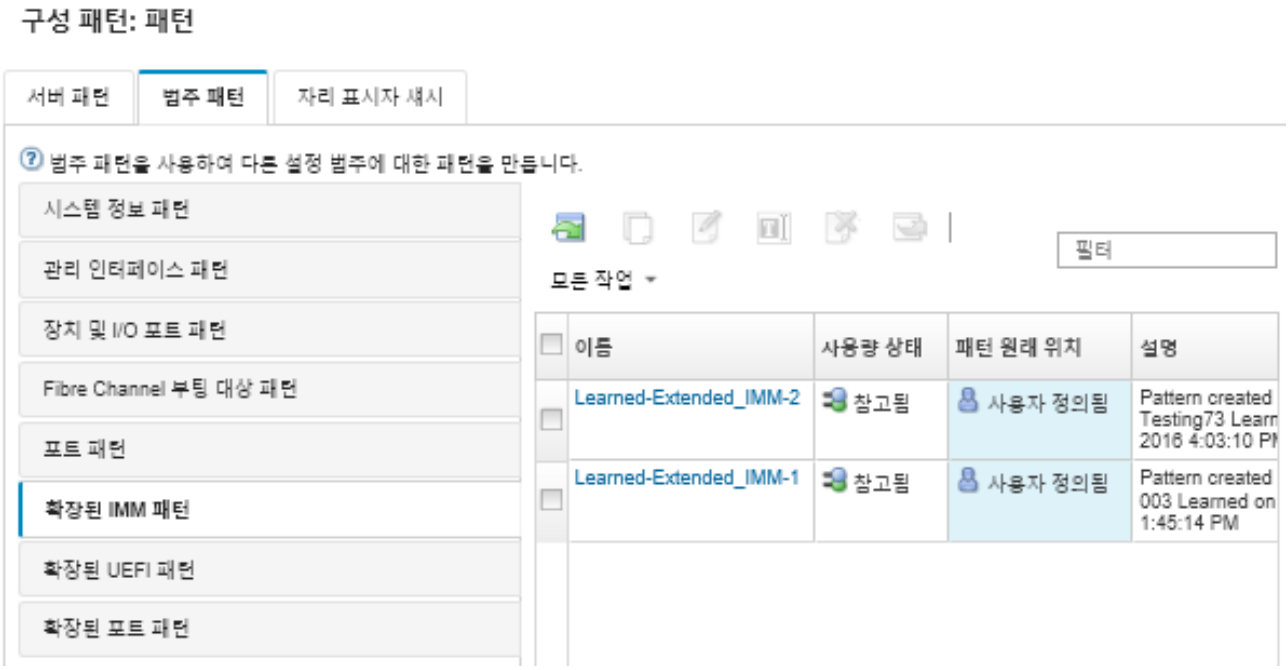
  참고: Flex System 장치의 경우 XClarity Administrator 서버를 찾는 데 사용할 IP 주소만 구성할 수 있습니다.
- NTP 설정을 구성하려면 **네트워크 설정 인터페이스 → 통합 모듈 NTP 설정**을 클릭하십시오. 최대 4개의 NTP 서버에 대한 호스트 이름과 주파수를 지정할 수 있습니다.

  참고: Flex System 장치의 경우 NTP 설정을 구성할 수 없습니다.
- (랙 서버만 해당) 데이터 및 시간을 설정하려면 **일반 설정 → 통합 모듈 클럭 설정**을 클릭하십시오. 시간대(UTC 오프셋)를 지정하고, 일광 절약 시간(DST)을 사용 또는 사용 중지하고, 호스트에서 UTC 또는 현지 시간을 사용할 것인지를 선택할 수 있습니다.
- 사용자 계정 보안 설정을 변경하려면 **계정 보안 구성**을 클릭하십시오.

단계 6. 현재 범주 패턴에 변경사항을 저장하려면 **저장**을 클릭하고, 새 범주 패턴에 변경사항을 저장하려면 **다른 이름으로 저장**을 클릭하십시오.

결과

수정된 범주 패턴은 구성 패턴: 범주 패턴 페이지의 **확장된 BMC 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **복사** 아이콘( )을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

확장 UEFI 설정 정의

확장된 UEFI(Unified Extensible Firmware Interface) 설정은 특정 관리 서버에서 가져와서 동적으로 작성됩니다. 기존 서버에서 서버 패턴을 작성하는 경우 Lenovo XClarity Administrator는

다음 패턴을 작성합니다. 확장된 UEFI 패턴을 수동으로 작성할 수는 없지만 이미 작성된 패턴을 복사하고 수정할 수는 있습니다.

이 작업 정보

다음 확장된 UEFI 패턴은 특정 환경에 대해 서버를 최적화하기 위해 Lenovo XClarity Administrator에 의해 미리 정의됩니다.

- **ESXi 설치 옵션**
- **효율성 – 성능 우선**
- **효율성 – 전력 우선**
- **최대 성능**
- **최소 전력**

참고:

- UEFI 보안 설정(예, 보안 부팅, TPM(신뢰할 수있는 플랫폼 모듈) 및 실제 존재 정책 구성)의 수정은 확장된 UEFI 패턴을 사용하여 지원되지 않습니다.
- **모든 작업 → 보안 → UEFI 관리자 암호**를 클릭하여 서버 페이지에서 선택한 ThinkSystem 및 ThinkAgile 서버의 UEFI 관리자 암호를 수정할 수 있습니다. Lenovo XClarity Controller 펌웨어 수준 20A가 필요합니다.

절차

확장된 UEFI 패턴을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **확장된 UEFI 패턴** 수직 탭을 클릭하십시오.

단계 4. 수정할 패턴을 선택하고 **편집** 아이콘( )을 클릭하십시오.

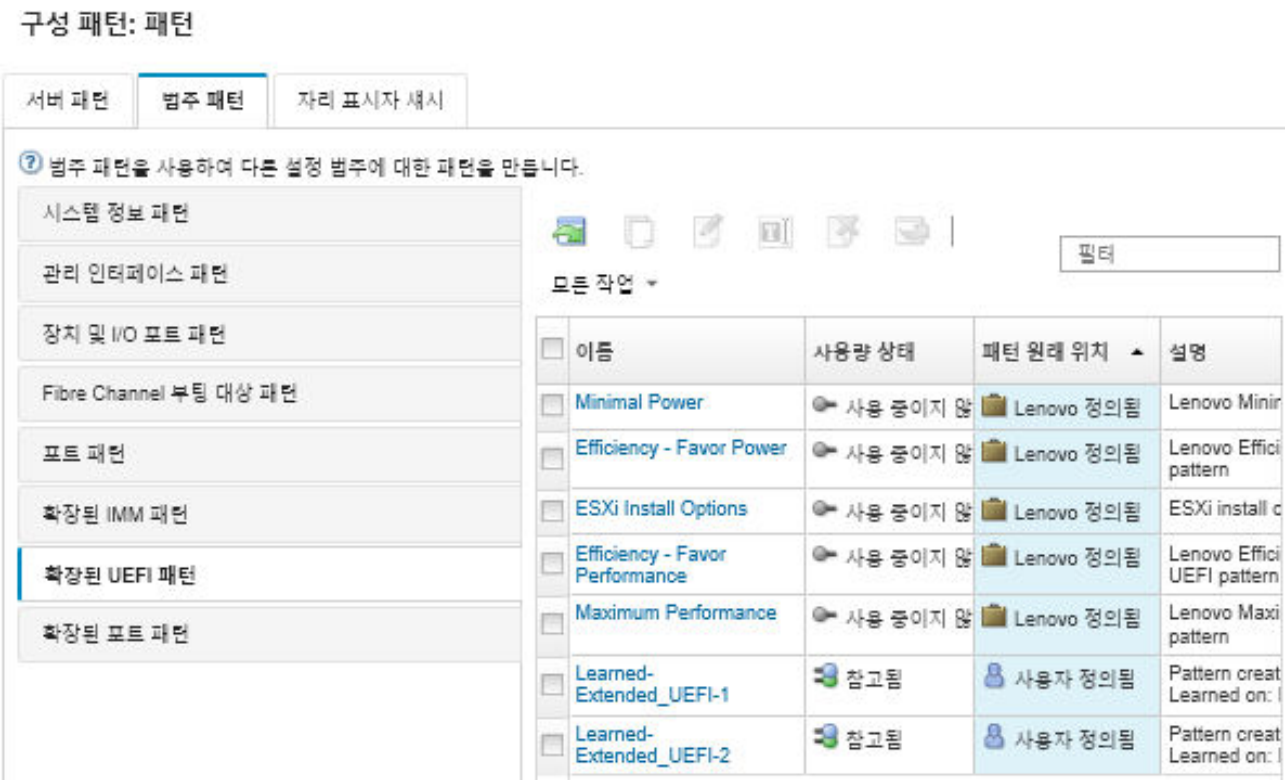
단계 5. 적합한 필드를 수정하십시오.

포함/제외 설정을 클릭하여 범주 패턴에 포함시킬 설정을 선택할 수 있습니다.

단계 6. 현재 범주 패턴에 변경사항을 저장하려면 **저장**을 클릭하고, 새 범주 패턴에 변경사항을 저장하려면 **다른 이름으로 저장**을 클릭하십시오.

결과

수정된 범주 패턴은 구성 패턴: 범주 패턴 페이지의 **확장된 UEFI 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **복사** 아이콘( )을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

확장 포트 설정 정의

확장된 관리 컨트롤러 설정은 특정 관리 서버에서 가져와서 동적으로 작성됩니다. 기존 서버에서 서버 패턴을 작성하는 경우 Lenovo XClarity Administrator는 다음 패턴을 작성합니다. 확장된 포트 패턴을 수동으로 작성할 수는 없지만 이미 작성된 패턴을 복사하고 수정할 수는 있습니다.

이 작업 정보

XClarity Administrator에서는 미리 정의된 다음 확장된 포트 패턴을 제공합니다.

- **가상 패브릭 밸런스 이더넷**. 가상 패브릭 모드 vNIC 모드를 위한 Lenovo 제공 포트 패턴(이더넷 전용)

Mellanox 및 Broadcom I/O 어댑터의 일부 장치 수준 설정은 모든 포트에서 동일한 값으로 설정해야 합니다. 설정이 다른 포트에서 다른 값으로 설정되면 한 포트의 설정이 사용되고 다른 포트의 설정은 준수되지 않습니다. 규정을 준수하지 않는 문제를 해결하려면 해당 장치 수준 설정에 대해 동일한 값을 선택하십시오.

Mellanox I/O 어댑터의 경우 다음 설정을 모든 포트에서 동일한 값으로 설정해야 합니다.

- 고급 전원 설정
- PCI 가상 기능 알림
- 슬롯 전력 리미터
- 가상화 모드

Broadcom I/O 어댑터의 경우 다음 설정을 모든 포트에서 동일한 값으로 설정해야 합니다.

- 배너 메시지 시간 초과

- BW 한계
- BW 한계 유효
- BW 예약
- BW 예약 유효
- PME 기능 사용
- PF MSI-X 벡터의 최대 수
- 다기능 모드
- VF당 MSI-X 벡터 수
- PF당 VF 수
- 옵션 ROM
- SR-IOV
- RDMA 지원

절차

확장된 포트 패턴을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **확장된 포트 패턴** 수직 탭을 클릭하십시오.

단계 4. 수정할 패턴을 선택하고 **편집** 아이콘()을 클릭하십시오.

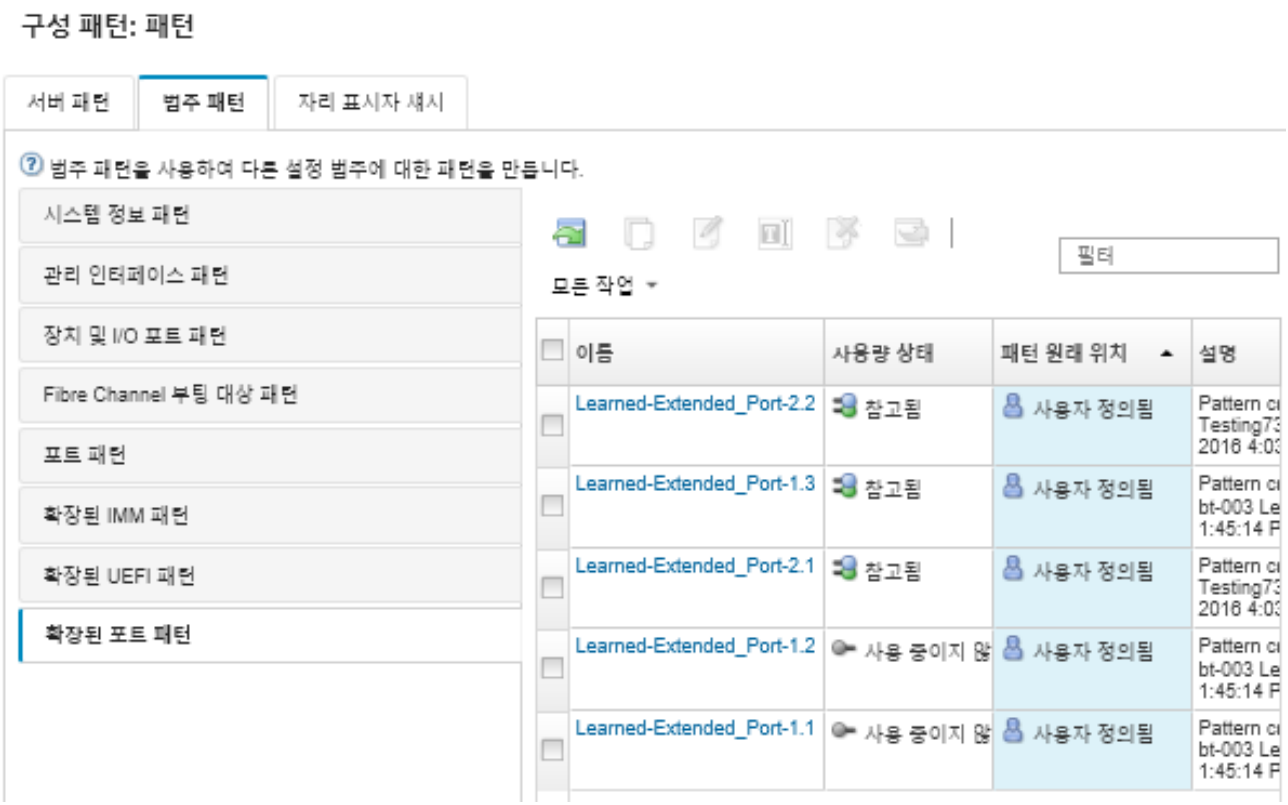
단계 5. 적합한 필드를 수정하십시오.

포함/제외 설정을 클릭하여 범주 패턴에 포함시킬 설정을 선택할 수 있습니다.

단계 6. 현재 범주 패턴에 변경사항을 저장하려면 **저장**을 클릭하고, 새 범주 패턴에 변경사항을 저장하려면 **다른 이름으로 저장**을 클릭하십시오.

결과

수정된 범주 패턴은 구성 패턴: 범주 패턴 페이지의 **확장된 포트 패턴** 탭에 나열됩니다.



이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.

- **복사** 아이콘( )을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

확장 SR635/SR655 BIOS 설정 정의

확장 SR635/SR655 BIOS 설정은 특정 관리되는 서버에서 학습되고 동적으로 생성됩니다. 기존 ThinkSystem SR635 또는 SR655 서버에서 서버 패턴을 작성할 때 Lenovo XClarity Administrator가 이러한 패턴을 작성합니다. 확장 SR635/SR655 BIOS 패턴을 수동으로 만들 수는 없지만 이미 만든 패턴을 복사하고 수정할 수는 있습니다.

절차

확장 SR635/SR655 BIOS 패턴을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **확장 SR635/SR655 BIOS 패턴** 수직 탭을 클릭하십시오.

단계 4. 수정할 패턴을 선택하고 **편집** 아이콘( )을 클릭하십시오.

단계 5. 적합한 필드를 수정하십시오.

포함/제외 설정을 클릭하여 범주 패턴에 포함시킬 설정을 선택할 수 있습니다.

단계 6. 현재 범주 패턴에 변경사항을 저장하려면 **저장**을 클릭하고, 새 범주 패턴에 변경사항을 저장하려면 **다른 이름으로 저장**을 클릭하십시오.

결과

수정된 범주 패턴은 구성 패턴: 범주 패턴 페이지의 **확장 SR635/SR655 BIOS 패턴** 탭에 나열됩니다.

이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.
- **복사** 아이콘()을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘()을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘()을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

확장된 ThinkServer CPlus BIOS 설정 정의

확장 ThinkServer CPlus BIOS 설정은 특정 관리되는 서버에서 학습되고 동적으로 생성됩니다. 기존 ThinkServer CPlus 서버에서 서버 패턴을 작성할 때 Lenovo XClarity Administrator가 이러한 패턴을 작성합니다. 확장된 ThinkServer CPlus BIOS 패턴을 수동으로 작성할 수는 없지만, 이미 작성된 패턴을 복사하고 수정할 수는 있습니다.

절차

확장된 ThinkServer CPlus BIOS 패턴을 수정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **범주 패턴** 탭을 클릭하십시오.

단계 3. **확장된 ThinkServer CPlus BIOS 패턴** 수직 탭을 클릭하십시오.

단계 4. 수정할 패턴을 선택하고 **편집** 아이콘()을 클릭하십시오.

단계 5. 적합한 필드를 수정하십시오.

포함/제외 설정을 클릭하여 범주 패턴에 포함시킬 설정을 선택할 수 있습니다.

단계 6. 현재 범주 패턴에 변경사항을 저장하려면 **저장**을 클릭하고, 새 범주 패턴에 변경사항을 저장하려면 **다른 이름으로 저장**을 클릭하십시오.

결과

수정된 범주 패턴은 구성 패턴: 범주 패턴 페이지의 **확장된 ThinkServer CPlus BIOS 패턴** 탭에 나열됩니다.

이 페이지에서 선택한 범주 패턴에 다음 작업을 수행할 수도 있습니다.
- **복사** 아이콘()을 클릭하여 기존 패턴을 복사합니다.
- **삭제** 아이콘()을 클릭하여 패턴을 삭제합니다.
- **이름 바꾸기** 아이콘()을 클릭하여 패턴의 이름을 바꿉니다.
- 패턴을 가져오고 내보냅니다(서버 및 범주 패턴 내보내기 및 가져오기 참조).

서버에 서버 패턴 배포

하나 이상의 관리되는 서버에 서버 패턴을 배포할 수 있습니다. Lenovo XClarity Administrator에서 관리되는 섀시 또는 자리 표시자 섀시에 있는 하나 이상의 비어 있는 베이에 서버 패턴을 배포할 수도 있습니다. 서버가 설치되기 전에 서버 패턴을 배포하면 관리 IP 주소를 예약하고, 가상 이더넷 또는 Fibre Channel 주소를 예약하고, 관련 스위치 내부 포트에 네트워크 설정을 푸시합니다.

시작하기 전에

관리되는 장치에 서버 패턴을 적용하기 전에 서버 구성 고려 사항을 읽으십시오(서버에 서버 패턴 배포 참조).

절차

관리되는 서버에 서버 패턴을 배포하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.

단계 2. **서버 패턴** 탭을 클릭하십시오.

단계 3. 배포할 서버 패턴을 선택하고 **배포** 아이콘()을 클릭하십시오.

선택한 서버 패턴이 **배포할 패턴** 목록에 나열된 서버 패턴 배포 대화 상자가 표시됩니다.

단계 4. 구성을 활성화할 시기를 선택하십시오.

- **전체**. 서버 전원을 즉시 켜거나 서버를 다시 시작하여 서버, 베이스보드 관리 컨트롤러 및 UEFI(Unified Extensible Firmware Interface) 구성을 활성화합니다.
- **부분**. (기본값) 관리 컨트롤러 구성을 즉시 활성화하지만 다음에 서버가 다시 시작될 때까지 서버 및 UEFI 구성 활성화가 지연됩니다. 프로필을 완전히 활성화하려면 먼저 수동으로 서버 전원을 켜거나 서버를 다시 시작해야 합니다.

  참고: IMM 설정(시스템 정보, 관리 인터페이스 및 확장 BMC 카테고리 패턴 포함)만 포함한 서버 패턴을 배치할 때는 서버를 재시작할 필요가 없습니다.
- **지연됨**. 서버, 관리 컨트롤러 및 UEFI 구성에 대한 프로필을 생성하지만 서버에서 구성 설정을 활성화하지 않습니다. 프로필을 완전히 활성화하려면 먼저 서버를 다시 시작하여 서버 프로필을 수동으로 활성화해야 합니다.

참고: 상대 스위치 내부 포트의 네트워크 설정은 활성화 구성에 상관 없이 배포되는 즉시 스위치로 푸시됩니다.

단계 5. 서버 패턴을 배포할 하나 이상의 서버나 비어 있는 섀시를 선택하십시오.

참고: 비어 있는 섀시 베이 목록을 표시하려면 **비어 있는 베이 표시**를 선택하십시오.

단계 6. **배포**를 클릭하십시오. 선택한 각 베이의 배포 상태를 나열하는 대화 상자가 표시됩니다.

단계 7. 배포 프로세스를 시작하려면 **배포**를 다시 클릭하십시오.

참고: 배포를 완료하려면 몇 분 정도 걸릴 수 있습니다. 배포 중에 서버 프로필이 작성되어 선택한 각 서버나 섀시 베이에 할당됩니다.

단계 8. **닫기**를 클릭하십시오.

완료한 후에

XClarity Administrator 메뉴 표시줄에서 **모니터링 → 작업**을 클릭하여 배포 진행 상태를 모니터링할 수 있습니다. **프로비저닝 → 서버 프로필**을 클릭하여 서버 프로필 작성을 모니터링할 수도 있습니다. 배포가 완료되면 생성된 서버 프로필을 검토하고 관리 IP 주소 및 가상화된 이더넷 또는 Fibre-Channel 주소를 기록하십시오.

기존 서버와 선택된 서버에 서버 패턴을 배포한 경우 다음을 선택하십시오.

- **전체** 활성화, 각 서버에 대해 서버 프로필이 작성되고 구성이 각 서버로 전파되며 각 서버를 다시 부팅하면 구성 변경사항이 활성화됩니다.
- **부분** 활성화, 각 서버에 대해 서버 프로필이 작성되고 구성이 각 서버로 전파됩니다. 구성 변경사항을 완전히 활성화하려면 수동으로 서버 전원을 켜거나 서버를 다시 시작해야 합니다(서버 전원 켜기 및 끄기 참조).
- **지연됨** 활성화, 각 서버에 대한 서버 프로필이 작성됩니다. 서버에서 서버 프로필을 수동으로 활성화해야 합니다(서버 프로필 활성화 참조).

관리되는 섀시 또는 자리 표시자 섀시의 비어 있는 베이에 서버 패턴을 배포한 경우 컴퓨팅 노드가 적합한 섀시 베이에 물리적으로 설치되고 Lenovo XClarity Administrator에서 검색되고 관리되면, 새로 설치된 컴퓨팅 노드에 서버 프로필을 배포하고 활성화해야 합니다(서버 프로필 활성화 참조).

하나 이상의 서버에 새 서버 패턴을 배포한 후 해당 서버가 시작되지 않는 경우 부팅 설정을 서버 패턴에 있는 기본 부팅 설정으로 덮어쓰는 문제가 발생할 수 있습니다. UEFI 모드로 설치된 운영 체제의 경우 부팅 구성을 복원하려면 기본 설정에 추가 구성 단계가 필요할 수 있습니다. Windows 또는 Linux에서 실행 중인 서버의 부팅 설정을 복원하는 예에 대해서는 서버 패턴 배포 후 부팅 설정 복구의 내용을 참조하십시오.

서버 패턴 수정

이후에 기존 서버 패턴의 구성을 변경할 수 있습니다. 원래 서버 패턴이 서버에 배포된 경우(사용 중인 경우) 변경된 서버 패턴을 해당 서버의 전체 또는 서브세트에 다시 배포할 수 있습니다.

이 작업 정보

참고: 변경된 서버 패턴을 서버 세트에 다시 배포하지 않도록 선택한 경우 해당 서버는 변경되지 않은 원래 서버 패턴과 연결된 상태로 유지됩니다.

서버 패턴을 편집하여 단일 위치에서 공통 구성을 제어하고 원래 가상 주소 할당 세트를 유지할 수 있습니다.

절차

서버 패턴을 수정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.

단계 2. **서버 패턴** 탭을 클릭하십시오.

단계 3. 편집할 서버 패턴을 선택하고 **편집** 아이콘()을 클릭하십시오. 서버 패턴 편집 마법사가 표시됩니다.

단계 4. 패턴 이름과 설명을 입력하십시오.

단계 5. 서버에 패턴을 배포할 때 적용할 로컬 스토리지 구성을 선택하고 **다음**을 클릭하십시오.

로컬 스토리지 설정에 대한 정보는 로컬 저장 장치 정의의 내용을 참조하십시오.

단계 6. **옵션:** I/O 어댑터 주소 지정을 수정하고 이 패턴으로 구성될 하드웨어와 일치하도록 추가 I/O 어댑터를 정의한 후 **다음**을 클릭하십시오.

I/O 어댑터 설정에 대한 정보는 I/O 어댑터 정의의 내용을 참조하십시오.

단계 7. 이 패턴을 서버에 배포할 때 적용할 부팅 순서를 정의하고 **다음**을 클릭하십시오.

SAN 부팅 대상 설정에 대한 정보는 부팅 옵션 정의의 내용을 참조하십시오.

단계 8. 기존 범주 패턴에서 펌웨어 설정을 선택하십시오.

만들기 아이콘()을 클릭하여 새 범주 패턴을 작성할 수 있습니다.

펌웨어 설정에 대한 정보는 펌웨어 설정 정의의 내용을 참조하십시오.

단계 9. 현재 서버 패턴에 구성 변경사항을 저장하려면 **저장**을 클릭하고, 새 서버 패턴에 구성 변경사항을 저장하려면 **다른 이름으로 저장**을 클릭하십시오.

단계 10. 변경 사항을 현재 서버 패턴 또는 새 서버 패턴에 저장하도록 선택하십시오.

- 변경 사항을 현재 서버 패턴에 저장하려면 **저장**을 클릭하십시오. 패턴 저장 및 재배포 대화 상자에서 다음 단계를 수행하십시오.
  1. 구성을 활성화할 시기를 선택하십시오.
     - **전체**. 서버 전원을 즉시 켜거나 서버를 다시 시작하여 서버, 베이스보드 관리 컨트롤러 및 UEFI(Unified Extensible Firmware Interface) 구성을 활성화합니다.

– **부분**. (기본값) 관리 컨트롤러 구성을 즉시 활성화하지만 다음에 서버가 다시 시작될 때까지 서버 및 UEFI 구성 활성화가 지연됩니다. 프로필을 완전히 활성화하려면 먼저 수동으로 서버 전원을 켜거나 서버를 다시 시작해야 합니다.

참고: IMM 설정(시스템 정보, 관리 인터페이스 및 확장 BMC 카테고리 패턴 포함)만 포함한 서버 패턴을 배치할 때는 서버를 재시작할 필요가 없습니다.

참고: 상대 스위치 내부 포트의 네트워크 설정은 활성화 구성에 상관 없이 배포되는 즉시 스위치로 푸시됩니다.

2. 구성 변경 사항을 다시 배포할 대상 서버를 선택하십시오. 원래 서버 패턴이 배치된 모든 서버 또는 해당 서버의 서브세트를 선택할 수 있습니다.
3. **다시 배포**를 클릭하십시오.

- 변경 사항을 새 서버 패턴에 저장하려면 **다른 이름으로 저장**을 클릭하십시오. 새 패턴을 배포하려면 서버에 서버 패턴 배포의 내용을 참조하십시오.

서버 및 범주 패턴 내보내기 및 가져오기

여러 Lenovo XClarity Administrator 인스턴스가 있는 경우 한 XClarity Administrator 인스턴스에서 서버 및 범주 패턴을 내보내어 다른 XClarity Administrator 인스턴스로 가져올 수 있습니다.

이 작업 정보

서버 및 범주 패턴만 내보낼 수 있습니다. 정책, 주소 풀 및 프로필은 내보낼 수 없습니다. 내보낸 패턴은 참조 주소 풀과 분리됩니다. 가져온 패턴의 주소 풀을 활용하려면 패턴을 편집하여 주소 풀을 가져온 대상 XClarity Administrator의 풀과 패턴을 다시 연결시키십시오.

참고: 서버 패턴을 내보내는 경우 연결된 범주 패턴도 내보냅니다.

절차

- 하나 이상의 패턴을 내보내려면 다음을 수행하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.
  2. **서버 패턴** 또는 **범주 패턴** 탭을 클릭하십시오.
  3. 내보낼 하나 이상의 패턴을 선택하십시오.
  4. **내보내기** 아이콘()을 클릭하십시오.
  5. **내보내기**를 클릭하여 패턴을 내보내십시오.
  6. 패턴 데이터 파일을 로컬 시스템에 저장하십시오.

     참고: 내보낸 패턴이 주소 풀을 참조하는 경우 패턴을 다른 XClarity Administrator 인스턴스로 가져올 때 충돌을 방지하기 위해 내보낸 패턴에서 이러한 참조가 제거됩니다. 패턴을 다시 가져오는 경우 가져온 패턴을 편집하여 원하는 주소 풀을 할당할 수 있습니다.
- 하나 이상의 패턴을 가져오려면 다음을 수행하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.
  2. **가져오기** 아이콘()을 클릭하여 패턴을 가져오십시오. 패턴 가져오기 대화 상자가 표시됩니다.
  3. **파일 선택**을 클릭하고 가져올 패턴 데이터 파일을 선택하십시오. 추가 패턴 데이터 파일에 대해 반복하십시오.
  4. **가져오기**를 클릭하여 선택한 파일을 가져오십시오.

     가져온 패턴, 이름 지정 충돌로 이름이 변경된 패턴 및 이미 있어서 건너뛴 패턴의 목록이 있는 요약 보고서가 표시됩니다.

서버 프로필 작업

*서버 프로필*은 특정 서버에 적용되는 서버 패턴의 인스턴스입니다. 하나 이상의 서버에 서버 패턴을 배포하는 경우 서버 프로필이 자동으로 생성되고 할당됩니다. 하나의 서버 프로필이 각 대상 서버에 대해 작성됩니다. 각 서버 프로필에는 단일 서버에 대한 특정 구성과 해당 특정 서버에 고유한 정보(예, 할당된 이름, IP 주소 및 MAC 주소)가 포함되어 있습니다.

이 작업 정보

서버 프로필은 베이스보드 관리 컨트롤러 시작 프로세스 중에 활성화됩니다. 다음을 선택할 수 있습니다.
- 패턴을 배포할 때 서버를 재부팅하여 서버 프로필을 즉시 활성화합니다.
- 다음 재부팅할 때까지 활성화를 지연시킵니다.
- 서버 프로필을 수동으로 활성화할 때까지 활성화를 지연시킵니다.

여러 서버 프로필은 하나의 서버 패턴에서 상속할 수 있습니다. 서버 패턴을 하나 이상의 서버에 배포하면 상위 서버 패턴과 범주 패턴을 편집하여 여러 서버에 구성 변경사항을 신속하게 배포할 수 있습니다. 종속 서버 프로필은 자동으로 업데이트되어 연결된 서버에 다시 배포됩니다. 서버 패턴을 편집하여 단일 위치에서 공통 구성을 제어할 수 있습니다.

기존 서버를 교체하거나 미리 프로비저닝된 서버를 섀시의 비어 있는 베이에 설치하는 경우 새 서버에서 구성 변경사항을 프로비저닝하려면 새 서버에 대한 서버 프로필을 활성화해야 합니다.

참고: 여러 서버에 서버 패턴을 배포할 수 있지만 여러 패턴을 단일 서버에 배포할 수는 없습니다.

변경 이유에 따라 여러 방법으로 서버와 연결된 서버 프로필을 변경할 수 있습니다.

- 서버를 이동하거나 서버의 용도를 변경하려는 경우:
  1. 현재 서버에 있는 현재 서버 프로필을 비활성화합니다(서버 프로필 비활성화 참조).
  2. 새 서버 패턴을 새 서버에 배포합니다(서버에 서버 패턴 배포 참조).
- 서버에 오류가 발생하여 대신 스페어 서버를 사용하려는 경우:
  1. 오류가 발생한 서버에 있는 현재 서버 프로필을 비활성화합니다(서버 프로필 비활성화 참조).
  2. 스패어 서버에서 동일한 서버 프로필을 활성화합니다(서버 프로필 활성화 참조).
  3. 오류가 발생한 서버를 수정한 경우 다음 단계를 반복하여 프로필을 다시 전환할 수 있습니다.
- 서버에 오류가 발생하여 하드웨어를 교체하려는 경우:
  1. 오류가 발생한 서버에 있는 현재 서버 프로필을 비활성화합니다(서버 프로필 비활성화 참조).
  2. 오류가 발생한 서버를 교체합니다.
  3. 새 서버에서 동일한 서버 프로필을 활성화합니다(서버 프로필 활성화 참조).

중요:

- 주소 가상화를 사용하는 경우 서버는 종료될 때까지 할당된 가상 MAC 또는 WWN 주소를 유지합니다. 주소 가상화를 사용하는 프로필을 비활성화하는 경우 기본적으로 **서버 전원 끄기** 확인란이 선택됩니다. 주소 충돌이 발생하지 않도록 하려면 다른 서버에 있는 비활성 프로필을 활성화하기 전에 원본 서버 전원을 꺼야 합니다.
- 가장 최근에 생성된 것이 아닌 프로필을 삭제하면 가상 MAC 및 WWN 주소가 주소 풀에서 해제되지 *않습니다*. 자세한 정보는 서버 프로필 삭제의 내용을 참조하십시오.
- 구성 패턴을 사용하지 않고 설정을 변경하거나 펌웨어 중에 펌웨어 문제나 잘못된 설정과 같은 문제가 발생한 경우 서버의 설정이 서버 프로필을 준수하지 못할 수 있습니다. 구성 패턴: 서버 프로필 페이지에서 각 서버의 준수 상태를 판별할 수 있습니다.

서버 프로필 활성화

대체되거나, 재할당되거나, 새로 설치된 관리되는 서버에서 서버 프로필을 활성화할 수 있습니다.

이 작업 정보

기존 서버를 교체하거나 미리 프로비저닝된 서버를 섀시의 비어 있는 베이에 설치하는 경우 새 서버에서 구성 변경사항을 프로비저닝하려면 새 서버에 대한 서버 프로필을 활성화해야 합니다.

중요:

- 주소 가상화를 사용하는 경우 서버는 종료될 때까지 할당된 가상 MAC 또는 WWN 주소를 유지합니다. 주소 가상화를 사용하는 프로필을 비활성화하는 경우 기본적으로 **서버 전원 끄기** 확인란이 선택됩니다. 주소 충돌이 발생하지 않도록 하려면 다른 서버에 있는 비활성 프로필을 활성화하기 전에 원본 서버 전원을 꺼야 합니다.
- 가장 최근에 생성된 것이 아닌 프로필을 삭제하면 가상 MAC 및 WWN 주소가 주소 풀에서 해제되지 *않습니다*. 자세한 정보는 서버 프로필 삭제의 내용을 참조하십시오.
- 구성 패턴을 사용하지 않고 설정을 변경하거나 펌웨어 중에 펌웨어 문제나 잘못된 설정과 같은 문제가 발생한 경우 서버의 설정이 서버 프로필을 준수하지 못할 수 있습니다. 구성 패턴: 서버 프로필 페이지에서 각 서버의 준수 상태를 판별할 수 있습니다.

절차

서버 프로필을 활성화하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 프로필**을 클릭하십시오. 구성 패턴: 서버 프로필 페이지가 표시됩니다.

단계 2. 활성화할 서버 프로필을 선택하십시오.

팁: 서버 프로필의 현재 상태가 **프로필 상태** 열에 나열됩니다. 비활성 또는 활성화 보류 중 상태인 서버 프로필을 활성화할 수 있습니다.

단계 3. **서버 프로필 활성화** 아이콘( )을 클릭하십시오.

단계 4. **활성화**를 클릭하십시오.

프로파일이 보류 중, 활성 또는 활성 실패 상태인 경우, 배포를 활성화할 시기를 선택할 수 있습니다.

- **전체**. 서버 전원을 즉시 켜거나 서버를 다시 시작하여 서버, 베이스보드 관리 컨트롤러 및 UEFI(Unified Extensible Firmware Interface) 구성을 활성화합니다.
- **부분**. (기본값) 관리 컨트롤러 구성을 즉시 활성화하지만 다음에 서버가 다시 시작될 때까지 서버 및 UEFI 구성 활성화가 지연됩니다. 프로필을 완전히 활성화하려면 먼저 수동으로 서버 전원을 켜거나 서버를 다시 시작해야 합니다.

  참고: IMM 설정(시스템 정보, 관리 인터페이스 및 확장 BMC 카테고리 패턴 포함)만 포함한 서버 패턴을 배치할 때는 서버를 재시작할 필요가 없습니다.

서버 프로필이 처음 활성화되면 프로필 상태가 "활성"으로 변경됩니다. 준수가 확인되면 상태가 "준수" 또는 "비준수"로 변경됩니다.

결과

구성 패턴: 서버 프로필 페이지에서 서버 프로필 상태가 활성으로 변경됩니다.

서버 프로필 비활성화

프로필을 비활성화하여 서버 또는 섀시에서 서버 프로필을 할당 취소할 수 있습니다.

절차

서버 프로필을 비활성화하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 프로필**을 클릭하십시오. 구성 패턴: 서버 프로필 페이지가 표시됩니다.

단계 2. 비활성화할 서버 프로필을 선택하십시오.

팁: 서버 프로필의 현재 상태가 **프로필 상태** 열에 나열됩니다.

단계 3. **서버 프로필 비활성화** 아이콘()을 클릭하십시오.

단계 4. 다음 비활성화 옵션 중 하나를 선택하십시오.

- **IMM ID 설정 재설정**. 프로필 구성 ID 설정(예, 베이스보드 관리 컨트롤러 호스트 이름, 장치 이름 또는 고정 IP 주소가 할당된 관리 인터페이스)을 재설정합니다. 연결된 서버 패턴을 통해 구성된 설정만 재설정됩니다.

  참고: 정적으로 할당된 IP 주소가 있는 서버의 경우 이 옵션은 DHCP 모드를 사용으로 설정합니다. 네트워크에서 DHCP 서버가 사용으로 설정되어 있지 않으면 수동으로 서버를 유효한 고정 IP 주소로 재구성해야 합니다. Converged, NeXtScale 및 System x 랙 및 타워 서버는 XClarity Administrator를 사용하여 다시 관리되어야 합니다.
- **서버 전원 끄기**. 서버 전원을 끕니다. 서버 전원을 다시 켜면 가상 주소 할당이 번인(burn-in) 기본값으로 되돌아갑니다.
- **강제 비활성화**. 서버가 제거되었거나 도달할 수 없는 경우에도 서버 프로필을 비활성화합니다.
- **스위치 내부 포트 설정**. UFP 모드를 비활성화하고 VLAN 정의에서 관련 구성원 vport를 제거하는 것을 포함하여 프로필로 구성된 스위치 내부 포트 설정을 기본값으로 재설정합니다. 연결된 서버 패턴을 통해 구성된 설정만 재설정됩니다.

  기본적으로 이 기능은 사용 불가능하도록 설정되어 있습니다.

  이전 스위치 포트 구성과 충돌하는 설정 없이 서버 프로파일을 다른 서버에 배포할 수 있는 상태로 스위치 포트를 두려면 이 옵션을 선택하십시오.

단계 5. **비활성화**를 클릭하십시오.

결과

구성 패턴: 서버 프로필 페이지에서 서버 프로필 상태가 비활성으로 변경됩니다.

참고: XClarity Administrator가 관리 컨트롤러와 통신할 수 없는 경우(예, 관리 컨트롤러가 오류 상태이거나 다시 시작되는 중인 경우) 서버 프로필 비활성화가 실패하여 서버 프로필이 비활성화되지 않습니다. 이 경우 비활성화를 다시 시도하고 강제 비활성화 옵션을 선택하여 프로필을 비활성화하십시오. 이전에 할당된 서버는 여전히 ID와 주소가 할당된 프로필로 구성됩니다. 주소 충돌을 방지하려면 서버 전원을 수동으로 끄고 인프라에서 서버를 제거해야 합니다.

서버 프로필 삭제

비활성화된 서버 프로필만 삭제할 수 있습니다.

시작하기 전에

삭제할 서버 프로필이 비활성화되어 있는지 확인하십시오(서버 프로필 비활성화 참조).

절차

서버 프로필을 삭제하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 프로필**을 클릭하십시오. 구성 패턴: 서버 프로필 페이지가 표시됩니다.

단계 2. 비활성 상태인 서버 프로필을 선택하십시오.

팁: 서버 프로필의 현재 상태가 **프로필 상태** 열에 나열됩니다.

단계 3. **삭제** 아이콘()을 클릭하십시오.

참고: 가장 최근에 생성된 프로필을 삭제하면 가상 MAC 또는 WWN 주소가 주소 풀에서 해제됩니다. 가장 최근에 생성된 것이 아닌 프로필을 삭제하면 가상 MAC 및 WWN 주소가 주소 풀에서 해제되지 *않습니다*.

자리 표시자 섀시 작업

물리적 하드웨어가 도착하기 전까지 서버 패턴에 대한 대상으로 작동하도록 ***자리 표시자 섀시***를 정의하여 나중에 Flex System 섀시에 설치될 서버를 미리 프로비저닝할 수 있습니다.

이 작업 정보

자리 표시자 섀시에 서버 패턴을 배포하는 경우 Lenovo XClarity Administrator는 Flex System 섀시에 있는 서버 14개 모두에 대한 서버 프로필을 작성하고 서버의 관리 IP 주소 및 가상 이더넷 또는 Fibre Channel 주소를 예약합니다.

하드웨어가 도착할 때 자리 표시자 섀시를 배포하여 14개의 모든 서버 프로필을 각각 배포하는 대신 자리 표시자 섀시를 배포하여 물리적 서버에서 서버 프로필을 활성화할 수 있도록 자리 표시자 섀시는 모든 서버 프로필을 번들로 만듭니다. 서버 프로필을 완전히 활성화하려면 각 서버를 다시 부팅해야 합니다.

자리 표시자 섀시 만들기

하드웨어를 설치하기 전에 미리 프로비저닝할 수 있는 자리 표시자 섀시를 작성할 수 있습니다. 섀시에서 컴퓨팅 노드를 프로비저닝하면 관리 IP 주소 및 가상 이더넷 또는 Fibre Channel 주소를 검색합니다.

절차

자리 표시자 섀시를 작성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **자리 표시자 섀시** 탭을 클릭하십시오.

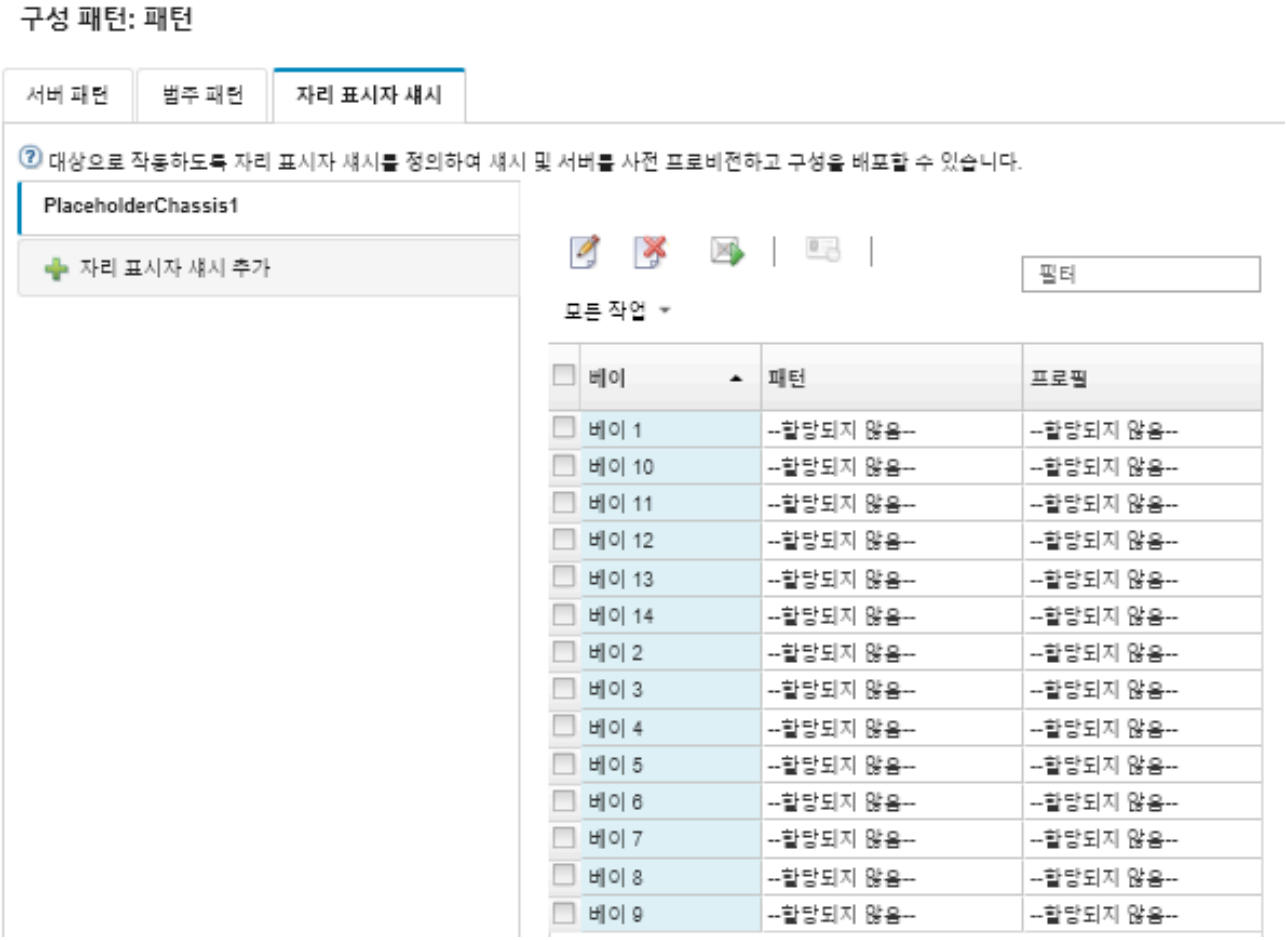
단계 3. **자리 표시자 섀시 추가** 수직 탭을 클릭하십시오.

단계 4. 자리 표시자 섀시의 이름과 설명을 입력하십시오.

단계 5. **추가**를 클릭하십시오.

완료한 후에

구성 패턴: 자리 표시자 섀시 페이지에 새 자리 표시자 섀시에 대한 수직 탭이 추가됩니다.



이 페이지에서 선택한 자리 표시자 섀시에 다음 작업을 수행할 수 있습니다.

- **배포** 아이콘()을 클릭하여 자리 표시자 섀시를 배포합니다.
- **편집** 아이콘()을 클릭하여 자리 표시자 섀시 이름과 설명을 수정합니다.
- 자리 표시자 섀시에 서버 패턴을 배포합니다(자리 표시자 섀시에 서버 패턴 배포 참조).
- 자리 표시자 섀시에서 서버 프로필을 비활성화합니다(서버 프로필 비활성화 참조).
- **삭제** 아이콘()을 클릭하여 자리 표시자 섀시를 삭제합니다.

자리 표시자 섀시에 서버 패턴 배포

자리 표시자 섀시의 각 베이에 서버 패턴을 배포할 수 있습니다. 서버가 Flex System 섀시에 설치되기 전에 서버 패턴을 배포하면 섀시의 각 서버 베이에 대한 서버 프로필을 작성하고 관리 IP 주소 및 가상 이더넷 또는 Fibre Channel 주소를 예약합니다.

절차

자리 표시자 섀시에 서버 패턴을 배포하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.

단계 2. **서버 패턴** 탭을 클릭하십시오.

단계 3. 자리 표시자 섀시에 배포할 서버 패턴을 선택하십시오.

단계 4. **배포** 아이콘()을 클릭하십시오. 사용 가능한 섀시 및 자리 표시자 섀시 목록이 있는 서버 패턴 배포 대화 상자가 표시됩니다.

단계 5. **활성화** 목록에서 **지연됨**을 선택하십시오.

단계 6. **비어 있는 베이 표시**를 클릭하십시오.

단계 7. 서버 패턴을 배포할 하나 이상의 자리 표시자 섀시를 선택하십시오.

단계 8. **배포**를 클릭하십시오. 선택한 각 베이의 배포 상태를 나열하는 대화 상자가 표시됩니다.

단계 9. 배포 프로세스를 시작하려면 **배포**를 다시 클릭하십시오.

자리 표시자 섀시에서 선택한 각 베이에 대해 서버 프로필이 작성되고 할당됩니다.

참고: 배포를 완료하려면 몇 분 정도 걸릴 수 있습니다.

단계 10. **닫기**를 클릭하십시오.

완료한 후에

XClarity Administrator 메뉴 표시줄에서 **모니터링 → 작업**을 클릭하여 배포 진행 상태를 모니터링할 수 있습니다. **프로비저닝 → 서버 프로필**을 클릭하여 서버 프로필 작성을 모니터링할 수도 있습니다. 배포가 완료되면 생성된 서버 프로필을 검토하고 관리 IP 주소 및 가상화된 이더넷 또는 Fibre-Channel 주소를 기록하십시오.

Flex System 섀시가 랙에 물리적으로 설치된 다음 XClarity Administrator에 의해 검색되고 관리되면, 자리 표시자 섀시를 배포하여 섀시에 있는 모든 서버를 프로비저닝할 수 있습니다(자리 표시자 섀시에 서버 패턴 배포 참조).

자리 표시자 섀시 배포

자리 표시자 섀시에 서버 패턴을 배포하여 자리 표시자 섀시를 미리 구성하고 실제 섀시를 검색하고 관리하면, 자리 표시자 섀시를 배포하여 실제 컴퓨팅 노드를 구성할 수 있습니다.

절차

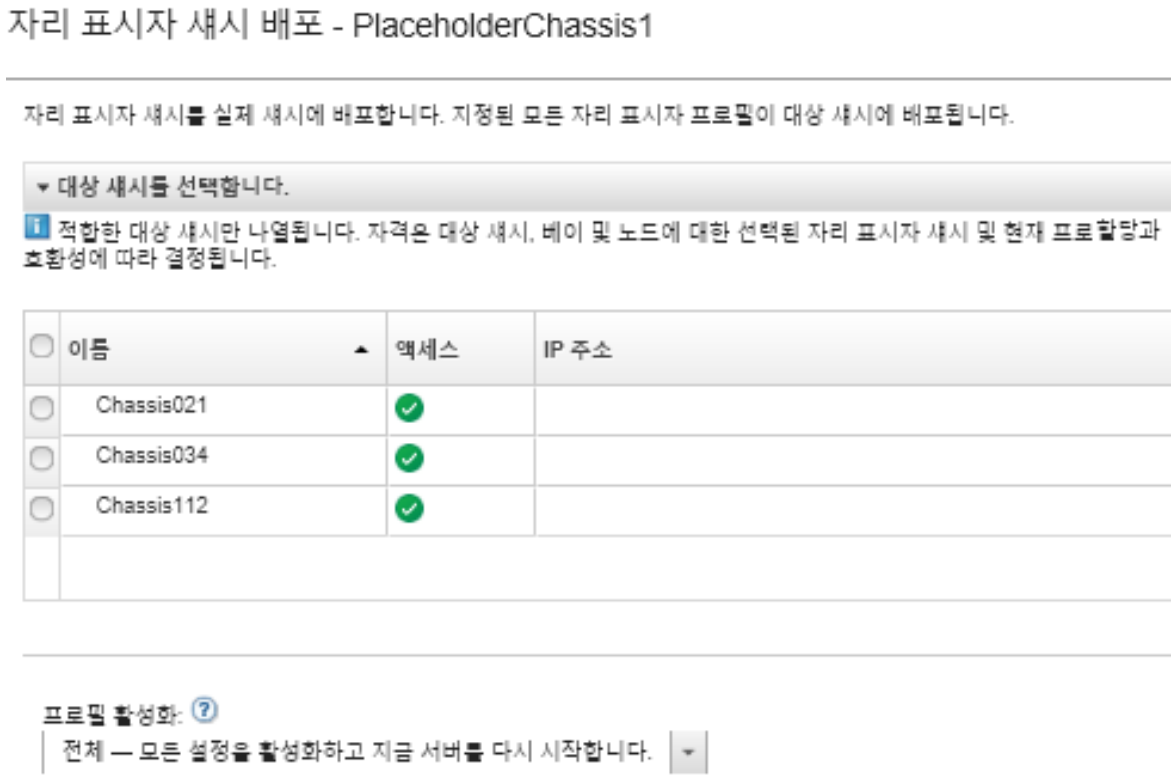
자리 표시자 섀시를 배포하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 구성 패턴**을 클릭하십시오. 서버 구성 패턴 페이지가 표시됩니다.

단계 2. **자리 표시자 섀시** 탭을 클릭하십시오.

단계 3. 배포할 자리 표시자 섀시에 대한 수직 탭을 선택하십시오.

단계 4. **자리 표시자 섀시 배포** 아이콘()을 클릭하여 자리 표시자 섀시 배포 대화 상자를 표시하십시오.



단계 5. 구성을 활성화할 시기를 선택하십시오.

참고: 상대 스위치 내부 포트의 네트워크 설정은 활성화 구성에 상관 없이 배포되는 즉시 스위치로 푸시됩니다.

- **전체**. 서버 전원을 즉시 켜거나 서버를 다시 시작하여 서버, 베이스보드 관리 컨트롤러 및 UEFI(Unified Extensible Firmware Interface) 구성을 활성화합니다.
- **부분**. (기본값) 관리 컨트롤러 구성을 즉시 활성화하지만 다음에 서버가 다시 시작될 때까지 서버 및 UEFI 구성 활성화가 지연됩니다. 프로필을 완전히 활성화하려면 먼저 수동으로 서버 전원을 켜거나 서버를 다시 시작해야 합니다.

  참고: IMM 설정(시스템 정보, 관리 인터페이스 및 확장 BMC 카테고리 패턴 포함)만 포함한 서버 패턴을 배치할 때는 서버를 재시작할 필요가 없습니다.

단계 6. **활성화**를 클릭하십시오.

스토리지 어댑터를 기본값으로 재설정

하나 이상의 서버에 대해 로컬 스토리지 어댑터를 기본 제조 설정으로 재설정할 수 있습니다.

이 작업 정보

주의: 이 작업은 로컬 스토리지 어댑터에서 모든 데이터를 지웁니다.

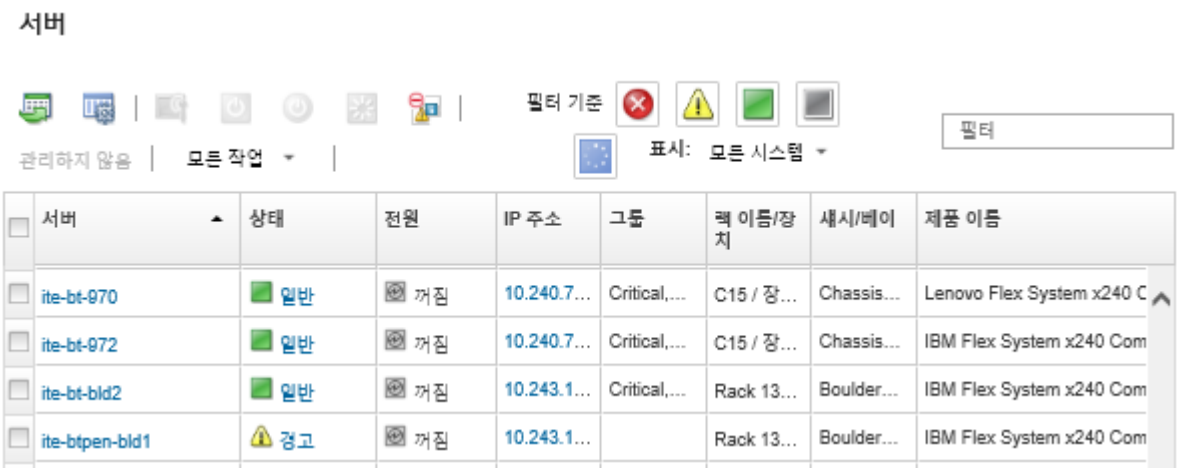
서버의 전원이 꺼져 있고 RAID 링크가 지원되는 경우 서버가 시스템 설치 프로그램으로 부팅되어 로컬 HDD 및 SSD 어댑터를 재설정합니다.

절차

하나 이상의 서버에 대한 RAID 구성을 지우려면 다음 단계를 완료하십시오.

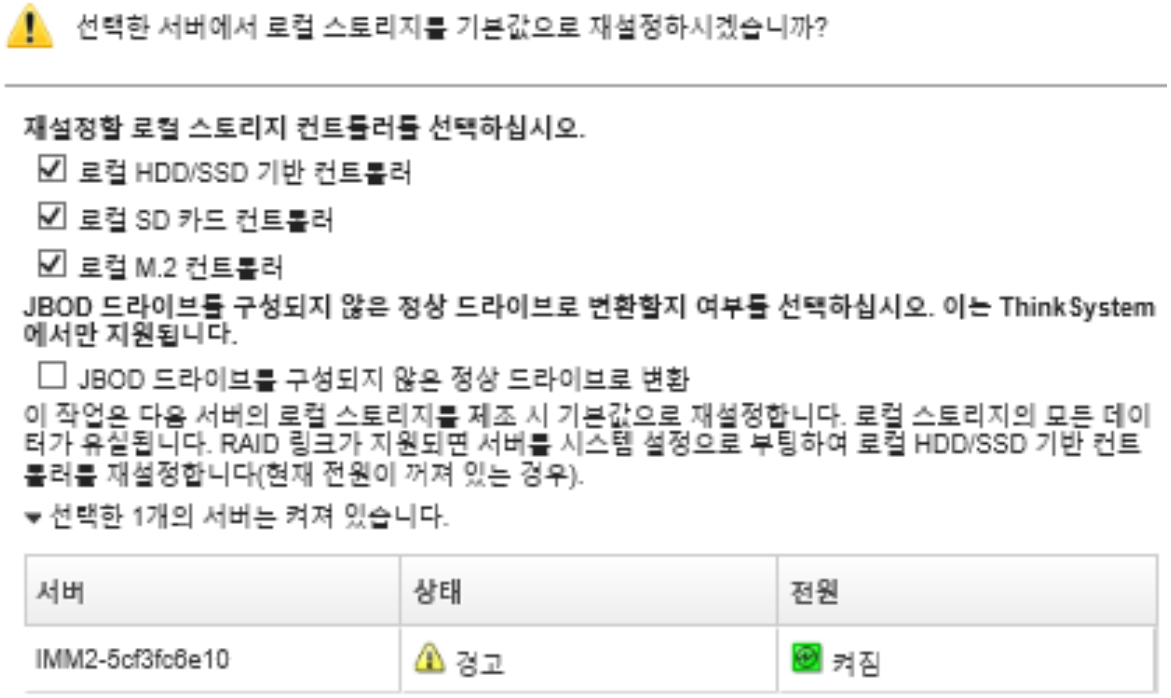
단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지는 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

관리할 서버를 더 쉽게 찾기 위해 테이블 열을 정렬할 수 있습니다. 또한 **모든 시스템** 드롭다운 목록에서 서버 유형을 선택하고 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버를 상세하게 필터링할 수 있습니다.



단계 2. 하나 이상의 서버를 선택하십시오.

단계 3. **모든 작업 → 서비스 → 로컬 스토리지를 기본값으로 재설정**을 선택하십시오. 추가 정보를 묻는 대화 상자가 표시됩니다.



단계 4. 재설정할 로컬 스토리지 어댑터를 선택하십시오.

단계 5. : (ThinkSystem 서버만 해당) JBOD 드라이브를 구성되지 않은 양호 상태로 변환하도록 선택했습니다.

단계 6. **스토리지 재설정**을 클릭하십시오.

메모리 구성

Intel® Optane™ DC 영구 메모리 DIMM의 영구 메모리를 암호화하고 복호화할 수 있습니다.

절차

영구 메모리를 암호화하고 복호화하려면 다음 절차를 완료하십시오.

단계 1. XClarity Administrator 메뉴에서 **하드웨어 → 서버**를 클릭하십시오. 서버 페이지는 모든 관리되는 서버(랙 서버 및 컴퓨팅 노드)의 표 형식 보기와 함께 표시됩니다.

단계 2. 구성할 하나 이상의 서버를 선택하십시오.

단계 3. **모든 작업 → 보안 → Intel Optane PMEM 작업**을 클릭하여 Intel Optane PMEM 작업 대화 상자를 표시하십시오.

단계 4. 수행하려는 보안 작업을 선택하십시오.

- **보안 사용**. 영구 메모리 영역에 기록되는 데이터가 지정된 암호를 사용하여 암호화됩니다.

  중요: 암호화 암호를 기록하십시오. 암호는 보안을 사용 안 함으로 설정하거나 암호를 지우는 데 필요합니다.

- **보안 사용 안 함**. 영구 메모리 영역에 기록된 데이터가 암호화되지 않습니다.

  영구 메모리 영역에 이미 저장된 데이터는 암호화된 상태로 유지되며 여전히 액세스할 수 있습니다.

  참고: 이 작업은 보안을 사용하고 암호가 설정된 경우에만 가능합니다. 현재 암호를 사용하여 이 작업을 인증해야 합니다. 모든 DIMM이 동일한 암호를 공유하는 경우에만 장치의 여러 DIMM에 대한 보안을 사용 안 함으로 설정할 수 있습니다.

- **보안 지우기**. 영구 메모리 영역에 저장된 데이터를 암호화하는 데 사용되는 암호를 지워서 데이터를 복구할 수 없도록 합니다.

  참고: 이 작업은 보안을 사용하고 암호가 설정된 경우에만 가능합니다. 현재 암호를 사용하여 이 작업을 인증해야 합니다.

- **암호 없이 보안 지우기**. 장치의 지정된 DIMM의 영구 메모리에 저장된 모든 데이터를 안전하게 지울 수 있습니다. 보안 지우기 후에는 모든 데이터를 복구할 수 없습니다.

  참고: 이 작업은 보안을 사용하지 않고 암호가 요구되지 않는 경우에만 가능합니다.

단계 5. 필요한 경우 암호를 지정하고 확인하십시오.

단계 6. **확인**을 누르십시오.

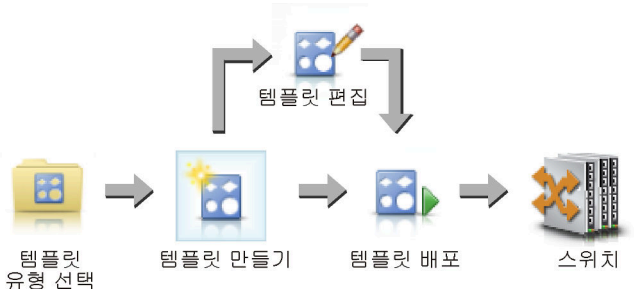
제 12 장 구성 템플릿을 사용하여 스위치 구성

템플릿을 사용하면 정의된 단일 구성 설정 세트에서 여러 CNOS 랙 스위치를 신속하게 프로비저닝할 수 있습니다.

이 작업 정보

XClarity Administrator에서 스위치 구성 템플릿을 사용하여 관리되는 스위치에 대한 전역 설정, 포트 채널, 가상 LAN, 가상 링크 집합 그룹(VLAG, Virtual Link Aggregation Group) 및 스파인 리프 토폴로지를 구성할 수 있습니다. 현재 CNOS를 실행하는 랙 스위치만 지원됩니다.

다음 그림은 관리되는 랙 스위치를 구성하는 워크플로우를 설명합니다.



1. **템플릿 유형을 선택하십시오.**

   *스위치 구성 템플릿*은 관련 스위치 설정을 그룹화합니다. 다음 유형의 스위치 구성 템플릿을 만들 수 있습니다.
   - **전역**. 시스템 적합성, 기본 VLAN 태그 및 L2 인터페이스 등의 전역 설정을 구성합니다.
   - **포트 채널**. 기본 및 고급 포트 채널 설정을 구성하고 포트 채널에서 포트를 제거하고 포트 채널을 삭제합니다.
   - **스파인 리프**. 기존 토폴로지에 스파인 리프 구성을 배포합니다.
   - VLAN(**가상 LAN**). VLAN 설정 및 속성을 구성하고 VLAN을 삭제합니다.
   - VLAG(**가상 링크 집합 그룹**). 기본, 고급 및 피어 VLAG 설정을 구성하고, VLAG 인스턴스를 만들고 삭제합니다.

2. **템플릿을 만드십시오.**

   데이터 센터에서 사용되는 여러 구성을 표시하는 여러 스위치 구성 템플릿을 만들 수 있습니다. 스위치 구성 템플릿을 사용하여 한 위치에서 일반적인 스위치 구성을 제어할 수 있습니다.

   스위치 구성 템플릿 만들기에 대한 자세한 정보는 스위치 구성 템플릿 만들기의 내용을 참조하십시오.

3. **템플릿을 하나 이상의 스위치에 배포하십시오.**

   CNOS를 실행하는 하나 이상의 개별 랙 스위치에 서버 패턴을 배포할 수 있습니다.

   스위치 구성 배포에 대한 자세한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

4. **템플릿을 편집하십시오.**

   스위치 구성 템플릿을 편집해도 초기 템플릿이 배포된 모든 스위치에 업데이트된 설정이 자동으로 배포되지 않습니다. 변경된 템플릿은 수동으로 다시 배포해야 합니다. 기록 페이지는 각 배포의 설정을 추적합니다.

기본 서버 구성 환경 설정

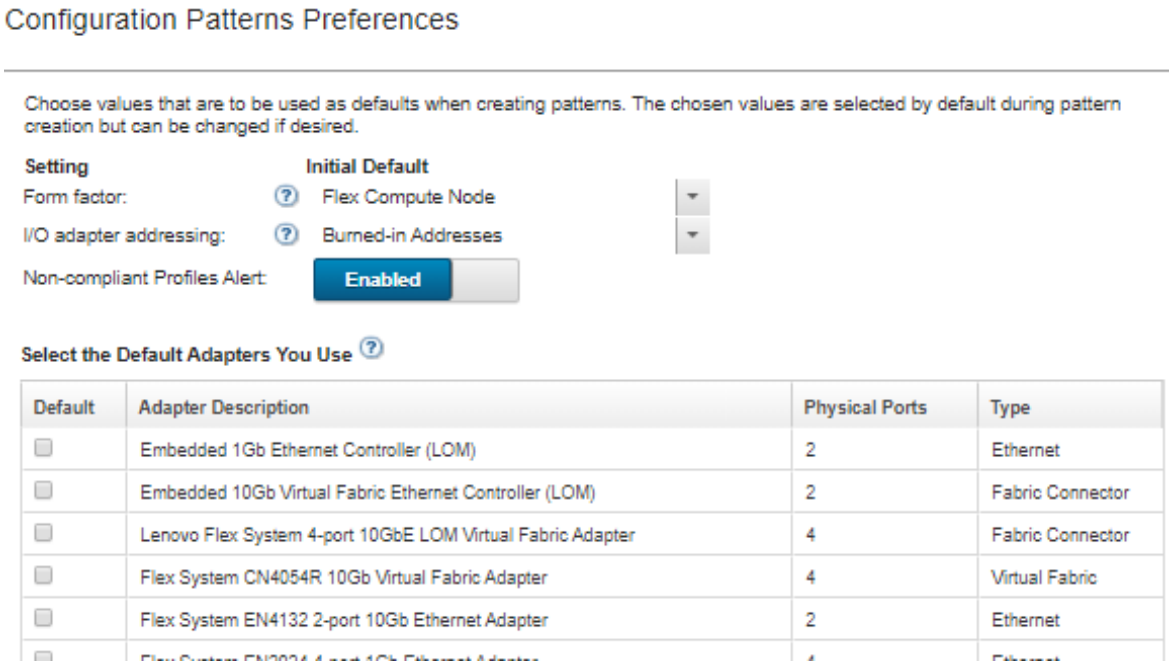
서버 구성 패턴을 작성할 때 기본적으로 선택될 값을 정의할 수 있습니다. 이 값은 서버 패턴 작성 중에 변경될 수 있습니다.

절차

기본 서버 구성을 설정하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝**을 클릭한 다음 **구성 패턴** 다음에 나오는 도움말 아이콘(?)을 클릭하면 구성 패턴: 시작하기 페이지가 표시됩니다.

단계 2. **구성 패턴 환경 설정**을 클릭하면 구성 패턴 환경 설정 대화 상자가 표시됩니다.



단계 3. 기본 서버 폼 팩터를 선택하십시오.

단계 4. 기본 I/O 어댑터 주소 지정 모드를 선택하십시오.

- **번인(burn-in)**. 공장 출하 시 어댑터와 함께 제공되는 기존 WWN(World Wide Name) 및 MAC(Media Access Control) 주소를 사용하십시오.
- **가상**. LAN 및 SAN 연결 관리를 단순화하려면 가상 I/O 어댑터 주소 지정을 사용하십시오. I/O 주소를 가상화하면 가상화된 Fibre WWN 및 이더넷 MAC 주소로 번인(burn-in) 하드웨어 주소를 다시 할당합니다. SAN 멤버십을 미리 구성하여 배포 속도를 높이고 하드웨어 교체 시 SAN 구역 지정 및 LAN 마스킹 할당 재구성 필요를 제거함으로써 장애 조치를 용이하게 할 수 있습니다.

  가상 주소 지정을 사용하는 경우 정의된 어댑터와 상관 없이 기본적으로 이더넷과 Fibre Channel 주소가 둘 다 할당됩니다. 이더넷 및 Fibre Channel 주소를 할당하는 소스 풀을 선택할 수 있습니다.

  주소 모드 옆에 있는 **편집** 아이콘(✎)을 클릭하여 가상 주소 설정을 편집할 수도 있습니다.

  제한사항: 가상 주소 지정은 Flex System 섀시의 서버에만 지원됩니다. 랙 및 타워 서버는 지원되지 않습니다.

단계 5. 서버의 구성 설정이 할당된 서버 구성 프로필과 일치하지 않을 때 경고 발생을 사용 또는 사용하지 않도록 선택하십시오.

  활성 프로필(ASSIGNED 또는 ERROR_ACTIVATING 상태)을 준수하지 않는 경우에만 경고가 발생합니다.

  서버 구성이 준수를 하거나 서버 프로필이 할당되지 않은 경우 비준수 프로필 경고가 삭제됩니다.

단계 6. 선호 어댑터로 사용하려는 기본 I/O 어댑터를 선택 목록에서 하나 이상 선택하십시오.

단계 7. **저장**을 클릭하십시오.

스위치 구성 템플릿 만들기

스위치 구성 템플릿을 만들 때 특정 유형의 구성에 대한 설정을 정의합니다.

시작하기 전에

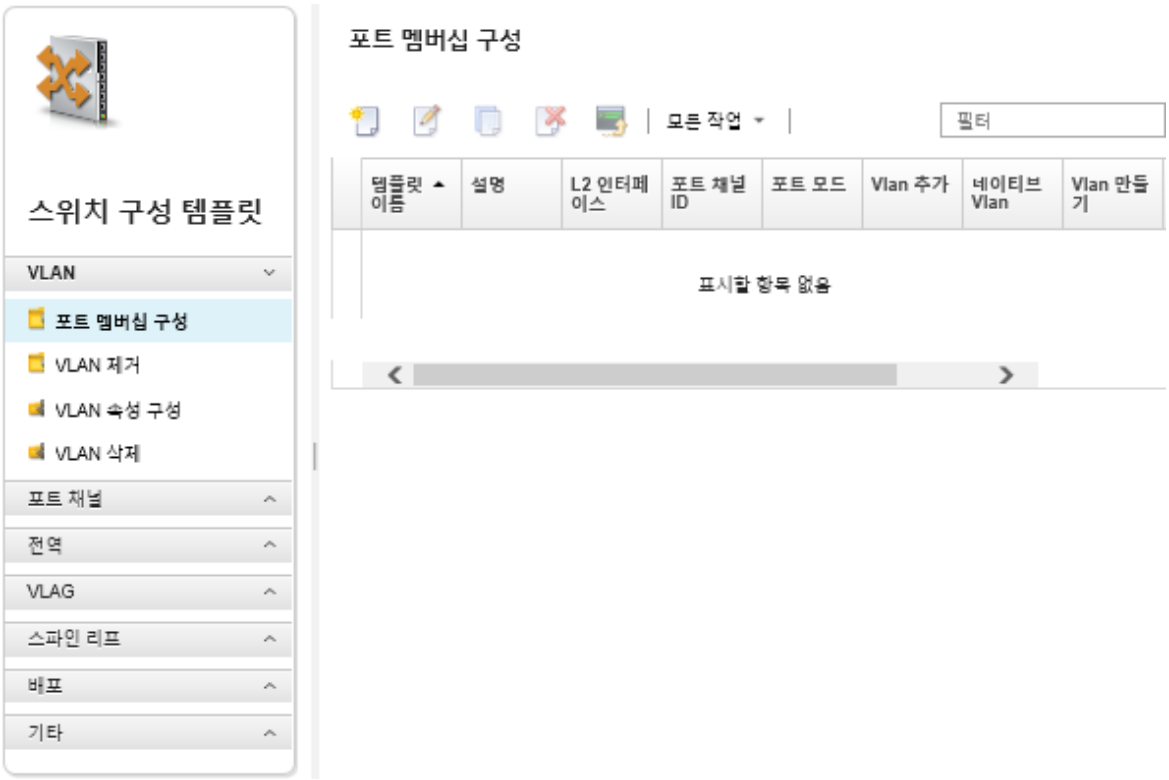
스위치 구성 템플릿을 만들기 전에 다음 제안을 고려하십시오.

- 동일한 하드웨어 옵션을 가지고 동일한 방식으로 구성하려는 스위치 그룹을 식별합니다. 스위치 구성 템플릿을 사용하여 여러 스위치에 동일한 구성 설정을 적용함으로써 한 위치에서 공통 구성을 제어할 수 있습니다.
- 사용자 지정하려는 구성 측면(예, 전역, 포트 채널 또는 VLAN 설정)을 식별합니다.

절차

스위치 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.



단계 2. 왼쪽 탐색 창에서 만들려는 템플릿 유형을 선택하십시오.

단계 3. **만들기** 아이콘( )을 클릭하여 새 템플릿 만들기 대화 상자를 표시하십시오.

이 대화 상자에 나열된 필드는 템플릿 유형에 따라 다릅니다.

단계 4. 템플릿을 저장하려면 **저장**을 클릭하고 하나 이상의 관리되는 랙 스위치에 템플릿을 즉시 배포하려면 **저장 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

완료한 후에

저장 및 배포를 클릭하면 스위치 템플릿 배포 페이지가 표시됩니다. 이 페이지에서 스위치 구성 템플릿을 특정 스위치에 배포할 수 있습니다.

저장을 클릭하면 스위치 구성 템플릿이 스위치 구성 템플릿 페이지에 저장됩니다. 이 페이지에서 선택한 서버 패턴에 다음 동작을 수행할 수 있습니다.

- 이름 열에서 템플릿 이름을 클릭하여 템플릿에 대한 세부 정보를 봅니다.
- 모든 템플릿의 집계된 목록을 보고 **기타 → 모든 템플릿**을 클릭하십시오.
- 템플릿을 배포합니다(대상 스위치에 스위치 구성 템플릿 배포 참조).
- **복사** 아이콘( )을 클릭하여 템플릿을 복사한 다음 수정합니다.
- **편집** 아이콘( )을 클릭하여 템플릿을 편집합니다.

  참고: 템플릿 변경 사항은 원래 템플릿이 배포된 스위치에 *자동으로 재배포되지 않습니다.*
- **이름 바꾸기** 아이콘( )을 클릭하여 패턴의 이름을 바꿉니다.
- **삭제** 아이콘( )을 클릭하여 패턴을 삭제합니다.

VLAN 포트 멤버십 설정 정의

VLAN 포트 멤버십 구성 템플릿을 사용하여 하나 이상(트렁크용)의 VLAN에 물리적 포트 및 포트 채널을 추가할 수 있습니다.

절차

포트 멤버십 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 **VLAN → 포트 멤버십 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

중요: 하나 이상의 물리적 L2 인터페이스 또는 포트 채널 ID를 지정해야 합니다.

- 템플릿의 이름과 설명을 입력하십시오.
- 하나 이상의 유효한 물리적 L2 인터페이스를 지정하십시오. 쉼표로 구분된 인터페이스 목록, 대시로 구분된 ID 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 예를 들면 다음과 같습니다.
  - 이더넷1/10
  - 이더넷1/3,5,7,9
  - 이더넷1/5-10,21-32
  - 이더넷2/2-5,7,9,11-13
- 하나 이상의 유효한 포트 채널 ID(포트 집계기 인터페이스)를 지정하십시오. 쉼표로 구분된 번호 목록, 대시로 구분된 번호 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 값과 범위는 1-4096의 숫자입니다. 예:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- 포트가 태그 지정된 트래픽 또는 태그 지정되지 않은 트래픽을 허용할지 여부를 선택합니다. 이는 다음 값 중 하나입니다.
  - access. 포트가 단일 VLAN에 대한 트래픽을 전달합니다.
  - trunk. (기본값) 포트가 스위치에서 액세스할 수 있는 모든 VLAN에 대한 트래픽을 전달합니다.

- 포트의 VLAN 멤버십 목록에 추가할 VLAN ID를 하나 이상 지정하십시오. 쉼표로 구분된 번호 목록, 대시로 구분된 번호 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 값과 범위는 1-4096의 숫자입니다. 예:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

  참고:

  - 포트 모드가 "access"로 설정된 경우 첫 번째 VLAN ID가 사용됩니다. 예를 들어, 범위 2-4,5,10-20에서는 2만 사용됩니다.
  - CNOS는 기본적으로 VLAN ID 4000-4095를 예약합니다. 예약된 VLAN ID(CNOS 또는 다른 사용자가 예약)를 사용하면 스위치 구성 배포에 실패할 수 있습니다.
- 태그 지정되지 않은 트래픽이 태그 지정된 기본 VLAN ID를 지정하십시오. 1-4096 사이의 숫자입니다.

  참고:
  - 이 필드는 포트 모드가 "trunk"로 설정된 경우에만 유효합니다.
  - 포트 모드가 지정되지 않거나 ID가 포트의 끝 상태 VLAN 외부에 있으면 포트는 실제로 태그 지정되지 않은 트래픽을 허용하지 않습니다.
- VLAN **만들기**를 선택하여 대상 스위치에 현재 누락된 VLAN ID를 생성합니다.

  포트가 생성되지 않은 VLAN에 속한 경우 해당 포트는 계속해서 해당 VLAN의 멤버이지만 해당 VLAN ID로 태그 지정된 상태로 포트에 도달하는 트래픽은 통과할 수 없습니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

VLAN 속성 정의

VLAN 속성 구성 템플릿을 사용하여 고급 VLAN 속성을 구성할 수 있습니다.

절차

VLAN 속성 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 VLAN → VLAN **속성 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 변경 사항을 적용할 VLAN ID를 지정하십시오. 1-4095 사이의 숫자입니다.

  참고: CNOS는 기본적으로 VLAN ID 4000-4095를 예약합니다. 예약된 VLAN ID(CNOS 또는 다른 사용자가 예약)를 사용하면 스위치 구성 배포에 실패할 수 있습니다.
- VLAN 사용자 지정 이름을 지정하십시오.
- VLAN이 활성(사용) 상태인지 또는 일시 중지(사용 안 함) 상태인지 선택하십시오.
- 대상 VLAN의 IP 멀티캐스트(IPMC) 플러드가 IPv4 또는 IPv6 인터페이스에서 제어(사용)되는지 여부를 선택하십시오. 이는 다음 값 중 하나입니다.
  - Disable. IPv4 및 IPv6을 사용할 수 없습니다.

- Enable. IPv4 및 IPv6을 사용할 수 있습니다.
- IPv4 Disable.
- IPv4 Enable
- IPv6 Disable
- IPv6 Enable

이 작업은 부가적입니다. 즉, "Disable" 상단에 "IPv4 Enable"을 배포하면 "IPv4 Enable"이 가능하지만 "IPv6 Enable" 상단에 배포하면 "Enable"이 가능합니다. disable 옵션의 경우 반대도 마찬가지입니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

VLAN 설정 제거

VLAN 제거 템플릿을 사용하여 VLAN에서 인터페이스를 제거할 수 있습니다.

절차

VLAN 제거 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 VLAN → VLAN 제거를 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

중요: 하나 이상의 물리적 L2 인터페이스 또는 포트 채널 ID를 지정해야 합니다.

- 템플릿의 이름과 설명을 입력하십시오.
- 하나 이상의 유효한 물리적 L2 인터페이스를 지정하십시오. 쉼표로 구분된 인터페이스 목록, 대시로 구분된 ID 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 예를 들면 다음과 같습니다.
  - 이더넷1/10
  - 이더넷1/1,3,5,7
  - 이더넷1/1-10,21-30
  - 이더넷2/1-5,7,9,11-13
- 하나 이상의 유효한 포트 채널 ID(포트 집계기 인터페이스)를 지정하십시오. 쉼표로 구분된 번호 목록, 대시로 구분된 번호 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 값과 범위는 1-4096의 숫자입니다. 예:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- 포트의 VLAN 멤버십 목록에서 제거할 VLAN ID를 하나 이상 지정하십시오. 쉼표로 구분된 번호 목록, 대시로 구분된 번호 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 값과 범위는 1-4096의 숫자입니다. 예:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

참고: 포트 모드가 "access"로 설정된 경우 VLAN을 제거하면 포트가 VLAN 1로 들어갑니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

VLAN 삭제

VLAN 삭제 템플릿을 사용하여 스위치에서 VLAN 구성을 제거할 수 있습니다.

절차

VLAN 삭제 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 VLAN → **VLAN 삭제**를 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 포트의 VLAN 멤버십 목록에서 제거할 VLAN ID를 하나 이상 지정하십시오. 쉼표로 구분된 번호 목록, 대시로 구분된 번호 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 값과 범위는 1-4096의 숫자입니다. 예:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

  참고: 예약된 VLAN ID는 삭제할 수 없습니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

포트 채널 기본 설정 정의

포트 채널 기본 구성 템플릿을 사용하여 포트 집계기를 만들고 포트를 집계기에 추가할 수 있습니다.

포트 채널에 포트가 있고 그 중 일부 포트가 템플릿의 일부인 경우, 템플릿이 배포될 때 해당 속성(포트 우선 순위, 모드 및 시간 초과)이 템플릿의 설정으로 업데이트됩니다.

절차

포트 채널 기본 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 **포트 채널 → 기본 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 하나 이상의 유효한 물리적 L2 인터페이스를 지정하십시오. 쉼표로 구분된 인터페이스 목록, 대시로 구분된 ID 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 예를 들면 다음과 같습니다.
  - 이더넷1/10
  - 이더넷1/3,5,7,9
  - 이더넷1/5-10,21-32

  - 이더넷2/2-5,7,9,11-13
- 만들거나 업데이트할 포트 채널 ID(포트 집계기 인터페이스)를 지정하십시오. 1-4095 사이의 숫자입니다.
- LACP(Link Aggregation Control Protocol) 포트 모드를 지정하십시오. 이는 다음 값 중 하나입니다.
  - Active. (기본값) LACP를 무조건 사용합니다.
  - Passive. LCAP 장치가 감지된 경우에만 LACP를 사용합니다.
  - Static. LCAP를 사용하지 않습니다.

  참고: Active 및 Passive는 동일한 집계기에서 혼합할 수 있지만 Static은 혼합할 수 없습니다.
- LACP 포트 우선 순위를 지정하십시오. 1-65535 사이의 숫자입니다.

  참고: LACP 포트 우선 순위는 LACP 포트 ID를 구성하기 위해 포트 번호와 함께 사용됩니다.
- LCAP가 개별 모드로 들어가기 전의 LACP 시간 초과 모드를 지정하십시오. 이는 다음 값 중 하나입니다.
  - Long. (기본값) 90초
  - Short. 3초

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

포트 채널 고급 설정 정의

포트 채널 고급 구성 템플릿을 사용하여 고급 포트 채널 속성을 구성할 수 있습니다.

절차

포트 채널 고급 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 **포트 채널 → 고급 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 업데이트할 포트 채널 ID(포트 집계기 인터페이스)를 지정하십시오. 1-4095 사이의 숫자입니다.
- LACP가 실패할 때 개별 포트를 활성 상태로 유지할지 여부를 선택하십시오. 이는 다음 값 중 하나입니다.
  - Active. (기본값) LACP를 무조건 사용합니다.
  - Suspend. LACP를 사용하지 않습니다.
- 포트 채널을 고려하는 데 필요한 최소 링크 수를 지정하십시오. 1-32 사이의 숫자입니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

포트 채널 삭제

포트 채널 삭제 템플릿을 사용하여 스위치에서 포트 채널을 제거할 수 있습니다.

절차

포트 채널 삭제 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 **포트 채널 → 포트 채널 삭제**를 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 삭제할 하나 이상의 포트 채널 ID(포트 집계기 인터페이스)를 지정하십시오. 쉼표로 구분된 번호 목록, 쉼표로 구분된 번호 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 값과 범위는 1-4096의 숫자입니다. 예:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

일반 스위치 설정 정의

전역 일반 구성 템플릿을 사용하여 일반 스위치 속성을 구성할 수 있습니다.

절차

스위치 전역 일반 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 **전역 → 일반 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- LACP 시스템 ID를 생성하는 데 사용되는 LACP 시스템 우선 순위를 지정하십시오. 1-65535 사이의 숫자입니다.
- 기본 VLAN 태그 지정을 사용할 위치를 선택하십시오. 이는 다음 값 중 하나입니다.
  - **수신 및 송신**
  - **송신만**

  참고: 이 속성은 CNOS 10.10.1 이상에서 지원됩니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

전역 L2 인터페이스 설정 정의

L2 인터페이스 구성 템플릿을 사용하여 L2 인터페이스에 VLAN 태그 지정 속성을 구성할 수 있습니다.

절차

L2 인터페이스 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서**전역 → L2 인터페이스 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 하나 이상의 유효한 물리적 L2 인터페이스를 지정하십시오. 쉼표로 구분된 인터페이스 목록, 대시로 구분된 ID 범위 또는 해당 목록과 범위를 조합하여 지정할 수 있습니다. 예를 들면 다음과 같습니다.
  - 이더넷1/10
  - 이더넷1/3,5,7,9
  - 이더넷1/5-10,21-32
  - 이더넷2/2-5,7,9,11-13
- 기본 VLAN 태그 지정을 사용할 위치를 선택하십시오. 이는 다음 값 중 하나입니다.
  - **수신 및 송신**
  - **송신만**

  참고: 이 속성은 CNOS 10.10.1 이상에서 지원됩니다.
- 터널링(QinQ) 지원을 사용 또는 사용 안 함으로 설정할지 여부를 선택하십시오.

  참고: 이 속성은 CNOS 10.10.1 이상에서 지원됩니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

피어 VLAG 설정 정의

VLAG 피어 구성 템플릿을 사용하여 VLAG 피어를 구성할 수 있습니다.

절차

VLAG 피어 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 VLAG → **피어 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- VLAG를 사용 또는 사용 안 함으로 설정할지 여부를 선택하십시오.
- 피어 1 및 피어 2의 경우 다음 필드를 완료하십시오. 두 피어의 필드를 설정해야 합니다.
  - 상태 확인에 사용할 VLAG 피어의 IIPv4 또는 IPv6 주소를 지정하십시오.
  - 두 피어 간에 사용되는 포트 채널의 ID를 지정하십시오. 1-4095 사이의 숫자입니다.
  - 상태 확인에 사용되는 VRF를 지정하십시오(예, 관리, 기본값 또는 customVRF).

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

VLAG 인스턴스 설정 정의

VLAG 인스턴스 구성 템플릿을 사용하여 VLAG 인스턴스를 만들거나 업데이트할 수 있습니다. VLAG 인스턴스는 VLAG가 단일 장치로 표시되는 두 스위치(일반적으로 포트 집계를 통해)에 연결되는 장치입니다.

절차

VLAG 인스턴스 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 VLAG → **인스턴스 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- VLAG ID를 지정하십시오. 1-64 사이의 숫자입니다.
- 피어 1과 피어 2에 연결되는 포트 채널의 ID를 지정하십시오. 이는 1-4095 사이의 숫자입니다.
- VLAG 인스턴스를 사용 또는 사용 안 함으로 설정할지 여부를 선택하십시오.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

VLAG 고급 설정 정의

VLAG 고급 구성 템플릿을 사용하여 고급 VLAG 속성을 구성할 수 있습니다.

절차

VLAG 고급 구성 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 VLAG → **고급 구성**을 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 기본 피어를 제어하는 데 사용되는 우선 순위를 지정하십시오. 1-65535 사이의 숫자입니다.

  이를 지정하지 않으면 스위치의 기본 우선 순위가 사용됩니다. CNOS의 경우 기본값은 0입니다.
- 동시에 재부팅한 후 VLAG가 온라인 상태가 되는 유예 기간(초)을 지정하십시오. 240-3600 사이의 숫자입니다.

  이를 지정하지 않으면 스위치의 기본값이 사용됩니다. CNOS의 경우 기본값은 300입니다.
- 동일한 네트워크에서 VLAG 설정을 차별화하는 데 사용되는 계층 ID를 지정하십시오. 1-512 사이의 숫자입니다.
- 피어가 다시 로드된 후 포트를 가져오는 것을 지연시키는 데 사용되는 vLAG 시작 지연 간격(초)을 지정하십시오. 0-3600 사이의 숫자입니다.

  이를 지정하지 않으면 스위치의 기본값이 사용됩니다. CNOS의 경우 기본값은 120입니다.
- VLAG가 실패하기 전의 VLAG 활성 유지 시도(응답하지 않은 hello 메시지) 수를 지정하십시오. 1-24 사이의 숫자입니다.

  이를 지정하지 않으면 스위치의 기본값이 사용됩니다. CNOS의 경우 기본값은 3입니다.
- VLAG 활성 유지 시도 사이의 간격(초)을 지정하십시오. 2-300 사이의 숫자입니다.

이를 지정하지 않으면 스위치의 기본값이 사용됩니다. CNOS의 경우 기본값은 5입니다.

- VLAG 활성 유지 재시도 사이의 간격(초)을 지정하십시오. 1-300 사이의 숫자입니다.

  이를 지정하지 않으면 스위치의 기본값이 사용됩니다. CNOS의 경우 기본값은 30입니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

VLAG 인스턴스 삭제

VLAG 인스턴스 삭제 템플릿을 사용하여 VLAG 인스턴스를 삭제할 수 있습니다.

절차

VLAG 인스턴스 삭제 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 분할창에서 **VLAG → 인스턴스 삭제**를 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- VLAG 인스턴스의 고유 ID를 지정하십시오. 1-64 사이의 숫자입니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

스파인 리프 토폴로지 정의

Spine-leaf 토폴로지 마법사 템플릿을 사용하여 물리적 토폴로지를 확인하고 관리되는 스위치에 SpineLeaf(L3 패브릭) 설정을 배포할 수 있습니다.

절차

Spine-leaf 토폴로지 마법사 템플릿을 만들려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 왼쪽 탐색 창에서 **스파인 리프 → 토폴로지 마법사**를 클릭하고 **만들기** 아이콘( )을 클릭하십시오.

단계 3. 새 템플릿 만들기 대화 상자에서 다음 정보를 지정하십시오.

- 템플릿의 이름과 설명을 입력하십시오.
- 스위치에서 실행 중인 BGP(Border Gateway Protocol) 프로토콜에 대한 자율 시스템(AS) 번호를 지정하십시오. 1-4294967295 사이의 숫자입니다.

  참고: 이는 CNOS 10.9.3 이상에서 지원됩니다.
- 스위치 간의 단일 링크 허용 여부를 선택하십시오.

  일반적으로 spine과 leaf 스위치 사이에 최소한 두 개의 링크가 없으면 배포가 실패합니다.

단계 4. 템플릿을 저장하려면 **만들기**를 클릭하고, 템플릿을 저장한 후 하나 이상의 관리되는 랙 스위치에 즉시 배포하려면 **만들기 및 배포**를 클릭하십시오.

템플릿 배포에 대한 정보는 대상 스위치에 스위치 구성 템플릿 배포의 내용을 참조하십시오.

대상 스위치에 스위치 구성 템플릿 배포

VLAN 포트 구성 템플릿을 만들어 VLAN 포트 설정을 정의할 수 있습니다.

이 작업 정보

배포에는 세 가지 유형이 있습니다.

- **정상**. 기본 계층형 아키텍처에서 하나 이상의 랙 스위치에 스위치 구성 설정을 배포합니다.
- VLAG. VLAG(가상 링크 집합 그룹) 아키텍처를 지원하는 두 스위치에 스위치 구성 설정을 배포합니다. 이 두 스위치는 동일한 모델 및 소프트웨어 버전이어야 합니다.
- **스파인 리프**. 하나 이상의 스파인 스위치 및 리프 스위치에 대한 배치 템플릿입니다.

절차

하나 이상의 관리되는 스위치에 스위치 구성 템플릿을 배포하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. 배포할 스위치 구성 템플릿을 하나 이상 선택하십시오.

단계 3. **배포** 아이콘()을 클릭하여 템플릿 배포 대화 상자를 표시하십시오.

단계 4. 템플릿을 배포할 스위치를 하나 이상 선택하십시오.

선택한 템플릿과 호환되는 스위치만 나열됩니다.

단계 5. **배포**를 클릭하십시오. 선택한 각 스위치의 배포 상태를 나열하는 대화 상자가 표시됩니다.

단계 6. 배포 프로세스를 시작하려면 **배포**를 다시 클릭하십시오.

참고: 배포를 완료하려면 몇 분 정도 걸릴 수 있습니다.

완료한 후에

배포 내역을 볼 수 있습니다(스위치 구성 배포 기록 보기 참조).

스위치 구성 배포 기록 보기

템플릿 이름, 템플릿 유형, 타임 스탬프 및 배포된 스위치 등 관리되는 스위치에 배포된 스위치 구성 템플릿에 대한 정보를 볼 수 있습니다. 각 배포에는 배포할 때의 템플릿 스냅샷이 포함되어 있습니다.

절차

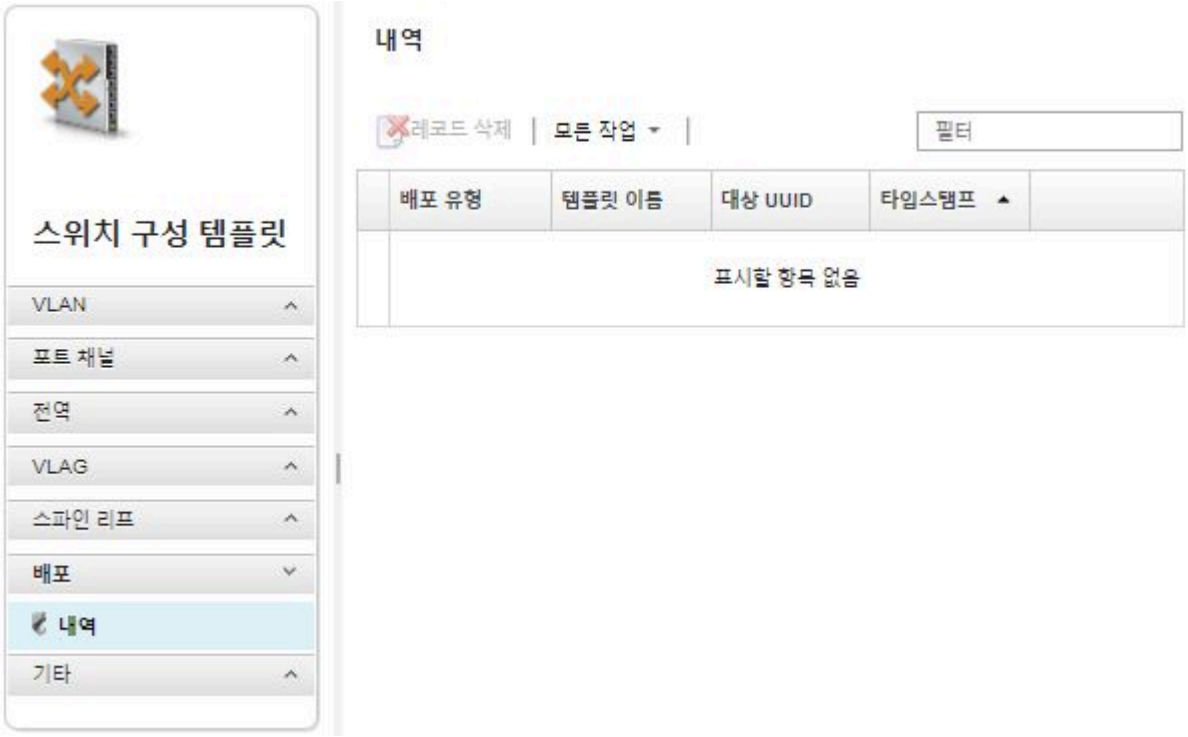
스위치 구성 배포 기록을 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 스위치 구성 템플릿**을 클릭하십시오. 스위치 구성 템플릿 페이지가 표시됩니다.

단계 2. **배포**를 확장하고 왼쪽 탐색 분할창에서 **내역**을 클릭하여 배포된 템플릿의 테이블을 표시하십시오.

상태 열은 구성 배포를 성공했는지 여부를 나타냅니다. 이는 다음 상태 중 하나입니다.

- **성공함**. 모든 대상 스위치에 대한 구성 배포가 성공적으로 완료되었습니다.
- **경고**. 하나 이상의 대상 스위치에 대한 구성 배포가 경고와 함께 완료되었습니다.
- **실패함**. 하나 이상의 대상 스위치에 대한 구성 배포가 실패했습니다.



완료한 후에

- 테이블에서 템플릿 이름을 클릭하여 배포된 항목과 성공 또는 실패한 항목 등 배포된 각 템플릿에 대한 정보를 보십시오.
- 배포를 선택하고 **삭제** 아이콘( )을 클릭하여 배포 기록을 지우십시오.

제 13 장 관리 장치에서 펌웨어 업데이트

Lenovo XClarity Administrator 웹 인터페이스에서 섀시, 서버, 스토리지 시스템 및 스위치 등의 관리 장치에 대한 펌웨어 업데이트를 다운로드, 설치 및 관리할 수 있습니다. 해당 장치의 펌웨어가 준수되도록 관리 장치에 펌웨어 준수 정책을 할당할 수 있습니다. 유효성 검증된 펌웨어 수준이 제안된 사정 정의된 정책과 일치하지 않는 경우 펌웨어 준수 정책을 작성하여 편집할 수도 있습니다.

자세히 알아보기:
- XClarity Administrator: 펌웨어 업데이트 시 효율 높이기
- Lenovo ThinkSystem 펌웨어 및 드라이버 업데이트 모범 사례
- XClarity Administrator: 베어메탈에서 클러스터로
- XClarity Administrator: 펌웨어 업데이트
- XClarity Administrator: 펌웨어 보안 업데이트 프로비저닝

시작하기 전에

펌웨어 업데이트 및 장치 드라이버 업데이트는 XClarity Administrator에서 별도의 프로세스이며, 이러한 프로세스 간에는 연결이 없습니다. 펌웨어와 동시에 장치 드라이버를 업데이트하는 것이 좋지만 XClarity Administrator은(는) 관리되는 장치의 펌웨어와 장치 드라이버 간에 준수를 유지하지는 않습니다.

이 작업 정보

참고: 운영 체제에서 펌웨어를 업데이트할 필요가 없습니다. 베어메탈 서버의 경우 펌웨어를 업데이트하기 전에 서버의 전원이 꺼져 있는지 확인하십시오.

다음 관리되는 장치에 대한 펌웨어 업데이트를 관리하고 적용할 수 있습니다.
- **섀시**. CMM 업데이트
- **ThinkAgile, ThinkSystem, System x, Converged, Flex System 및 NeXtScale 서버**. 베이스보드 관리 컨트롤러, UEFI, DSA, mezzanine 및 어댑터 업데이트
- **RackSwitch 및 Flex System 스위치**
- **Lenovo Storage 및 ThinkSystem DM 스토리지 장치**
- **IBM TS4300 테이프 라이브러리 장치**

다음 장치의 펌웨어는 XClarity Administrator을(를) 통해 업데이트할 수 없습니다.
- **ThinkServer 서버**. 펌웨어 업데이트 방법에 대한 정보를 찾으려면 서버와 함께 제공된 설명서를 참조하십시오.
- **Flex Power Systems 컴퓨팅 노드**. Flex Power Systems 컴퓨팅 노드에 대한 펌웨어를 업데이트할 수 있는 몇 가지 방법이 있습니다. 자세한 정보는 IBM Flex System p260/p460 계산 노드 온라인 설명서의 내용을 참조하십시오. 다른 Flex Power Systems 컴퓨팅 노드에 대한 프로세스도 유사합니다.
- **스택 모드 또는 보호 모드의 Flex 스위치**. 스택 스위치에서 펌웨어를 업데이트할 수 *없습니다*. 스택된 모든 스위치에 대해서는 펌웨어 업데이트가 사용 불가능합니다.
- **Flex 스위치**. 다음 스위치를 사용하는 경우 펌웨어 업데이트 방법에 대한 정보를 찾으려면 스위치와 함께 제공된 설명서를 참조하십시오.
  - Cisco Nexus B22 Fabric Extender

절차

다음 그림은 관리되는 서버에서 펌웨어를 업데이트하는 워크플로우를 설명합니다.

단계 1. 펌웨어 업데이트 리포지토리 관리

*펌웨어 업데이트 리포지토리*에는 사용 가능한 업데이트 카탈로그와 관리되는 장치에 적용할 수 있는 업데이트 패키지가 포함되어 있습니다.

*카탈로그*에는 XClarity Administrator에서 지원하는 모든 장치에 현재 사용할 수 있는 펌웨어 업데이트에 대한 정보가 있습니다. 카탈로그는 펌웨어 업데이트를 장치 유형별로 구성합니다. 카탈로그를 새로 고치면 XClarity Administrator가 Lenovo 웹 사이트에서 사용 가능한 최신 펌웨어 업데이트에 대한 정보를 검색하고(메타데이터 .xml 또는 .json 파일 및 readme .txt 파일 포함) 이 정보를 펌웨어 업데이트 리포지토리에 저장합니다. 페이로드 파일(.exe)이 다운로드되지 않았습니다. 카탈로그 새로 고침에 대한 자세한 정보는 제품 카탈로그 새로 고침의 내용을 참조하십시오.

새 펌웨어 업데이트가 사용 가능한 경우 관리 장치에서 해당 펌웨어를 업데이트하려면 먼저 업데이트 패키지를 다운로드해야 합니다. 카탈로그를 새로 고쳐도 업데이트 패키지를 자동으로 다운로드하지는 않습니다. 펌웨어 업데이트 리포지토리 페이지의 **제품 카탈로그** 테이블은 다운로드된 업데이트 패키지와 다운로드할 수 있는 업데이트 패키지를 식별합니다.

몇 가지 방법으로 펌웨어 업데이트를 다운로드할 수 있습니다.

- **펌웨어 업데이트 리포지토리 팩**

  펌웨어 업데이트 리포지토리 팩은 지원되는 대부분의 장치 및 새로 고친 기본 펌웨어 준수 정책에 대해 XClarity Administrator 릴리스와 동시에 사용할 수 있는 최신 펌웨어 모음입니다. 이러한 리포지토리 팩을 가져온 다음 관리 서버 업데이트 페이지에서 적용합니다. 펌웨어 업데이트 리포지토리 팩을 적용하는 경우 팩의 각 업데이트 패키지가 펌웨어 업데이트 리포지토리에 추가되고 모든 관리 가능한 장치에 대해 기본 펌웨어 준수 정책이 자동으로 작성됩니다. 미리 정의된 이 정책을 복사할 수는 있지만 변경할 수는 없습니다.

  다음 리포지토리 팩을 사용할 수 있습니다.

  - lnvgy_sw_lxca_cmmswitchrepo*x*-*x.x.x*_anyos_noarch. 모든 CMM 및 Flex System 스위치에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_storagerackswitchrepo*x*-*x.x.x*_anyos_noarch. 모든 RackSwitch 스위치 및 Lenovo Storage 장치에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_systemxrepo*x*-*x.x.x*_anyos_noarch. 모든 Converged HX 시리즈, Flex System, NeXtScale 및 System x 서버에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_thinksystemrepo*x*-*x.x.x*_anyos_noarch. 모든 ThinkAgile 및 ThinkSystem 서버에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_thinksystemv2repo*x*-*x.x.x*_anyos_noarch. 모든 ThinkAgile 및 ThinkSystem V2 서버에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_thinksystemv3repo*x*-*x.x.x*_anyos_noarch. 모든 ThinkAgile 및 ThinkSystem V3 서버에 대한 펌웨어 업데이트가 포함됩니다.

  펌웨어 업데이트 리포지토리 팩이 관리 서버 업데이트 페이지의 **다운로드 상태** 열에 있는 리포지토리에 저장되는지 여부를 판별할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

  - **다운로드됨**. 펌웨어 업데이트 리포지토리 팩이 리포지토리에 저장됩니다.
  - **다운로드되지 않음**. 펌웨어 업데이트 리포지토리 팩이 사용 가능하지만 리포지토리에 저장되지 않습니다.

- UpdateXpress System Pack(UXSP)

참고: XCC2가 있는 서버의 경우 이러한 팩을 펌웨어 번들이라고 합니다. *번들*은 패키지 이름 및 미리 정의된 정책 이름에 사용됩니다.

UXSP에는 운영 체제별로 정리된 최신의 사용 가능한 펌웨어 및 장치 드라이버 업데이트가 포함되어 있습니다. UXSP를 다운로드하는 경우 XClarity Administrator는 카탈로그에 나열된 버전을 기반으로 하여 UXSP를 다운로드하고 업데이트 패키지를 펌웨어 업데이트 리포지토리에 저장합니다. UXSP를 다운로드하면 UXSP의 각 펌웨어 업데이트가 펌웨어 업데이트 리포지토리에 추가되고 **개별 업데이트** 탭에 나열되며 관리 가능한 모든 장치에 대해 다음 이름을 사용하여 기본 펌웨어 준수 정책이 자동으로 생성됩니다. 미리 정의된 이 정책을 복사할 수는 있지만 변경할 수는 없습니다.

- *{uxsp-version}-{date}-{server-short-name}*-UXSP (예: `v1.50-2017-11-22-SD530-UXSP`)
- *{uxsp-version}-{buildnumber}-{server-short-name}*-bundle(예: `22a.0-kaj92va-SR650V3-bundle`)

참고: 펌웨어 업데이트: 리포지토리 페이지에서 UXSP를 다운로드하거나 가져오면, 펌웨어 업데이트가 다운로드되어 리포지토리에 저장됩니다. 장치 드라이버 업데이트가 삭제됩니다. UXSP를 사용한 Windows 장치 드라이버 업데이트 다운로드 또는 가져오기에 대한 정보는 OS 장치 드라이버 리포지토리 관리의 내용을 참조하십시오.

UXSP가 펌웨어 업데이트: 리포지토리 페이지의 **개별 업데이트**의 **다운로드 상태** 열에 있는 펌웨어 업데이트 리포지토리에 저장되는지 여부를 판단할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

- **다운로드됨**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 리포지토리에 저장됩니다.
- *x* / *y* **다운로드됨**. 업데이트 패키지의 펌웨어 업데이트 전체가 아닌 일부가 리포지토리에 저장됩니다. 괄호 안의 숫자는 사용 가능한 업데이트 수와 저장된 업데이트 수를 나타내며, 특정 장치 유형에 대한 업데이트는 없습니다.
- **다운로드되지 않음**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 사용 가능하지만 리포지토리에 저장되지 않습니다.

- **개별 펌웨어 업데이트 적용**

  한 번에 개별 펌웨어 업데이트 패키지를 다운로드할 수 있습니다. 펌웨어 업데이트 패키지를 다운로드하는 경우 XClarity Administrator는 카탈로그에 나열된 버전을 기반으로 하여 업데이트를 다운로드하고 업데이트 패키지를 펌웨어 업데이트 리포지토리에 저장합니다. 그런 다음 각 관리 장치의 해당 업데이트 패키지를 사용하여 펌웨어 준수 정책을 작성할 수 있습니다.

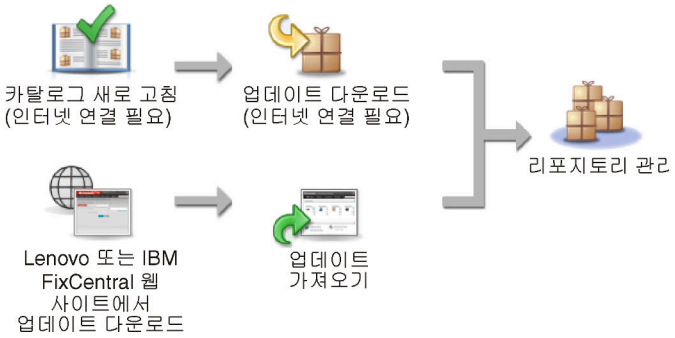
  참고: 코어 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 pDSA)는 운영 체제에 독립적입니다. RHEL 6 또는 SLES 11 운영 체제의 펌웨어 업데이트 패키지를 사용하여 컴퓨팅 노드와 랙 서버를 업데이트합니다. 관리되는 서버에 사용할 펌웨어 업데이트 패키지에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

  특정 *펌웨어 업데이트*가 펌웨어 업데이트: 리포지토리 페이지에서 **개별 업데이트** 탭의 **다운로드 상태** 열에 있는 펌웨어 업데이트 리포지토리에 저장되는지 판별할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

  - **다운로드됨**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 리포지토리에 저장됩니다.
  - *x* / *y* **다운로드됨**. 업데이트 패키지의 펌웨어 업데이트 전체가 아닌 일부가 리포지토리에 저장됩니다. 괄호 안의 숫자는 사용 가능한 업데이트 수와 저장된 업데이트 수를 나타내며, 특정 장치 유형에 대한 업데이트는 없습니다.
  - **다운로드되지 않음**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 사용 가능하지만 리포지토리에 저장되지 않습니다.

카탈로그를 새로 고치고 펌웨어 업데이트를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. 인터넷에 연결되어 있지 않은 경우 웹 브라우저를 사용하여

XClarity Administrator 호스트에 대한 네트워크 액세스 권한이 있는 워크스테이션에 파일을 수동으로 다운로드한 다음 파일을 펌웨어 업데이트 리포지토리로 가져올 수 있습니다.



펌웨어 업데이트를 XClarity Administrator(으)로 수동으로 가져올 때 필수 파일인 페이로드(이미지 및 MIB), 메타데이터, 변경 기록 및 readme 파일을 포함해야 합니다. 예를 들어, 다음과 같습니다.

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

주의:

- 이러한 필수 파일만 가져오십시오. 펌웨어 다운로드 웹 사이트에 있는 다른 파일은 가져오지 마십시오.
- 업데이트 패키지에 XML 파일이 없는 경우 업데이트를 가져올 수 없습니다.
- 업데이트와 연결된 모든 필수 파일이 포함되지 않은 경우 리포지토리에서는 업데이트가 다운로드되지 않았음을 표시하고, 이는 가져오기가 부분적으로 수행됨을 의미합니다. 그런 다음 해당 파일을 선택하고 가져와서 누락된 파일을 가져올 수 있습니다.
- 코어 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 pDSA)는 운영 체제에 독립적입니다. RHEL 6 또는 SLES 11 운영 체제의 펌웨어 업데이트 패키지를 사용하여 컴퓨팅 노드와 랙 서버를 업데이트합니다. 관리되는 서버에 사용할 펌웨어 업데이트 패키지에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

펌웨어 업데이트에 대한 자세한 정보는 펌웨어 업데이트 리포지토리 관리의 내용을 참조하십시오.

단계 2. **(옵션) 펌웨어 준수 정책 만들기 및 할당**

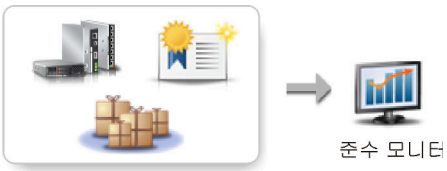
*펌웨어 준수 정책*은 주의가 필요한 장치를 플래그 지정하여 특정 관리되는 장치의 펌웨어가 현재 또는 특정 수준에 있도록 합니다. 각 펌웨어 준수 정책은 장치의 준수 상태를 유지하려면 어떤 장치를 모니터링하고 어떤 펌웨어 수준을 설치해야 하는지 식별합니다. 장치 또는 펌웨어 구성 요소 수준에서 준수 정책을 설정할 수 있습니다. 그러면 XClarity Administrator에서 이러한 정책을 사용하여 관리되는 장치의 상태를 확인하고 규정을 위반한 장치를 식별합니다.

펌웨어 준수 정책을 작성하면 다음과 같은 경우에 XClarity Administrator가 장치에 플래그를 지정하도록 선택할 수 있습니다.

- 장치의 펌웨어 수준이 낮습니다.
- 장치의 펌웨어가 이행 대상 버전과 일치하지 않습니다.

XClarity Administrator는 **리포지토리의 최신 펌웨어**라는 미리 정의된 펌웨어 준수 정책과 함께 제공됩니다. 새 펌웨어를 다운로드하거나 리포지토리로 가져오는 경우 리포지토리에 사용 가능한 최신 펌웨어 버전이 포함되도록 이 정책이 업데이트됩니다.

펌웨어 준수 정책이 장치에 할당된 후 장치 인벤토리가 변경되거나 펌웨어 업데이트 리포지토리가 변경되는 경우 XClarity Administrator이(가) 각 장치의 준수 상태를 검사합니다. 장치의 펌웨어가 할당 된 정책을 준수하지 않으면 XClarity Administrator해당 장치가 펌웨어 업데이트 : 적용 / 활성화 펌웨어 준수 정책에 지정한 규칙에 따라 페이지



하드웨어, 카탈로그 및 정책 변경

예를 들어 모든 ThinkSystem SR850 장치에 설치된 펌웨어의 기준 수준을 정의하는 펌웨어 준수 정책을 작성한 다음 모든 관리 ThinkSystem SR850 장치에 해당 펌웨어 준수 정책을 할당할 수 있습니다. 펌웨어 업데이트 리포지토리를 새로 고치고 새 펌웨어 업데이트가 추가되면 해당 컴퓨팅 노드가 준수 안됨 상태가 될 수 있습니다. 이러한 경우 XClarity Administrator는 펌웨어 업데이트: 적용/활성화 페이지를 업데이트하여 장치가 준수되지 않음을 표시하고 경고를 생성합니다.

참고: 할당된 펌웨어 준수 정책의 요구 사항을 충족하지 않는 장치에 대한 경고를 표시하거나 숨길 수 있습니다(전역 펌웨어 업데이트 설정 구성 참조). 알림은 기본적으로 숨겨져 있습니다.

펌웨어 준수 정책에 대한 자세한 정보는 펌웨어 준수 정책 생성 및 할당의 내용을 참조하십시오.

단계 3. **업데이트 적용 및 활성화**

XClarity Administrator는 펌웨어 업데이트를 관리되는 장치에 자동으로 적용하지 않습니다. 펌웨어를 업데이트하려면 선택한 장치에서 업데이트를 수동으로 적용하고 활성화해야 합니다. 다음 방법 중 하나로 펌웨어를 적용할 수 있습니다.

- **준수 정책을 사용하여 번들 펌웨어 업데이트 적용**

  해당하는 펌웨어 업데이트 패키지가 포함된 번들 이미지를 사용하여 할당된 펌웨어 준수 정책에 따라 선택한 장치의 모든 구성 요소에 펌웨어 업데이트를 적용할 수 있습니다.

  번들 업데이트 프로세스는 먼저 베이스보드 관리 컨트롤러와 UEFI를 대역 외 방식으로 업데이트합니다. 이러한 업데이트가 완료되면 프로세스에서 시스템 유형에 따라 준수 정책에 남아 있는 펌웨어의 번들 이미지를 생성합니다. 그런 다음 프로세스에서 이미지를 선택한 장치에 마운트하고 장치를 다시 시작하여 이미지를 부팅합니다. 남은 업데이트를 수행하기 위해 이미지가 자동으로 실행됩니다.

  주의: 업데이트 프로세스를 시작하기 전에 선택한 장치의 전원이 꺼집니다. 실행 중인 워크로드가 중지되었는지 혹은 가상화된 환경에서 작업 중인 경우 해당 작업이 다른 서버로 이동되었는지 확인하십시오. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.

  참고:

  - 번들 펌웨어 업데이트 적용은 ThinkSystem SR635 및 SR655 서버에만 지원됩니다.
  - 번들 펌웨어 업데이트 적용은 IPv4 주소에만 지원됩니다. IPv6 주소는 지원되지 않습니다.
  - 전체 인벤토리 정보를 검색하려면 각 대상 장치가 한 번 이상 OS로 부팅되었어야 합니다.
  - 번들 업데이트 기능을 사용하려면 베이스보드 관리 컨트롤러 펌웨어 v2.94 이상이 필요합니다.
  - 리포지토리 팩의 펌웨어 업데이트 또는 개별 펌웨어 업데이트만 사용됩니다. UpdateXpress System Packs (UXSPs)는 지원되지 않습니다.

- 다운로드된 펌웨어 업데이트만 적용됩니다. 제품 카탈로그를 새로 고치고 적합한 펌웨어 업데이트를 다운로드하십시오(제품 카탈로그 새로 고침 및 펌웨어 업데이트 다운로드 중 참조).

  참고: XClarity Administrator가 처음 설치되면 제품 카탈로그와 리포지토리가 비어 있습니다.

- 준수 검사는 ThinkSystem SR635 및 SR655 서버의 베이스보드 관리 컨트롤러와 UEFI에만 지원됩니다. 그러나 XClarity Administrator에서는 사용 가능한 모든 하드웨어 구성 요소에 대해 펌웨어 업데이트 적용을 시도합니다.
- 업데이트는 할당된 펌웨어 준수 정책에 따라 적용됩니다. 구성 요소의 하위 집합은 업데이트할 수 없습니다.
- Lenovo XClarity Provisioning Manager(LXPM), LXPM Windows 드라이버 또는 LXPM Linux 드라이버용 펌웨어 업데이트를 ThinkSystem SR635 및 SR655 서버에 적용하려면 XClarity Administrator v3.2 이상이 필요합니다.
- 현재 설치된 버전이 할당된 준수 정책보다 높으면 베이스보드 관리 컨트롤러 및 UEFI 업데이트를 건너뜁니다.
- 펌웨어 준수 정책을 작성하여 펌웨어 업데이트를 적용할 장치에 할당해야 합니다. 자세한 정보는 펌웨어 준수 정책 생성 및 할당의 내용을 참조하십시오.
- 업데이트 프로세스를 시작하기 전에 선택한 장치의 전원이 꺼집니다. 실행 중인 워크로드가 중지되었는지 혹은 가상화된 환경에서 작업 중인 경우 해당 작업이 다른 서버로 이동되었는지 확인하십시오.

- **준수 정책을 사용 또는 사용하지 않고 선택한 펌웨어 업데이트 적용**

  해당하는 펌웨어 업데이트 패키지를 사용하여 할당된 펌웨어 준수 정책에 따라 선택한 구성 요소 및 장치에 펌웨어 업데이트를 적용할 수 있습니다. 준수 정책을 사용하지 않고도 선택한 구성 요소 및 장치에 현재 설치된 펌웨어 이후 버전의 펌웨어 업데이트를 적용할 수도 있습니다.

  특정 장치의 모든 구성 요소에 업데이트를 적용할 수 있습니다. 또한 베이스보드 관리 컨트롤러나 UEFI 등 선택한 장치의 구성 요소 하위 집합에만 업데이트를 적용할 수도 있습니다.

  펌웨어 업데이트를 활성화하려면 장치를 다시 시작해야 합니다. 장치 재시작은 파괴적이므로 주의하십시오. 업데이트 프로세스의 일부로 장치를 다시 시작하거나(*즉시 활성화*) 유지 관리 창에서 장치를 다시 시작할 수 있을 때까지 기다리도록(*지연된 활성화*) 선택할 수 있습니다. 이 경우 업데이트를 적용하려면 장치를 수동으로 다시 시작해야 합니다.

  관리되는 장치에 대한 펌웨어를 업데이트하도록 선택하는 경우 다음 단계가 발생합니다.

  1. XClarity Administrator는 장치에 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 DSA)를 보냅니다.
  2. 장치가 다시 시작되면 장치에서 펌웨어 업데이트가 활성화됩니다.
  3. 서버의 경우 XClarity Administrator가 네트워크 어댑터 및 하드 드라이브 업데이트와 같은 옵션 장치에 대한 업데이트를 보냅니다. XClarity Administrator는 이러한 업데이트를 적용하면 서버가 다시 시작됩니다.
  4. 장치를 다시 시작하거나 즉시 활성화를 선택하는 경우 옵션 장치에 대한 업데이트가 활성화됩니다.

  참고:

  - 준수 정책을 사용하여 업데이트를 적용하는 경우 펌웨어 준수 정책을 생성하고 각 대상 장치에 할당해야 합니다. 자세한 정보는 펌웨어 준수 정책 생성 및 할당의 내용을 참조하십시오.
  - 여러 구성 요소에 대한 업데이트가 포함된 펌웨어 업데이트 패키지를 설치하도록 선택하는 경우 업데이트 패키지를 적용하는 모든 구성 요소가 업데이트됩니다.
  - CMM 및 Flex 스위치에 대한 업데이트는 지연된 활성화를 선택한 경우에도 항상 즉시 활성화됩니다.

장치 세트에서 업데이트를 수행하는 경우 XClarity Administrator에서는 다음 순서로 업데이트를 수행합니다.

- 섀시 CMM
- RackSwitch 및 Flex System 스위치
- Flex 계산 노드와 랙 및 타워 서버
- Lenovo Storage 장치

주의: 관리되는 장치에서 펌웨어 업데이트를 적용하려면 먼저 다음 작업을 완료해야 합니다.

- 관리되는 장치에서 펌웨어를 업데이트하기 전에 펌웨어 업데이트 고려사항을 읽으십시오(펌웨어 업데이트 고려사항 참조).
- 처음에는 업데이트가 지원되지 않는 장치가 보기에서 숨겨집니다. 지원되지 않는 장치는 업데이트하도록 선택할 수 없습니다.
- 기본적으로 감지된 모든 구성 요소가 업데이트 적용이 가능한 것으로 나열됩니다. 그러나 하위 수준 펌웨어를 사용하면 구성 요소가 인벤토리에 표시되지 않거나 전체 버전 정보를 보고하지 못할 수 있습니다. 업데이트를 적용할 수 있는 모든 정책 기반 패키지를 나열하려면 **모든 작업 ➙ 전역 설정** 및 **하위 수준 장치에 대한 향상된 지원**을 클릭하십시오. 이 옵션을 선택하면 "기타 사용 가능한 소프트웨어"가 감지되지 않은 장치의 설치된 버전 열에 나열됩니다. 자세한 정보는 전역 펌웨어 업데이트 설정 구성의 내용을 참조하십시오.

  참고:

  - 관리되는 장치에 대한 업데이트가 진행 중인 경우에는 전역 설정을 변경할 수 없습니다.
  - 추가 옵션을 생성하는 데는 몇 분 정도 걸립니다. 몇 분 후에 **새로 고침** 아이콘()을 클릭하여 표를 새로 고쳐야 할 수 있습니다.
- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 ➙ 작업**을 클릭하십시오.
- 펌웨어 업데이트 리포지토리가 배포할 펌웨어 패키지를 가지고 있는지 확인하십시오. 그렇지 않은 경우 제품 카탈로그를 새로 고치고 적합한 펌웨어 업데이트를 다운로드하십시오(제품 카탈로그 새로 고침 및 펌웨어 업데이트 다운로드 중 참조).

  참고: XClarity Administrator가 처음 설치되면 제품 카탈로그와 리포지토리가 비어 있습니다.

  필수 펌웨어를 설치하려는 경우 필수 펌웨어가 리포지토리에도 다운로드되는지 확인해야 합니다.

  경우에 따라 펌웨어를 업데이트하는 데 여러 버전이 필요할 수 있으며 모든 버전을 리포지토리에 다운로드해야 합니다. 예를 들어, IBM FC5022 SAN 확장 가능 스위치를 v7.4.0a에서 v8.2.0a로 업그레이드하려면 먼저 v8.0.1-pha를 설치하고 v8.1.1과 v8.2.0a를 순서대로 설치해야 합니다. 스위치를 v8.2.0a로 업데이트하려면 세 버전이 모두 리포지토리에 있어야 합니다.
- 일반적으로 펌웨어 업데이트를 활성화하려면 장치를 다시 시작해야 합니다. 업데이트 프로세스 중에 장치를 다시 시작하려는 경우(*즉시 활성화*) 실행 중인 워크로드가 중지되었거나, 가상화된 환경에서 작업 중이라면 다른 서버로 이동했는지 확인하십시오.

업데이트 설치에 대한 자세한 정보는 펌웨어 업데이트 적용 및 활성화의 내용을 참조하십시오.

펌웨어 업데이트 고려사항

Lenovo XClarity Administrator를 사용하여 관리되는 장치의 펌웨어 업데이트를 시작하기 전에 다음 중요 고려사항을 검토하십시오.

- 일반 고려사항
- CMM 고려사항

- 베이스보드 관리 컨트롤러 고려 사항
- ThinkSystem 장치 고려 사항
- Flex System 장치 고려 사항
- 저장 장치 고려사항

일반 고려사항

- **펌웨어의 최소 필수 수준.**

  XClarity Administrator를 사용하여 관리되는 장치의 펌웨어를 업데이트하기 전에 각 관리되는 장치에 설치된 펌웨어가 최소 필수 수준인지 확인하십시오. 필요한 최소 펌웨어 수준은 XClarity Administrator 지원 – 호환성 웹 페이지에서 **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하여 확인할 수 있습니다.

  참고: I/O 장치 지원 및 알려진 제한사항에 대한 정보는 XClarity Administrator 지원 – 호환성 웹 페이지의 내용을 참조하십시오.

- **모든 구성 요소를 펌웨어 업데이트 리포지토리에 포함된 수준으로 업데이트하십시오.**

  Flex System 구성 요소의 펌웨어 업데이트는 함께 테스트되고 릴리스되므로 Flex System 섀시에 있는 모든 구성 요소에서 동일한 펌웨어 수준을 유지할 것을 권장합니다. 따라서 동일한 유지 관리 창에서 섀시에 있는 모든 구성 요소의 펌웨어를 업데이트하는 것이 중요합니다. XClarity Administrator는 선택한 업데이트를 올바른 순서대로 자동으로 적용합니다.

- **UXSP를 다운로드할 때 LXPM Linux 드라이버 및 LXPM Windows 드라이버가 포함되지 않음**

  Lenovo XClarity Provisioning Manager (LXPM)Linux 및 Windows 드라이버는 UpdateXpress System Pack(UXSP)에 포함되지 않습니다. 이 업데이트 패키지를 장치에 적용하려면 최신 펌웨어 업데이트 리포지토리 팩을 다운로드하거나 개별 패키지를 수동으로 다운로드하고 해당 패키지를 포함하도록 펌웨어 준수 정책을 만들어야 합니다.

- **일부 펌웨어 업데이트는 장치 드라이버의 최소 수준에 따라 다릅니다.**

  서버에 어댑터와 I/O 펌웨어 업데이트를 적용하기 전에 장치 드라이버를 최소 수준으로 업데이트해야 할 수 있습니다. 일반적으로 펌웨어 업데이트는 장치 드라이버의 특정 수준에 종속되지 않습니다. 이러한 종속성에 대해서는 펌웨어 업데이트 readme를 참조하고 펌웨어를 업데이트하기 전에 운영 체제에서 장치 드라이버를 업데이트하십시오. XClarity Administrator는 운영 체제에서 장치 드라이버를 업데이트하지 않습니다.

- **펌웨어를 업데이트하기 전에 XClarity Administrator를 재부팅하십시오.**

  이전 펌웨어 업데이트 시도가 실패하는 경우 펌웨어를 업데이트하기 전에 XClarity Administrator를 재부팅하십시오. 관리 서버를 재부팅하면 펌웨어 업데이트에 사용되는 시스템 예약 계정이 관리되는 장치에서 동기화됩니다.

- **펌웨어 업데이트가 중단되면 장치에서 워크로드가 중지되어야 합니다.**

  업데이트를 즉시 활성화하도록 선택하면 관리되는 장치의 펌웨어 업데이트 수행이 중단됩니다. 즉시 활성화를 사용하여 펌웨어를 업데이트하기 전에 장치를 중지해야 합니다.

  서버에서 펌웨어를 업데이트하는 경우 서버가 시스템 종료되고 유지 관리 운영 체제에 배치되어 어댑터, 디스크 드라이브 및 SSD의 장치 드라이버를 업데이트합니다.

  펌웨어 업데이트 프로세스 중에 주어진 섀시의 Flex 스위치가 순서대로 업데이트되고 다시 시작됩니다. 중복 데이터 경로를 구현하면 중단을 줄일 수 있지만 펌웨어 업데이트 중에 여전히 네트워크 연결이 잠시 중단될 수 있습니다.

- **XClarity Administrator가 실행되는 서버에서 펌웨어를 업데이트하는 경우 XClarity Administrator를 사용하지 마십시오.**

  XClarity Administrator이(가) 관리 중인 서버에서 실행되는 하이퍼바이저 호스트에서 실행 중인 경우 해당 서버에서 펌웨어를 업데이트하는 데 XClarity Administrator을(를) 사용하지 마십시오. 펌웨어 업데이트가 즉시 활성화로 적용되는 경우 XClarity Administrator는 대상 서버를 강제로 다시

시작합니다. 이로 인해 하이퍼바이저 호스트와 XClarity Administrator도 다시 시작됩니다. 지연된 활성화로 적용되는 경우 대상 시스템이 다시 시작될 때까지 일부 펌웨어만 적용됩니다.

CMM 고려사항

- **펌웨어를 업데이트하기 전에 CMM을 가상으로 재배치합니다.**

  3주 넘게 실행되었고 듀얼 CMM 구성을 사용하며 2PET12Q를 통해 펌웨어 수준 스택 릴리스 1.3.2.1 2PET12K를 실행하는 CMM을 업데이트하는 경우 펌웨어를 업데이트하기 전에 기본 및 대기 CMM을 모두 가상으로 재배치해야 합니다(CMM 가상 재배치 참조).

베이스보드 관리 컨트롤러 고려 사항

- **보류 중인 활성화 상태에 필요한 최소 BMC 수준**

  보류 중인 활성화 상태를 보려면 다음 펌웨어 버전이 서버의 기본 베이스보드 관리 컨트롤러에 설치되어 있어야 합니다.
  - IMM2: TCOO46F, TCOO46E 이상(플랫폼에 따라 다름)
  - XCC: CDI328M, PSI316N, TEI334I 이상(플랫폼에 따라 다름)

- **업데이트가 기본 관리 컨트롤러 및 UEFI 펌웨어 파티션에 적용되었습니다.**

  베이스보드 관리 컨트롤러(BMC) 및 UEFI 업데이트를 관리 컨트롤러 및 UEFI 각각의 기본 및 백업 펌웨어 파티션에 적용할 수 있습니다.

  관리 컨트롤러 및 UEFI 업데이트를 서버의 기본 펌웨어 파티션에만 적용할 수도 있습니다. 기본적으로 관리 컨트롤러는 기본 관리 컨트롤러가 제대로 실행되고 새 수준이 백업으로 승격할 준비가 된 후에 백업 관리 컨트롤러 파티션을 기본 관리 컨트롤러 파티션과 동기화하도록 구성됩니다. 그러나 관리 컨트롤러는 기본적으로 UEFI 백업 파티션을 동기화하도록 구성되지 않습니다. 따라서 관리 컨트롤러에서 다음 옵션 중 하나를 고려해 보십시오.

  - UEFI 백업 파티션의 자동 동기화를 사용합니다.

    이렇게 하면 기본 및 백업 파티션 둘 다 동일한 수준의 펌웨어를 실행하게 됩니다(또한 백업 UEFI 펌웨어가 관리 컨트롤러 펌웨어와 호환됨).

  - 관리 컨트롤러 백업 파티션의 자동 동기화를 사용하지 않습니다.

    권장하지는 않지만 이를 통해 관리 컨트롤러와 UEFI의 펌웨어 수준을 완벽하게 제어할 수 있습니다. 그러나 두 파티션에 대한 관리 컨트롤러와 UEFI 펌웨어를 수동으로 업데이트해야 합니다.

  펌웨어 준수 정책을 사용하여 각 장치에 적용할 업데이트를 판별합니다. 펌웨어 준수 정책에 대한 자세한 정보는 펌웨어 준수 정책 생성 및 할당의 내용을 참조하십시오.

  참고: 관리 컨트롤러 및 UEFI가 백업 펌웨어를 기본 펌웨어와 자동으로 동기화하도록 구성된 경우 XClarity Administrator가 백업 뱅크를 업데이트할 필요가 없습니다. 이 경우 서버에 업데이트를 적용할 때 백업 뱅크 업데이트를 지우거나 펌웨어 준수 정책에서 백업 뱅크를 제거할 수 있습니다.

- **관리 컨트롤러를 재설정하는 경우의 VMware vSphere ESXi 시스템 실패(보라색 호스트 진단 화면) 가능성**

  서버에서 VMware vSphere ESXi를 실행하는 경우 서버에서 펌웨어를 업데이트하기 전에 다음 최소 VMware ESXi 수준이 설치되어 있는지 확인하십시오.

  - VMware vSphere ESXi 5.0을 실행하는 경우 최소 수준 5.0u2(update 2)를 설치하십시오.
  - VMware vSphere ESXi 5.1을 실행하는 경우 최소 수준 5.1u1(update 1)을 설치하십시오.

  해당 최소 수준을 설치하지 않으면 관리 컨트롤러 펌웨어가 적용되고 활성화되는 등 관리 컨트롤러가 재설정될 때마다 VMware vSphere ESXi 시스템 실패(보라색 호스트 진단 화면)가 발생할 수 있습니다.

  참고: 이 문제는 ESXi v5.5에는 영향을 미치지 않습니다.

ThinkSystem 장치 고려 사항

- **20A, 이전의 XCC 펌웨어 버전을 실행하는 ThinkSystem SE350 서버의 경우, 베이스보드 관리 컨트롤러에 KCS를 통한 IPMI 액세스를 수동으로 사용 설정해야 관리 컨트롤러가 XClarity Administrator과(와) 통신할 수 있습니다.**

  ThinkSystem SE350 서버의 경우, KCS를 통한 IPMI가 기본적으로 비활성화되어 있습니다. XCC 펌웨어 버전 20A 이상을 실행하는 ThinkSystem SE350 서버의 경우, 펌웨어를 업데이트하는 동안 XClarity Administrator에서 자동으로 KCS를 통한 IPMI를 사용 설정한 후 펌웨어 업데이트가 완료되면 사용 중지합니다. 그러나 20A 이전의 XCC 펌웨어 버전을 실행하는 ThinkSystem SE350 서버의 경우, **BMC 구성 → 보안 → KCS를 통한 IPMI 액세스**를 클릭하여 Lenovo XClarity Controller 사용자 인터페이스에서 이 옵션을 수동으로 활성화해야 합니다.

- ThinkSystem SR635 및 SR655 서버의 경우 다음 제한 사항이 적용됩니다.
  - 즉시 활성화만 지원됩니다. 지연 활성화 및 우선 활성화는 지원되지 않습니다.
  - XClarity Administrator v3.1.1 이상에서는 번들 업데이트 기능을 사용하여 베이스보드 관리 컨트롤러, UEFI, 디스크 드라이브 및 IO 옵션을 포함한 ThinkSystem SR635 및 SR655 서버의 모든 구성 요소를 업데이트할 수 있습니다.

    주의: 업데이트 프로세스를 시작하기 전에 선택한 장치의 전원이 꺼집니다. 실행 중인 워크로드가 중지되었는지 혹은 가상화된 환경에서 작업 중인 경우 해당 작업이 다른 서버로 이동되었는지 확인하십시오. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.

    참고:
    - 번들 펌웨어 업데이트 적용은 ThinkSystem SR635 및 SR655 서버에만 지원됩니다.
    - 번들 펌웨어 업데이트 적용은 IPv4 주소에만 지원됩니다. IPv6 주소는 지원되지 않습니다.
    - 전체 인벤토리 정보를 검색하려면 각 대상 장치가 한 번 이상 OS로 부팅되었어야 합니다.
    - 번들 업데이트 기능을 사용하려면 베이스보드 관리 컨트롤러 펌웨어 v2.94 이상이 필요합니다.
    - 리포지토리 팩의 펌웨어 업데이트 또는 개별 펌웨어 업데이트만 사용됩니다. UpdateXpress System Packs (UXSPs)는 지원되지 않습니다.
    - 다운로드된 펌웨어 업데이트만 적용됩니다. 제품 카탈로그를 새로 고치고 적합한 펌웨어 업데이트를 다운로드하십시오(제품 카탈로그 새로 고침 및 펌웨어 업데이트 다운로드 중 참조).

      참고: XClarity Administrator가 처음 설치되면 제품 카탈로그와 리포지토리가 비어 있습니다.
    - 준수 검사는 ThinkSystem SR635 및 SR655 서버의 베이스보드 관리 컨트롤러와 UEFI에만 지원됩니다. 그러나 XClarity Administrator에서는 사용 가능한 모든 하드웨어 구성 요소에 대해 펌웨어 업데이트 적용을 시도합니다.
    - 업데이트는 할당된 펌웨어 준수 정책에 따라 적용됩니다. 구성 요소의 하위 집합은 업데이트할 수 없습니다.
    - Lenovo XClarity Provisioning Manager(LXPM), LXPM Windows 드라이버 또는 LXPM Linux 드라이버용 펌웨어 업데이트를 ThinkSystem SR635 및 SR655 서버에 적용하려면 XClarity Administrator v3.2 이상이 필요합니다.
    - 현재 설치된 버전이 할당된 준수 정책보다 높으면 베이스보드 관리 컨트롤러 및 UEFI 업데이트를 건너뜁니다.
    - 펌웨어 준수 정책을 작성하여 펌웨어 업데이트를 적용할 장치에 할당해야 합니다. 자세한 정보는 펌웨어 준수 정책 생성 및 할당의 내용을 참조하십시오.
    - 업데이트 프로세스를 시작하기 전에 선택한 장치의 전원이 꺼집니다. 실행 중인 워크로드가 중지되었는지 혹은 가상화된 환경에서 작업 중인 경우 해당 작업이 다른 서버로 이동되었는지 확인하십시오.

    기존 업데이트 기능을 사용하여 베이스보드 관리 컨트롤러 및 UEFI에만 펌웨어 업데이트를 적용할 수도 있습니다.

  - XClarity Administrator v3.0:
    - 펌웨어를 20A에서 20B 또는 20C로 업데이트하면 관리 데이터가 올바르게 업데이트되지 않습니다. 이 문제를 해결하려면 장치를 관리 해제한 다음 다시 관리하도록 설정하거나 XClarity Administrator를 다시 시작하십시오.
    - 펌웨어 업데이트 다운그레이드는 지원되지 않습니다.
- **DHCPv6 또는 정적으로 할당된 IPv6 주소를 사용하는 ThinkSystem 서버에서는 펌웨어 업데이트가 지원되지 않습니다.**

  ThinkSystem 서버에서 IPv6 주소 지정을 사용하는 경우 펌웨어 업데이트는 IPv6 LLA(Link-Local Address) 및 상태 비저장 주소에서만 지원됩니다.
- **버전 20D로 펌웨어를 업데이트하는 경우 UEFI와 XCC를 함께 업데이트해야 합니다.**

  버전 20D의 경우 UEFI 및 Lenovo XClarity Controller(XCC)를 함께 업데이트해야 합니다. XCC 또는 UEFI 중 하나만 업데이트하면 문제가 발생합니다.

Flex System 장치 고려 사항

- **업데이트할 Flex 스위치의 전원이 켜져 있어야 합니다.**
- **Flex System 1.3.2 이전의 관리 컨트롤러 펌웨어 수준인 컴퓨팅 노드를 업데이트하는 경우 즉시 활성화를 선택하십시오.**

  Flex System 1.3.2, 2사분기 라이프사이클 릴리스를 컴퓨팅 노드에 적용하는 경우 컴퓨팅 노드를 업데이트하려면 *즉시 활성화*를 선택해야 합니다. 즉시 활성화는 업데이트 프로세스 중에 컴퓨팅 노드를 강제로 다시 시작합니다.
- **Flex 스위치는 XClarity Administrator에서 도달 가능한 IP 주소로 구성되어야 합니다.**

  XClarity Administrator가 펌웨어 업데이트를 다운로드하고 적용할 수 있도록 대상 Flex 스위치에 XClarity Administrator와 통신할 수 있는 IP 주소가 할당되어야 합니다.
- **확장 가능한 복합체(예, x480 X6 및 x880 X6 노드)에 대한 업데이트 지원.**

  확장 가능한 노드(예, Flex System x480 X6 및 x880 X6 계산 노드)에서의 업데이트 지원은 컴플렉스가 *단일 파티션*으로 구성되는 구성으로 제한됩니다. 단일 파티션에는 다중 노드 컴플렉스의 일부인 모든 컴퓨팅 노드가 포함됩니다. XClarity Administrator를 사용하여 여러 파티션으로 구성된 컴플렉스를 업데이트할 수 없습니다.

  확장 가능한 복합체(예, Flex System x480 X6 및 x880 X6 계산 노드)의 여러 서버가 포함된 파티션에 펌웨어 준수 정책을 할당한 경우 XClarity Administrator는 기본적으로 파티션의 각 서버에 대한 모든 관리 컨트롤러 및 UEFI에서 펌웨어를 업데이트합니다. 그러나 파티션에서 구성 요소 서브세트를 선택한 경우 XClarity Administrator는 파티션의 선택한 구성 요소에서만 펌웨어를 업데이트합니다.
- **CMM2를 v1.30(1AON06C) 이상으로 업데이트하기 전에 Flex 스위치가 EHCM L3(Enhanced Configuration and Management Level 3 버전)을 실행 중이어야 합니다.**

  CMM2 및 Flex 스위치는 EHCM 프로토콜을 사용하여 통신합니다. 이 프로토콜은 XClarity Administrator에서 Flex 스위치를 업데이트하는 데 필요합니다. CMM2를 v1.30(1AON06C) 이상으로 업데이트하는 경우 XClarity Administrator는 Flex 스위치가 EHCM L3을 실행 중인지 확인하고, 그렇지 않은 경우 먼저 Flex 스위치를 EHCM-L3을 지원하는 버전으로 업데이트해야 한다는 경고와 함께 CMM 업데이트를 취소합니다. CMM 펌웨어를 업데이트할 때 **이미 호환되는 구성 요소 업데이트 시도**를 선택하여 이 유효성 검증을 덮어쓸 수 있습니다.

  주의: 현재 EHCM L3를 지원하는 Flex System EN6131 이더넷 스위치 및 IB6131 InfiniBand 스위치의 펌웨어 버전이 없습니다. 이는 CMM2를 펌웨어 v1.30(1AON06C) 이상으로 업데이트하면 더 이상 XClarity Administrator를 사용하여 해당 스위치를 업데이트할 수 없음을 의미합니다. 임시 해결책은 섀시의 관리 컨트롤러 웹 인터페이스 또는 명령줄 인터페이스를 사용하여 스위치를 업데이트하는 것입니다.

Flex System 스위치	버전	릴리스 날짜
CN4093	7.8.4.0	2014년 6월
EN4023	6.0.0	2015년 4월
EN4093	7.8.4.0	2014년 6월
EN4093R	7.8.4.0	2014년 6월
EN6132	사용할 수 없음	사용할 수 없음
FC3171	9.1.3.02.00	2014년 6월
FC5022	7.4.0b1	2016년 3월
IB6132	사용할 수 없음	사용할 수 없음
SI4091	7.8.4.0	2014년 6월
SI4093	7.8.4.0	2014년 6월

참고: EN2092 1-Gb 이더넷 확장 가능 스위치에는 EHCM L3가 필요하지 않으며 이 제한사항도 없습니다.

저장 장치 고려사항

- **ThinkSystem DM 스토리지 장치 고려 사항**

  ThinkSystem DM 스토리지 장치의 펌웨어를 업데이트하려면 장치에서 v9.7 이상을 실행 중이어야 합니다.

  다운그레이드는 부 버전에만 지원됩니다. 예를 들어 9.7P11을 9.7P9로 다운그레이드할 수 있지만, 9.8을 9.7로 다운그레이드할 수는 없습니다.

  ThinkSystem DM 시리즈 스토리지 장치의 펌웨어를 다운로드하려면 다음을 따르십시오.

  - 하나 이상의 ThinkSystem DM 시리즈 스토리지 장치가 XClarity Administrator에서 관리되어야 합니다.
  - 각 ThinkSystem DM 시리즈 스토리지 장치가 하드웨어 서비스 및 지원을 받을 수 있어야 합니다.
  - 펌웨어 업데이트: 리포지토리 페이지에서 ThinkSystem DM 시리즈 스토리지 장치가 있는 국가를 지정해야 합니다. 다음 국가에서는 장치에 암호화된 펌웨어만 다운로드할 수 있습니다. 아르메니아, 벨라루스, 중국, 쿠바, 이란, 카자흐스탄, 키르기스스탄, 북한, 러시아, 수단, 시리아

- **디스크 드라이브는 JBOD, 온라인, 준비 또는 구성되지 않음(양호) 상태여야 합니다.**

  디스크 드라이브에서 펌웨어를 업데이트하려면 RAID 상태가 JBOD, 온라인, 준비 또는 구성되지 않음(양호) 상태여야 합니다. 다른 상태는 지원되지 않습니다. 디스크 드라이브의 RAID 상태를 판별하려면 장치의 인벤토리 페이지로 이동하여 **드라이브** 섹션을 확장하고 디스크 드라이브의 **RAID 상태** 열을 확인하십시오(관리 서버의 세부 정보 보기 참조).

- **펌웨어 버전이 디스크 드라이브와 SSD를 감지할 수 없습니다.**

  XClarity Administrator는 설치된 펌웨어 버전만 감지하고 MegaRAID 또는 NVME 어댑터에 연결된 디스크 드라이브 및 SSD(solid-state drive)에 대한 컴플라이언스 검사를 수행합니다. 설치된 다른 드라이브에 지원되지 않는 펌웨어 수준이 있거나 드라이브가 펌웨어 버전 보고를 지원하지 않을 수 있습니다. 그러나 펌웨어 업데이트는 선택한 경우 해당 드라이브에 적용됩니다.

- **NVMe 펌웨어는 대상 구성 요소로 식별되지 않아도 적용됩니다.**

  적용/활성화 페이지에서 SSD(solid state drive)에 대한 NVMe 펌웨어 버전이 나열됩니다. 검색된 NVMe 장치에 대해 대상 펌웨어 업데이트가 식별되지 않는 경우 대상 시스템을 업데이트하려고 시도하면 경고 메시지가 표시됩니다. 그러나 대상 구성 요소에서 식별되지 않는 경우에도 HDD/SSD 업데이트가 적용되므로 NVMe 펌웨어가 여전히 업데이트됩니다.

- **XClarity Administrator에서 ServeRAID M5115 PSoC3 업데이트 패키지를 적용하려면 68의 최소 설치 수준이 필요합니다.**

68 이전 버전에서의 ServeRAID M5115 PSoC3(Programmable System-on-Chip) 업데이트는 제어된 방식으로 수행되어야 합니다.

팁: CMM 웹 인터페이스에 로그인하고 대상 컴퓨팅 노드의 **펌웨어** 탭을 선택하여 ServeRAID M5115 PSoC3의 코드 버전을 볼 수 있습니다. 그런 다음 ServeRAID M5115 어댑터의 확장 카드를 선택하십시오. PSoc3 코드 버전은 GENERIC 펌웨어 유형입니다.

68 이전 버전이 설치된 경우 XClarity Administrator를 사용하여 업데이트할 수 없습니다. 대신 CMM(Chassis Management Module) 웹 인터페이스 또는 명령줄 인터페이스(CLI)에서 다음 단계를 수행해야 합니다.

- **CMM 웹 인터페이스를 사용하는 경우:**
  1. CMM(Chassis Management Module) 웹 인터페이스에 로그인하십시오.
  2. 기본 메뉴에서 **서비스 및 지원 → 고급**을 클릭하십시오.
  3. **서비스 재설정** 탭을 클릭하십시오.
  4. 해당 라디오 버튼을 클릭하여 적합한 컴퓨팅 노드를 선택하십시오.
  5. **재설정** 풀 다운 버튼에서 **가상 재배치**를 클릭하십시오.
  6. **확인**을 클릭하여 설정을 확인하십시오.
- **CMM CLI를 사용하는 경우**:
  - CMM SSH(Secure Shell) 인터페이스에 로그인하십시오.
  - 다음 명령을 입력하여 가상 재배치를 수행하십시오.
    ```
    'service -vr -T blade[x]
    ```
    여기서 *x*는 재배치할 컴퓨팅 노드의 베이 번호입니다.

시스템 전원이 다시 켜지면 운영 체제를 부팅하고 추출된 임베디드 업데이트 패키지를 사용하여 ServeRAID M5115 PSoC3를 업데이트하십시오. 다음 단계를 완료하여 임베디드 패키지를 추출하십시오.

- **Microsoft Windows를 사용하는 경우:**

  업데이트 패키지(lnvgy_fw_psoc3_m5115-70_windows_32-64.exe)를 열어서 하드 드라이브로 추출을 선택하십시오. 그런 다음 임베디드 패키지를 추출할 경로를 선택하십시오.
- **Linux를 사용하는 경우:**

  다음 명령을 실행하십시오.

  ```
  lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x
  ```

  여기서 *x*는 임베디드 패키지를 추출할 위치입니다.

펌웨어 업데이트 리포지토리 관리

*펌웨어 업데이트 리포지토리*에는 사용 가능한 업데이트 카탈로그와 관리되는 장치에 적용할 수 있는 업데이트 패키지가 포함되어 있습니다.

이 작업 정보

*카탈로그*에는 XClarity Administrator에서 지원하는 모든 장치에 현재 사용할 수 있는 펌웨어 업데이트에 대한 정보가 있습니다. 카탈로그는 펌웨어 업데이트를 장치 유형별로 구성합니다. 카탈로그를 새로 고치면 XClarity Administrator가 Lenovo 웹 사이트에서 사용 가능한 최신 펌웨어 업데이트에 대한 정보를 검색하고(메타데이터 .xml 또는 .json 파일 및 readme .txt 파일 포함) 이 정보를 펌웨어 업데이트 리포지토리에 저장합니다. 페이로드 파일(.exe)이 다운로드되지 않았습니다. 카탈로그 새로 고침에 대한 자세한 정보는 제품 카탈로그 새로 고침의 내용을 참조하십시오.

새 펌웨어 업데이트가 사용 가능한 경우 관리 장치에서 해당 펌웨어를 업데이트하려면 먼저 업데이트 패키지를 다운로드해야 합니다. 카탈로그를 새로 고쳐도 업데이트 패키지를 자동으로 다운로드하지는 않습니

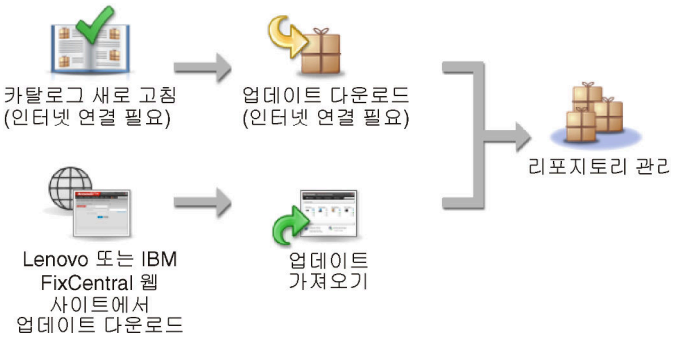
다. 펌웨어 업데이트 리포지토리 페이지의 **제품 카탈로그** 테이블은 다운로드된 업데이트 패키지와 다운로드할 수 있는 업데이트 패키지를 식별합니다.

몇 가지 방법으로 펌웨어 업데이트를 다운로드할 수 있습니다.

- **펌웨어 업데이트 리포지토리 팩**. 레포지트리 팩에는 지원되는 모든 장치 및 새로 고친 기본 펌웨어 준수 정책이 포함되어 있습니다. 이러한 리포지토리 팩을 가져온 다음 관리 서버 업데이트 페이지에서 적용합니다.
- UpdateXpress System Pack(UXSP). UXSP에는 운영 체제별로 정리된 최신의 사용 가능한 펌웨어 및 장치 드라이버 업데이트가 포함되어 있습니다. 펌웨어 업데이트: 리포지토리 페이지에서 UXSP를 다운로드하면 펌웨어 업데이트가 다운로드되며 리포지토리에 저장됩니다. 장치 드라이버 업데이트가 제외됩니다.

  참고: XCC2가 있는 서버의 경우 이러한 팩을 펌웨어 *번들*이라고 합니다.
- **개별 펌웨어 업데이트 적용**. 카탈로그에 나열된 버전을 기반으로 한 번에 개별 펌웨어 업데이트 패키지를 다운로드할 수 있습니다.

카탈로그를 새로 고치고 펌웨어 업데이트를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. 인터넷에 연결되어 있지 않은 경우 웹 브라우저를 사용하여 XClarity Administrator 호스트에 대한 네트워크 액세스 권한이 있는 워크스테이션에 파일을 수동으로 다운로드한 다음 파일을 펌웨어 업데이트 리포지토리로 가져올 수 있습니다.



펌웨어 업데이트를 XClarity Administrator(으)로 수동으로 가져올 때 필수 파일인 페이로드(이미지 및 MIB), 메타데이터, 변경 기록 및 readme 파일을 포함해야 합니다. 예를 들어, 다음과 같습니다.

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

주의:

- 이러한 필수 파일만 가져오십시오. 펌웨어 다운로드 웹 사이트에 있는 다른 파일은 가져오지 마십시오.
- 업데이트 패키지에 XML 파일이 없는 경우 업데이트를 가져올 수 없습니다.
- 업데이트와 연결된 모든 필수 파일이 포함되지 않은 경우 리포지토리에서는 업데이트가 다운로드되지 않았음을 표시하고, 이는 가져오기가 부분적으로 수행됨을 의미합니다. 그런 다음 해당 파일을 선택하고 가져와서 누락된 파일을 가져올 수 있습니다.
- 코어 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 pDSA)는 운영 체제에 독립적입니다. RHEL 6 또는 SLES 11 운영 체제의 펌웨어 업데이트 패키지를 사용하여 컴퓨팅 노드와 랙 서버를 업데이트합니다. 관리되는 서버에 사용할 펌웨어 업데이트 패키지에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

펌웨어 업데이트를 리포지토리에 다운로드하면 각 업데이트에 대한 정보가 제공되며, 여기에는 릴리스 날짜, 크기, 정책 사용 및 심각도 등이 포함되어 있습니다. 심각도는 업데이트 적용에 대한 영향과 필요를 표시하며 환경이 영향을 받는 정도를 평가하는 데 도움을 줍니다.

- **초기 릴리스**. 이는 펌웨어의 첫 번째 릴리스입니다.
- **위험**. 펌웨어 릴리스에 데이터 손상, 보안 또는 안정성 문제를 위한 긴급한 수정사항이 포함되어 있습니다.
- **제안됨**. 펌웨어 릴리스에 발생하기 쉬운 문제에 대한 중요한 수정 사항이 포함되어 있습니다.
- **중요하지 않음**. 펌웨어 릴리스에 사소한 수정 사항, 성능 개선 사항 및 텍스트 변경 사항이 포함되어 있습니다.

참고:

- 심각도는 이전에 릴리스된 버전의 업데이트와 관련됩니다. 예를 들어 설치된 펌웨어가 v1.01이고 업데이트 v1.02가 위험 상태이며 업데이트 v1.03이 권장 상태인 경우 설치가 누적되므로 업데이트 1.02부터 1.03까지는 권장되지만 업데이트 v1.01부터 v1.03까지는 위험 상태입니다(v1.03이 v1.02 위험 문제를 포함함).
- 특정 시스템 유형 또는 운영 체제에만 위험하거나 권장되는 특수한 상황이 발생할 수 있습니다. 추가 정보는 릴리스 정보를 참조하십시오.

절차

제품 카탈로그에서 사용 가능한 펌웨어 업데이트를 보려면 다음 단계를 완료하십시오.

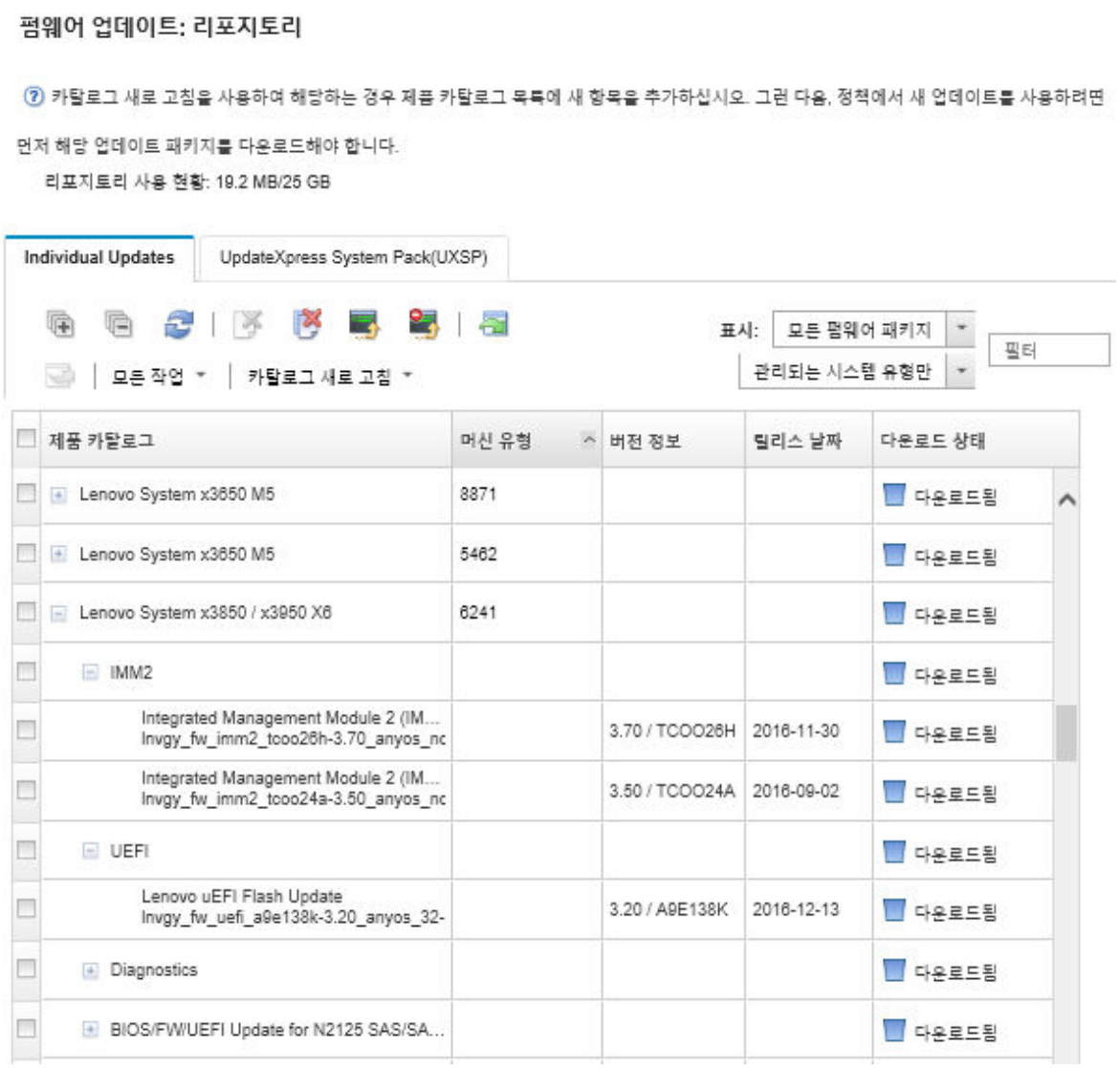
단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 리포지토리**를 클릭하십시오. 장치 유형별로 구성된 사용 가능한 펌웨어 업데이트 패키지 목록이 있는 펌웨어 업데이트 리포지토리 페이지가 표시됩니다.

단계 2. **개별 업데이트** 탭을 클릭하여 사용 가능한 펌웨어 업데이트 패키지에 대한 정보를 보거나 **UpdateXpress System Pack(UXSP)** 탭을 클릭하여 사용 가능한 UXSP에 대한 정보를 보십시오.

단계 3. 장치 및 장치 구성 요소를 확장하여 해당 장치에 대한 업데이트 패키지와 펌웨어 업데이트를 나열하십시오.

테이블 열을 정렬하고 **모두 확장** 아이콘( ) 및 **모두 축소** 아이콘( )을 클릭하여 특정 펌웨어 업데이트를 더 쉽게 찾을 수 있습니다. 또한 특정 사용 기간의 펌웨어 업데이트, 모든 서버 유형의 펌웨어 업데이트 또는 관리되는 서버 유형의 펌웨어 업데이트만 나열하기 위해 **표시** 메뉴에서 옵션을 선택하거나 **필터** 필드에 텍스트를 입력하여 표시되는 장치 및 펌웨어 업데이트 목록을 필터링할 수 있습니다. 특정 장치를 검색하면 해당 장치만 나열됩니다. 펌웨어 업데이트는 장치 이름 아래에 표시되지 않습니다.

참고: 서버의 경우 특정 업데이트 패키지는 서버 유형을 기반으로 하여 사용 가능합니다. 예를 들어 Flex System x240 계산 노드와 같은 서버를 확장하는 경우 해당 컴퓨팅 노드에 특정하게 사용 가능한 업데이트 패키지가 표시됩니다.



결과

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 카탈로그에서 현재 펌웨어 업데이트 정보로 페이지를 새로 고칩니다.
- **카탈로그 새로 고치기**를 클릭하여 사용 가능한 업데이트에 대한 최신 정보를 검색합니다.이 정보 검색을 완료하는 데 몇 분이 걸릴 수 있습니다. 자세한 정보는 제품 카탈로그 새로 고침의 내용을 참조하십시오.
- 제품 카탈로그에서 업데이트 패키지 또는 업데이트를 하나 이상 선택하고 **다운로드** 아이콘()을 클릭하여 펌웨어 업데이트를 리포지토리에 추가합니다. 펌웨어 업데이트를 다운로드하여 리포지토리에 추가하면 상태가 "다운로드됨"으로 변경됩니다.

  참고: XClarity Administrator 사용자 인터페이스를 통해 업데이트를 확보하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. 인터넷에 연결되지 않은 경우 이전에 다운로드한 업데이트를 가져올 수 있습니다.

  업데이트 다운로드에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.
- 업데이트를 하나 이상 선택하고 **가져오기** 아이콘()을 클릭하여 수동으로 다운로드한 펌웨어 업데이트를 XClarity Administrator에 대한 네트워크 액세스 권한이 있는 워크스테이션으로 가져오십시오. 업데이트 가져오기에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

- 업데이트를 하나 이상 선택하고 **다운로드 취소** 아이콘()을 클릭하여 현재 진행 중인 펌웨어 다운로드를 중지합니다.다운로드 취소는 진행 중인 *모든*펌웨어 다운로드를 취소합니다. 작업 로그에서 특정 펌웨어 다운로드의 자세한 진행 상황을 모니터링하고 중지할 수 있습니다(작업 모니터링 XClarity Administrator온라인 문서에서 .
- 리포지토리에서 업데이트 패키지 또는 개별 업데이트를 삭제합니다(펌웨어 업데이트 삭제 참조).
- 펌웨어 업데이트 리포지토리에 있는 펌웨어 업데이트를 로컬 시스템으로 내보냅니다(펌웨어 업데이트 내보내기 및 가져오기 참조).

펌웨어 업데이트에 원격 리포지토리 사용

기본적으로Lenovo XClarity Administrator은(는) 펌웨어 업데이트를 저장하기 위해 로컬(내부) 리포지토리를 사용합니다. SSHFS(SSH 파일 시스템)를 통해 탑재된 원격 공유를 원격 리포지토리로 사용하여 XClarity Administrator 로컬 리포지토리에 사용 가능한 디스크 공간을 확보할 수 있습니다. 이렇게 하면 원격 리포지토리에서 직접 펌웨어 업데이트 파일을 사용하여 장치의 펌웨어 준수를 유지 관리할 수 있습니다.

시작하기 전에

원격 공유에는 펌웨어 업데이트만 저장할 수 있습니다. Windows 장치 드라이버 및 XClarity Administrator 업데이트는 로컬 업데이트 리포지토리에만 저장할 수 있습니다.

포트 22의 SFTP 서비스가 원격 공유 서버에서 열려 있어야 합니다. 베이스보드 관리 컨트롤러가 이 포트에 액세스할 수 있어야 합니다.

원격 공유는 펌웨어 리포지토리로 사용되는 경우 SFTP 서버로 사용됩니다. SSHD 구성을 업데이트할 때 SFTP를 사용 중지하지 않아야 합니다.

이 작업 정보

펌웨어 업데이트 리포지토리의 위치를 변경할 때 원래 리포지토리의 모든 펌웨어 업데이트를 새 리포지토리로 복사할 수 있습니다.

위치를 전환한 후에 원본 리포지토리의 펌웨어 업데이트 파일이 자동으로 정리되지는 *않습니다*.

XClarity Administrator에 원격 리포지토리에 대한 읽기-쓰기 권한이 있는 경우 로컬 리포지토리를 사용할 때와 동일하게 작동합니다. 그러나 XClarity Administrator에 읽기 전용 권한만 있는 경우 카탈로그를 새로 고치거나 리포지토리에 업데이트를 다운로드하고 가져올 수 없습니다.

동일한 원격 리포지토리를 여러 XClarity Administrator 인스턴스에서 공유할 수 없지만, 하나의 XClarity Administrator 인스턴스에서 리포지토리가 변경되어도 다른 XClarity Administrator 인스턴스에 자동으로 알리지 않습니다. 최신 세부 정보를 보려면 리포지토리를 새로 고쳐야 합니다. 리포지토리를 새로 고치려면 펌웨어 업데이트: 리포지토리 페이지에서 **모든 작업 → 리포지토리 새로 고침**을 클릭하십시오.

참고: 펌웨어 업데이트 리포지토리가 여러 XClarity Administrator 인스턴스에서 사용되는 원격 공유에 있는 경우 펌웨어 업데이트 및 UXSP를 삭제할 때 주의하십시오.

절차

원격 펌웨어 업데이트 리포지토리를 사용하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator에 원격 공유를 추가합니다(원격 공유 관리 참고).

단계 2. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하십시오. 펌웨어 업데이트 리포지토리 페이지가 표시됩니다.

단계 3. **모든 작업 → 리포지토리 위치 바꾸기**를 클릭하여 리포지토리 위치 바꾸기 대화 상자를 표시합니다.

단계 4. **리포지토리 위치** 드롭 다운 목록에서 방금 생성한 원격 공유를 선택합니다.

단계 5. 필요한 경우 **현재 리포지토리 정리**를 선택하여 현재 저장소 위치에서 펌웨어 업데이트 파일을 삭제합니다.

단계 6. 필요한 경우 **현재 리포지토리에서 새 리포지토리로 업데이트 패키지 복사**를 선택하여 리포지토리 위치를 전환하기 전에 펌웨어 업데이트 파일을 새 리포지토리 위치에 복사합니다.

기본적으로 새 위치에 있는 펌웨어 업데이트 파일은 복사되지 않습니다(건너뜀). 필요한 경우 **덮어쓰기 규칙** 드롭 다운 목록을 사용하여 기존의 모든 파일을 덮어쓰거나 크기나 수정 날짜가 다른 기존 파일만 덮어쓰도록 선택할 수 있습니다.

단계 7. **확인**을 누르십시오.

펌웨어 업데이트 패키지를 새 리포지토리에 복사하기 위한 작업이 만들어집니다. XClarity Administrator 메뉴 표시줄에서 **모니터링 → 작업**을 클릭하여 작업 진행 상태를 모니터링할 수 있습니다.

제품 카탈로그 새로 고침

제품 카탈로그에는 섀시, 서버 및 Flex 스위치를 포함하여 Lenovo XClarity Administrator에서 지원하는 모든 장치에 사용 가능한 모든 펌웨어 업데이트에 대한 정보가 있습니다.

시작하기 전에

제품 카탈로그를 새로 고치려면 인터넷에 연결되어 있어야 합니다.

카탈로그 새로 고침을 완료하려면 몇 분 정도가 걸릴 수 있습니다.

이 작업 정보

카탈로그를 새로 고치면 XClarity Administrator가 Lenovo XClarity 지원 웹 사이트에서 사용 가능한 최신 펌웨어 업데이트에 대한 정보를 검색하고 해당 정보를 펌웨어 업데이트 리포지토리에 저장합니다.

카탈로그를 새로 고치면 사용 가능한 펌웨어 업데이트에 대한 정보만 리포지토리에 추가합니다. 업데이트 패키지는 다운로드하지 않습니다. 업데이트를 설치에 적용하려면 펌웨어 업데이트를 다운로드해야 합니다. 업데이트 다운로드에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

절차

제품 카탈로그를 새로 고치려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하십시오. 펌웨어 업데이트 리포지토리 페이지가 표시됩니다.

단계 2. **개별 업데이트** 탭을 클릭하여 개별 펌웨어 업데이트 패키지에 대한 정보를 검색하거나 UpdateXpress System Pack(UXSP) 탭을 클릭하여 UXSP에 대한 정보를 검색하십시오.

단계 3. **카탈로그 새로 고침**을 클릭하고 다음 옵션 중 하나를 클릭하여 사용 가능한 최신 펌웨어 업데이트에 대한 정보를 얻으십시오.

- **선택 항목 새로 고침 - 최신 항목 한정**. 선택한 장치에만 사용 가능한 최신 버전의 펌웨어 업데이트 정보를 검색합니다.
- **모두 새로 고침 - 최신 항목 한정**. 지원되는 모든 장치에 대한 최신 버전의 모든 펌웨어 업데이트 정보를 검색합니다.
- **선택 항목 새로 고침**. 선택한 장치에만 사용 가능한 모든 버전의 펌웨어 업데이트 정보를 검색합니다.
- **모두 새로 고침**. 지원되는 모든 장치에 대한 모든 버전의 모든 펌웨어 업데이트 정보를 검색합니다.

팁: 모든 작업 ➡ 새로 고침 및 모든 관리되는 장치에 대한 최신 다운로드 또는 **모든 작업 ➡ 새로 고침 및 선택한 장치에 대한 최신 다운로드**를 클릭하여 한 번에 제품 카탈로그를 새로 고치고 최신 펌웨어를 다운로드할 수 있습니다.

펌웨어 업데이트 다운로드 중

인터넷 액세스에 따라 펌웨어 업데이트 리포지토리에서 펌웨어 업데이트를 다운로드하거나 가져올 수 있습니다. 관리 장치에서 펌웨어를 업데이트하려면 먼저 펌웨어 업데이트 리포지토리에서 펌웨어 업데이트가 사용 가능해야 합니다.

시작하기 전에

펌웨어를 다운로드하기 전에 Lenovo XClarity Administrator에서 필요로 하는 모든 포트 및 인터넷 액세스가 사용 가능한지 확인하십시오. 포트에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성 및 방화벽 및 프록시 서버의 내용을 참조하십시오.

펌웨어 업데이트 리포지토리에 장치 유형이 나열되지 않는 경우 해당 장치 유형에 대한 개별 펌웨어 업데이트를 다운로드하거나 가져오려면 먼저 해당 유형의 자치를 관리해야 합니다.

중요:

- XClarity Administrator v1.1.1 이전의 경우, Lenovo 데이터 센터 지원 웹 사이트에서 Lenovo Hardware의 펌웨어 업데이트를 수동으로 다운로드하고 가져와야 합니다.
- XClarity Administrator은(는) Lenovo 웹 사이트에서 펌웨어 업데이트 리포지토리로 RackSwitch 스위치 및 Lenovo DE, DX, SS 시리즈 스토리지 장치의 업데이트를 다운로드할 수 없습니다. 대신 Lenovo 웹 사이트에서 XClarity Administrator 호스트에 대한 네트워크 액세스 권한이 있는 워크스테이션으로 이러한 업데이트를 수동으로 다운로드하고 가져오거나 사용 가능한 모든 펌웨어 업데이트가 있는 *펌웨어 업데이트 리포지토리 팩*을 다운로드하여 적용해야 합니다.
- Internet Explorer 및 Microsoft Edge 웹 브라우저에는 4GB의 업로드 제한이 있습니다. 가져오는 파일의 크기가 4GB보다 큰 경우, 다른 웹 브라우저(예, Chrome 또는 Firefox).
- ThinkSystem DM 시리즈 스토리지 장치의 펌웨어를 다운로드하려면 다음을 따르십시오.
  - 하나 이상의 ThinkSystem DM 시리즈 스토리지 장치가 XClarity Administrator에서 관리되어야 합니다.
  - 각 ThinkSystem DM 시리즈 스토리지 장치가 하드웨어 서비스 및 지원을 받을 수 있어야 합니다.
  - 펌웨어 업데이트: 리포지토리 페이지에서 ThinkSystem DM 시리즈 스토리지 장치가 있는 국가를 지정해야 합니다. 다음 국가에서는 장치에 암호화된 펌웨어만 다운로드할 수 있습니다. 아르메니아, 벨라루스, 중국, 쿠바, 이란, 카자흐스탄, 키르기스스탄, 북한, 러시아, 수단, 시리아

이 작업 정보

몇 가지 방법으로 펌웨어 업데이트를 다운로드할 수 있습니다.

- **펌웨어 업데이트 리포지토리 팩**

  펌웨어 업데이트 리포지토리 팩은 지원되는 대부분의 장치 및 새로 고친 기본 펌웨어 준수 정책에 대해 XClarity Administrator 릴리스와 동시에 사용할 수 있는 최신 펌웨어 모음입니다. 이러한 리포지토리 팩을 가져온 다음 관리 서버 업데이트 페이지에서 적용합니다. 펌웨어 업데이트 리포지토리 팩을 적용하는 경우 팩의 각 업데이트 패키지가 펌웨어 업데이트 리포지토리에 추가되고 모든 관리 가능한 장치에 대해 기본 펌웨어 준수 정책이 자동으로 작성됩니다. 미리 정의된 이 정책을 복사할 수는 있지만 변경할 수는 없습니다.

  다음 리포지토리 팩을 사용할 수 있습니다.

  - lnvgy_sw_lxca_cmmswitchrepo*x-x.x.x*_anyos_noarch. 모든 CMM 및 Flex System 스위치에 대한 펌웨어 업데이트가 있습니다.

  - lnvgy_sw_lxca_storagerackswitchrepo*x-x.x.x*_anyos_noarch. 모든 RackSwitch 스위치 및 Lenovo Storage 장치에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_systemxrepo*x-x.x.x*_anyos_noarch. 모든 Converged HX 시리즈, Flex System, NeXtScale 및 System x 서버에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_thinksystemrepo*x-x.x.x*_anyos_noarch. 모든 ThinkAgile 및 ThinkSystem 서버에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_thinksystemv2repo*x-x.x.x*_anyos_noarch. 모든 ThinkAgile 및 ThinkSystem V2 서버에 대한 펌웨어 업데이트가 있습니다.
  - lnvgy_sw_lxca_thinksystemv3repo*x-x.x.x*_anyos_noarch. 모든 ThinkAgile 및 ThinkSystem V3 서버에 대한 펌웨어 업데이트가 포함됩니다.

  펌웨어 업데이트 리포지토리 팩이 관리 서버 업데이트 페이지의 **다운로드 상태** 열에 있는 리포지토리에 저장되는지 여부를 판별할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

  - **다운로드됨**. 펌웨어 업데이트 리포지토리 팩이 리포지토리에 저장됩니다.
  - **다운로드되지 않음**. 펌웨어 업데이트 리포지토리 팩이 사용 가능하지만 리포지토리에 저장되지 않습니다.

- UpdateXpress System Pack(UXSP)

  참고: XCC2가 있는 서버의 경우 이러한 팩을 펌웨어 번들이라고 합니다. *번들*은 패키지 이름 및 미리 정의된 정책 이름에 사용됩니다.

  UXSP에는 운영 체제별로 정리된 최신의 사용 가능한 펌웨어 및 장치 드라이버 업데이트가 포함되어 있습니다. UXSP를 다운로드하는 경우 XClarity Administrator는 카탈로그에 나열된 버전을 기반으로 하여 UXSP를 다운로드하고 업데이트 패키지를 펌웨어 업데이트 리포지토리에 저장합니다. UXSP를 다운로드하면 UXSP의 각 펌웨어 업데이트가 펌웨어 업데이트 리포지토리에 추가되고 **개별 업데이트** 탭에 나열되며 관리 가능한 모든 장치에 대해 다음 이름을 사용하여 기본 펌웨어 준수 정책이 자동으로 생성됩니다. 미리 정의된 이 정책을 복사할 수는 있지만 변경할 수는 없습니다.
  - *{uxsp-version}-{date}-{server-short-name}*-UXSP (예: `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}*-bundle(예: `22a.0-kaj92va-SR650V3-bundle`)

  참고: 펌웨어 업데이트: 리포지토리 페이지에서 UXSP를 다운로드하거나 가져오면, 펌웨어 업데이트가 다운로드되어 리포지토리에 저장됩니다. 장치 드라이버 업데이트가 삭제됩니다. UXSP를 사용한 Windows 장치 드라이버 업데이트 다운로드 또는 가져오기에 대한 정보는 OS 장치 드라이버 리포지토리 관리의 내용을 참조하십시오.

  UXSP가 펌웨어 업데이트: 리포지토리 페이지의 **개별 업데이트**의 **다운로드 상태** 열에 있는 펌웨어 업데이트 리포지토리에 저장되는지 여부를 판단할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

  - **다운로드됨**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 리포지토리에 저장됩니다.
  - *x* / *y* **다운로드됨**. 업데이트 패키지의 펌웨어 업데이트 전체가 아닌 일부가 리포지토리에 저장됩니다. 괄호 안의 숫자는 사용 가능한 업데이트 수와 저장된 업데이트 수를 나타내며, 특정 장치 유형에 대한 업데이트는 없습니다.
  - **다운로드되지 않음**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 사용 가능하지만 리포지토리에 저장되지 않습니다.

- **개별 펌웨어 업데이트 적용**

  한 번에 개별 펌웨어 업데이트 패키지를 다운로드할 수 있습니다. 펌웨어 업데이트 패키지를 다운로드하는 경우 XClarity Administrator는 카탈로그에 나열된 버전을 기반으로 하여 업데이트를 다운로드하고 업데이트 패키지를 펌웨어 업데이트 리포지토리에 저장합니다. 그런 다음 각 관리 장치의 해당 업데이트 패키지를 사용하여 펌웨어 준수 정책을 작성할 수 있습니다.

  참고: 코어 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 pDSA)는 운영 체제에 독립적입니다. RHEL 6 또는 SLES 11 운영 체제의 펌웨어 업데이트 패키지를 사용하여 컴퓨팅 노드와 랙 서버를 업데이트

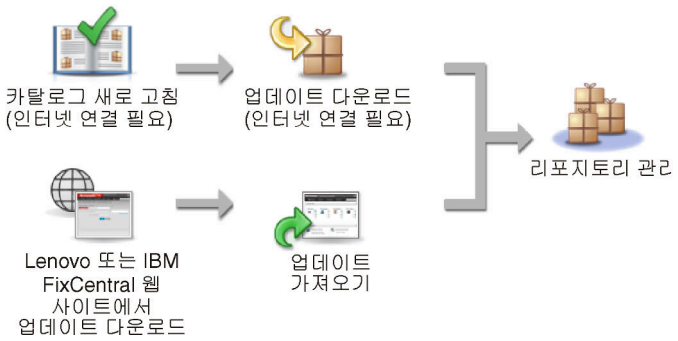
합니다. 관리되는 서버에 사용할 펌웨어 업데이트 패키지에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

특정 *펌웨어 업데이트*가 펌웨어 업데이트: 리포지토리 페이지에서 **개별 업데이트** 탭의 **다운로드 상태** 열에 있는 펌웨어 업데이트 리포지토리에 저장되는지 판별할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

- **다운로드됨**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 리포지토리에 저장됩니다.
- *x* / *y* **다운로드됨**. 업데이트 패키지의 펌웨어 업데이트 전체가 아닌 일부가 리포지토리에 저장됩니다. 괄호 안의 숫자는 사용 가능한 업데이트 수와 저장된 업데이트 수를 나타내며, 특정 장치 유형에 대한 업데이트는 없습니다.
- **다운로드되지 않음**. 전체 업데이트 패키지 또는 개별 펌웨어 업데이트가 사용 가능하지만 리포지토리에 저장되지 않습니다.

XClarity Administrator를 설치하거나 새 릴리스로 업데이트하는 경우 최신 리포지토리 팩을 다운로드하여 최신 펌웨어 업데이트가 있는지 확인하는 것이 좋습니다. 그런 다음 반복 작업을 예약하여 카탈로그를 새로 고쳐 마지막 리포지토리 팩 이후 웹에 게시된 개별 업데이트를 찾은 다음 한 번에 하나씩 해당 업데이트를 온라인에서 다운로드할 수 있습니다.

카탈로그를 새로 고치고 펌웨어 업데이트를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. 인터넷에 연결되어 있지 않은 경우 웹 브라우저를 사용하여 XClarity Administrator 호스트에 대한 네트워크 액세스 권한이 있는 워크스테이션에 파일을 수동으로 다운로드한 다음 파일을 펌웨어 업데이트 리포지토리로 가져올 수 있습니다.



펌웨어 업데이트를 XClarity Administrator(으)로 수동으로 가져올 때 필수 파일인 페이로드(이미지 및 MIB), 메타데이터, 변경 기록 및 readme 파일을 포함해야 합니다. 예를 들어, 다음과 같습니다.

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

참고: 코어 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 pDSA)는 운영 체제에 독립적입니다. RHEL 6 또는 SLES 11 운영 체제의 펌웨어 업데이트 패키지를 사용하여 컴퓨팅 노드와 랙 서버를 업데이트합니다.

리포지토리가 50%보다 많이 차면 페이지에 메시지가 표시됩니다. 리포지토리가 85%보다 많이 차면 페이지에 다른 메시지가 표시됩니다. 리포지토리에 사용되는 공간을 줄이려는 경우 사용되지 않는 이미지 파일과 정책을 제거할 수 있습니다. **프로비저닝 → 준수 정책**을 클릭하고 삭제할 정책을 하나 이상 선택한 다음 **작업 → 정책 및 펌웨어 패키지 삭제**를 클릭하여 사용되지 않는 펌웨어 준수 정책 및 연결된 펌웨어 패키지를 제거할 수 있습니다.

다음 테이블에서는 펌웨어 업데이트 리포지토리 팩, UXSPs 및 개별 펌웨어 업데이트 패키지를 획득하는 방법 간의 차이를 요약합니다.

업데이트 패키지	파일을 다운로드하고 가져오기 위한 UI 페이지	파일을 수동으로 다운로드하기 위한 웹 페이지	펌웨어 업데이트 리포지토리 새로 고침 여부	펌웨어 준수 정책 자동으로 새로 고침 여부
펌웨어 업데이트 리포지토리 팩	관리 서버 업데이트 페이지 **참고:** 리포지토리 팩을 가져와서 적용해야 합니다.	XClarity Administrator 다운로드 웹 페이지	예	예
UpdateXpress System Pack	펌웨어 업데이트: 리포지토리 페이지, UXSP(UpdateXpress System Pack) 탭	Lenovo XClarity Essentials UpdateXpress 웹 페이지	예	예
펌웨어 업데이트	펌웨어 업데이트: 리포지토리 페이지, **개별 업데이트** 탭	Lenovo 데이터 센터 지원 웹 사이트 **참고:** 다음 장치의 경우 Fix Central 웹 사이트의 내용을 참조하십시오. • Flex System x220 유형 2585, 7906 • Flex System x222 계산 노드 유형 2589, 7916 • Flex System x240 유형 7863, 8737, 8738, 8956 • Flex System x280 / x480 / x880 X6 유형 4259, 7903 • Flex System x440 유형 2584, 7917	예	아니요

절차

하나 이상의 펌웨어 업데이트를 다운로드하려면 다음 단계를 완료하십시오.

- 하나 이상의 *펌웨어 업데이트 리포지토리 팩*을 가져오려면 다음을 수행하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **관리 → 관리 서버 업데이트**를 클릭하여 관리 서버 업데이트 페이지를 표시하십시오.
  2. 최신 리포지토리 팩 다운로드:
     - XClarity Administrator가 인터넷에 연결된 경우:
       a. **카탈로그 새로 고침 → 모든 관리되는 항목 새로 고침 – 최신 항목 한정**을 클릭하여 최신 업데이트에 대한 정보를 검색하십시오. 새 관리 서버 업데이트 및 펌웨어 업데이트 리포지토리 팩이 "관리 서버 업데이트" 페이지의 테이블에 나열됩니다.

          리포지토리 새로 고침을 완료하려면 몇 분 정도가 걸릴 수 있습니다.

          참고: 리포지토리를 새로 고쳐도 페이로드 파일을 자동으로 다운로드하지는 않습니다. 메타데이터 및 readme 파일만 다운로드됩니다.

       b. 다운로드하려는 펌웨어 업데이트 리포지토리 팩을 선택하십시오.

          팁: 선택한 패키지의 **유형** 열에 "추가 팩"이 있는지 확인하십시오.

       c. **선택 항목 다운로드** 아이콘( )을 클릭하십시오. 다운로드가 완료되면 해당 소프트웨어 업데이트의 **다운로드 상태**가 "다운로드됨"으로 변경됩니다.

- XClarity Administrator가 인터넷에 연결되지 않은 경우:
  a. XClarity Administrator 다운로드 웹 페이지에서 XClarity Administrator 호스트에 대한 네트워크 연결이 있는 워크스테이션으로 펌웨어 업데이트 리포지토리 팩을 다운로드하십시오.
  b. 관리 서버 업데이트 페이지에서 **가져오기** 아이콘()을 클릭하십시오.
  c. **파일 선택**을 클릭하고 워크스테이션에서 펌웨어 업데이트 리포지토리 팩 위치를 찾아보십시오.
  d. 모든 패키지 파일을 선택하고 **열기**를 클릭하십시오.

     업데이트에 대한 이미지 또는 페이로드 파일(.zip, .bin, .uxz 또는 .tgz), 변경 기록 파일(.chg) 및 readme 파일(.txt)과 메타데이터 파일(.xml 또는 .json)을 가져와야 합니다. 선택되었지만 메타데이터 파일에 지정되지 않은 모든 파일이 삭제됩니다. 메타데이터 파일을 포함하지 않는 경우 업데이트를 가져올 수 없습니다.
  e. **가져오기**를 클릭하십시오.

     가져오기를 완료하면 펌웨어 업데이트 리포지토리 팩이 관리 서버 업데이트 페이지의 테이블에 나열되고 각 업데이트의 **다운로드 상태**가 "다운로드됨"이 됩니다.

3. 펌웨어 업데이트 리포지토리에 설치할 펌웨어 업데이트 리포지토리 팩을 선택하십시오.

   참고: 다운로드 상태가 "다운로드됨"이고 **유형**이 "패치"인지 확인하십시오.
4. **업데이트 수행** 아이콘()을 클릭하여 펌웨어 업데이트 패키지를 리포지토리에 추가하십시오.
5. 업데이트가 완료되고 XClarity Administrator가 다시 시작될 때까지 몇 분 정도 기다리십시오.
6. 웹 브라우저를 새로 고쳐서 업데이트가 완료되었는지 판별하십시오.

   업데이트가 완료되면 관리 서버 업데이트 페이지가 표시되고 **적용된 상태** 열이 "적용됨"으로 변경됩니다.
7. 웹 브라우저 캐시를 지우십시오.

- 하나 이상의 *UXSPs*를 다운로드하는 방법.
  1. XClarity Administrator 메뉴 표시줄에서, **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하여 펌웨어 업데이트 리포지토리 페이지를 표시하십시오.
  2. UpdateXpress System Pack(UXSP) 탭을 클릭하십시오.
  3. 다음과 같이 최신 UXSP를 다운로드하십시오.
     - XClarity Administrator가 인터넷에 연결된 경우:

       카탈로그를 새로 고치고 모든 관리되는 장치에 대한 최신 UXSP를 다운로드하려면 **모든 작업 → 새로 고침 및 모든 관리되는 장치에 대한 최신 다운로드**를 클릭하십시오.

       카탈로그를 새로 고치고 선택한 장치에 대한 최신 UXSP만 다운로드하려면 다음을 수행하십시오.
       a. 장치를 확장하여 사용 가능한 UXSP 목록을 표시하십시오.
       b. 다운로드할 하나 이상의 UXSP를 선택하십시오.
       c. **모든 작업 → 새로 고침 및 선택한 장치에 대한 최신 다운로드**를 클릭하십시오.

          다운로드가 완료되면 선택한 UXSP의 **다운로드 상태**가 "다운로드됨"으로 변경됩니다.
     - XClarity Administrator가 인터넷에 연결되지 않은 경우:
       a. Lenovo XClarity Essentials UpdateXpress 웹 페이지에서 XClarity Administrator 호스트에 대한 네트워크 연결이 있는 워크스테이션으로 UXSP를 다운로드하십시오.
       b. XClarity Administrator에서, **가져오기** 아이콘()을 클릭하십시오.
       c. **파일 선택**을 클릭하고 워크스테이션에서 UXSP 위치를 찾아보십시오.
       d. 모든 패키지 파일을 선택하고 **열기**를 클릭하십시오.

          업데이트에 대한 이미지 또는 페이로드 파일(.zip, .bin, .uxz 또는 .tgz), 변경 기록 파일(.chg) 및 readme 파일(.txt)과 메타데이터 파일(.xml 또는 .json)을 가져와야 합니다.

선택되었지만 메타데이터 파일에 지정되지 않은 모든 파일이 삭제됩니다. 메타데이터 파일을 포함하지 않는 경우 업데이트를 가져올 수 없습니다.

e. **가져오기**를 클릭하십시오.

가져오기를 완료하면 펌웨어 업데이트 리포지토리 팩이 관리 서버 업데이트 페이지의 테이블에 나열되고 각 업데이트의 다운로드 상태가 " "다운로드 완료"가 됩니다."

- 한 번에 각 *펌웨어 업데이트 패키지*를 다운로드하는 방법.
  1. XClarity Administrator 메뉴 표시줄에서, **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하여 펌웨어 업데이트 리포지토리 페이지를 표시하십시오.
  2. ThinkSystem DM 시리즈 스토리지 장치용 펌웨어를 다운로드하는 경우 스토리지 장치가 있는 국가를 선택하십시오.
  3. **개별 업데이트** 탭을 클릭합니다.
  4. 최신 개별 펌웨어 업데이트 다운로드.
     - XClarity Administrator가 인터넷에 연결된 경우:

       카탈로그를 새로 고치고 모든 관리되는 장치에 대한 최신 펌웨어를 다운로드하려면 **모든 작업 → 새로 고침 및 모든 관리되는 장치에 대한 최신 다운로드**를 클릭하십시오.

       카탈로그를 새로 고치고 선택한 장치에 대한 최신 펌웨어만 다운로드하려면 다음을 수행하십시오.

       a. 장치를 확장하여 사용 가능한 펌웨어 업데이트 목록을 표시하십시오.

       b. 다운로드할 하나 이상의 펌웨어 업데이트를 선택하십시오.

          팁: 업데이트 패키지는 여러 개의 펌웨어 업데이트로 구성할 수 있습니다. 펌웨어 업데이트를 다운로드하는 경우 전체 업데이트 패키지 또는 특정 패키지를 다운로드하도록 선택할 수 있습니다. 한 번에 여러 개의 패키지를 다운로드하도록 선택할 수도 있습니다.

       c. **모든 작업 → 새로 고침 및 선택한 장치에 대한 최신 다운로드**를 클릭하십시오.

          다운로드가 완료되면 선택한 펌웨어 업데이트의 **다운로드 상태**가 "다운로드됨"으로 변경됩니다.

     - XClarity Administrator가 인터넷에 연결되지 않은 경우:

       a. 펌웨어 업데이트 패키지를 Lenovo 데이터 센터 지원 웹 사이트에서 XClarity Administrator 호스트에 대한 네트워크 연결이 있는 워크스테이션에 다운로드하십시오.

          다음 서버의 경우 Fix Central 웹 사이트에서 SLES 11 운영 체제에 대한 펌웨어 업데이트를 다운로드하십시오.

          - Flex System x220 유형 2585, 7906
          - Flex System x222 계산 노드 유형 2589, 7916
          - Flex System x240 유형 7863, 8737, 8738, 8956
          - Flex System x280 / x480 / x880 X6 유형 4259, 7903
          - Flex System x440 유형 2584, 7917

          다른 모든 서버의 경우 Lenovo XClarity 지원 웹 사이트에서 RHEL 6 운영 체제에 대한 펌웨어 업데이트를 다운로드하십시오.

       b. XClarity Administrator에서, **가져오기** 아이콘()을 클릭하십시오.

       c. **파일 선택**을 클릭하고 워크스테이션에서 펌웨어 업데이트 위치를 찾아보십시오.

       d. 모든 패키지 파일을 선택하고 **열기**를 클릭하십시오.

          업데이트에 대한 이미지 또는 페이로드 파일(.zip, .bin, .uxz 또는 .tgz), 변경 기록 파일(.chg) 및 readme 파일(.txt)과 메타데이터 파일(.xml 또는 .json)을 가져와야 합니다. 선택되었지만 메타데이터 파일에 지정되지 않은 모든 파일이 삭제됩니다.

          주의:

- 이러한 필수 파일만 가져오십시오. 펌웨어 다운로드 웹 사이트에 있는 다른 파일은 가져오지 마십시오.
- 업데이트 패키지에 XML 파일이 없는 경우 업데이트를 가져올 수 없습니다.
- 업데이트와 연결된 모든 필수 파일이 포함되지 않은 경우 리포지토리에서는 업데이트가 다운로드되지 않았음을 표시하고, 이는 가져오기가 부분적으로 수행됨을 의미합니다. 그런 다음 해당 파일을 선택하고 가져와서 누락된 파일을 가져올 수 있습니다.
- 코어 펌웨어 업데이트(예, 관리 컨트롤러, UEFI 및 pDSA)는 운영 체제에 독립적입니다. RHEL 6 또는 SLES 11 운영 체제의 펌웨어 업데이트 패키지를 사용하여 컴퓨팅 노드와 랙 서버를 업데이트합니다. 관리되는 서버에 사용할 펌웨어 업데이트 패키지에 대한 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

e. **가져오기**를 클릭하십시오.

카탈로그를 새로 고치고 펌웨어를 다운로드하는 데 몇 분 정도 걸릴 수 있습니다. 업데이트가 다운로드되어 리포지토리에 저장되면 제품 카탈로그의 행이 강조표시되고 **다운로드 상태** 열이 "다운로드됨"으로 변경됩니다.

참고: 일부 스위치의 시스템 유형이 16진수로 표시될 수 있습니다.

완료한 후에

모든 **작업** → **전역 설정**을 클릭하여 펌웨어 리포지토리 페이지에서 업데이트 리포지토리(펌웨어, OS 장치 드라이버 및 관리 서버 업데이트 포함)의 최대 크기를 구성할 수 있습니다. 최소 크기는 50GB입니다. 최대 크기는 로컬 시스템의 디스크 공간 크기에 따라 다릅니다.

펌웨어 업데이트 내보내기 및 가져오기

리포지토리에 있는 개별 펌웨어 업데이트 및 UXSP(UpdateXpress System Pack)를 로컬 시스템으로 내보낼 수 있습니다.

이 작업 정보

리포지토리에 있는 펌웨어 업데이트만 내보낼 수 있습니다. 선택한 펌웨어 업데이트의 다운로드 상태가 "다운로드됨"인지 확인하십시오.

업데이트 이미지 또는 페이로드 파일(.zip, .bin, .uxz 또는 .tgz), 메타데이터 파일(.xml 또는 .json), 변경 기록 파일(.chg) 및 readme 파일(.txt) 등 펌웨어 업데이트와 관련된 모든 파일을 내보냅니다.

주의: 펌웨어 업데이트 파일의 이름을 변경하지 마십시오.

절차

- 펌웨어 업데이트를 내보내려면 다음을 수행하십시오.
  1. **개별 업데이트** 탭 또는 UpdateXpress System Pack(UXSP) 탭을 클릭하십시오.
  2. 하나 이상의 펌웨어 업데이트를 선택하십시오.
  3. **내보내기** 아이콘( )을 클릭하십시오.
- 펌웨어 업데이트를 가져오려면 다음을 수행하십시오.

  Lenovo XClarity Administrator에서 수동으로 내보낸 파일과 웹에서 수동으로 다운로드한 파일을 가져올 수 있습니다. 자세한 정보는 펌웨어 업데이트 다운로드 중의 내용을 참조하십시오.

펌웨어 업데이트 삭제

펌웨어 업데이트 리포지토리에서 펌웨어 업데이트 및 UpdateXpress System Pack(UXSP)을 삭제할 수 있습니다.

시작하기 전에

삭제할 펌웨어 업데이트가 포함된 펌웨어 준수 정책을 사용하는 모든 실행 중이거나 예약된 업데이트 작업이 완료되거나 취소되었는지 확인하십시오(작업 모니터링 참조).

업데이트를 삭제하기 전에 해당 업데이트가 펌웨어 준수 정책에서 사용 중이지 않은지 확인하십시오. 현재 하나 이상의 펌웨어 준수 정책에서 사용되는 펌웨어 업데이트 패키지는 삭제할 수 없습니다.

UXSP를 삭제하면 해당 UXSP에 대해 자동으로 생성된 펌웨어 준수 정책도 삭제됩니다.

참고: 펌웨어 업데이트 리포지토리가 여러 XClarity Administrator 인스턴스에서 사용되는 원격 공유인 경우 펌웨어 업데이트 및 UXSP를 삭제할 때 주의하십시오.

절차

리포지토리에서 하나 이상의 펌웨어 업데이트를 삭제하려면 다음 단계를 완료하십시오.

단계 1. 모든 관리되는 장치에서 삭제할 펌웨어 업데이트가 포함된 모든 펌웨어 준수 정책을 할당 해제하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **적용/활성화**를 클릭하십시오. 펌웨어 업데이트 적용/활성화 페이지가 표시됩니다.

b. 펌웨어 준수 정책을 사용하는 관리되는 장치에 대해 "할당 없음"을 선택하거나 **할당된 정책** 열에서 다른 펌웨어 준수 정책을 선택하십시오.

단계 2. 삭제할 펌웨어 업데이트가 포함된 모든 사용자 정의된 펌웨어 준수 정책 또는 편집된 펌웨어 준수 정책을 삭제하여 삭제할 펌웨어 업데이트를 제거하십시오.

a. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 준수 정책**을 클릭하십시오. 펌웨어 업데이트 준수 정책 페이지가 표시됩니다.

b. 펌웨어 준수 정책을 선택한 다음 **삭제** 아이콘( )을 선택하여 정책을 삭제하거나 **편집** 아이콘( )을 클릭하여 정책에서 펌웨어 업데이트를 제거하십시오.

단계 3. 펌웨어 업데이트를 삭제하십시오.

- **개별 펌웨어 업데이트 적용**
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하십시오. 펌웨어 업데이트 리포지토리 페이지가 표시됩니다.
  2. **개별 업데이트** 탭을 클릭합니다.
  3. 삭제할 펌웨어 업데이트를 하나 이상 선택하십시오.
  4. **이미지만 삭제** 아이콘( )을 클릭하여 이미지 또는 페이로드 파일(.zip, .bin, .uxz 또는 .tgz)만 삭제하십시오. 업데이트를 쉽게 다시 다운로드할 수 있도록 업데이트에 대한 정보가 유지됩니다. 또는 **전체 업데이트 패키지 삭제** 아이콘( )을 클릭하여 이미지 또는 페이로드 파일, 변경 기록 파일(.chg), readme 파일(.txt) 및 메타데이터 파일(.xml 또는 .json)을 포함한 전체 업데이트 패키지를 삭제하십시오.

  펌웨어 업데이트를 삭제하면 페이로드 파일이 제거되지만 업데이트 정보가 포함된 메타데이터 파일은 그대로 유지되어 필요한 경우 업데이트를 쉽게 다시 다운로드할 수 있으며, **다운로드 상태**가 '다운로드되지 않음'으로 바뀝니다.
- UXSP
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 리포지토리**를 클릭하십시오. 펌웨어 업데이트 리포지토리 페이지가 표시됩니다.
  2. UpdateXpress System Pack (UXSP) 탭을 클릭하십시오.
  3. 삭제할 UXSP를 하나 이상 선택하십시오.
  4. **UXSP 및 관련 정책 삭제** 아이콘( )을 클릭하여 이미지 또는 페이로드 파일, 변경 기록 파일(.chg), readme 파일(.txt) 및 메타데이터 파일(.xml 또는 .json)을 포함한 전체 UXSP를 삭제하십시오.

  선택한 UXSP가 사용 중인 (장치에 할당된) 정책과 관련되어 있으면, UXSP, 정책 및 패키지 업데이트 삭제 대화 상자가 표시됩니다. 할당된 정책뿐만 아니라 UXSP 및 할당되지 않은 정책을 삭제할지 여부를 선택하고 **확인**을 클릭하십시오.

펌웨어 준수 정책 생성 및 할당

*펌웨어 준수 정책*은 주의가 필요한 장치를 플래그 지정하여 특정 관리되는 장치의 펌웨어가 현재 또는 특정 수준에 있도록 합니다. 각 펌웨어 준수 정책은 장치의 준수 상태를 유지하려면 어떤 장치를 모니터링하고 어떤 펌웨어 수준을 설치해야 하는지 식별합니다. 장치 또는 펌웨어 구성 요소 수준에서 준수 정책을 설정할 수 있습니다. 그러면 XClarity Administrator에서 이러한 정책을 사용하여 관리되는 장치의 상태를 확인하고 규정을 위반한 장치를 식별합니다.

시작하기 전에

펌웨어 준수 정책을 생성할 때 정책에 할당될 장치에 적용할 대상 업데이트 버전을 선택합니다. 정책을 생성하기 전에 대상 버전에 대한 펌웨어 업데이트가 업데이트 리포지토리에 있는지 확인하십시오 (펌웨어 업데이트 다운로드 중 참조).

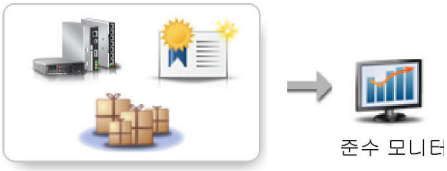
펌웨어 업데이트 리포지토리에 장치 유형이 나열되지 않는 경우 해당 유형의 장치에 대한 준수 정책을 작성하려면 먼저 해당 유형의 장치를 관리한 다음 전체 펌웨어 업데이트 세트를 다운로드하거나 가져와야 합니다.

이 작업 정보

펌웨어 준수 정책을 작성하면 다음과 같은 경우에 XClarity Administrator가 장치에 플래그를 지정하도록 선택할 수 있습니다.
- 장치의 펌웨어 수준이 낮습니다.
- 장치의 펌웨어가 이행 대상 버전과 일치하지 않습니다.

XClarity Administrator는 **리포지토리의 최신 펌웨어**라는 미리 정의된 펌웨어 준수 정책과 함께 제공됩니다. 새 펌웨어를 다운로드하거나 리포지토리로 가져오는 경우 리포지토리에 사용 가능한 최신 펌웨어 버전이 포함되도록 이 정책이 업데이트됩니다.

펌웨어 준수 정책이 장치에 할당된 후 장치 인벤토리가 변경되거나 펌웨어 업데이트 리포지토리가 변경되는 경우 XClarity Administrator이(가) 각 장치의 준수 상태를 검사합니다. 장치의 펌웨어가 할당된 정책을 준수하지 않으면 XClarity Administrator해당 장치가 펌웨어 업데이트 : 적용 / 활성화 펌웨어 준수 정책에 지정한 규칙에 따라 페이지



하드웨어, 카탈로그 및 정책 변경

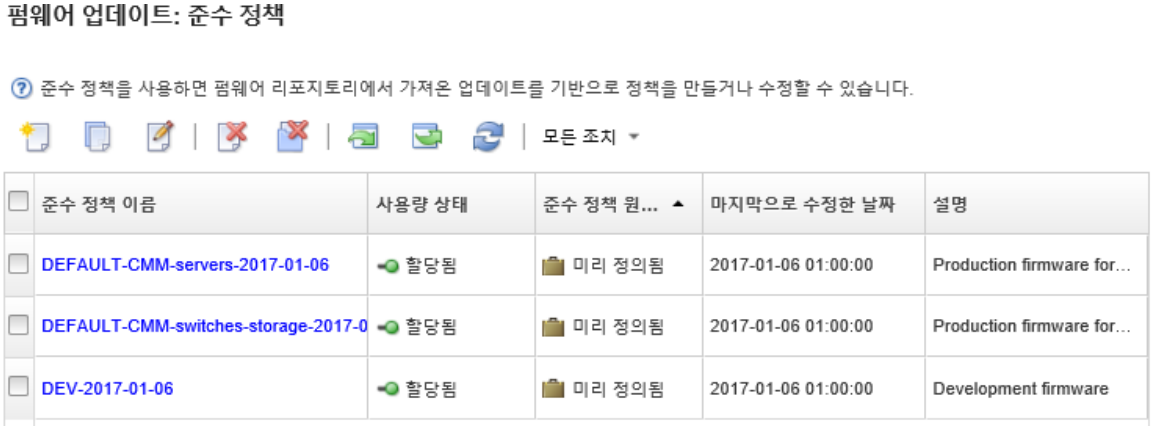
예를 들어 모든 ThinkSystem SR850 장치에 설치된 펌웨어의 기준 수준을 정의하는 펌웨어 준수 정책을 작성한 다음 모든 관리 ThinkSystem SR850 장치에 해당 펌웨어 준수 정책을 할당할 수 있습니다. 펌웨어 업데이트 리포지토리를 새로 고치고 새 펌웨어 업데이트가 추가되면 해당 컴퓨팅 노드가 준수 안됨 상태가 될 수 있습니다. 이러한 경우 XClarity Administrator는 펌웨어 업데이트: 적용/활성화 페이지를 업데이트하여 장치가 준수되지 않음을 표시하고 경고를 생성합니다.

참고: 할당된 펌웨어 준수 정책의 요구 사항을 충족하지 않는 장치에 대한 경고를 표시하거나 숨길 수 있습니다(전역 펌웨어 업데이트 설정 구성 참조). 알림은 기본적으로 숨겨져 있습니다.

절차

펌웨어 준수 정책을 생성 및 할당하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 준수 정책**을 클릭하십시오. 모든 기존 펌웨어 준수 정책 목록이 있는 준수 정책 페이지가 표시됩니다.



단계 2. 펌웨어 준수 정책을 만듭니다.

1. **만들기** 아이콘( )을 클릭하여 새 정책 만들기 대화 상자를 표시하십시오.

2. 펌웨어 준수 정책의 이름과 설명을 지정하십시오.
3. 각 장치에 대해 다음 기준에 따라 테이블을 작성하십시오.
   - **장치 유형**. 이 정책을 적용할 장치 또는 구성 요소 유형을 선택하십시오.

     팁: 서버를 선택한 경우 준수 수준이 UXSP 수준에서 수행됩니다. 그러나 서버를 확장하여 베이스보드 관리 컨트롤러 또는 UEFI와 같은 각 구성 요소에 대해 특정 펌웨어 수준을 지정할 수도 있습니다.
   - **이행 대상**. 적용 가능한 장치 및 하위 구성 요소에 대한 준수 대상을 지정하십시오.

     서버의 경우 다음 값 중 하나를 선택할 수 있습니다.
     - **기본값**. 각 하위 구성 요소의 준수 대상을 기본값(예: 해당 장치의 리포지토리에 있는 최신 펌웨어 세트)으로 변경합니다.
     - **업데이트 안 함**. 각 하위 구성 요소에 대한 준수 대상을 "업데이트 안 함"으로 변경합니다.

     하위 구성 요소가 없는 장치(예, CMM, 스위치 또는 스토리지 장치) 또는 서버의 하위 구성 요소에 대해 다음 값 중 하나를 선택할 수 있습니다.
     - *<firmware_level>*. 기준 펌웨어 수준을 지정합니다.
     - **업데이트 안 함**. 펌웨어를 업데이트하지 않도록 지정합니다. 백업 관리 컨트롤러의 펌웨어는 기본적으로 업데이트되지 않습니다.

     참고: 서버의 하위 구성 요소에 대한 기본값을 변경하면 해당 서버의 준수 대상이 **사용자 지정**으로 변경됩니다.
   - **준수 규칙**. 펌웨어 업데이트: 적용/활성화의 **설치된 버전** 열에서 장치가 미준수로 플래그 지정된 경우 지정하십시오.
     - **하위인 경우 플래그 지정**. 장치에 설치된 펌웨어 수준이 펌웨어 준수 정책에 지정된 수준보다 낮은 경우 장치가 미준수로 플래그 지정됩니다. 예를 들어 컴퓨팅 노드에서 네

트워크 어댑터를 교체하고 해당 네트워크 어댑터의 펌웨어가 펌웨어 준수 정책에서 식별된 수준보다 낮은 경우 컴퓨팅 노드가 미준수로 플래그 지정됩니다.

- **정확히 일치하지 않는 경우 플래그 지정**. 장치에 설치된 펌웨어 수준이 펌웨어 준수 정책과 정확히 일치하지 않는 경우 장치가 미준수로 플래그 지정됩니다. 예를 들어 컴퓨팅 노드에서 네트워크 어댑터를 교체하고 해당 네트워크 어댑터의 펌웨어가 펌웨어 준수 정책에서 식별된 수준과 다른 경우 컴퓨팅 노드가 미준수로 플래그 지정됩니다.
- **플래그 없음**. 준수하지 않는 장치는 플래그 지정되지 않습니다.

4. **옵션:** 시스템 유형을 확장하여 패키지의 각 업데이트를 표시하고 이행 대상으로 사용할 펌웨어 수준을 선택하거나 "업데이트 안 함"을 선택하여 해당 장치에서 펌웨어가 업데이트되지 않도록 하십시오.
5. **만들기**를 클릭하십시오.

   펌웨어 준수 정책은 펌웨어 업데이트: 준수 정책 페이지의 테이블에 나열됩니다. 이 테이블에는 사용 상태, 정책의 근본(사용자 정의되었는지 또는 미리 정의되었는지) 및 최근 수정 날짜가 표시됩니다.

단계 3. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하십시오. 관리되는 장치 목록이 있는 펌웨어 업데이트: 적용/활성화 페이지가 표시됩니다.

단계 4. 장치에 펌웨어 준수 정책을 할당합니다.

- **단일 장치**

  각 장치에 대해 **할당된 준수 정책** 열의 드롭다운 메뉴에서 정책을 선택하십시오.

  각 장치에 적용 가능한 펌웨어 준수 정책 목록에서 선택할 수 있습니다. 현재 장치에 정책이 할당되지 않은 경우 할당된 정책이 **할당 없음**으로 설정됩니다. 장치에 적용 가능한 정책이 없는 경우 할당된 정책이 **적용 가능한 정책 없음**으로 설정됩니다.

- **여러 개의 장치**

  1. **옵션:** 펌웨어 준수 정책을 할당할 장치를 하나 이상 선택하십시오.
  2. **정책 할당** 아이콘()을 클릭하여 정책 할당 대화 상자를 표시하십시오.

  3. **할당할 정책** 드롭다운 메뉴에서 펌웨어 준수 정책을 선택하십시오.

     선택된 모든 장치에 적용 가능한 펌웨어 준수 정책 목록에서 선택할 수 있습니다. 대화 상자를 열기 전에 장치를 선택하지 않으면 모든 정책이 나열됩니다.

     정책을 할당 취소하려면 **할당 없음**을 선택하십시오.

  4. 정책 할당에 대해 다음 범위 중 하나를 선택하십시오.
     - **다음에 해당하는 모든 장치…**
     - **다음에 해당하는 일부 장치만…**

5. 장치 기준을 하나 이상 선택하십시오.
   - **할당된 정책 없음**
   - **미준수(현재 할당된 정책 덮어쓰기)**
   - **준수(현재 할당된 정책 덮어쓰기)**
   - **모니터링 안 함(현재 할당된 정책 덮어쓰기)**
   - **기타(현재 할당된 정책 덮어쓰기)**. 이 설정은 데이터가 없거나 업데이트에 지원되지 않는 보류 중 상태와 같은 기타 상태의 장치에 적용됩니다. 도움말 아이콘( )에 커서를 가져가서 적용 가능한 장치 목록을 보십시오.

   참고: 모니터링 안 함 및 **기타** 기준은 해당 상태의 장치가 있는 경우에만 나열됩니다.
6. **확인**을 누르십시오.

   펌웨어 업데이트: 리포지토리 페이지의 **할당된 정책** 열에 나열된 정책이 선택한 펌웨어 준수 정책의 이름으로 변경됩니다.

완료한 후에

펌웨어 준수 정책을 작성하면 선택한 펌웨어 준수 정책에 다음 작업을 수행할 수 있습니다.

- 테이블에서 정책 이름을 클릭하여 할당된 장치 목록을 비롯한 정책 세부 정보를 확인합니다.
- **복사** 아이콘( )을 클릭하여 선택한 정책의 복제본을 작성합니다.
- **편집** 아이콘( )을 클릭하여 선택한 정책의 이름을 변경하거나 정책을 수정합니다.미리 정의된 펌웨어 준수 정책 또는 관리되는 장치에 할당된 정책은 편집할 수 없습니다.

  더 이상 할당된 특정 장치에 적용되지 않도록 할당된 정책을 수정하면 해당 장치에서 정책이 자동으로 할당 해제됩니다.

  미리 정의된 **최신 펌웨어** 정책의 이름을 변경하거나 정책을 수정할 수 없습니다.
- **정책 삭제** 아이콘( )을 클릭하여 선택한 펌웨어 준수 정책을 삭제하거나 **정책 및 펌웨어 패키지 삭제** 아이콘( )을 클릭하여 해당 정책에서만 사용되는 연결된 모든 펌웨어 업데이트와 선택한 펌웨어 준수 정책을 삭제합니다.장치에 할당된 경우에도 정책을 삭제할 수 있습니다.

  장치에 할당된 정책을 삭제하면 정책은 삭제되기 전에 할당 해제됩니다.

  사전 정의된 **최신 펌웨어** 정책은 삭제할 수 없습니다. 그러나 **전역 설정** 아이콘( )을 선택한 후 **최신 펌웨어 정책 사용 안 함**을 선택하여 정책을 비활성화할 수 있습니다. 이 옵션을 선택하면 최신 펌웨어 정책이 관리되는 장치에서 할당 해제되고 리포지토리에 사용 가능한 최신 펌웨어 버전이 포함되도록 정책이 더 이상 업데이트되지 않습니다.
- 정책을 선택하고 클릭하여 **내보내기** 아이콘( )을 클릭하여 선택한 정책을 로컬 시스템으로 내보냅니다. 그런 다음 **가져오기** 아이콘( )을 클릭하여 정책을 다른 XClarity Administrator 인스턴스로 가져올 수 있습니다.

펌웨어 준수 정책을 작성한 후 특정 장치에 정책을 할당하고(펌웨어 준수 정책 생성 및 할당 참조), 해당 장치에 대한 업데이트를 적용하고 활성화할 수 있습니다(펌웨어 업데이트 적용 및 활성화 참조).

준수하지 않는 장치 식별

펌웨어 준수 정책이 관리 장치에 할당된 경우 해당 장치의 펌웨어가 해당 정책을 준수하는지 여부를 판별할 수 있습니다.

절차

장치의 펌웨어가 할당된 펌웨어 준수 정책을 준수하는지 여부를 판별하려면 Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하여 펌웨어 업데이트: 준수 정책 페이지를 표시하고 해당 장치의 **설치된 버전** 열을 확인하십시오.

설치된 버전 열에 다음 값 중 하나가 포함되어 있습니다.

- **펌웨어 버전**. 장치에 설치된 펌웨어 버전이 할당된 정책을 준수합니다.
- **호환**. 장치에 설치된 펌웨어가 할당된 정책을 준수합니다.
- **미준수**. 장치에 설치된 펌웨어가 할당된 정책을 준수하지 않습니다.
- **준수 정책 세트 없음**. 장치에 펌웨어 준수 정책이 할당되지 않습니다.

새로 고침 아이콘( )을 클릭하여 **설치된 버전** 열의 내용을 새로 고칠 수 있습니다.

전역 펌웨어 업데이트 설정 구성

펌웨어 업데이트를 적용하면 전역 설정이 기본 설정으로 사용됩니다.

이 작업 정보

전역 설정 페이지에서 다음 설정을 구성할 수 있습니다.
- 하위 수준 장치에 대한 향상된 지원
- 할당된 정책을 준수하지 않는 장치에 대한 경고
- 할당된 정책이 없는 장치에 펌웨어 준수 정책 자동 할당
- 펌웨어 준수 정책에 연결된 대상이 없는 펌웨어 구성 요소가 있는 장치의 비준수 상태

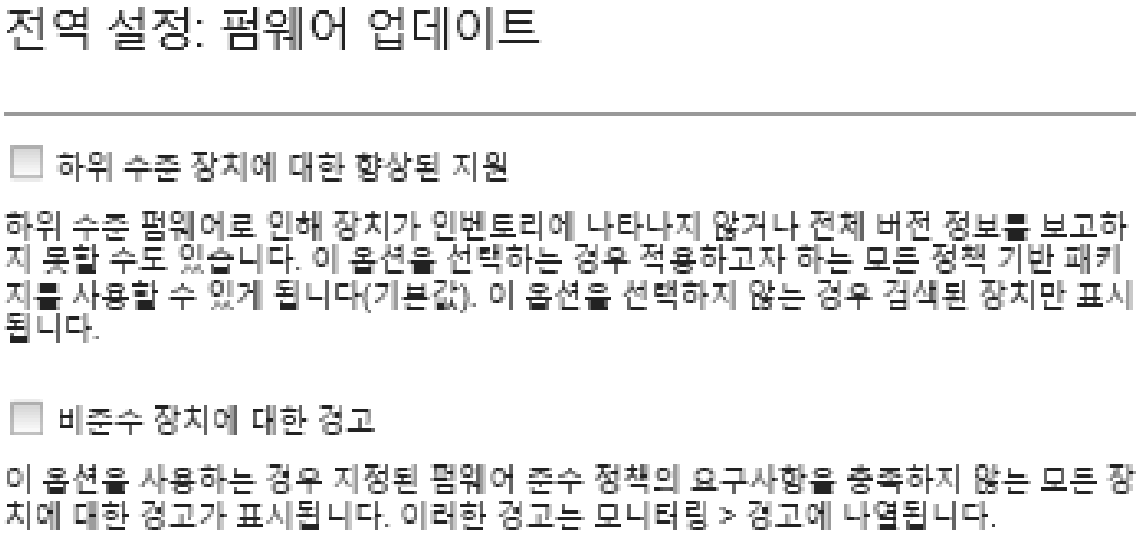
절차

모든 서버에 사용할 전역 설정을 구성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하십시오. 펌웨어 업데이트: 적용/활성화 페이지가 표시됩니다.

단계 2. **업데이트(정책 포함)** 또는 **업데이트(정책 제외)** 탭을 클릭하십시오.

단계 3. **모든 작업 → 전역 설정**을 클릭하여 전역 설정: 펌웨어 업데이트 대화 상자를 표시합니다.



단계 4. 다음 옵션을 선택하십시오.

- **늦은 버전 장치 고급 지원**을 선택하여 모든 장치에 대한 인벤토리 및 정식 버전 정보를 표시하십시오. 펌웨어가 낮은 버전이거나 장치가 인벤토리에 있지 않은 경우에도 그렇게 하십시오.

- **비준수 장치에 대한 경고**를 선택하여 경고 페이지에서 할당된 펌웨어 준수 정책의 요구 사항을 충족하지 않는 장치에 대한 경고를 표시합니다. 경고는 기본적으로 경고 페이지에서 숨겨집니다. 자세한 정보는 활성 경고 보기XClarity Administrator온라인 설명서에서 .
- 할당된 정책이 없는 장치에 펌웨어 호환 정책의 자동 할당을 사용하지 않으려면 **자동 정책 할당 해제**를 선택하십시오. 이 옵션을 선택하지 않으면 XClarity Administrator을(를) 다시 시작하거나 새 장치를 관리할 때 정책이 없는 장치에 펌웨어 준수 정책이 할당됩니다.
- **대상이 없는 펌웨어에 대한 비준수 보고**를 선택하여 펌웨어 준수 정책에서 펌웨어 구성 요소에 연결된 대상이 없는 경우 장치를 비준수로 플래그 지정하십시오. 이 옵션을 선택하지 않으면 대상이 없는 장치가 준수로 플래그 지정됩니다.

단계 5. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

펌웨어 업데이트 적용 및 활성화

Lenovo XClarity Administrator는 펌웨어 업데이트를 관리되는 장치에 자동으로 적용하지 않습니다. 준수 정책을 사용하거나 사용하지 않고 펌웨어 업데이트를 적용하도록 선택할 수 있습니다.

시작하기 전에

준수 정책을 사용하는 경우 여러 장치에서 동시에 업데이트를 예약할 수 있습니다. XClarity Administrator는 올바른 순서대로 장치를 자동으로 업데이트합니다. CMM이 먼저 업데이트되고, 그 다음에 스위치, 서버, 스토리지 장치가 업데이트됩니다.

다운로드된 펌웨어 업데이트만 적용할 수 있습니다.

펌웨어 업데이트를 수행하는 경우 XClarity Administrator는 업데이트를 완료하기 위해 하나 이상의 작업을 시작합니다.

펌웨어 업데이트가 진행되는 동안에는 대상 장치가 잠깁니다. 업데이트 프로세스가 완료될 때까지 대상 장치에서 다른 관리 작업을 시작할 수 없습니다.

펌웨어 업데이트가 장치에 적용되면 펌웨어 업데이트를 완전히 활성화하기 위해 한 번 이상 다시 시작해야 할 수 있습니다. 장치를 즉시 다시 시작할지, 활성화를 지연할지 또는 활성화의 우선 순위를 매길지 선택할 수 있습니다. 즉시 다시 시작하도록 선택하면 XClarity Administrator는 필요한 재시작 횟수를 최소화합니다. 활성화를 지연하도록 선택하면 다음에 장치가 다시 시작될 때 업데이트가 활성화됩니다. 우선 순위가 매겨진 활성화를 선택하는 경우 업데이트가 베이스 보드 관리 컨트롤러에서 즉시 활성화되며, 다른 모든 펌웨어 업데이트는 다음에 장치가 다시 시작될 때 활성화됩니다.

한 번에 최대 50개의 장치에서 선택한 펌웨어를 업데이트할 수 있습니다. 50개가 넘는 장치에서 선택한 펌웨어를 업데이트하도록 선택하면 나머지 장치는 대기 상태가 됩니다. 업데이트된 장치에서 활성화가 완료되거나 업데이트된 장치가 보류 유지 관리 모드 상태(해당 장치를 다시 시작해야 하는 경우)가 되면 대기 중인 장치가 "선택한 펌웨어 업데이트" 대기열에서 제거됩니다. 보류 유지 관리 모드 상태의 장치가 다시 시작되면 최대 횟수의 펌웨어 업데이트가 이미 진행 중인 경우에도 장치는 유지 관리 모드로 부팅되고 업데이트 프로세스를 계속합니다.

한 번에 최대 10개의 장치에서 번들 펌웨어를 업데이트할 수 있습니다. 10개가 넘는 장치에서 번들 펌웨어를 업데이트하도록 선택하면 나머지 장치는 대기 상태가 됩니다. 번들 펌웨어 업데이트가 수행된 장치에서 활성화가 완료되면 대기 중인 장치가 "번들 펌웨어 업데이트" 대기열에서 제거됩니다.

주의: RHEL(Red Hat® Enterprise Linux) v7 이상에서는 그래픽 모드에서 운영 체제를 다시 시작하면 기본적으로 서버가 일시 중단됩니다. XClarity Administrator에서 **정상적으로 다시 시작** 또는 **즉시 다시 시작** 작업을 수행하려면 먼저 전원 버튼의 동작을 변경하여 전원을 끄도록 운영 체제를 수동으로 구성해야 합니다. 지시사항은 Red Hat 데이터 마이그레이션 및 관리 안내서: 그래픽 대상 모드에서 전원 버튼을 누르면 동작 변경.

참고: XClarity Administrator는 LAN-over-USB 인터페이스를 자동으로 사용 설정합니다.

준수 정책을 사용하여 번들 펌웨어 업데이트 적용

Lenovo XClarity Administrator에서 관리되는 장치가 규정을 준수하지 않는 것으로 확인하면 해당하는 펌웨어 업데이트 패키지가 포함된 번들 이미지를 사용하여 할당된 펌웨어 준수 정책을 준수하지 않는 선택된 ThinkSystem SR635 및 SR655 서버의 *모든* 구성 요소에 펌웨어 업데이트를 수동으로 적용할 수 있습니다. *번들 이미지*는 업데이트 프로세스 중에 준수 정책에서 모든 펌웨어 업데이트 패키지를 수집하여 만들어집니다.

시작하기 전에

- 관리되는 장치에서 펌웨어를 업데이트하기 전에 펌웨어 업데이트 고려사항을 읽으십시오(펌웨어 업데이트 고려사항 참조).
- 처음에는 업데이트가 지원되지 않는 장치가 보기에서 숨겨집니다. 지원되지 않는 장치는 업데이트하도록 선택할 수 없습니다.
- 기본적으로 감지된 모든 구성 요소가 업데이트 적용이 가능한 것으로 나열됩니다. 그러나 하위 수준 펌웨어를 사용하면 구성 요소가 인벤토리에 표시되지 않거나 전체 버전 정보를 보고하지 못할 수 있습니다. 업데이트를 적용할 수 있는 모든 정책 기반 패키지를 나열하려면 **모든 작업 → 전역 설정** 및 **하위 수준 장치에 대한 향상된 지원**을 클릭하십시오. 이 옵션을 선택하면 "기타 사용 가능한 소프트웨어"가 감지되지 않은 장치의 설치된 버전 열에 나열됩니다. 자세한 정보는 전역 펌웨어 업데이트 설정 구성의 내용을 참조하십시오.

  참고:

  - 관리되는 장치에 대한 업데이트가 진행 중인 경우에는 전역 설정을 변경할 수 없습니다.
  - 추가 옵션을 생성하는 데는 몇 분 정도 걸립니다. 몇 분 후에 **새로 고침** 아이콘()을 클릭하여 표를 새로 고쳐야 할 수 있습니다.
- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.
- 번들 펌웨어 업데이트 적용은 ThinkSystem SR635 및 SR655 서버에만 지원됩니다.
- 번들 펌웨어 업데이트 적용은 IPv4 주소에만 지원됩니다. IPv6 주소는 지원되지 않습니다.
- 전체 인벤토리 정보를 검색하려면 각 대상 장치가 한 번 이상 OS로 부팅되었어야 합니다.
- 번들 업데이트 기능을 사용하려면 베이스보드 관리 컨트롤러 펌웨어 v2.94 이상이 필요합니다.
- 리포지토리 팩의 펌웨어 업데이트 또는 개별 펌웨어 업데이트만 사용됩니다. UpdateXpress System Packs (UXSPs)는 지원되지 않습니다.
- 다운로드된 펌웨어 업데이트만 적용됩니다. 제품 카탈로그를 새로 고치고 적합한 펌웨어 업데이트를 다운로드하십시오(제품 카탈로그 새로 고침 및 펌웨어 업데이트 다운로드 중 참조).

  참고: XClarity Administrator가 처음 설치되면 제품 카탈로그와 리포지토리가 비어 있습니다.
- 준수 검사는 ThinkSystem SR635 및 SR655 서버의 베이스보드 관리 컨트롤러와 UEFI에만 지원됩니다. 그러나 XClarity Administrator에서는 사용 가능한 모든 하드웨어 구성 요소에 대해 펌웨어 업데이트 적용을 시도합니다.
- 업데이트는 할당된 펌웨어 준수 정책에 따라 적용됩니다. 구성 요소의 하위 집합은 업데이트할 수 없습니다.
- Lenovo XClarity Provisioning Manager(LXPM), LXPM Windows 드라이버 또는 LXPM Linux 드라이버용 펌웨어 업데이트를 ThinkSystem SR635 및 SR655 서버에 적용하려면 XClarity Administrator v3.2 이상이 필요합니다.
- 현재 설치된 버전이 할당된 준수 정책보다 높으면 베이스보드 관리 컨트롤러 및 UEFI 업데이트를 건너뜁니다.

- 펌웨어 준수 정책을 작성하여 펌웨어 업데이트를 적용할 장치에 할당해야 합니다. 자세한 정보는 펌웨어 준수 정책 생성 및 할당의 내용을 참조하십시오.
- 업데이트 프로세스를 시작하기 전에 선택한 장치의 전원이 꺼집니다. 실행 중인 워크로드가 중지되었는지 혹은 가상화된 환경에서 작업 중인 경우 해당 작업이 다른 서버로 이동되었는지 확인하십시오.

주의: 업데이트 프로세스를 시작하기 전에 선택한 장치의 전원이 꺼집니다. 실행 중인 워크로드가 중지되었는지 혹은 가상화된 환경에서 작업 중인 경우 해당 작업이 다른 서버로 이동되었는지 확인하십시오. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.

이 작업 정보

번들 업데이트 프로세스는 먼저 베이스보드 관리 컨트롤러와 UEFI를 대역 외 방식으로 업데이트합니다. 이러한 업데이트가 완료되면 프로세스에서 시스템 유형에 따라 준수 정책에 남아 있는 펌웨어의 번들 이미지를 생성합니다. 그런 다음 프로세스에서 이미지를 선택한 장치에 마운트하고 장치를 다시 시작하여 이미지를 부팅합니다. 남은 업데이트를 수행하기 위해 이미지가 자동으로 실행됩니다.

한 번에 최대 10개의 장치에서 번들 펌웨어를 업데이트할 수 있습니다. 10개가 넘는 장치에서 번들 펌웨어를 업데이트하도록 선택하면 나머지 장치는 대기 상태가 됩니다. 번들 펌웨어 업데이트가 수행된 장치에서 활성화가 완료되면 대기 중인 장치가 "번들 펌웨어 업데이트" 대기열에서 제거됩니다.

장치에서 구성 요소를 업데이트하는 동안 오류가 발생하는 경우 펌웨어 업데이트 프로세스가 특정 구성 요소에 대한 펌웨어를 업데이트하지 않습니다. 그러나 펌웨어 업데이트 프로세스는 장치의 다른 구성 요소와 현재 펌웨어 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.

절차

관리되는 장치에 번들 이미지 형식으로 펌웨어 업데이트를 적용하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하십시오. 펌웨어 업데이트: 적용/활성화 페이지가 표시됩니다.

단계 2. **업데이트(정책 포함)** 탭을 클릭하십시오.

단계 3. 펌웨어 업데이트를 적용할 장치 및 구성 요소를 하나 이상 선택하십시오.

특정 장치를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 특정 섀시, 랙 또는 그룹에 있는 장치만 나열하도록 **표시** 메뉴의 옵션을 선택하거나 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하거나 특정 상태의 장치만 나열하도록 다음 아이콘을 클릭하여 표시되는 장치 목록을 필터링할 수 있습니다.

- **호환 장치 숨기기** 아이콘()
- **비호환 장치 상태 숨기기** 아이콘()
- **할당된 준수 정책이 없는 장치 숨기기** 아이콘()
- **모니터링되지 않는 장치 숨기기** 아이콘()
- **펌웨어 활성화를 보류 중인 장치 숨기기** 아이콘()
- **준수 오류가 있는 장치 숨기기** 아이콘()
- **업데이트에 지원되지 않는 장치 숨기기** 아이콘()
- **펌웨어 업데이트 중인 장치 숨기기** 아이콘()
- **스테이징할 수 없는 펌웨어가 있는 장치 숨기기** 아이콘()

그룹 열은 각 장치가 멤버인 그룹을 나타냅니다. 그룹 열에 마우스를 올리면 그룹 유형별로 전체 그룹 목록을 가져올 수 있습니다.

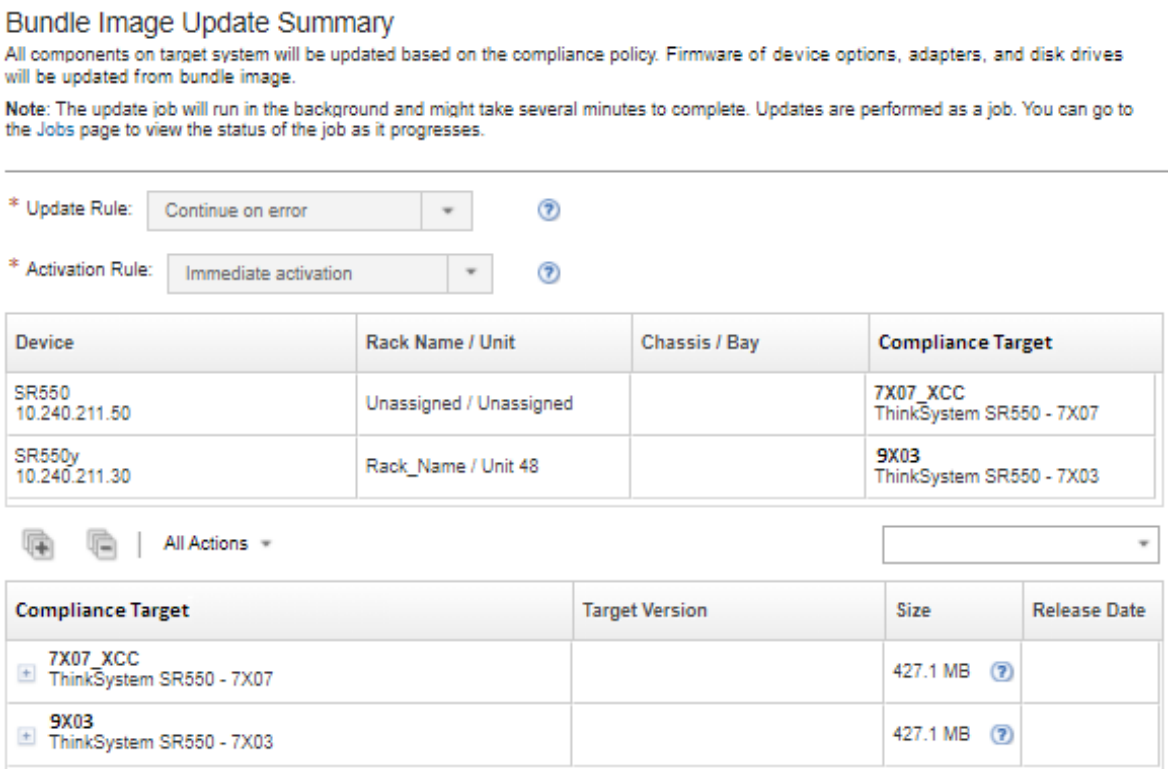
설치된 버전 열은 설치된 펌웨어 버전, 준수 상태 또는 장치 상태를 나타냅니다.

준수 상태는 다음 중 하나입니다.
- **준수**
- **준수 오류**
- **미준수**
- **준수 정책 세트 없음**
- **모니터링 안 함**

장치 상태는 다음 중 하나입니다.
- **업데이트 지원되지 않음**
- **업데이트 진행 중**

펌웨어 업데이트: 적용/활성화

단계 4. **번들 이미지에서 업데이트 수행** 아이콘( )을 클릭하십시오. 번들 이미지 업데이트 요약 대화 상자가 표시됩니다. 이 대화 상자에는 번들 이미지에 포함된 선택한 장치 및 펌웨어 업데이트가 나열됩니다.



단계 5. **번들 이미지에서 업데이트 수행**을 클릭하여 즉시 업데이트하거나 **일정**을 클릭하여 이 업데이트가 나중에 실행되도록 예약하십시오.

완료한 후에

펌웨어 업데이트를 적용할 때 서버가 유지 관리 모드로 전환되지 못하는 경우 업데이트를 다시 적용해 보십시오.

업데이트가 제대로 완료되지 않은 경우 문제 해결 및 정정 작업에 대해서는 XClarity Administrator 온라인 설명서에서 펌웨어 업데이트 및 리포지토리 문제의 내용을 참조하십시오.

펌웨어 업데이트: 적용/활성화 페이지에서 다음 작업을 수행할 수 있습니다.

- **모든 작업 → CSV로 보기 내보내기**를 클릭하여 각 관리되는 장치에 대한 펌웨어 및 준수 정보를 내보냅니다.

  참고: CSV 파일에는 현재 보기에 있는 필터링된 정보만 포함됩니다. 보기에서 필터링되어 제외된 정보와 숨겨진 열의 정보는 포함되지 않습니다.

- 장치를 선택하고 **업데이트 취소** 아이콘( )을 클릭하여 장치에 업데이트 적용을 취소합니다.

  참고: 시작할 대기열에 있는 펌웨어 업데이트를 취소할 수 있습니다. 업데이트 프로세스가 시작된 후 업데이트 프로세스가 유지 관리 모드로 변경하거나 장치를 다시 시작하는 등 업데이트 적용 이외의 작업을 수행하는 경우에만 펌웨어 업데이트를 취소할 수 있습니다.

- 적용 / 활성화 페이지의 **상태** 열에서 펌웨어 업데이트의 상태를 직접 봅니다.
- 작업 로그에서 업데이트 프로세스의 상태를 모니터링합니다. Lenovo XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오.

  작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

펌웨어 업데이트 작업이 완료되면 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하여 펌웨어 업데이트: 적용/활성화 페이지로 돌아간 다음 **새로 고침** 아이콘()을 클릭하여 장치가 준수되고 있음을 확인할 수 있습니다. 각 장치에서 활성화된 현재 펌웨어 버전은 **설치된 버전** 열에 나열되어 있습니다.

준수 정책을 사용하여 선택한 펌웨어 업데이트 적용

Lenovo XClarity Administrator에서 준수하지 않는 장치를 식별하면 해당 관리되는 장치에서 펌웨어 업데이트를 수동으로 적용하고 활성화할 수 있습니다. 펌웨어 준수 정책에 적용되는 모든 펌웨어 업데이트 또는 정책의 특정 펌웨어 업데이트만 적용하고 활성화하도록 선택할 수 있습니다. 다운로드된 펌웨어 업데이트만 적용됩니다.

자세히 알아보기:

- XClarity Administrator: 펌웨어 업데이트 시 효율 높이기
- Lenovo ThinkSystem 펌웨어 및 드라이버 업데이트 모범 사례
- XClarity Administrator: 베어메탈에서 클러스터로
- XClarity Administrator: 펌웨어 업데이트
- XClarity Administrator: 펌웨어 보안 업데이트 프로비저닝

시작하기 전에

- 관리되는 장치에서 펌웨어를 업데이트하기 전에 펌웨어 업데이트 고려사항을 읽으십시오(펌웨어 업데이트 고려사항 참조).
- 처음에는 업데이트가 지원되지 않는 장치가 보기에서 숨겨집니다. 지원되지 않는 장치는 업데이트하도록 선택할 수 없습니다.
- 기본적으로 감지된 모든 구성 요소가 업데이트 적용이 가능한 것으로 나열됩니다. 그러나 하위 수준 펌웨어를 사용하면 구성 요소가 인벤토리에 표시되지 않거나 전체 버전 정보를 보고하지 못할 수 있습니다. 업데이트를 적용할 수 있는 모든 정책 기반 패키지를 나열하려면 **모든 작업 → 전역 설정** 및 **하위 수준 장치에 대한 향상된 지원**을 클릭하십시오. 이 옵션을 선택하면 "기타 사용 가능한 소프트웨어"가 감지되지 않은 장치의 설치된 버전 열에 나열됩니다. 자세한 정보는 전역 펌웨어 업데이트 설정 구성의 내용을 참조하십시오.

  참고:

  – 관리되는 장치에 대한 업데이트가 진행 중인 경우에는 전역 설정을 변경할 수 없습니다.

– 추가 옵션을 생성하는 데는 몇 분 정도 걸립니다. 몇 분 후에 **새로 고침** 아이콘()을 클릭하여 표를 새로 고쳐야 할 수 있습니다.

- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.
- 펌웨어 업데이트 리포지토리가 배포할 펌웨어 패키지를 가지고 있는지 확인하십시오. 그렇지 않은 경우 제품 카탈로그를 새로 고치고 적합한 펌웨어 업데이트를 다운로드하십시오(제품 카탈로그 새로 고침 및 펌웨어 업데이트 다운로드 중 참조).

  참고: XClarity Administrator가 처음 설치되면 제품 카탈로그와 리포지토리가 비어 있습니다.

  필수 펌웨어를 설치하려는 경우 필수 펌웨어가 리포지토리에도 다운로드되는지 확인해야 합니다.

  경우에 따라 펌웨어를 업데이트하는 데 여러 버전이 필요할 수 있으며 모든 버전을 리포지토리에 다운로드해야 합니다. 예를 들어, IBM FC5022 SAN 확장 가능 스위치를 v7.4.0a에서 v8.2.0a로 업그레이드하려면 먼저 v8.0.1-pha를 설치하고 v8.1.1과 v8.2.0a를 순서대로 설치해야 합니다. 스위치를 v8.2.0a로 업데이트하려면 세 버전이 모두 리포지토리에 있어야 합니다.
- 일반적으로 펌웨어 업데이트를 활성화하려면 장치를 다시 시작해야 합니다. 업데이트 프로세스 중에 장치를 다시 시작하려는 경우(*즉시 활성화*) 실행 중인 워크로드가 중지되었거나, 가상화된 환경에서 작업 중이라면 다른 서버로 이동했는지 확인하십시오.
- ThinkSystem SR635 및 SR655 서버의 경우 기존 업데이트 기능을 사용하여 베이스보드 관리 컨트롤러 및 UEFI 펌웨어 업데이트만 적용할 수 있습니다. 관리 컨트롤러 펌웨어 버전 AMBT10M 이상, UEFI 펌웨어 버전 CFE114L 이상이 필요합니다. 모든 구성 요소(관리 컨트롤러, UEFI, 디스크 드라이브 및 IO 옵션 포함)를 업데이트하려면 번들 업데이트 기능을 사용하십시오(준수 정책을 사용하여 번들 펌웨어 업데이트 적용 참조).

이 작업 정보

- 한 번에 최대 50개의 장치에서 선택한 펌웨어를 업데이트할 수 있습니다. 50개가 넘는 장치에서 선택한 펌웨어를 업데이트하도록 선택하면 나머지 장치는 대기 상태가 됩니다. 업데이트된 장치에서 활성화가 완료되거나 업데이트된 장치가 보류 유지 관리 모드 상태(해당 장치를 다시 시작해야 하는 경우)가 되면 대기 중인 장치가 "선택한 펌웨어 업데이트" 대기열에서 제거됩니다. 보류 유지 관리 모드 상태의 장치가 다시 시작되면 최대 횟수의 펌웨어 업데이트가 이미 진행 중인 경우에도 장치는 유지 관리 모드로 부팅되고 업데이트 프로세스를 계속합니다.
- 현재 설치된 펌웨어 이후 버전의 펌웨어를 적용하고 활성화할 수 있습니다.
- 특정 장치에 대한 모든 업데이트를 적용하도록 선택할 수 있습니다. 그러나 장치를 확장하여 베이스보드 관리 컨트롤러 또는 UEFI와 같은 특정 구성 요소에 대한 업데이트를 지정하도록 선택할 수도 있습니다.
- 여러 구성 요소에 대한 업데이트가 포함된 펌웨어 업데이트 패키지를 설치하도록 선택하는 경우 업데이트 패키지를 적용하는 모든 구성 요소가 업데이트됩니다.

절차

관리되는 장치에 업데이트를 적용하고 활성화하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하십시오. 펌웨어 업데이트: 적용/활성화 페이지가 표시됩니다.

단계 2. **업데이트(정책 포함)** 탭을 클릭하십시오.

단계 3. 펌웨어 업데이트를 적용할 장치를 하나 이상 선택하십시오.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 특정 섀시, 랙 또는 그룹에 있는 장치만 나열하도록 **표시** 메뉴의 옵션을 선택하거나 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하거나 특정 상태의 장치만 나열하도록 다음 아이콘을 클릭하여 표시되는 장치 목록을 필터링할 수 있습니다.

- **호환 장치 숨기기** 아이콘()

- **비호환 장치 상태 숨기기 아이콘(**  **)**
- **할당된 준수 정책이 없는 장치 숨기기 아이콘(**  **)**
- **모니터링되지 않는 장치 숨기기 아이콘(**  **)**
- **펌웨어 활성화를 보류 중인 장치 숨기기 아이콘(**  **)**
- **준수 오류가 있는 장치 숨기기 아이콘(**  **)**
- **업데이트에 지원되지 않는 장치 숨기기 아이콘(**  **)**
- **펌웨어 업데이트 중인 장치 숨기기 아이콘(**  **)**
- **스테이징할 수 없는 펌웨어가 있는 장치 숨기기 아이콘(**  **)**

그룹 열은 각 장치가 멤버인 그룹을 나타냅니다. 그룹 열에 마우스를 올리면 그룹 유형별로 전체 그룹 목록을 가져올 수 있습니다.

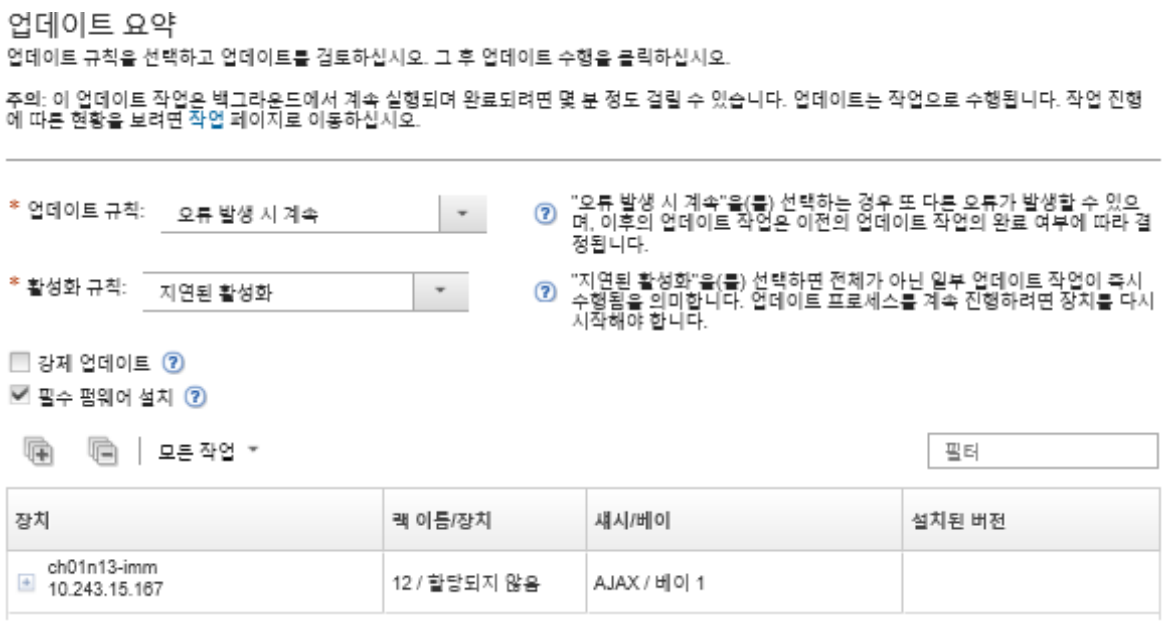
설치된 버전 열은 설치된 펌웨어 버전, 준수 상태 또는 장치 상태를 나타냅니다.

준수 상태는 다음 중 하나입니다.
-  **준수**
-  **준수 오류**
-  **미준수**
-  **준수 정책 세트 없음**
-  **모니터링 안 함**

장치 상태는 다음 중 하나입니다.
-  **업데이트 지원되지 않음**
-  **업데이트 진행 중**

참고: 설치된 펌웨어 버전이 활성화 보류 중이면, "2.20/A9E12EUS(보류 활성화)"와 같이 해당하는 각 장치의 설치된 펌웨어 버전 또는 준수 상태에 "(보류 활성화)"가 추가됩니다. 보류 중인 활성화 상태를 보려면 다음 펌웨어 버전이 서버의 기본 베이스보드 관리 컨트롤러에 설치되어 있어야 합니다.
- IMM2: TCOO46F, TCOO46E 이상(플랫폼에 따라 다름)
- XCC: CDI328M, PSI316N, TEI334I 이상(플랫폼에 따라 다름)

단계 4. **업데이트 수행** 아이콘( )을 클릭하십시오. 업데이트 요약 대화 상자가 표시됩니다.



단계 5. 다음 업데이트 규칙 중 하나를 선택하십시오.

- **오류 발생 시 모든 업데이트 중지**. 대상 장치에서 임의의 구성 요소(예, 어댑터 또는 관리 컨트롤러)를 업데이트하는 중 오류가 발생하는 경우 현재 펌웨어 업데이트 작업에서 선택한 모든 장치에 대한 펌웨어 업데이트 프로세스가 중지됩니다. 이 경우 해당 장치의 업데이트 패키지에서는 어떤 업데이트도 적용되지 않습니다. 선택한 모든 시스템에 설치된 현재 펌웨어는 이후에도 유효합니다.
- **오류 발생 시 계속**. 장치에서 임의의 장치를 업데이트하는 중에 오류가 발생하는 경우 펌웨어 업데이트 프로세스가 특정 장치에 대한 펌웨어를 업데이트할 수 없습니다. 그러나 펌웨어 업데이트 프로세스는 장치의 다른 장치를 계속해서 업데이트하고 현재 펌웨어 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.

- **오류 발생 시 다음 시스템으로 이동**. 장치에서 임의의 장치를 업데이트하는 중에 오류가 발생하는 경우 펌웨어 업데이트 프로세스는 해당 특정 장치에 대한 펌웨어를 업데이트하는 모든 시도를 중지하므로 해당 장치에 설치된 현재 펌웨어가 계속해서 적용되게 됩니다. 펌웨어 업데이트 프로세스는 현재 펌웨어 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.

단계 6. 다음 활성화 규칙 중 하나를 선택하십시오.

- **즉시 활성화**. 업데이트 프로세스 중에는 전체 업데이트 프로세스가 완료될 때까지 장치가 자동으로 여러 차례 다시 시작될 수 있습니다. 계속 진행하려면 장치의 모든 응용 프로그램을 정지해야 합니다.
- **지연된 활성화**. 업데이트 작업 중 일부만 수행됩니다. 업데이트 프로세스를 계속 진행하려면 장치를 다시 시작해야 합니다. 그런 다음, 업데이트 작업이 완료될 때까지 재시작이 여러 차례 반복됩니다.

  상태가 **펌웨어 유지 관리 모드 보류 중**으로 변경되면 이벤트가 발생하여 서버를 다시 시작해야 할 때 이를 알려줍니다.

  어떠한 이유로 장치가 다시 시작되면 지연된 업데이트 프로세스가 완료됩니다.

  이 활성화 규칙은 서버 및 랙 스위치에 대해서만 지원됩니다. CMM 및 Flex 스위치는 이 설정과 상관 없이 즉시 활성화됩니다.

  상태가 **펌웨어 유지 관리 모드 보류 중**으로 변경되면 이벤트가 발생하여 서버를 다시 시작해야 할 때 이를 알려줍니다.

  지연된 업데이트 프로세스는 장치가 어떤 이유로든 다시 시작될 때 완료됩니다(수동 다시 시작 포함). 서버를 다시 시작해야 하는 시간 제한은 없습니다.

  XClarity Administrator는 한 번에 최대 50대의 장치에 대해 활성화가 지연된 업데이트를 적용할 수 있습니다. 50대를 초과하는 장치에 대해 활성화가 지연된 업데이트를 적용하려고 할 경우 나머지 장치는 대기 상태가 됩니다. 업데이트 중인 장치가 **펌웨어 유지 관리 모드 보류 중 상태**인 경우 장치가 대기 상태에서 벗어납니다.

  중요:

  - 업데이트 작업 중에 XClarity Administrator가 다시 시작될 경우 업데이트 작업이 오류와 함께 중지됩니다.
  - XClarity Administrator가 다운되거나 연결이 불가한 동안 **펌웨어 유지 관리 모드 보류 중** 상태의 서버가 다시 시작될 경우 서버가 BMU로 부팅되지만 XClarity Administrator는 BMU에 연결할 수 없으며 60초 후 시간이 초과되므로 베이스보드 관리 컨트롤러에 의해 시스템 전원 상태가 복원됩니다(전원이 꺼진 경우 전원을 끄고 전원이 켜진 경우 다시 시작됨).
- **우선 순위가 매겨진 활성화**. 베이스 보드 관리 컨트롤러의 펌웨어 업데이트는 즉시 활성화됩니다. 다른 모든 펌웨어 업데이트는 다음에 장치가 다시 시작될 때 활성화됩니다. 그런 다음, 업데이트 작업이 완료될 때까지 재시작이 여러 차례 반복됩니다. 이 규칙은 서버에 대해서만 지원됩니다.

  상태가 펌웨어 유지 관리 모드 보류 중으로 변경되면 이벤트가 발생하여 서버를 다시 시작해야 할 때 이를 알려줍니다.

참고: 이를 사용하는 경우 Wake-on-LAN 부팅 옵션은 서버 전원을 끄는 XClarity Administrator 작업을 방해할 수 있습니다. 예를 들어 사용자 네트워크의 Wake-on-LAN 클라이언트에서 "Wake on Magic 패킷" 명령을 실행하는 경우 펌웨어 업데이트를 방해합니다.

단계 7. **옵션:** 펌웨어 수준이 최신인 경우에도 선택한 구성 요소의 펌웨어를 업데이트하거나 선택한 구성 요소에 현재 설치된 것보다 이전 수준의 펌웨어 업데이트를 적용하려면 **강제 업데이트**를 선택하십시오.

참고: 하위 수준을 지원하는 장치 옵션, 어댑터 및 드라이브에는 이전 수준의 펌웨어를 적용할 수 있습니다. 하위 수준이 지원되는지 확인하려면 하드웨어 설명서를 참조하십시오.

단계 8. **옵션:** 전제조건 펌웨어를 설치하지 않으려고 하는 경우, **전제조건 펌웨어 설치**를 삭제하십시오. 기본값으로 전제조건 펌웨어가 설치됩니다.

참고: 사전 필수 펌웨어 업데이트에 **지연된 활성화** 또는 **우선 순위가 지정된 활성화**를 사용하는 경우 사전 필수 펌웨어를 활성화하려면 서버를 다시 시작해야 할 수 있습니다. 초기 재시작 후, 나머지 펌웨어 업데이트는 **즉시 활성화**를 사용하여 설치됩니다.

단계 9. **옵션: 즉시 활성화**를 선택한 경우, 업데이트 중에 서버가 재부팅되면 펌웨어 업데이트가 완료된 후 **메모리 테스트**를 선택하여 메모리 테스트를 실행합니다.

이 옵션은 ThinkSystem v1 및 v2 서버(ThinkSystem SR635, SR645, SR655, SR665 서버 제외)에 지원됩니다.

단계 10. **업데이트 수행**을 클릭하여 즉시 업데이트하거나 **일정**을 클릭하여 이 업데이트가 나중에 실행되도록 예약하십시오.

필요한 경우 관리되는 장치에서 전원 작업을 수행할 수 있습니다. 전원 작업은 **지연된 활성화**가 선택되고, 장치가 "유지 관리 보류 중" 상태로 대기 중일 때 업데이트를 계속하려는 경우에 유용합니다. 이 페이지에서 관리되는 장치에 전원 동작을 수행하려면 **모든 작업 → 전원 작업**을 클릭하고 다음 전원 작업 중 하나를 클릭하십시오.

- **전원 켜기**
- **OS 종료 및 전원 끄기**
- **전원 끄기**
- **OS 종료 및 다시 시작**
- **다시 시작**

완료한 후에

펌웨어 업데이트를 적용할 때 서버가 유지 관리 모드로 전환되지 못하는 경우 업데이트를 다시 적용해 보십시오.

업데이트가 제대로 완료되지 않은 경우 문제 해결 및 정정 작업에 대해서는 XClarity Administrator 온라인 설명서에서 펌웨어 업데이트 및 리포지토리 문제의 내용을 참조하십시오.

펌웨어 업데이트: 적용/활성화 페이지에서 다음 작업을 수행할 수 있습니다.

- **모든 작업 → CSV로 보기 내보내기**를 클릭하여 각 관리되는 장치에 대한 펌웨어 및 준수 정보를 내보냅니다.

  참고: CSV 파일에는 현재 보기에 있는 필터링된 정보만 포함됩니다. 보기에서 필터링되어 제외된 정보와 숨겨진 열의 정보는 포함되지 않습니다.

- 장치를 선택하고 **업데이트 취소** 아이콘()을 클릭하여 장치에 업데이트 적용을 취소합니다.

  참고: 시작할 대기열에 있는 펌웨어 업데이트를 취소할 수 있습니다. 업데이트 프로세스가 시작된 후 업데이트 프로세스가 유지 관리 모드로 변경하거나 장치를 다시 시작하는 등 업데이트 적용 이외의 작업을 수행하는 경우에만 펌웨어 업데이트를 취소할 수 있습니다.

- 적용 / 활성화 페이지의 **상태** 열에서 펌웨어 업데이트의 상태를 직접 봅니다.
- 작업 로그에서 업데이트 프로세스의 상태를 모니터링합니다. Lenovo XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오.

  작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

펌웨어 업데이트 작업이 완료되면 프로비저닝 ➙ **펌웨어 업데이트: 적용/활성화**를 클릭하여 펌웨어 업데이트: 적용/활성화 페이지로 돌아간 다음 **새로 고침** 아이콘()을 클릭하여 장치가 준수되고 있음을 확인할 수 있습니다. 각 장치에서 활성화된 현재 펌웨어 버전은 **설치된 버전** 열에 나열되어 있습니다.

준수 정책을 사용하지 않고 선택한 펌웨어 업데이트 적용

준수 정책을 사용하지 않고 단일 관리되는 장치나 장치 그룹에 현재 설치된 펌웨어보다 최신인 펌웨어를 신속하게 적용하고 활성화할 수 있습니다.

자세히 알아보기:

- XClarity Administrator: 펌웨어 업데이트 시 효율 높이기
- Lenovo ThinkSystem 펌웨어 및 드라이버 업데이트 모범 사례
- XClarity Administrator: 베어메탈에서 클러스터로
- XClarity Administrator: 펌웨어 업데이트
- XClarity Administrator: 펌웨어 보안 업데이트 프로비저닝

시작하기 전에

- 관리되는 장치에서 펌웨어를 업데이트하기 전에 펌웨어 업데이트 고려사항을 읽으십시오(펌웨어 업데이트 고려사항 참조).
- 처음에는 업데이트가 지원되지 않는 장치가 보기에서 숨겨집니다. 지원되지 않는 장치는 업데이트하도록 선택할 수 없습니다.
- 기본적으로 감지된 모든 구성 요소가 업데이트 적용이 가능한 것으로 나열됩니다. 그러나 하위 수준 펌웨어를 사용하면 구성 요소가 인벤토리에 표시되지 않거나 전체 버전 정보를 보고하지 못할 수 있습니다. 업데이트를 적용할 수 있는 모든 정책 기반 패키지를 나열하려면 **모든 작업 ➙ 전역 설정** 및 **하위 수준 장치에 대한 향상된 지원**을 클릭하십시오. 이 옵션을 선택하면 "기타 사용 가능한 소프트웨어"가 감지되지 않은 장치의 설치된 버전 열에 나열됩니다. 자세한 정보는 전역 펌웨어 업데이트 설정 구성의 내용을 참조하십시오.

  참고:

  – 관리되는 장치에 대한 업데이트가 진행 중인 경우에는 전역 설정을 변경할 수 없습니다.

  – 추가 옵션을 생성하는 데는 몇 분 정도 걸립니다. 몇 분 후에 **새로 고침** 아이콘()을 클릭하여 표를 새로 고쳐야 할 수 있습니다.

- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 작업을 실행 중인 경우 다른 모든 작업이 완료될 때까지 업데이트 작업이 큐잉됩니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.
- 펌웨어 업데이트 리포지토리가 배포할 펌웨어 패키지를 가지고 있는지 확인하십시오. 그렇지 않은 경우 제품 카탈로그를 새로 고치고 적합한 펌웨어 업데이트를 다운로드하십시오(제품 카탈로그 새로 고침 및 펌웨어 업데이트 다운로드 중 참조).

  참고: XClarity Administrator가 처음 설치되면 제품 카탈로그와 리포지토리가 비어 있습니다.

  필수 펌웨어를 설치하려는 경우 필수 펌웨어가 리포지토리에도 다운로드되는지 확인해야 합니다.

  경우에 따라 펌웨어를 업데이트하는 데 여러 버전이 필요할 수 있으며 모든 버전을 리포지토리에 다운로드해야 합니다. 예를 들어, IBM FC5022 SAN 확장 가능 스위치를 v7.4.0a에서 v8.2.0a로 업그레이드하려면 먼저 v8.0.1-pha를 설치하고 v8.1.1과 v8.2.0a를 순서대로 설치해야 합니다. 스위치를 v8.2.0a로 업데이트하려면 세 버전이 모두 리포지토리에 있어야 합니다.
- 일반적으로 펌웨어 업데이트를 활성화하려면 장치를 다시 시작해야 합니다. 업데이트 프로세스 중에 장치를 다시 시작하려는 경우(*즉시 활성화*) 실행 중인 워크로드가 중지되었거나, 가상화된 환경에서 작업 중이라면 다른 서버로 이동했는지 확인하십시오.

이 작업 정보

- 한 번에 최대 50개의 장치에서 선택한 펌웨어를 업데이트할 수 있습니다. 50개가 넘는 장치에서 선택한 펌웨어를 업데이트하도록 선택하면 나머지 장치는 대기 상태가 됩니다. 업데이트된 장치에서 활성화가 완료되거나 업데이트된 장치가 보류 유지 관리 모드 상태(해당 장치를 다시 시작해야 하는 경우)가 되면 대기 중인 장치가 "선택한 펌웨어 업데이트" 대기열에서 제거됩니다. 보류 유지 관리 모드 상태의 장치가 다시 시작되면 최대 횟수의 펌웨어 업데이트가 이미 진행 중인 경우에도 장치는 유지 관리 모드로 부팅되고 업데이트 프로세스를 계속합니다.
- 현재 설치된 펌웨어 이후 버전의 펌웨어를 적용하고 활성화할 수 있습니다.
- 특정 장치에 대한 모든 업데이트를 적용하도록 선택할 수 있습니다. 그러나 장치를 확장하여 베이스보드 관리 컨트롤러 또는 UEFI와 같은 특정 구성 요소에 대한 업데이트를 지정하도록 선택할 수도 있습니다.
- 여러 구성 요소에 대한 업데이트가 포함된 펌웨어 업데이트 패키지를 설치하도록 선택하는 경우 업데이트 패키지를 적용하는 모든 구성 요소가 업데이트됩니다.

절차

관리되는 장치에 업데이트를 적용하고 활성화하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 펌웨어 업데이트: 적용/활성화**를 클릭하십시오. 펌웨어 업데이트: 적용/활성화 페이지가 표시됩니다.

단계 2. **업데이트(정책 제외)** 탭을 클릭하십시오.

단계 3. 업데이트하려는 각 장치의 **다운로드한 최신 버전** 열에서 펌웨어 수준을 선택하십시오.

단계 4. 업데이트할 장치를 하나 이상 선택하십시오.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 특정 섀시, 랙 또는 그룹에 있는 장치만 나열하도록 **표시** 메뉴의 옵션을 선택하거나 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하거나 특정 상태의 장치만 나열하도록 다음 아이콘을 클릭하여 표시되는 장치 목록을 필터링할 수 있습니다.

- **일부 이후 버전이 있는 구성 요소 숨기기** 아이콘()
- **이후 버전이 없는 구성 요소 숨기기** 아이콘()
- **업데이트에 지원되지 않는 장치 숨기기** 아이콘()
- **펌웨어 업데이트 중인 장치 숨기기** 아이콘()
- **스테이징할 수 없는 펌웨어가 있는 장치 숨기기** 아이콘()

그룹 열은 각 장치가 멤버인 그룹을 나타냅니다. 그룹 열에 마우스를 올리면 그룹 유형별로 전체 그룹 목록을 가져올 수 있습니다.

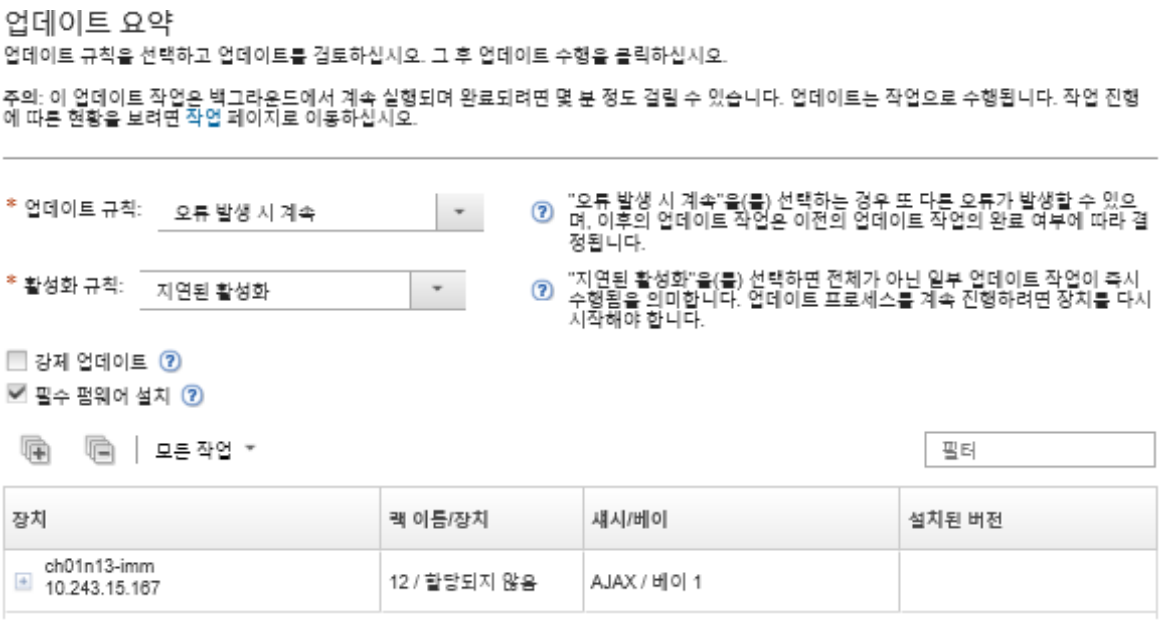
설치된 버전 열은 설치된 펌웨어 버전, 준수 상태 또는 장치 상태를 나타냅니다.

준수 상태는 다음 중 하나입니다.
- **준수**
- **준수 오류**
- **미준수**
- **준수 정책 세트 없음**
- **모니터링 안 함**

장치 상태는 다음 중 하나입니다.
- **업데이트 지원되지 않음**
- **업데이트 진행 중**

참고: 설치된 펌웨어 버전이 활성화 보류 중이면, "2.20/A9E12EUS(보류 활성화)"와 같이 해당하는 각 장치의 설치된 펌웨어 버전 또는 준수 상태에 "(보류 활성화)"가 추가됩니다. 보류 중인 활성화 상태를 보려면 다음 펌웨어 버전이 서버의 기본 베이스보드 관리 컨트롤러에 설치되어 있어야 합니다.
- IMM2: TCOO46F, TCOO46E 이상(플랫폼에 따라 다름)
- XCC: CDI328M, PSI316N, TEI334I 이상(플랫폼에 따라 다름)

단계 5. **업데이트 수행** 아이콘( )을 클릭하십시오. 업데이트 요약 대화 상자가 표시됩니다.



단계 6. 다음 업데이트 규칙 중 하나를 선택하십시오.

- **오류 발생 시 모든 업데이트 중지**. 대상 장치에서 임의의 구성 요소(예, 어댑터 또는 관리 컨트롤러)를 업데이트하는 중 오류가 발생하는 경우 현재 펌웨어 업데이트 작업에서 선택한 모든 장치에 대한 펌웨어 업데이트 프로세스가 중지됩니다. 이 경우 해당 장치의 업데이트 패키지에서는 어떤 업데이트도 적용되지 않습니다. 선택한 모든 시스템에 설치된 현재 펌웨어는 이후에도 유효합니다.
- **오류 발생 시 계속**. 장치에서 임의의 장치를 업데이트하는 중에 오류가 발생하는 경우 펌웨어 업데이트 프로세스가 특정 장치에 대한 펌웨어를 업데이트할 수 없습니다. 그러나 펌웨어 업데이트 프로세스는 장치의 다른 장치를 계속해서 업데이트하고 현재 펌웨어 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.
- **오류 발생 시 다음 시스템으로 이동**. 장치에서 임의의 장치를 업데이트하는 중에 오류가 발생하는 경우 펌웨어 업데이트 프로세스는 해당 특정 장치에 대한 펌웨어를 업데이트하는 모든 시도를 중지하므로 해당 장치에 설치된 현재 펌웨어가 계속해서 적용되게 됩니다. 펌웨어 업데이트 프로세스는 현재 펌웨어 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.

참고: 이를 사용하는 경우 Wake-on-LAN 부팅 옵션은 서버 전원을 끄는 XClarity Administrator 작업을 방해할 수 있습니다. 예를 들어 사용자 네트워크의 Wake-on-LAN 클라이언트에서 "Wake on Magic 패킷" 명령을 실행하는 경우 펌웨어 업데이트를 방해합니다.

단계 7. 다음 활성화 규칙 중 하나를 선택하십시오.

- **즉시 활성화**. 업데이트 프로세스 중에는 전체 업데이트 프로세스가 완료될 때까지 장치가 자동으로 여러 차례 다시 시작될 수 있습니다. 계속 진행하려면 장치의 모든 응용 프로그램을 정지해야 합니다.
- **지연된 활성화**. 업데이트 작업 중 일부만 수행됩니다. 업데이트 프로세스를 계속 진행하려면 장치를 다시 시작해야 합니다. 그런 다음, 업데이트 작업이 완료될 때까지 재시작이 여러 차례 반복됩니다.

  상태가 **펌웨어 유지 관리 모드 보류 중**으로 변경되면 이벤트가 발생하여 서버를 다시 시작해야 할 때 이를 알려줍니다.

  어떠한 이유로 장치가 다시 시작되면 지연된 업데이트 프로세스가 완료됩니다.

  이 활성화 규칙은 서버 및 랙 스위치에 대해서만 지원됩니다. CMM 및 Flex 스위치는 이 설정과 상관 없이 즉시 활성화됩니다.

  상태가 **펌웨어 유지 관리 모드 보류 중**으로 변경되면 이벤트가 발생하여 서버를 다시 시작해야 할 때 이를 알려줍니다.

지연된 업데이트 프로세스는 장치가 어떤 이유로든 다시 시작될 때 완료됩니다(수동 다시 시작 포함). 서버를 다시 시작해야 하는 시간 제한은 없습니다.

XClarity Administrator는 한 번에 최대 50대의 장치에 대해 활성화가 지연된 업데이트를 적용할 수 있습니다. 50대를 초과하는 장치에 대해 활성화가 지연된 업데이트를 적용하려고 할 경우 나머지 장치는 대기 상태가 됩니다. 업데이트 중인 장치가 **펌웨어 유지 관리 모드 보류 중 상태**인 경우 장치가 대기 상태에서 벗어납니다.

중요:

- 업데이트 작업 중에 XClarity Administrator가 다시 시작될 경우 업데이트 작업이 오류와 함께 중지됩니다.
- XClarity Administrator가 다운되거나 연결이 불가한 동안 **펌웨어 유지 관리 모드 보류 중** 상태의 서버가 다시 시작될 경우 서버가 BMU로 부팅되지만 XClarity Administrator는 BMU에 연결할 수 없으며 60초 후 시간이 초과되므로 베이스보드 관리 컨트롤러에 의해 시스템 전원 상태가 복원됩니다(전원이 꺼진 경우 전원을 끄고 전원이 켜진 경우 다시 시작됨).

- **우선 순위가 매겨진 활성화**. 베이스 보드 관리 컨트롤러의 펌웨어 업데이트는 즉시 활성화됩니다. 다른 모든 펌웨어 업데이트는 다음에 장치가 다시 시작될 때 활성화됩니다. 그런 다음, 업데이트 작업이 완료될 때까지 재시작이 여러 차례 반복됩니다. 이 규칙은 서버에 대해서만 지원됩니다.

  상태가 펌웨어 유지 관리 모드 보류 중으로 변경되면 이벤트가 발생하여 서버를 다시 시작해야 할 때 이를 알려줍니다.

참고: 이를 사용하는 경우 Wake-on-LAN 부팅 옵션은 서버 전원을 끄는 XClarity Administrator 작업을 방해할 수 있습니다. 예를 들어 사용자 네트워크의 Wake-on-LAN 클라이언트에서 "Wake on Magic 패킷" 명령을 실행하는 경우 펌웨어 업데이트를 방해합니다.

단계 8. **옵션:** 펌웨어 수준이 최신인 경우에도 선택한 구성 요소의 펌웨어를 업데이트하거나 선택한 구성 요소에 현재 설치된 것보다 이전 수준의 펌웨어 업데이트를 적용하려면 **강제 업데이트**를 선택하십시오.

참고: 하위 수준을 지원하는 장치 옵션, 어댑터 및 드라이브에는 이전 수준의 펌웨어를 적용할 수 있습니다. 하위 수준이 지원되는지 확인하려면 하드웨어 설명서를 참조하십시오.

단계 9. **옵션:** 전제조건 펌웨어를 설치하지 않으려고 하는 경우, **전제조건 펌웨어 설치**를 삭제하십시오. 기본값으로 전제조건 펌웨어가 설치됩니다.

참고: 사전 필수 펌웨어 업데이트에 **지연된 활성화** 또는 **우선 순위가 지정된 활성화**를 사용하는 경우 사전 필수 펌웨어를 활성화하려면 서버를 다시 시작해야 할 수 있습니다. 초기 재시작 후, 나머지 펌웨어 업데이트는 **즉시 활성화**를 사용하여 설치됩니다.

단계 10. **옵션:** **즉시 활성화**를 선택한 경우, 업데이트 중에 서버가 재부팅되면 펌웨어 업데이트가 완료된 후 **메모리 테스트**를 선택하여 메모리 테스트를 실행합니다.

이 옵션은 ThinkSystem v1 및 v2 서버(ThinkSystem SR635, SR645, SR655, SR665 서버 제외)에 지원됩니다.

단계 11. **업데이트 수행**을 클릭하여 즉시 업데이트하거나 **일정**을 클릭하여 이 업데이트가 나중에 실행되도록 예약하십시오.

필요한 경우 관리되는 장치에서 전원 작업을 수행할 수 있습니다. 전원 작업은 **지연된 활성화**가 선택되고, 장치가 "유지 관리 보류 중" 상태로 대기 중일 때 업데이트를 계속하려는 경우에 유용합니다. 이 페이지에서 관리되는 장치에 전원 동작을 수행하려면 **모든 작업 → 전원 작업**을 클릭하고 다음 전원 작업 중 하나를 클릭하십시오.
- **전원 켜기**
- **OS 종료 및 전원 끄기**
- **전원 끄기**

- OS 종료 및 다시 시작
- 다시 시작

완료한 후에

펌웨어 업데이트를 적용할 때 서버가 유지 관리 모드로 전환되지 못하는 경우 업데이트를 다시 적용해 보십시오.

업데이트가 제대로 완료되지 않은 경우 문제 해결 및 정정 작업에 대해서는 XClarity Administrator 온라인 설명서에서 펌웨어 업데이트 및 리포지토리 문제의 내용을 참조하십시오.

펌웨어 업데이트: 적용/활성화 페이지에서 다음 작업을 수행할 수 있습니다.

- 모든 **작업** → CSV로 **보기 내보내기**를 클릭하여 각 관리되는 장치에 대한 펌웨어 및 준수 정보를 내보냅니다.

  참고: CSV 파일에는 현재 보기에 있는 필터링된 정보만 포함됩니다. 보기에서 필터링되어 제외된 정보와 숨겨진 열의 정보는 포함되지 않습니다.
- 장치를 선택하고 **업데이트 취소** 아이콘( )을 클릭하여 장치에 업데이트 적용을 취소합니다.

  참고: 시작할 대기열에 있는 펌웨어 업데이트를 취소할 수 있습니다. 업데이트 프로세스가 시작된 후 업데이트 프로세스가 유지 관리 모드로 변경하거나 장치를 다시 시작하는 등 업데이트 적용 이외의 작업을 수행하는 경우에만 펌웨어 업데이트를 취소할 수 있습니다.
- 적용 / 활성화 페이지의 **상태** 열에서 펌웨어 업데이트의 상태를 직접 봅니다.
- 작업 로그에서 업데이트 프로세스의 상태를 모니터링합니다. Lenovo XClarity Administrator 메뉴에서 **모니터링** → **작업**을 클릭하십시오.

  작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

펌웨어 업데이트 작업이 완료되면 **프로비저닝** → **펌웨어 업데이트: 적용/활성화**를 클릭하여 펌웨어 업데이트: 적용/활성화 페이지로 돌아간 다음 **새로 고침** 아이콘( )을 클릭하여 장치가 준수되고 있음을 확인할 수 있습니다. 각 장치에서 활성화된 현재 펌웨어 버전은 **설치된 버전** 열에 나열되어 있습니다.

제 14 장 관리되는 서버에서 Windows 장치 드라이버 업데이트

UpdateXpress System Pack(UXSP) 창을 사용하여 배포된 Windows 운영 체제에서 OS 장치 드라이버를 업데이트할 수 있습니다.

시작하기 전에

Windows 드라이버 업데이트 페이지에서 OS 장치 드라이버를 관리 및 배포하고 관리되는 서버에 대한 전원 작업을 수행하려면, lxc-os-admin, lxc-supervisor, lxc-admin 또는 lxc-hw-admin 권한이 있어야 합니다.

펌웨어 업데이트 및 장치 드라이버 업데이트는 XClarity Administrator에서 별도의 프로세스이며, 이러한 프로세스 간에는 연결이 없습니다. 펌웨어와 동시에 장치 드라이버를 업데이트하는 것이 좋지만 XClarity Administrator은(는) 관리되는 장치의 펌웨어와 장치 드라이버 간에 준수를 유지하지는 않습니다.

이 작업 정보

Windows UpdateXpress System Pack(UXSP)에는 지원되는 Windows 버전용 및 Windows를 지원하는 Lenovo 서버용 Windows 장치 드라이버가 들어 있습니다.

Windows Server 2012 R2 이상용 장치 드라이버만 지원됩니다. XClarity Administrator는 Linux 또는 VMware 장치 드라이버 업데이트를 지원하지 않습니다.

운영 체제를 배포할 때 장치 드라이버를 설치하는 방법에 대한 내용은 베어메탈 서버에 운영 체제 설치의 내용을 참조하십시오.

절차

단계 1. **OS 장치 드라이버 업데이트용 Windows Server 구성**

Lenovo XClarity Administrator는 HTTPS 또는 HTTP 를 통해 수신 대기하는 Windows 원격 관리(WinRM) 서비스를 사용하여 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행합니다. OS 장치 드라이버를 업데이트하기 전에 대상 서버에서 WinRM 서비스를 올바르게 구성해야 합니다(OS 장치 드라이버 업데이트용 Windows Server 구성 참조).

단계 2. **OS 장치 드라이버 리포지토리 관리**

*OS 장치 드라이버 리포지토리*에는 사용 가능한 Windows 장치 드라이버 카탈로그와 관리되는 장치에 적용할 수 있는 장치 드라이버 패키지가 있습니다.

*카탈로그*에는 모든 Windows UpdateXpress System Packs (UXSPs)에 대한 정보와 Windows를 지원하는 모든 Lenovo 서버에 사용할 수 있는 장치 드라이버 업데이트에 대한 정보가 있습니다. 카탈로그는 장치 드라이버 업데이트를 장치 유형별로 구성합니다. 카탈로그를 새로 고치면 XClarity Administrator가 Lenovo 데이터 센터 지원 웹 사이트(메타데이터 .xml 및 readme .txt 파일 포함)에서 사용 가능한 UXSP에 대한 정보를 검색하고 해당 정보를 리포지토리에 저장합니다. 페이로드 파일(.exe)이 다운로드되지 않았습니다. 카탈로그 새로 고침에 대한 자세한 정보는 OS 장치 드라이버 카탈로그 새로 고침의 내용을 참조하십시오.

리포지토리에서 Windows UXSP를 다운로드하거나 가져올 수 있습니다. Windows UXSP에는 지원되는 Windows 버전용 및 Windows를 지원하는 Lenovo 서버용 Windows 장치 드라이버가 있습니다. 관리되는 서버에서 Windows 장치 드라이버를 업데이트하려면 리포지토리에서 UXSP를 사용할 수 있어야 합니다. 장치 드라이버 다운로드에 대한 자세한 정보는 Windows 장치 드라이버 다운로드 의 내용을 참조하십시오.

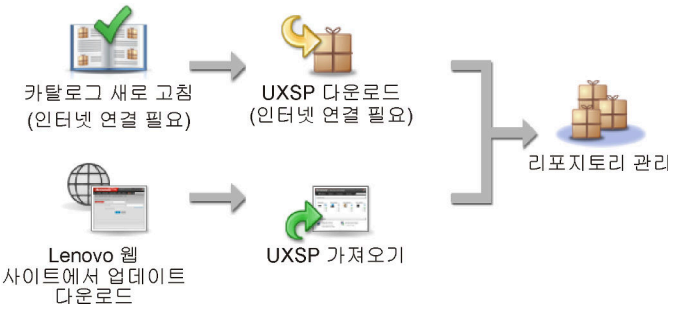
UXSP가 Windows 드라이버 업데이트 리포지토리 페이지의 개별 업데이트 탭에 있는 다운로드 상태 열의 OS 장치 드라이버 리포지토리에 저장되는지 여부를 결정할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

- **다운로드됨**. 전체 패키지 또는 개별 업데이트가 리포지토리에 저장됩니다.
- ***x*/*y*개가 다운로드됨**. 패키지의 일부 업데이트는 리포지토리에 저장됩니다. 괄호 안의 숫자는 사용 가능한 업데이트 수와 저장된 업데이트 수를 나타내며, 특정 장치 유형에 대한 업데이트는 없습니다.
- **다운로드되지 않음**. 전체 패키지 또는 개별 업데이트가 사용 가능하지만 리포지토리에 저장되지 않습니다.

참고: Windows 드라이버 업데이트 리포지토리 페이지에서 UXSP를 다운로드하거나 가져오면, 장치 드라이버가 다운로드되어 리포지토리에 저장됩니다. 펌웨어 업데이트가 삭제됩니다. 펌웨어 업데이트 다운로드 또는 가져오기에 대한 정보는 펌웨어 업데이트 리포지토리 관리의 내용을 참조하십시오.

카탈로그를 새로 고치고 UXSP를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. 인터넷에 연결되어 있지 않으면, UXSP을 웹 브라우저를 사용하는 XClarity Administrator 호스트에 대한 액세스 권한이 있는 워크 스테이션에 수동으로 다운로드할 수 있습니다. 이 UXSP 다운로드는 zip 형식 파일이며, 페이로드(.exe), 메타 데이터 (.xml) 및 변경 내역 파일(.chg) 및 추가 정보 파일 (.txt)을 비롯하여 UXSP에 대한 모든 필수 장치 드라이버 파일이 들어 있습니다.

참고: 펌웨어(fw) 파일이 필요하지 않고 제거된 메시지가 확인할 수 있습니다. Windows 장치 드라이버만 이 프로세스를 사용하여 업데이트되므로 정상입니다.



주의:

- UXSP를 가져오기 전에 압축을 풀지 마십시오.
- Windows UXSP에는 장치 드라이버 및 펌웨어 업데이트가 들어 있습니다. UXSP를 리포지토리로 가져오고 경고 메시지가 표시되면, Windows UXSP의 펌웨어 업데이트가 삭제됩니다. 장치 드라이버만 가져옵니다.

단계 3. **OS 장치 드라이버 적용**

XClarity Administrator는 관리되는 서버에 장치 드라이버를 자동으로 업데이트하지 않습니다. 장치 드라이버를 업데이트하려면 선택한 서버에 장치 드라이버를 수동으로 적용해야 합니다.

주의: 관리되는 서버에서 장치 드라이버를 업데이트하기 전에, 다음 고려 사항을 검토하고 해당하는 전제 조건 조치를 완료했는지 확인하십시오.

- 지원되지 않는 장치는 업데이트하도록 선택할 수 없습니다.
- 관리되는 서버에서 장치 드라이버를 업데이트하기 전에 장치 드라이버 업데이트 고려사항을 읽으십시오(OS 장치 드라이버 업데이트 고려 사항 참조).
- 배포하려는 UXSP 및 장치 드라이버가 리포지토리에 있는지 확인하십시오(Windows 장치 드라이버 다운로드 참조).

참고: XClarity Administrator가 처음 설치되면 카탈로그와 리포지토리가 비어 있습니다.

- XClarity Administrator는 HTTPS 또는 HTTP를 통해 수신되는 Windows 원격 관리(WinRM) 서비스를 사용하여 HTTPS가 기본값인 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행할 수 있습니다. HTTP를 사용하려면, Windows 드라이버 업데이트: 적용 페이지에서 **모든 작업 → 전역 설정**를 클릭한 다음 **Windows 드라이버 업데이트에 HTTPS 사용**을 삭제합니다.

  주의: HTTP를 사용할 때, Windows 사용자 자격 증명이 암호화 *없이* 네트워크를 통해 전송되며 일반적으로 사용 가능한 네트워크 문제 해결 도구를 사용하여 쉽게 볼 수 있습니다.

  중요:

  - 대상 서버의 Windows 원격 관리(WinRM)가 구성되어 XClarity Administrator에 정의되어 있는 것과 같은 설정(HTTPS 또는 HTTP)을 사용하도록 확인하십시오. (OS 장치 드라이버 업데이트용 Windows Server 구성 참조)
  - 대상 서버의 WinRM가 기본 인증으로 구성되어 있는지 확인하십시오.
  - HTTPS를 사용하는 경우, 대상 서버의 WinRM이 allowUnencrypted=false로 구성되어 있는지 확인하십시오.
- PowerShell이 대상 서버에서 지원되는지 확인하십시오.
- 장치 드라이버를 업데이트하기 전에 대상 서버의 전원이 켜져 있는지 확인하십시오. 서버의 전원이 켜져 있지 않으면 대상 서버를 선택하고 **모든 작업 → 전원 작업 → 전원 켜기**를 클릭하십시오.
- XClarity Administrator에 호스트 운영 체제에 액세스하는 데 필요한 정보가 있는지 확인하십시오(관리되는 서버에서 운영 체제에 대한 액세스 관리 참조).
- OS 장치 드라이버를 업데이트할 때 도메인 계정을 사용하려면 필요한 구성 파일을 생성했는지 확인하십시오(OS 장치 드라이버 업데이트를 위한 도메인 계정 구성 참조).
- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 실행 중인 작업에 의해 잠긴 관리되는 서버에서는 장치 드라이버를 업데이트할 수 없습니다. 다른 업데이트 작업이 대상 서버에서 실행 중인 경우 이 업데이트 작업은 현재 업데이트 작업이 완료될 때까지 대기합니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.

OS 장치 드라이버 업데이트에 대한 자세한 정보는 Windows 장치 드라이버 적용의 내용을 참조하십시오.

OS 장치 드라이버 업데이트 고려 사항

Lenovo XClarity Administrator를 사용하여 관리되는 장치의 OS 장치 드라이버 업데이트를 시작하기 전에 다음 중요 고려사항을 검토하십시오.

참고: Windows 드라이버 업데이트 페이지에서 장치 드라이버를 관리 및 배포하고 관리되는 서버에 대한 전원 작업을 수행하려면 lxc-os-admin, lxc-supervisor, lxc-admin 또는 lxc-hw-admin 권한이 있어야 합니다.

네트워크 고려사항

- UpdateXpress System Pack(UXSP)를 다운로드하기 전에 필수 포트와 인터넷 주소가 사용 가능해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성 및 방화벽 및 프록시 서버의 내용을 참조하십시오.
- 운영 체제에 액세스하려면 XClarity Administrator가 관리 및 데이터 네트워크에 액세스할 수 있어야 합니다.
- XClarity Administrator가 XClarity Administrator 네트워크 액세스를 구성할 때 선택한 네트워크 인터페이스(Eth0 또는 Eth1)를 통해 대상 서버(베이스보드 관리 컨트롤러 및 서버의 데이터 네트워크)와 통신할 수 있어야 하고 인터페이스가 IPv4 주소 또는 IPv6 자동 ULA 주소로 구성되어야 합니다.

운영 체제 배포에 사용할 인터페이스를 지정하려면 네트워크 액세스 구성의 내용을 참조하십시오.

운영 체제 배포 네트워크 및 인터페이스에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 네트워크 고려사항의 내용을 참조하십시오.

- IP 주소는 호스트 운영 체제에서 고유해야 합니다.
- XClarity Administrator는 HTTPS 또는 HTTP를 통해 수신되는 Windows 원격 관리(WinRM) 서비스를 사용하여 HTTPS가 기본값인 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행할 수 있습니다. HTTP를 사용하려면, Windows 드라이버 업데이트: 적용 페이지에서 **모든 작업 → 전역 설정**를 클릭한 다음 **Windows 드라이버 업데이트에 HTTPS 사용**을 삭제합니다.

  주의: HTTP를 사용할 때, Windows 사용자 자격 증명이 암호화 *없이* 네트워크를 통해 전송되며 일반적으로 사용 가능한 네트워크 문제 해결 도구를 사용하여 쉽게 볼 수 있습니다.

관리되는 장치 고려사항

- ThinkAgile, ThinkSystem SR635 및 ThinkSystem SR655 서버의 경우 Windows 장치 드라이버가 지원되지 않습니다.
- ThinkSystem, Lenovo System x 및 Lenovo Flex System 서버만 지원됩니다.
- XClarity Administrator는 관리 컨트롤러와 운영 체제 간의 관계를 유효성 검증하지 않습니다. 베이스보드 관리 컨트롤러를 사용하여 서버의 전원을 켜거나 끌 수 있습니다.
- LAN-over-USB 인터페이스가 사용 가능한지 확인하십시오. LAN-over-USB는 OS 장치 드라이버를 업데이트할 때 사용됩니다.

운영 체제 및 장치 드라이버 고려사항

- 다음 운영 체제의 장치 드라이버를 업데이트할 수 있습니다.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  참고: XClarity Administrator 버전이 릴리스되면 XClarity Administrator는 Microsoft에서 지원하는 Windows 버전에서만 테스트됩니다.
- 대상 서버에서 HTTPS에 대해 Windows 원격 관리(WinRM)가 구성되어야 합니다(OS 장치 드라이버 업데이트용 Windows Server 구성 참조).
- PowerShell이 대상 서버에서 지원되어야 합니다.
- OS IP 주소 및 자격 증명을 포함하여 대상 서버의 호스트 운영 체제에 액세스하는 데 필요한 정보를 제공해야 합니다(관리되는 서버에서 운영 체제에 대한 액세스 관리 참조). 관리자 권한이 있는 사용자 계정에 대한 자격 증명을 제공해야 합니다.
- XClarity Administrator는 호환되지 않는 장치 드라이버만 업데이트합니다. 서버의 버전이 선택한 UXSP 버전보다 이전 버전인 경우 장치 드라이버가 호환되지 않습니다. 선택한 UXSP의 버전과 같거나 이후 버전의 장치 드라이버는 건너 뜁니다.
- 장치 드라이버 준수는 하드웨어가 있는 경우에만 정확합니다. 하드웨어가 없어도 장치 드라이버는 여전히 서버에 적용됩니다. 누락된 하드웨어가 서버에 추가되면, Windows에서 최신 버전을 로드합니다.
- System x 서버는 XClarity Administrator와 함께 제공되는 일부 사전 정의된 장치 드라이버를 지원하지 않습니다. 이러한 서버에 장치 드라이버를 배포하려면, 필요한 장치 드라이버만 포함하는 사용자 정의 프로필을 만드십시오.

OS 장치 드라이버 리포지토리 관리

*OS 장치 드라이버 리포지토리*에는 카탈로그 및 다운로드된 Windows 장치 드라이버가 있습니다.

이 작업 정보

*카탈로그*에는 모든 Windows UpdateXpress System Packs (UXSPs)에 대한 정보와 Windows를 지원하는 모든 Lenovo 서버에 사용할 수 있는 장치 드라이버 업데이트에 대한 정보가 있습니다. 카탈로그는 장치 드라이버 업데이트를 장치 유형별로 구성합니다. 카탈로그를 새로 고치면 XClarity Administrator가 Lenovo 데이터 센터 지원 웹 사이트(메타데이터 .xml 및 readme .txt 파일 포함)에서 사용 가능한 UXSP에 대한 정보를 검색하고 해당 정보를 리포지토리에 저장합니다. 페이로드 파일(.exe)이 다운로드되지 않았습니다. 카탈로그 새로 고침에 대한 자세한 정보는 OS 장치 드라이버 카탈로그 새로 고침의 내용을 참조하십시오.

Windows UpdateXpress System Pack(UXSP)에는 지원되는 Windows 버전용 및 Windows를 지원하는 Lenovo 서버용 Windows 장치 드라이버가 들어 있습니다. 리포지토리에서 Windows UXSP를 다운로드하거나 가져올 수 있습니다. Windows UXSP에는 지원되는 Windows 버전용 및 Windows를 지원하는 Lenovo 서버용 Windows 장치 드라이버가 있습니다. 관리되는 서버에서 Windows 장치 드라이버를 업데이트하려면 리포지토리에서 UXSP를 사용할 수 있어야 합니다.장치 드라이버 다운로드에 대한 자세한 정보는 Windows 장치 드라이버 다운로드 의 내용을 참조하십시오.

카탈로그를 새로 고치고 UXSP를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. 인터넷에 연결되어 있지 않으면, UXSP을 웹 브라우저를 사용하는 XClarity Administrator 호스트에 대한 액세스 권한이 있는 워크 스테이션에 수동으로 다운로드할 수 있습니다. 이 UXSP 다운로드는 zip 형식 파일이며, 페이로드(.exe), 메타 데이터 (.xml) 및 변경 내역 파일(.chg) 및 추가 정보 파일(.txt)을 비롯하여 UXSP에 대한 모든 필수 장치 드라이버 파일이 들어 있습니다.

UXSP가 리포지토리에 다운로드되면 팩의 각 장치 드라이버에 대한 정보가 Windows 드라이버 업데이트 리포지토리 페이지에 추가됩니다. 이러한 정보에는 릴리스 날짜, 크기 및 심각도 등이 있습니다. 심각도는 업데이트 적용에 대한 영향과 필요를 표시하며 환경이 영향을 받는 정도를 평가하는 데 도움을 줍니다.

- **초기 릴리스**. 이는 장치 드라이버의 첫 번째 릴리스입니다.
- **위험**. 이 장치 드라이버에는 데이터 손상, 보안 또는 안정성 문제를 위한 긴급한 수정사항이 포함되어 있습니다.
- **제안됨**. 이 장치 드라이버에는 발생하기 쉬운 문제에 대한 중요한 수정 사항이 포함되어 있습니다.
- **중요하지 않음**. 이 장치 드라이버에는 사소한 수정 사항, 성능 개선 사항 및 텍스트 변경 사항이 포함되어 있습니다.

참고:

- 심각도는 이전에 릴리스된 버전의 장치 드라이버와 관련됩니다. 예를 들어 설치된 장치 드라이버가 v1.01이고 업데이트 v1.02가 위험 상태이며 업데이트 v1.03이 권장 상태인 경우 설치가 누적되므로 업데이트 1.02부터 1.03까지는 권장되지만 업데이트 v1.01부터 v1.03까지는 위험 상태입니다 (v1.03이 v1.02 위험 문제를 포함함).
- 업데이트가 특정 시스템 유형에만 위험하거나 권장되는 특수한 상황이 발생할 수 있습니다. 추가 정보는 릴리스 정보를 참조하십시오.

절차

리포지토리에서 사용 가능한 UXSP 및 장치 드라이버를 보려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 리포지토리**를 클릭하십시오. 장치 유형별로 구성된 사용 가능한 UXSP 목록이 있는 Windows 드라이버 업데이트 리포지토리 페이지가 표시됩니다.

단계 2. 서버 유형을 확장한 다음 해당 서버 유형에 사용 가능한 UXSP를 확장하여 해당 서버 유형에 사용할 수 있는 장치 드라이버를 나열하십시오.

테이블 열을 정렬하고 모두 **확장** 아이콘( ) 및 모두 **축소** 아이콘( )을 클릭하여 특정 장치 드라이버를 보다 쉽게 찾을 수 있습니다. 또한 특정 사용 기간의 장치 드라이버, 모든 서버 유형의 장치 드라이버 또는 관리되는 서버 유형의 장치 드라이버만 나열하기 위해 **표시** 메뉴에서 옵션을 선택하거나 **필터** 필드에 텍스트를 입력하여 표시되는 서버 유형 및 장치 드라이버 목록을 필터링할 수 있습니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **카탈로그 새로 고침**을 클릭하여 사용 가능한 UXSP에 대한 최신 정보를 검색합니다.

  이 정보 검색을 완료하는 데 몇 분이 걸릴 수 있습니다. 자세한 정보는 OS 장치 드라이버 카탈로그 새로 고침의 내용을 참조하십시오.
- 카탈로그를 새로 고친 다음 **다운로드** 아이콘( )을 클릭하여 XClarity Administrator를 사용하는 UXSP 및 장치 드라이버를 다운로드합니다. UXSP 및 장치 드라이버를 다운로드하여 리포지토리에 추가하면 상태가 "다운로드됨"으로 변경됩니다.

  UXSP 및 장치 드라이버 다운로드에 대한 자세한 정보는 Windows 장치 드라이버 다운로드 의 내용을 참조하십시오.
- 웹에서 워크스테이션으로 수동으로 다운로드한 UXSP 또는 XClarity Administrator에서 내보낸 장치 드라이버를 가져옵니다(Windows 장치 드라이버 다운로드 참조).
- **다운로드 취소** 아이콘( )을 클릭하여 현재 진행 중인 선택한 다운로드를 중지합니다.
- **삭제** 아이콘( )을 클릭하여 선택한 UXSP 또는 개별 장치 드라이버를 리포지토리에서 삭제합니다.

OS 장치 드라이버 카탈로그 새로 고침

OS 장치 드라이버 카탈로그에는 모든 Windows UpdateXpress System Pack(UXSP)에 대한 정보와 Windows 장치 드라이버를 지원하는 모든 Lenovo 서버에 사용할 수 있는 장치 드라이버에 대한 정보가 있습니다.

시작하기 전에

Lenovo XClarity Administrator가 인터넷에 연결되어 있는지 확인하십시오.

이 작업 정보

카탈로그를 새로 고치면 XClarity Administrator가 Lenovo 데이터 센터 지원 웹 사이트(메타데이터 .xml 및 readme .txt 파일 포함)에서 사용 가능한 UXSP에 대한 정보를 검색하고 해당 정보를 리포지토리에 저장합니다. 페이로드 파일(.exe)이 다운로드되지 않았습니다. 관리되는 서버에서 장치 드라이버를 업데이트하려면 먼저 원하는 UXSP 및 OS 장치 드라이버 페이로드를 다운로드해야 합니다. 장치 드라이버 다운로드에 대한 자세한 정보는 Windows 장치 드라이버 다운로드 의 내용을 참조하십시오.

참고: 카탈로그 새로 고침을 완료하려면 몇 분 정도가 걸릴 수 있습니다.

절차

카탈로그를 새로 고치려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 리포지토리**를 클릭하여 Windows 드라이버 업데이트 리포지토리 페이지를 표시합니다.

단계 2. **카탈로그 새로 고침**을 클릭하고 다음 옵션 중 하나를 클릭하여 사용 가능한 최신 UXSP에 대한 정보를 얻으십시오.

- **선택 항목 새로 고침 - 최신 항목 한정**. 선택한 서버에만 사용 가능한 최신 UXSP 버전에 대한 정보를 검색합니다.
- **모두 새로 고침 - 최신 항목 한정**. 지원되는 모든 서버의 최신 UXSP 버전에 대한 정보를 검색합니다.
- **선택 항목 새로 고침**. 선택한 서버에만 사용 가능한 모든 UXSP 버전에 대한 정보를 검색합니다.
- **모두 새로 고침**. 지원되는 모든 서버에 사용 가능한 모든 UXSP 버전에 대한 정보를 검색합니다.

단계 3. **카탈로그 새로 고침**을 클릭하여 즉시 새로 고치거나 **일정**을 클릭하여 이 새로 고침이 나중에 실행되도록 예약하십시오.

Windows 장치 드라이버 다운로드

Windows UpdateXpress System Pack(UXSP)에는 지원되는 Windows 버전용 및 Windows를 지원하는 Lenovo 서버용 Windows 장치 드라이버가 들어 있습니다. 리포지토리에서 Windows UXSP를 다운로드하거나 가져올 수 있습니다. Windows UXSP에는 지원되는 Windows 버전용 및 Windows를 지원하는 Lenovo 서버용 Windows 장치 드라이버가 있습니다. 관리되는 서버에서 Windows 장치 드라이버를 업데이트하려면 리포지토리에서 UXSP를 사용할 수 있어야 합니다.

시작하기 전에

UpdateXpress System Pack(UXSP)를 다운로드하기 전에 필요한 모든 포트와 인터넷 주소가 사용 가능한지 확인하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성 및 방화벽 및 프록시 서버의 내용을 참조하십시오.

XClarity Administrator를 사용하여 UXSP를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다.

Internet Explorer 및 Microsoft Edge 웹 브라우저에는 4GB의 업로드 제한이 있습니다. 가져오는 파일의 크기가 4GB보다 큰 경우, 다른 웹 브라우저(예, Chrome 또는 Firefox).

이 작업 정보

카탈로그를 새로 고치고 UXSP를 다운로드하려면 XClarity Administrator가 인터넷에 연결되어 있어야 합니다. XClarity Administrator가 인터넷에 연결되어 있지 않으면 웹 브라우저를 사용하여 XClarity Administrator 호스트에 대한 네트워크 액세스가 있는 워크스테이션에 파일을 수동으로 다운로드한 다음 업데이트를 펌웨어 업데이트 리포지토리로 가져올 수 있습니다.

UXSP가 Windows 드라이버 업데이트 리포지토리 페이지의 **다운로드 상태** 열에 있는 리포지토리에 저장되는지 여부를 판별할 수 있습니다. 이 열에는 다음 값이 포함됩니다.

- **다운로드됨**. UXSP의 모든 장치 드라이버 또는 개별 장치 드라이버가 리포지토리에 다운로드됩니다.
- *x* / *y* **다운로드됨**. UXSP의 전체 장치 드라이버가 아닌 일부가 리포지토리에 다운로드됩니다. 괄호 안의 숫자는 사용 가능한 장치 드라이버 수와 다운로드 장치 드라이버 수를 나타냅니다.

- **다운로드되지 않음**. UXSP 또는 개별 장치 드라이버는 Lenovo 지원 사이트에 있지만 리포지토리에 다운로드되지는 않습니다.

UXSP 및 장치 드라이버에 사용 가능한 공간이 50% 이상 가득 차면 Windows 드라이버 업데이트 리포지토리 페이지에 메시지가 표시됩니다. 리포지토리가 85%보다 많이 차면 페이지에 다른 메시지가 표시됩니다. 리포지토리에서 사용되는 공간을 줄이기 위해 대상 파일을 선택한 후 **삭제** 아이콘( )을 클릭하여 사용하지 않는 파일을 제거할 수 있습니다. 자세한 정보는 디스크 공간 관리의 내용을 참조하십시오.

주의: Windows UXSP에는 장치 드라이버 및 펌웨어 업데이트가 들어 있습니다. UXSP를 리포지토리로 가져오고 경고 메시지가 표시되면, Windows UXSP의 펌웨어 업데이트가 삭제됩니다. 장치 드라이버만 가져옵니다.

절차

UXSP 및 특정 장치 드라이버를 다운로드하려면, 다음 절차 중 하나를 수행하십시오.

- XClarity Administrator가 인터넷에 연결된 경우:
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 리포지토리**를 클릭하여 Windows 드라이버 업데이트 리포지토리 페이지를 표시합니다.
  2. **카탈로그 새로 고침**을 클릭하고 다음 옵션 중 하나를 클릭하여 사용 가능한 최신 UXSP에 대한 정보를 얻으십시오.
     - **선택 항목 새로 고침 - 최신 항목 한정**. 선택한 서버에만 사용 가능한 최신 UXSP 버전에 대한 정보를 검색합니다.
     - **모두 새로 고침 - 최신 항목 한정**. 지원되는 모든 서버의 최신 UXSP 버전에 대한 정보를 검색합니다.
     - **선택 항목 새로 고침**. 선택한 서버에만 사용 가능한 모든 UXSP 버전에 대한 정보를 검색합니다.
     - **모두 새로 고침**. 지원되는 모든 서버에 사용 가능한 모든 UXSP 버전에 대한 정보를 검색합니다.

     참고: 카탈로그 새로 고침을 완료하려면 몇 분 정도가 걸릴 수 있습니다.
  3. 서버 유형을 확장하여 사용 가능한 UXSP 목록을 표시합니다. UXSP를 확장하여 사용 가능한 장치 드라이버 목록을 확인하십시오.

4. 다운로드할 대상 UXSP 및 장치 드라이버를 하나 이상 선택하십시오.
5. **선택 항목 다운로드** 아이콘()을 클릭하십시오.
6. **다운로드**를 클릭하여 즉시 다운로드하거나 **일정**을 클릭하여 이 다운로드가 나중에 실행되도록 예약하십시오.

   UXSP를 다운로드하는 데 몇 분 정도 걸릴 수 있습니다. UXSP 및 장치 드라이버가 다운로드되어 리포지토리에 저장되면 카탈로그의 행이 강조표시되고 **다운로드 상태** 열이 "다운로드됨"으로 변경됩니다.

   작업 로그에서 다운로드 프로세스의 상태를 모니터링할 수 있습니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오. 작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

- XClarity Administrator가 인터넷에 연결되지 *않은* 경우:
  1. Lenovo 데이터 센터 지원 웹 사이트에서 XClarity Administrator 호스트에 대한 네트워크 연결이 있는 워크스테이션으로 UXSP를 다운로드하십시오.
  2. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 리포지토리**를 클릭하여 Windows 드라이버 업데이트 리포지토리 페이지를 표시합니다.
  3. **가져오기** 아이콘()을 클릭하십시오.
  4. **파일 선택**을 클릭하고 워크스테이션에서 UXSP 위치를 찾아보십시오.
  5. UXSP .zip 파일(가져오기 전에 zip 파일의 압축을 풀지 않음)을 클릭한 다음 **열기**를 클릭하십시오.

     UXSP .zip 파일에는 메타데이터 파일(.xml), 페이로드(.exe), 변경 기록 파일(.chg) 및 readme 파일(.txt)이 들어 있습니다.
  6. **가져오기**를 클릭하십시오.

     작업 로그에서 가져오기 프로세스의 상태를 모니터링할 수 있습니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오. 작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

완료한 후에

이 페이지에서 선택한 UXSP에 다음 작업을 수행할 수 있습니다.

- **다운로드 취소** 아이콘()을 클릭하여 현재 진행 중인 다운로드를 취소합니다.
- **삭제** 아이콘()을 클릭하여 UXSP와 연관된 모든 파일을 삭제합니다.

OS 장치 드라이버 업데이트용 Windows Server 구성

Lenovo XClarity Administrator는 HTTPS 또는 HTTP 를 통해 수신 대기하는 Windows 원격 관리(WinRM) 서비스를 사용하여 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행합니다. OS 장치 드라이버를 업데이트하기 전에 대상 서버에서 WinRM 서비스를 올바르게 구성해야 합니다.

시작하기 전에

필수 포트가 사용 가능해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 포트 사용 가능성의 내용을 참조하십시오.

OS 장치 드라이버를 업데이트하기 전에 Windows Server를 구성하는 방법에 대한 자세한 내용은 XClarity Administrator: OS 장치 드라이버 업데이트 준비(백서)의 내용을 참조하십시오.

절차

Windows Server를 구성하여 OS 장치 드라이버 업데이트를 지원하려면, 다음 단계를 완료하십시오.

- HTTPS의 경우
  1. 각 대상 Windows 시스템에서 서버 인증서에 서명하고 서버 인증서를 설치하십시오.

     중요: 인증서에는 다음 정보가 포함되어야 합니다.

     - 주제에서 도메인 구성 요소가 설정되어 있는지 확인합니다(예, DC=labs, DC=com, DC=company).
     - 주제 대체 이름에서 DNS 이름 및 호스트 IP 주소가 설정되어 있는지 확인하십시오(예, DNS Name=node1325C554A6F.labs.company.com 및 IP Address=10.245.43.149).
  2. 관리 명령 프롬프트에서 다음 명령 중 하나를 실행하여 HTTPS 연결을 통해 원격 관리 명령 및 데이터를 구성한 다음 제안된 구성 변경 사항을 확인하십시오.

     -
     ```
     winrm quickconfig -transport:https
     ```
     -
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     WinRM 설명서에 따라 WinRM HTTPS 수신기를 수동으로 설정하려면, HTTPS 웹 페이지에 대한 WinRM을 구성하는 방법의 내용을 참조하십시오.
  3. 관리 명령 프롬프트에서 다음 명령을 실행하여 로컬 Windows의 기본 인증 사용자를 사용합니다.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  4. 컴플라이언스 검사 및 드라이버 업데이트 수행에서 발생 가능한 시간 초과 및 WinRM 요청 오류 전송을 방지하려면, 관리 명령 프롬프트에서 다음 명령을 실행하여 WinRM 응답 시간 초과의 기본값을 늘리십시오. 280000의 값을 권장합니다. 자세한 정보는 Windows Remote 설치 및 구성 관리 웹 페이지의 내용을 참조하십시오.
     ```
     winrm set winrm/config @{MaxTimeoutms="280000"}
     ```
  5. WinRM HTTPS 수신기용으로 구성한 방화벽에서 포트를 여십시오. 기본 HTTPS 포트는 5986입니다. 예를 들면 다음과 같습니다.
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
     protocol=TCP localport=5986
     ```
  6. HTTPS 수신기를 사용하는 경우 다음 단계를 수행하여 인증서를 XClarity Administrator 신뢰 저장소에 추가합니다. 인증서를 신뢰 저장소에 추가하면 XClarity Administrator가 연결하는 WinRM HTTPS 수신기를 신뢰할 수 있습니다. Windows 원격 관리 서비스에 대해 신뢰할 수 있어야 하는 추가 인증 경로에 대해 다음 단계를 반복하십시오.

     a. 대상 Windows 시스템에 대한 서버 인증서에 서명하는 데 사용한 인증 기관 루트 인증서를 확인하고 수집하십시오. CA 루트 인증서에 액세스할 수 없는 경우 인증서 경로 자체에서 서버 인증서 자체 또는 다른 인증서를 수집하십시오.

     b. XClarity Administrator 메뉴 표시줄에서 **관리 → 보안**을 클릭하여 보안 페이지를 표시하십시오.

     c. 인증서 관리 섹션에서 **신뢰할 수 있는 인증서**를 클릭하십시오.

     d. **만들기** 아이콘( )을 클릭하여 인증서 추가 대화 상자를 표시하십시오.

     e. 1단계에서 수집한 인증서 파일을 찾아보거나 인증서 파일의 내용을 텍스트 상자에 복사하십시오/붙여 넣으십시오.

     f. **만들기**를 클릭하십시오.
  7. WinRM 수신기가 대상 Windows 시스템에서 실행되면 XClarity Administrator는 이러한 시스템에 연결되고 장치 드라이버 업데이트를 수행할 수 있습니다.
- HTTP의 경우
  1. 관리 명령 프롬프트에서 다음 명령을 실행하여 HTTP 연결을 통해 원격 관리 명령 및 데이터를 구성한 다음 제안된 구성 변경 사항을 확인하십시오.
     ```
     winrm quickconfig
     ```

2. 관리 명령 프롬프트에서 다음 명령을 실행하여 로컬 Windows의 기본 인증 사용자를 사용합니다.
   `winrm set winrm/config/service/Auth @{Basic="true"}`
3. 관리 명령 프롬프트에서 다음 명령을 실행하여 이 시스템의 업데이트 명령에 필요한 메모리를 할당하십시오.
   `winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}`
4. 관리 명령 프롬프트에서 다음 명령을 실행하여 암호화되지 않은 데이터를 허용하십시오.
   `winrm set winrm/config/service @{AllowUnencrypted="true"}`
5. WinRM HTTP 수신기용으로 구성한 방화벽에서 포트를 여십시오. 기본 HTTPS 포트는 5985입니다. 예를 들면 다음과 같습니다.
   `netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow protocol=TCP localport=5985`

WinRM 수신기가 대상 Windows 시스템에서 실행되면 XClarity Administrator는 이러한 시스템에 연결되고 장치 드라이버 업데이트를 수행할 수 있습니다.

OS 장치 드라이버 업데이트를 위한 도메인 계정 구성

도메인 컨트롤러로 권한을 쉽게 관리하기 위해 도메인 계정을 사용할 수 있습니다. OS 장치 드라이버를 업데이트할 때 도메인 계정을 사용하려면 도메인 계정을 구성해야 합니다.

시작하기 전에

도메인 계정을 구성하기 전에 관리되는 Windows 서버가 도메인 네트워크에 있는지 확인하십시오.

Lenovo XClarity Administrator에 Windows 사용자 계정을 추가할 때 `USER@DOMAIN` 형식을 사용하십시오. `DOMAIN/USER` 형식은 지원되지 않습니다.

절차

도메인 계정을 구성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 적용**을 클릭하십시오. Windows 드라이버 업데이트: 적용 페이지가 표시됩니다.

단계 2. **모든 작업 → 도메인 계정 관리**를 클릭하십시오. 도메인 계정 페이지가 표시됩니다.

단계 3. **만들기** 아이콘()을 클릭하여 도메인 계정의 영역을 추가하십시오. 영역 만들기 대화 상자가 표시됩니다.

단계 4. 영역의 이름 및 하나 이상의 핵심 배포 센터 호스트 이름을 지정하십시오. **추가** 아이콘()을 사용하여 호스트 이름을 더 추가하고 **제거** 아이콘()을 사용하여 호스트 이름을 제거하십시오.

단계 5. **확인**을 클릭하여 영역을 저장하십시오.

단계 6. 원하는 경우 도메인 계정 페이지에서 기본으로 사용할 영역을 선택하십시오.

단계 7. **저장**을 클릭하여 구성을 저장하십시오.

완료한 후에

도메인 계정 구성 페이지에서 다음 작업을 수행할 수 있습니다.

- **편집** 아이콘()을 클릭하여 선택한 영역을 수정합니다.
- **삭제** 아이콘()을 클릭하여 선택된 영역을 삭제합니다.

전역 Windows 장치 드라이버 업데이트 설정 구성

Windows 장치 드라이버 업데이트를 적용하면 전역 설정이 기본 설정으로 사용됩니다.

이 작업 정보

전역 설정 페이지에서 다음 설정을 구성할 수 있습니다.
- Windows 드라이버 업데이트에 HTTPS 사용
- 설치된 하드웨어의 장치 드라이버 표시

절차

모든 서버에 사용할 전역 설정을 구성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 적용**을 클릭하십시오. Windows 드라이버 업데이트: 적용 페이지가 표시됩니다.

단계 2. **모든 작업 → 전역 설정**을 클릭하여 전역 설정: Windows 드라이버 업데이트 적용 대화 상자를 표시하십시오.

단계 3. 다음 옵션을 선택하십시오.

- HTTPS를 통해 청취되는 Windows 원격 관리(WinRM) 서비스를 사용하여 HTTPS가 기본값인 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행하려면 **Windows 드라이버 업데이트에 HTTPS 사용**을 선택하십시오.

  HTTP를 사용하려면 이 설정을 선택 취소하십시오.

  주의: HTTP를 사용할 때, Windows 사용자 자격 증명이 암호화 *없이* 네트워크를 통해 전송되며 일반적으로 사용 가능한 네트워크 문제 해결 도구를 사용하여 쉽게 볼 수 있습니다.
- 관리되는 하드웨어의 장치 드라이버만 나열하려면 **설치된 하드웨어의 장치 드라이버 표시**를 선택하십시오.

  가져온 각 UXSP(UpdateXpress System Pack)에 있는 모든 장치 드라이버를 나열하려면 이 설정을 선택 취소하십시오.

  중요: 이 옵션을 선택한 후 Windows 드라이버 업데이트: 적용 페이지에서 **준수 검사** 아이콘()을 클릭하여 준수 검사를 수행해야 합니다.

단계 4. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

Windows 장치 드라이버 적용

Windows를 실행하는 관리되는 서버에 장치 드라이버를 적용할 수 있습니다.

시작하기 전에

- Lenovo XClarity Administrator는 HTTPS 또는 HTTP 를 통해 수신 대기하는 Windows 원격 관리(WinRM) 서비스를 사용하여 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행합니다. OS 장치 드라이버를 업데이트하기 전에 대상 서버에서 WinRM 서비스를 올바르게 구성해야 합니다(OS 장치 드라이버 업데이트용 Windows Server 구성 참조).
- 지원되지 않는 장치는 업데이트하도록 선택할 수 없습니다.

- 관리되는 서버에서 장치 드라이버를 업데이트하기 전에 장치 드라이버 업데이트 고려사항을 읽으십시오(OS 장치 드라이버 업데이트 고려 사항 참조).
- 배포하려는 UXSP 및 장치 드라이버가 리포지토리에 있는지 확인하십시오(Windows 장치 드라이버 다운로드 참조).

  참고: XClarity Administrator가 처음 설치되면 카탈로그와 리포지토리가 비어 있습니다.
- XClarity Administrator는 HTTPS 또는 HTTP를 통해 수신되는 Windows 원격 관리(WinRM) 서비스를 사용하여 HTTPS가 기본값인 대상 Windows 시스템에서 장치 드라이버 업데이트 명령을 실행할 수 있습니다. HTTP를 사용하려면, Windows 드라이버 업데이트: 적용 페이지에서 **모든 작업 → 전역 설정**를 클릭한 다음 **Windows 드라이버 업데이트에 HTTPS 사용**을 삭제합니다.

  주의: HTTP를 사용할 때, Windows 사용자 자격 증명이 암호화 *없이* 네트워크를 통해 전송되며 일반적으로 사용 가능한 네트워크 문제 해결 도구를 사용하여 쉽게 볼 수 있습니다.

  중요:

  - 대상 서버의 Windows 원격 관리(WinRM)가 구성되어 XClarity Administrator에 정의되어 있는 것과 같은 설정(HTTPS 또는 HTTP)을 사용하도록 확인하십시오. (OS 장치 드라이버 업데이트용 Windows Server 구성 참조)
  - 대상 서버의 WinRM가 기본 인증으로 구성되어 있는지 확인하십시오.
  - HTTPS를 사용하는 경우, 대상 서버의 WinRM이 allowUnencrypted=false로 구성되어 있는지 확인하십시오.
- PowerShell이 대상 서버에서 지원되는지 확인하십시오.
- 장치 드라이버를 업데이트하기 전에 대상 서버의 전원이 켜져 있는지 확인하십시오. 서버의 전원이 켜져 있지 않으면 대상 서버를 선택하고 **모든 작업 → 전원 작업 → 전원 켜기**를 클릭하십시오.
- XClarity Administrator에 호스트 운영 체제에 액세스하는 데 필요한 정보가 있는지 확인하십시오(관리되는 서버에서 운영 체제에 대한 액세스 관리 참조).
- OS 장치 드라이버를 업데이트할 때 도메인 계정을 사용하려면 필요한 구성 파일을 생성했는지 확인하십시오(OS 장치 드라이버 업데이트를 위한 도메인 계정 구성 참조).
- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 실행 중인 작업에 의해 잠긴 관리되는 서버에서는 장치 드라이버를 업데이트할 수 없습니다. 다른 업데이트 작업이 대상 서버에서 실행 중인 경우 이 업데이트 작업은 현재 업데이트 작업이 완료될 때까지 대기합니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.

이 작업 정보

XClarity Administrator는 호환되지 않는 장치 드라이버만 업데이트합니다. 서버의 버전이 선택한 UXSP 버전보다 이전 버전인 경우 장치 드라이버가 호환되지 않습니다. 선택한 UXSP의 버전과 같거나 이후 버전의 장치 드라이버는 건너 뜁니다.

절차

관리되는 서버에 Windows 장치 드라이버를 적용하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → Windows 드라이버 업데이트: 적용**을 클릭하여 Windows 드라이버 업데이트: 적용 페이지를 표시합니다.

중요:

- 대상 서버에서 장치 드라이버를 찾고 준수 여부를 확인하려면 대상 서버를 선택하고 준수 검사를 실행해야 합니다. 준수 검사를 처음 실행한 후, 행을 확장하여 대상 서버의 장치 드라이버 목록을 볼 수 있습니다.
- **Windows 시스템** 열은 호스트 운영 체제의 호스트 이름 또는 IP 주소를 식별합니다.
- **서버** 열은 관리되는 서버의 이름과 IP 주소를 식별합니다.

단계 2. 하나 이상의 대상 서버 및 장치 드라이버를 선택하십시오.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 서버 목록을 필터링할 수도 있습니다.

팁:

- 특정 운영 체제의 모든 장치 드라이버를 업데이트하도록 선택하거나 운영 체제를 확장하고 특정 장치만 업데이트하도록 선택할 수 있습니다.
- **업데이트 상태** 열에는 각 서버의 인증 상태와 각 장치 드라이버의 업데이트 상태가 표시됩니다.
- OS **자격 증명** 열에는 운영 체제를 인증하는 데 사용되는 저장된 자격 증명이 표시됩니다(예, "901 – company\USER1").

  대상 서버의 호스트 운영 체제에 OS 자격 증명이 정의되어 있지 않으면 OS 자격 증명 편집 대화 상자가 표시됩니다. 단일 대상 서버의 경우 이 작업에 사용할 사용자 이름과 암호를 지정하십시오. 여러 대상 서버의 경우 각 서버에 사용할 저장된 자격 증명을 선택하십시오. 그런 다음 **저장**을 클릭하십시오.

  참고: OS 자격 증명 편집 대화 상자에서 선택한 OS 자격 증명이 호스트 운영 체제에 대해 저장되지 않습니다. OS 자격 증명을 저장하려면 관리되는 서버에서 운영 체제에 대한 액세스 관리XClarity Administrator 온라인 설명서에서 .

단계 3. **인증 검사** 아이콘( )을 클릭하여 인증 및 사전 필수 구성 요소 검사를 실행합니다.

XClarity Administrator는 OS **자격 증명** 열에 나열된 저장된 자격 증명을 사용하여 호스트 운영 체제에 연결하고 OS 버전을 판별하고 WinRM이 사용되는지 확인하고 추가 사전 필수 구성 요소 검사를 수행한 다음 호스트 OS와 연결을 끊습니다.

호스트 운영 체제에 대한 저장된 자격 증명 변경에 대한 내용은 관리되는 서버에서 운영 체제에 대한 액세스 관리의 내용을 참조하십시오.

단계 4. 각 대상 서버에 대해 **이행 대상** 열에서 장치 드라이버를 업데이트하는 데 사용할 대상 UXSP를 선택하십시오.

단계 5. 대상 서버를 다시 선택하고 **준수 검사** 아이콘( )을 클릭하여 각 장치 드라이버의 준수 여부를 확인하십시오.

준수 검사는 **설치된 드라이버 버전** 열의 준수 상태를 업데이트합니다. 이 열은 할당된 UXSP에 대해 측정된 서버의 전체 준수 상태와 각 장치 드라이버의 설치된 버전 및 준수 상태를 표시합니다.

- **준수**. 설치된 장치 드라이버가 할당된 UXSP의 버전과 같거나 이후 버전입니다.
- **미준수**. 설치된 장치 드라이버가 할당된 UXSP의 버전보다 이전 버전입니다. 이 링크를 클릭하면 비준수에 대한 자세한 정보를 얻을 수 있습니다.

참고: 장치 드라이버 준수는 하드웨어가 있는 경우에만 정확합니다. 하드웨어가 없어도 장치 드라이버는 여전히 서버에 적용됩니다. 누락된 하드웨어가 서버에 추가되면, Windows에서 최신 버전을 로드합니다.

단계 6. **업데이트 수행** 아이콘()을 클릭하십시오.

단계 7. 다음 업데이트 규칙 중 하나를 선택하십시오.

- **오류 발생 시 모든 업데이트 중지**. 대상 장치에서 장치 드라이버를 업데이트하는 동안 오류가 발생하면 현재 장치 드라이버 업데이트 작업의 모든 대상 장치에 대한 업데이트 프로세스가 중지됩니다. 이 경우 대상 장치의 UXSP에는 어떠한 장치 드라이버 업데이트도 적용되지 않습니다. 모든 대상 장치에 설치된 현재 장치 드라이버는 이후에도 유효합니다.
- **오류 발생 시 계속**. 대상 장치에서 장치 드라이버를 업데이트하는 중에 오류가 발생하는 경우 업데이트 프로세스가 특정 장치에 대한 장치 드라이버를 업데이트할 수 없습니다. 그러나 업데이트 프로세스는 장치의 다른 장치 드라이버를 계속해서 업데이트하고 현재 장치 드라이버 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.
- **오류 발생 시 다음 시스템으로 이동**. 장치에서 장치 드라이버를 업데이트하는 중에 오류가 발생하는 경우 업데이트 프로세스는 해당 특정 장치에 대한 장치 드라이버를 업데이트하는 모든 시도를 중지하므로 해당 장치에 설치된 현재 장치 드라이버가 계속해서 적용되게 됩니다. 업데이트 프로세스는 현재 장치 드라이버 업데이트 작업에 있는 모든 기타 장치를 계속해서 업데이트합니다.

단계 8. **업데이트 수행**을 클릭하여 즉시 업데이트하거나 **일정**을 클릭하여 이 업데이트가 나중에 실행되도록 예약하십시오.

완료한 후에

업데이트를 적용할 때 대상 서버가 유지 관리 모드로 전환되지 못하는 경우 업데이트를 다시 적용해 보십시오.

업데이트가 제대로 완료되지 않은 경우 문제 해결 및 정정 작업에 대해서는 OS 장치 드라이버 업데이트 고려 사항의 내용을 참조하십시오.

Windows 드라이버 업데이트: 적용 페이지에서 다음 작업을 수행할 수 있습니다.

- 적용 페이지의 **업데이트 상태** 열에서 장치 드라이버 업데이트 상태를 직접 봅니다.
- 작업 로그에서 장치 드라이버 업데이트의 상태를 모니터링합니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오.

  작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

  업데이트 작업이 완료되면 Windows 드라이버 업데이트: 적용 페이지에서 해당 장치가 호환되는지 확인할 수 있습니다. 각 장치에서 활성화된 현재 드라이버 버전은 **설치된 드라이버 버전** 열에 나열되어 있습니다.

제 15 장 베어메탈 서버에 운영 체제 설치

Lenovo XClarity Administrator를 사용하여 OS 이미지 리포지토리를 관리하고 운영 체제 이미지를 최대 28개의 베어메탈 서버에 동시 배포할 수 있습니다.

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

시작하기 전에

90일 무료 평가판이 만료된 후에도 XClarity Administrator을(를) 사용하여 무료로 하드웨어를 관리하고 모니터할 수 있습니다. 그러나 계속해서 OS 배포 기능을 사용하려면 XClarity Administrator 고급 기능을 지원하는 각 관리되는 서버에 대해 전체 기능 사용 라이센스를 구입해야 합니다. Lenovo XClarity Pro은(는) 서비스 및 지원에 대한 자격과 전체 기능 사용 라이센스를 제공합니다. Lenovo XClarity Pro 구입에 대한 자세한 정보는 Lenovo 담당자 또는 공인 비즈니스 파트너에게 문의하십시오. 자세한 정보는 XClarity Administrator 온라인 설명서에서 전체 기능 사용 라이센스 설치의 내용을 참조하십시오.

이 작업 정보

XClarity Administrator는 일반적으로 운영 체제가 설치되어 있지 않은 ***베어메탈*** 서버에 운영 체제 이미지를 배포하는 간단한 방법을 제공합니다.

주의: 운영 체제가 설치된 서버에 운영 체제를 배포하는 경우 XClarity Administrator는 대상 디스크의 파티션을 덮어쓰는 새로운 설치를 수행합니다.

몇 가지 요소가 서버에 운영 체제를 배포하는 데 필요한 시간을 결정합니다.

- 서버에 설치된 RAM의 양은 서버가 시작되는 데 걸리는 시간에 영향을 줍니다.
- 서버에 설치된 I/O 어댑터의 수와 유형은 XClarity Administrator가 서버의 인벤토리를 수행하는 데 걸리는 시간의 양에 영향을 줍니다. 서버가 시작될 때 UEFI 펌웨어가 시작되는 데 걸리는 시간의 양에도 영향을 줍니다. 운영 체제 배포 중에는 서버가 여러 번 다시 시작됩니다.
- 네트워크 트래픽. XClarity Administrator는 데이터 네트워크 또는 운영 체제 배포 네트워크를 통해 운영 체제 이미지를 다운로드합니다.
- Lenovo XClarity Administrator 가상 어플라이언스가 설치된 호스트의 하드웨어 구성. RAM의 양, 프로세서, 하드 드라이브 스토리지는 다운로드 시간에 영향을 줄 수 있습니다.

중요: XClarity Administrator에서 운영 체제 이미지를 배포하려면, XClarity Administrator 인터페이스(Eth0 또는 Eth1) 중 최소 하나는 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결을 가지고 있어야 합니다. 운영 체제 배포는 네트워크 액세스 페이지에 정의된 인터페이스를 사용합니다. 네트워크 설정에 대한 자세한 정보는 네트워크 액세스 구성의 내용을 참조하십시오.

서버에서 베어메탈 운영 체제 배포를 수행하기 전에 펌웨어를 최신 수준으로 업데이트하고 구성 패턴을 사용하여 서버를 구성하여 서버를 준비하십시오. 자세한 정보는 관리 장치에서 펌웨어 업데이트 및 구성 패턴을 사용하여 서버 구성의 내용을 참조하십시오.

주의: Converged 및 ThinkAgile 어플라이언스에서 베어메탈 운영 체제 배포를 수행하는 데 XClarity Administrator를 사용하지 *않는* 것이 좋습니다.

절차

다음 그림은 서버에 OS 이미지를 배포하는 워크플로우를 설명합니다.

단계 1. **OS 이미지 가져오기.**

서버에 OS 이미지를 배포하려면 먼저 리포지토리에 운영 체제를 가져와야 합니다. OS 이미지를 가져올 때 XClarity Administrator는 다음과 같이 합니다.

- 운영 체제를 가져오기 전에 OS 이미지 리포지토리에 충분한 공간이 있는지 확인합니다. 이미지를 가져올 충분한 공간이 없는 경우 리포지토리에서 기존 이미지를 삭제하고 다시 새 이미지 가져오기를 시도하십시오.
- 해당 이미지의 프로필을 하나 이상 만들고 그 프로필을 OS 이미지 리포지토리에 저장합니다. 각 *프로필*에는 OS 이미지와 설치 옵션이 포함됩니다. 사전 정의된 OS 이미지 프로필에 대한 자세한 정보는 운영 체제 이미지 프로필의 내용을 참조하십시오.

*기본 운영 체제*는 OS 이미지 리포지토리로 가져온 전체 OS 이미지입니다. 가져온 기본 이미지에는 해당 이미지의 설치 구성을 설명하는 미리 정의된 프로필이 들어 있습니다. 특정 구성에 배포할 수 있는 기본 OS 이미지에서 사용자 지정 프로필을 만들 수 있습니다.

지원되는 *사용자 지정 운영 체제*를 가져올 수도 있습니다. 이 사용자 지정 이미지에는 배포할 수 없는 미리 정의된 자리 표시자 프로필이 포함되어 있습니다. 배포할 수 있는 사용자 지정 프로필을 가져오거나 자리 표시자 프로필을 기반으로 사용자 지정 프로필을 만들어야 합니다. 사용자 지정 프로필을 추가하면 자리 표시자 프로필이 자동으로 제거됩니다.

Microsoft Windows 서버 2016 및 2019의 경우, 사용자 지정 운영 시스템 이미지가 제공될 때마다 가져올 수 있습니다. 가져온 기본 이미지에는 해당 이미지의 설치 구성을 설명하는 미리 정의된 프로필이 들어 있습니다. 사용자 지정 OS 이미지에 사용자 지정 프로필을 만들 수 없습니다.

지원되는 기본 및 사용자 정의 운영 체제 목록은 지원되는 운영 체제Lenovo XClarity Administrator 온라인 설명서에서 지원되는 운영 체제의 내용을 참조하십시오.

단계 2. **(옵션) OS 이미지를 사용자 지정합니다.**

장치 드라이버, 부팅 파일(Windows만 해당), 구성 설정, 무인 파일, 설치 후 스크립트 및 소프트웨어를 추가하여 OS 이미지를 사용자 지정할 수 있습니다. 기본 OS 이미지를 사용자 지정하는 경우 XClarity Administrator는 사용자 지정 파일과 설치 옵션이 포함된 사용자 지정 OS 이미지 프로필을 만듭니다.

OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

단계 3. **전역 설정을 구성하십시오.**

전역 설정은 운영 체제 배포를 위해 기본값의 역할을 하는 구성 옵션입니다. 다음 전역 설정을 구성할 수 있습니다.

- 운영 체제 배포에 사용할 관리자 사용자 계정의 암호
- 서버에 IP 주소를 지정하는 방법
- 설치된 운영 체제를 활성화하는 데 사용할 라이센스 키
- Active Directory 도메인을 Windows 운영 체제 배포의 일부로 선택적으로 결합

단계 4. **네트워크 설정을 구성하십시오.**

운영 체제를 배포할 각 서버에 대해 네트워크 설정을 지정할 수 있습니다.

DHCP를 사용하여 IP 주소를 동적으로 할당하는 경우 MAC 주소를 구성해야 합니다.

고정 IP 주소를 사용하는 경우 특정 서버에 운영 체제를 배포하려면 먼저 해당 서버에 대해 다음 네트워크 설정을 구성해야 합니다. 이러한 설정을 구성하면 서버의 배포 상태가 "준비"로 변경됩니다. (일부 필드에서는 고정 IPv6 주소를 사용할 수 없음.)

- 호스트 이름

  호스트 이름은 다음 규칙을 준수해야 합니다.
  - 관리되는 각 서버의 호스트 이름은 고유해야 합니다.
  - 호스트 이름은 마침표(.)로 구분된 문자열(레이블)을 포함할 수 있습니다.
  - 각 레이블은 ASCII 문자, 숫자 및 대시(-)를 포함할 수 있지만 문자열은 대시로 시작하거나 끝날 수 없으며 모든 숫자를 포함할 수도 없습니다.
  - 첫 번째 레이블의 길이는 2 – 15자일 수 있습니다. 그 다음 레이블의 길이는 2 – 63자일 수 있습니다.
  - 호스트 이름의 총 길이는 255자를 초과해서는 안 됩니다.
- 운영 체제를 설치할 호스트에 있는 포트의 MAC 주소.

  기본적으로 MAC 주소는 AUTO로 설정됩니다. 이 설정은 배포에 사용하고 구성할 수 있는 이더넷 포트를 자동으로 감지합니다. 기본적으로 감지된 첫 번째 MAC 주소(포트)가 사용됩니다. 다른 MAC 주소에서 연결이 감지되면 새로 감지된 MAC 주소를 배포에 사용하기 위해 XClarity Administrator 호스트가 자동으로 다시 시작됩니다..

  OS 배치에 사용되는 MAC 주소 포트의 상태는 네트워크 설정 대화 상자의 **MAC 주소** 드롭다운 메뉴에서 알 수 있습니다. 여러 개의 포트가 사용되었거나 모든 포트가 다운되었을 때, AUTO가 기본값으로 사용됩니다.

  참고:

  - 가상 네트워크 포트는 지원되지 않습니다. 하나의 물리적 네트워크 포트를 사용하여 여러 가상 네트워크 포트를 시뮬레이션하지 마십시오.
  - 서버의 네트워크 설정이 자동으로 설정되어 있으면 슬롯 1 – 16에서 XClarity Administrator이(가) 네트워크 포트를 자동으로 감지할 수 있습니다. 슬롯 1 – 16에서 하나 이상의 포트가 XClarity Administrator에 연결되어 있어야 합니다.
  - MAC 주소에 슬롯 17 이상의 네트워크 포트를 사용하려면 AUTO를 사용할 수 없습니다. 대신 서버의 네트워크 설정을 사용하려는 특정 포트의 MAC 주소로 설정해야 합니다.
  - ThinkServer 서버의 경우 모든 호스트 MAC 주소가 표시되지는 않습니다. 대부분의 경우 AnyFabric 이더넷 어댑터의 MAC 주소가 네트워크 설정 편집 대화 상자에 나열됩니다. 다른 이더넷 어댑터(예, Lan-On-Motherboard)의 MAC 주소는 나열되지 않습니다. 어댑터에 대한 MAC 주소가 사용 불가능한 경우 비VLAN 배포에 AUTO 방법을 사용하십시오.
- IP 주소 및 서브넷 마스크
- IP 게이트웨이
- 최대 두 개의 DNS(Domain Name System) 서버
- 최대 전송 단위(MTU) 속도
- VLAN ID(VLAN IP 모드를 사용하는 경우)

VLAN을 사용하도록 선택하는 경우 구성 중인 호스트 네트워크 어댑터에 VLAN ID를 할당할 수 있습니다.

단계 5. **스토리지 옵션을 선택하십시오.**

각 배포에 대해 운영 체제를 배포할 선호 스토리지 위치를 선택할 수 있습니다. 운영 체제에 따라 로컬 디스크 드라이브, 내장 하이퍼바이저 키 또는 SAN에 배포할 수 있습니다.

단계 6. **추가 옵션 및 사용자 지정 구성 설정을 선택하고 OS 이미지를 배포하십시오.**

OS 배포 및 사용자 지정 구성 설정을 위한 라이센스 키와 같은 추가 배포 옵션을 구성할 수 있습니다. Microsoft Windows를 설치할 경우 함께 사용할 Active Directory 도메인도 구성할 수 있습니다.

참고:

- 특정 사용자 지정 OS 프로필에 대한 사용자 지정 구성 설정을 정의한 경우 프로필을 서버에 배포하기 전에 필수 사용자 지정 구성 설정 값을 정의해야 합니다.
- 사용자 정의 설정이 포함된 사용자 지정 OS 프로필을 배포할 때 모든 대상 서버는 동일한 사용자 지정 OS 프로필을 사용해야 하며 사용자 정의 설정 값은 모든 대상 서버에 적용됩니다.

그런 다음 배포에 대한 대상 서버 및 배포할 OS 이미지를 선택할 수 있습니다. 운영 체제를 배포하려면 서버의 배포 상태는 "준비여야 합니다."

최대 28개의 서버에 운영 체제 이미지를 동시 배포할 수 있습니다.

운영 체제 이미지 배포를 시도하기 전에 운영 체제 배포 고려사항의 내용을 검토하십시오.

운영 체제 배포 고려사항

운영 체제 이미지 배포를 시도하기 전에 다음 고려사항의 내용을 검토하십시오.

Lenovo XClarity Administrator 고려사항

- 현재 대상 서버에서 실행 중인 작업이 없어야 합니다. 활성 작업의 목록을 확인하려면 **모니터링 → 작업**을 클릭하십시오.
- 대상 서버에 지연되었거나 부분적으로 활성화된 서버 패턴이 없어야 합니다. 서버 패턴이 관리 서버에서 지연되거나 부분적으로 활성화된 경우 모든 구성 설정을 적용하려면 서버를 다시 시작해야 합니다. 부분적으로 활성화된 서버 패턴이 있는 서버에 운영 체제 배포를 시도하지 마십시오. 서버의 구성 상태를 확인하려면 관리되는 서버의 요약 페이지에 있는 **구성 상태** 필드를 참조하십시오 (관리 서버의 세부 정보 보기 참조).
- 운영 체제를 배포하는 데 사용할 관리자 계정의 암호가 전역 설정: 운영 체제 배포 대화 상자에 지정되어 있어야 합니다. 암호 설정에 대한 자세한 정보는 전역 OS 배포 설정 구성의 내용을 참조하십시오.
- 전역 기본 설정이 이 운영 체제 배포에 대해 올바른지 확인하십시오(전역 OS 배포 설정 구성 참조).

운영 체제 고려사항

- 설치된 운영 체제를 활성화하기 위한 모든 해당 운영 체제 라이센스가 있어야 합니다. 사용자는 운영 체제 제조업체에서 직접 라이센스를 얻을 책임이 있습니다.
- 배포하려는 운영 체제 이미지가 OS 이미지 리포지토리에 이미 로드되어 있어야 합니다. 이미지 가져오기에 대한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.
- XClarity Administrator 리포지토리의 운영 체제 이미지는 특정 하드웨어 플랫폼에서만 지원되지 않을 수 있습니다. 선택한 서버에서 지원하는 OS 이미지 프로필만 OS 이미지 배포 페이지에 나열됩니다. 운영 체제가 특정 서버와 호환되는지 여부를 Lenovo OS 상호 운용성 안내서 웹 사이트에서 판별할 수 있습니다.
- Windows의 경우 Windows 프로필을 배포하기 전에 먼저 부팅 파일을 OS 이미지 리포지토리로 가져와야 합니다. Lenovo는 미리 정의된 WinPE_64.wim 부팅 파일을 장치 드라이버 세트와 함께 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있어, **장치 드라이버** 또는 **부팅 파일** 탭에서 번들 파일을 가져올 수 있습니다.
- SLES 15 및 15 SP1에서는 서버 OS 지원 센터 웹 페이지에서 설치 프로그램 이미지와 관련 패키지 이미지를 모두 가져와야 합니다. SLES 15 SP2 이상의 경우 SUSE Linux Enterprise Server 15 및 15 SP1의 통합 설치 프로그램 및 패키지 DVD가 더 이상 사용되지 않으므로 전체 설치 미디어 이미지만 가져오면 됩니다.

- ThinkSystem 서버의 경우, XClarity Administrator에는 최종 운영 체제의 기본 네트워크 및 스토리지 구성은 물론 운영 체제 설치를 가능하게 하는 기본 제공하지 않는 장치 드라이버가 포함되어 있습니다. 다른 서버의 경우 배포할 운영 체제 이미지에 적절한 이더넷, Fibre Channel 및 하드웨어의 스토리지 어댑터 장치 드라이버가 포함되어야 합니다. I/O 어댑터 장치 드라이버가 운영 체제에 포함되지 않은 경우 어댑터는 OS 배포에 대해 지원되지 않습니다. 필요한 최신 기본 제공 I/O 어댑터 장치 드라이버 및 부팅 파일을 가지려면 항상 최신 운영 체제를 설치하십시오. 또한 XClarity Administrator로 가져온 운영 체제에 기본 제공하지 않는 장치 드라이버 및 부팅 파일을 추가할 수도 있습니다(XClarity Administrator 온라인 설명서에서 OS 이미지 프로필 사용자 지정 참조).

  VMware의 경우 최신 어댑터 지원이 포함되는 ESXi용 최신 Lenovo Custom Image를 사용하십시오. 해당 이미지 확보에 대한 자세한 정보는 VMware 지원 – 다운로드 웹 페이지의 내용을 참조하십시오.
- ThinkSystem 서버의 경우 SLES 12 SP2를 배포하려면 kISO 프로필을 사용해야 합니다. kISO 프로필을 얻으려면 기본 SLES 운영 체제를 가져온 후 적절한 SLES kISO 이미지를 가져와야 합니다. Linux 지원 – 다운로드 웹 페이지에서 SLES kISO 이미지를 다운로드할 수 있습니다.

  참고:

  – SLES kISO 이미지는 가져온 OS 이미지의 최대 수를 계산합니다.

  지원되는 기본 및 사용자 정의 운영 체제 목록은 지원되는 운영 체제Lenovo XClarity Administrator 온라인 설명서에서 지원되는 운영 체제의 내용을 참조하십시오.

  – 모든 kISO 프로필을 삭제하는 경우 기본 SLES 운영 체제를 삭제한 다음 기본 운영 체제 및 kISO 이미지를 다시 가져와 SLES 12 SP2를 ThinkSystem 서버에 배포해야 합니다.

  – kISO 프로필을 기반으로 사용자 지정 OS 프로필을 만드는 경우 기본 운영 체제에서 미리 정의된 장치 드라이버는 포함되지 않습니다. kISO에 포함된 장치 드라이버가 대신 사용됩니다. 사용자 지정 OS 프로필에 장치 드라이브를 추가할 수도 있습니다(사용자 지정 OS 이미지 프로필 만들기 참조).

특정 운영 체제의 제한사항에 대한 자세한 정보는 지원되는 운영 체제의 내용을 참조하십시오.

네트워크 고려사항

- 모든 필요한 포트가 열려 있어야 합니다(배포된 운영 체제에 대한 포트 가용성 참조).
- XClarity Administrator가 XClarity Administrator 네트워크 액세스를 구성할 때 선택한 인터페이스(Eth0 또는 Eth1)를 통해 대상 서버(베이스보드 관리 컨트롤러 및 서버의 데이터 네트워크)와 통신할 수 있는지 확인하십시오.

  운영 체제 배포에 사용할 인터페이스를 지정하려면 네트워크 액세스 구성의 내용을 참조하십시오.

  운영 체제 배포 네트워크 및 인터페이스에 대한 자세한 정보는 XClarity Administrator 온라인 설명서에서 네트워크 고려사항의 내용을 참조하십시오.
- IP 주소가 호스트 운영 체제에 대해 고유한지 확인하십시오. 배포 프로세스 중에 XClarity Administrator는 네트워크 주소에 대해 지정한 중복 IP 주소를 확인합니다.
- 네트워크가 느리거나 불안정한 경우 운영 체제를 배포할 때 예기치 않은 결과가 표시될 수 있습니다.
- 관리에 사용되는 XClarity Administrator 네트워크 인터페이스는 전역 설정(운영 체제 배포 대화상자)에서 선택한 것과 동일한 IP 주소 방법을 사용하여 베이스보드 관리 컨트롤러에 연결되도록 구성해야 합니다. 예를 들어 관리를 위해 eth0을 사용하도록 XClarity Administrator을 설정하고, 배포된 OS를 구성할 때 수동으로 할당된 고정 IPv6 주소를 사용하도록 선택한 경우, eth0을 베이스보드 관리 컨트롤러에 연결하는 IPv6 주소로 구성해야 합니다.
- OS 배포 전역 설정에서 IPv6 주소를 사용하도록 선택하면 XClarity Administrator의 IPv6 주소를 베이스보드 관리 컨트롤러 및 서버의 데이터 네트워크로 라우팅할 수 있어야 합니다.
- IPv6 모드는 ThinkServer에 지원되지 않습니다(XClarity Administrator 온라인 설명서에서 IPv6 구성 제한 참조).
- DHCP를 사용하여 IP 주소를 동적으로 할당하는 경우 MAC 주소를 구성해야 합니다.

- 고정 IP 주소를 사용하는 경우 특정 서버에 운영 체제를 배포하려면 먼저 해당 서버에 대해 다음 네트워크 설정을 구성해야 합니다. 이러한 설정을 구성하면 서버의 배포 상태가 "준비"로 변경됩니다. (일부 필드에서는 고정 IPv6 주소를 사용할 수 없음.)
  - 호스트 이름

    호스트 이름은 다음 규칙을 준수해야 합니다.
    - 관리되는 각 서버의 호스트 이름은 고유해야 합니다.
    - 호스트 이름은 마침표(.)로 구분된 문자열(레이블)을 포함할 수 있습니다.
    - 각 레이블은 ASCII 문자, 숫자 및 대시(-)를 포함할 수 있지만 문자열은 대시로 시작하거나 끝날 수 없으며 모든 숫자를 포함할 수도 없습니다.
    - 첫 번째 레이블의 길이는 2 - 15자일 수 있습니다. 그 다음 레이블의 길이는 2 – 63자일 수 있습니다.
    - 호스트 이름의 총 길이는 255자를 초과해서는 안 됩니다.
  - 운영 체제를 설치할 호스트에 있는 포트의 MAC 주소.

    기본적으로 MAC 주소는 AUTO로 설정됩니다. 이 설정은 배포에 사용하고 구성할 수 있는 이더넷 포트를 자동으로 감지합니다. 기본적으로 감지된 첫 번째 MAC 주소(포트)가 사용됩니다. 다른 MAC 주소에서 연결이 감지되면 새로 감지된 MAC 주소를 배포에 사용하기 위해 XClarity Administrator 호스트가 자동으로 다시 시작됩니다..

    OS 배치에 사용되는 MAC 주소 포트의 상태는 네트워크 설정 대화 상자의 **MAC 주소** 드롭다운 메뉴에서 알 수 있습니다. 여러 개의 포트가 사용되었거나 모든 포트가 다운되었을 때, AUTO가 기본값으로 사용됩니다.

    참고:

    - 가상 네트워크 포트는 지원되지 않습니다. 하나의 물리적 네트워크 포트를 사용하여 여러 가상 네트워크 포트를 시뮬레이션하지 마십시오.
    - 서버의 네트워크 설정이 자동으로 설정되어 있으면 슬롯 1 – 16에서 XClarity Administrator이(가) 네트워크 포트를 자동으로 감지할 수 있습니다. 슬롯 1 – 16에서 하나 이상의 포트가 XClarity Administrator에 연결되어 있어야 합니다.
    - MAC 주소에 슬롯 17 이상의 네트워크 포트를 사용하려면 AUTO를 사용할 수 없습니다. 대신 서버의 네트워크 설정을 사용하려는 특정 포트의 MAC 주소로 설정해야 합니다.
    - ThinkServer 서버의 경우 모든 호스트 MAC 주소가 표시되지는 않습니다. 대부분의 경우 AnyFabric 이더넷 어댑터의 MAC 주소가 네트워크 설정 편집 대화 상자에 나열됩니다. 다른 이더넷 어댑터(예, Lan-On-Motherboard)의 MAC 주소는 나열되지 않습니다. 어댑터에 대한 MAC 주소가 사용 불가능한 경우 비VLAN 배포에 AUTO 방법을 사용하십시오.
  - IP 주소 및 서브넷 마스크
  - IP 게이트웨이
  - 최대 두 개의 DNS(Domain Name System) 서버
  - 최대 전송 단위(MTU) 속도
  - VLAN ID(VLAN IP 모드를 사용하는 경우)
- VLAN을 사용하도록 선택하는 경우 구성 중인 호스트 네트워크 어댑터에 VLAN ID를 할당할 수 있습니다.

운영 체제 배포 네트워크 및 인터페이스에 대한 자세한 정보는 관리되는 서버에 대한 네트워크 설정 구성 및 XClarity Administrator 온라인 설명서에서 관리되는 서버에 대한 네트워크 설정 구성 및 네트워크 고려사항의 내용을 참조하십시오.

스토리지 및 부팅 옵션 고려 사항

- 운영 체제를 배포하기 전에 대상 서버의 UEFI 부팅 옵션이 "UEFI boot only"로 설정되어 있는지 확인하십시오. "Legacy-only" 및 "UEFI first, then legacy" 부팅 옵션은 운영 체제 배포에 지원되지 않습니다.
- 각 서버는 하드웨어 RAID 어댑터가 설치 및 구성되어 있어야 합니다.

주의:

  - 하드웨어 RAID로 설정된 스토리지만 지원됩니다.
  - 일반적으로 온보드 Intel SATA 스토리지 어댑터에 있는 소프트웨어 RAID 또는 JBOD로 설정된 스토리지는 지원되지 않습니다. 그러나 하드웨어 RAID 어댑터가 없는 경우 SATA 어댑터를 운영 체제 배포에 대해 사용 설정된 AHCI SATA 모드로 설정하거나 구성되지 않은 정상 디스크를 JBOD로 설정하면 경우에 따라 작동할 수 있습니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 OS 설치 프로그램이 XClarity Administrator를 설치하려는 디스크를 찾을 수 없음의 내용을 참조하십시오.

    이 예외는 M.2 드라이브에는 적용되지 않습니다.
  - 관리되는 장치에 하드웨어 RAID용으로 구성되지 않은 로컬 드라이브(SATA, SAS 또는 SSD) 및 M.2 드라이브가 둘 다 있는 경우 M.2 드라이브를 사용하려면 로컬 드라이브를 사용 안 함으로 설정해야 하고 로컬 드라이브를 사용하려면 M.2 드라이브를 사용 안 함으로 설정해야 합니다. 마법사의 로컬 스토리지 탭에서 로컬 디스크 사용 안 함을 선택하거나 기존 서버에서 구성 패턴을 생성한 다음 확장된 UEFI 패턴에서 M.2 장치를 사용 안 함으로 설정하여 구성 패턴에서 온보드 스토리지 컨트롤러 장치와 레거시 및 UEFI 스토리지 옵션 ROM을 사용 안 함으로 설정할 수 있습니다.
  - SATA 어댑터를 사용하는 경우 SATA 모드를 "IDE"로 설정해서는 *안됩니다*.
- 서버 마더보드나 HBA 컨트롤러에 연결된 NVMe 스토리지는 지원되지 않고 장치에 설치되어서는 안됩니다. 그렇지 않으면 비NVMe 스토리지에 OS 배치를 할 수 없습니다.
- RHEL을 배포하는 경우 대상 스토리지의 LUN과 동일한 LUN에 연결된 다중 포트는 지원되지 않습니다.
- 서버에 보안 부팅 모드를 사용하지 않아야 합니다. 보안 부팅 모드를 사용하는 운영 체제를 배포하는 경우(예, Windows) 보안 부팅 모드를 사용 안 함으로 설정하고 운영 체제를 배포한 다음 보안 부팅 모드를 다시 사용하도록 설정하십시오.
- 서버에 Microsoft Windows를 배포하는 경우 첨부된 드라이브에 기존 시스템 파티션이 없어야 합니다(XClarity Administrator 온라인 설명서에서 첨부된 디스크 드라이브에 있는 기존 시스템 파티션으로 인해 OS 배포가 실패함 참조).
- ThinkServer 서버의 경우 다음 요구사항이 충족되는지 확인하십시오.
  - 서버의 부팅 설정에는 `UEFI Only`로 설정된 Storage OpROM Policy가 포함되어야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 ThinkServer 서버에서 OS 설치 프로그램을 부팅할 수 없음 - XClarity Administrator의 내용을 참조하십시오.
  - ESXi를 배포하는 중이고 PXE 부팅 가능한 네트워크 어댑터가 있는 경우 운영 체제를 배포하기 전에 네트워크 어댑터에서 PXE 지원을 사용 안 함으로 설정하십시오. 배포가 완료되면 원하는 경우 PXE 지원을 다시 사용으로 설정할 수 있습니다.
  - ESXi를 배포하는 중이고 운영 체제를 설치할 드라이브가 아닌 부팅 순서 목록에 부팅 가능한 장치가 있는 경우 운영 체제를 배포하기 전에 부팅 순서 목록에서 부팅 가능한 장치를 제거하십시오. 배포가 완료된 후 이 부팅 가능한 장치를 다시 목록에 추가할 수 있습니다. 설치된 드라이브가 목록의 맨 위에 있는지 확인하십시오.

스토리지 위치 설정에 대한 자세한 정보는 관리되는 서버에 대한 스토리지 위치 선택의 내용을 참조하십시오.

관리되는 장치 고려사항

- 특정 장치의 운영 체제 배포 제한 사항에 대한 자세한 내용은 XClarity Administrator 지원 – 호환성 웹 페이지에서 참조할 수 있습니다. **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하십시오.
- 대상 서버에 마운트된 매체(예, ISO)가 없는지 확인하십시오. 또한 관리 컨트롤러에 열려 있는 활성 원격 미디어 세션이 없는지 확인하십시오.
- BIOS의 타임스탬프가 현재 날짜 및 시간으로 설정되었는지 확인하십시오.
- 시스템 보호가 사용 설정되고 작업이 **OS 부팅 방지**로 설정된 XCC2가 있는 서버의 경우 시스템 보호가 장치에서 호환되는지 확인하십시오. 시스템 보호가 호환되지 않으면 장치가 부팅 프로세스를 완료할 수 없어 OS 배포에 실패합니다. 이러한 장치를 프로비저닝하려면 시스템 보호 부팅 프롬프트에 수동으로 응답하여 장치가 정상적으로 부팅되도록 하십시오.

- ThinkSystem 및 System x 서버의 경우, Legacy BIOS 옵션이 사용 안 함으로 설정되어 있는지 확인하십시오. BIOS/UEFI (F1) Setup utility에서 UEFI **설정 → 시스템 설정**을 클릭하고 Legacy BIOS가 사용 안 함으로 설정되어 있는지 확인하십시오.
- Flex System 서버의 경우 섀시 전원이 켜져 있어야 합니다.
- Converged, NeXtScale 및 System x 서버의 경우 원격 관리를 위한 FoD(Feature on Demand) 키가 설치되어야 합니다. 원격 관리 상태가 서버 페이지에서 사용, 사용 안 함 또는 서버에 설치되어 있지 않은지 여부를 판별할 수 있습니다(관리 서버의 상태 보기 참조). 서버에 설치되는 FoD 키에 대한 자세한 정보는 Features on Demand 키 보기의 내용을 참조하십시오.
- ThinkSystem 서버 및 ThinkAgile 어플라이언스의 경우 운영 체제 배포를 위해 XClarity Controller Enterprise 기능이 필요합니다. 자세한 정보는 Features on Demand 키 보기의 내용을 참조하십시오.
- Converged 및 ThinkAgile 어플라이언스의 경우 베어메탈 운영 체제 배포를 수행하는 데 XClarity Administrator를 사용하지 *않는* 것이 좋습니다.

지원되는 운영 체제

Lenovo XClarity Administrator는 여러 운영 체제 배포를 지원합니다. 지원되는 버전의 운영 체제만 XClarity Administrator OS 이미지 리포지토리로 로드할 수 있습니다.

중요:

- 특정 장치의 운영 체제 배포 제한 사항에 대한 자세한 내용은 XClarity Administrator 지원 – 호환성 웹 페이지에서 참조할 수 있습니다. **호환성** 탭을 클릭한 다음 해당 장치 유형에 대한 링크를 클릭하십시오.
- XClarity Administrator의 암호화 관리 기능을 사용하면 통신을 특정한 최소 SSL/TLS 모드로 제한할 수 있습니다. 예를 들어 TLS 1.2를 선택한 경우 TLS 1.2를 지원하는 설치 과정 및 강력한 암호화 알고리즘을 갖춘 운영 체제만 XClarity Administrator를 통해 배포될 수 있습니다.
- XClarity Administrator 리포지토리의 운영 체제 이미지는 특정 하드웨어 플랫폼에서만 지원되지 않을 수 있습니다. 선택한 서버에서 지원하는 OS 이미지 프로필만 OS 이미지 배포 페이지에 나열됩니다. 운영 체제가 특정 서버와 호환되는지 여부를 Lenovo OS 상호 운용성 안내서 웹 사이트에서 판별할 수 있습니다.
- Lenovo 서버 및 솔루션에 대한 OS 및 하이퍼바이저 관련 호환성 및 지원 정보와 리소스는 서버 OS 지원 센터 웹 페이지의 내용을 참조하십시오.

다음 테이블은 XClarity Administrator가 배포할 수 있는 64비트 운영 체제를 나열합니다.

운영 체제	버전	참고
CentOS Linux	7.2 and later 8.0 8.1 8.2	**참고:** • 별도로 명시하지 않는 한 기존 및 이후의 모든 부 버전이 지원됩니다. • DHCP, 고정 IPv4 및 고정 IPv6 주소가 지원됩니다. • VLAN 태깅이 지원되지 않습니다. • 기본 제공하지 않는 드라이버는 지원되지 않습니다. • OS 프로파일 사용자 정의가 지원되지 않습니다. • CentOS 8.3은 지원되지 않습니다.
Microsoft® Windows® Azure Stack HCI	20H2 21H2	OS 프로파일 사용자 정의가 지원되지 않습니다.
Microsoft Windows Client	10 21H2 10 22H2 11 22H2	

운영 체제	버전	참고
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	리테일과 볼륨 라이센스 사본 둘 다 지원됩니다. 참고: XClarity Administrator 버전이 릴리스되면 XClarity Administrator는 Microsoft에서 지원하는 Windows 버전에서만 테스트됩니다. 다음은 *지원되지 않습니다*. • Windows 리셀러 옵션 키트(ROK) • Windows Server 반기 채널(SAC) v1709, v1803 및 v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Windows Server 2012 평가본 • 내장 하이퍼바이저 키가 있는 관리되는 서버에 대한 Windows Server 이미지 Intel CLX 프로세서가 포함된 서버의 Windows Server 2012 R2 Windows 이미지를 배포하기 전에 대상 서버에서 내장 하이퍼바이저 키를 물리적으로 제거해야 합니다. 이는 가상화 프로필 중 하나를 통해 Hyper-V를 포함합니다. – 데이터 센터 – 데이터 센터 코어 – 데이터 센터 가상화(Hyper-V) – 데이터 센터 가상화 코어(코어가 있는 Hyper-V) – 표준 – 표준 코어 – 표준 가상화(Hyper-V) – 표준 코어(코어가 있는 Hyper-V)
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x 9.x	KVM 포함 참고: • 별도로 명시하지 않는 한 기존 및 이후의 모든 부 버전이 지원됩니다. • DVD 버전의 OS 이미지를 가져올 때 DVD1만 지원됩니다. • RHEL을 ThinkSystem 서버에 설치할 때 RHEL v7.4 이상이 권장됩니다. • RHEL 7.2를 배포하려면 전역 IP 할당이 IPv4 주소를 사용하도록 설정되어야 합니다. 전역 설정에 대한 정보는 전역 OS 배포 설정 구성의 내용을 참조하십시오. • OS 설치 프로그램의 시간 초과로 인해 낮은 대역폭의 IPv6 네트워크에서 OS 배포 실패가 관찰되었습니다. • VLAN 태깅이 지원되지 않습니다.
Rocky Linux	8.x 9.x	참고: • 별도로 명시하지 않는 한 기존 및 이후의 모든 부 버전이 지원됩니다. • DHCP, 고정 IPv4 및 고정 IPv6 주소가 지원됩니다. • VLAN 태깅이 지원되지 않습니다. • 기본 제공하지 않는 드라이버는 지원되지 않습니다.

운영 체제	버전	참고
SUSE® Linux Enterprise Server(SLES)	12.x 15.x	KVM 및 Xen 하이퍼바이저 포함 **참고:** • 별도로 명시하지 않는 한 기존 및 이후의 모든 서비스 팩이 지원됩니다. • DVD 버전의 OS 이미지를 가져올 때 DVD1만 지원됩니다. • OS 설치 프로그램의 시간 초과로 인해 낮은 대역폭의 IPv6 네트워크에서 OS 배포 실패가 확인되었습니다. • ThinkSystem 서버에 SLES 12 SP2를 배포하려면 kISO 프로필을 사용해야 합니다. kISO 프로필을 얻으려면 적절한 SLES kISO 이미지를 가져와야 합니다. 자세한 정보는 운영 체제 배포 고려사항의 내용을 참조하십시오. • SLES 15 및 15 SP1에서는 서버 OS 지원 센터 웹 페이지에서 설치 프로그램 이미지와 관련 패키지 이미지를 모두 가져와야 합니다. SLES 15 SP2 이상의 경우 SUSE Linux Enterprise Server 15 및 15 SP1의 통합 설치 프로그램 및 패키지 DVD가 더 이상 사용되지 않으므로 전체 설치 미디어 이미지만 가져오면 됩니다. • VLAN 태깅이 지원되지 않습니다.
Ubuntu 서버	20.04.x 22.04.x	**참고:** • 선택한 스토리지 옵션(로컬 디스크 드라이브, M.2 드라이브 또는 FC SAN 볼륨)에 이미지를 설치할 수 있습니다. • 별도로 명시하지 않는 한 기존 및 이후의 모든 부 버전이 지원됩니다. • DHCP만 지원됩니다. 고정 IPv4 및 고정 IPv6 주소는 지원되지 *않습니다*. • VLAN 태깅이 지원되지 *않습니다*. • 기본 제공하지 않는 드라이버는 지원되지 *않습니다*. • OS 프로파일 사용자 정의가 지원되지 *않습니다*.
VMware vSphere® Hypervisor(ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.x	기본 VMware vSphere Hypervisor(ESXi) 이미지 및 Lenovo VMware ESXi Custom 이미지가 지원됩니다. Lenovo VMware ESXi Custom 이미지는 펌웨어, 플랫폼 진단 및 향상된 하드웨어 경고에 대한 업데이트와 구성 등의 온라인 플랫폼 관리 기능을 제공하기 위해 선택한 하드웨어에 맞게 사용자 지정됩니다. Lenovo 관리 도구는 선택한 System x 서버에서 ESXi를 간단하게 관리할 수 있도록 지원합니다. 이 이미지는 VMware 지원 – 다운로드 웹 페이지에서 다운로드할 수 있습니다. 이미지에 제공된 라이센스는 60일 무료 평가판입니다. VMware의 모든 라이센싱 요구사항을 충족할 책임이 있습니다. **중요:** • 모든 기존 및 향후 업데이트 팩은 별도로 명시되지 않은 이상 6.0, 6.5, 6.7, 7.0 및 8.0 버전과 호환됩니다. • 기본 ESXi 이미지(Lenovo 사용자 지정 없이)에는 네트워크와 스토리지에 대한 기본 제공 장치 드라이버만 포함되어 있습니다. 기본 이미지에는 기본 제공하지 않는 장치 드라이버(Lenovo VMware ESXi Custom 이미지에 포함되어 있음)가 없습니다. 사용자 지정 OS 이미지 프로필을 만들어 기본 제공하지 않는 장치 드라이버를 추가할 수 있습니다(OS 이미지 프로필 사용자 지정 참조). • 일부 버전의 Lenovo VMware ESXi Custom 이미지에서는 System x, ThinkSystem 및 ThinkServer에 대한 별도의 이미지가 있습니다. 특정 릴리스에 대해 한 번에 한 이미지만 OS 이미지 리포지토리에 존재할 수 있습니다. • 특정 구형 서버에서는 ESXi 배포가 지원되지 않습니다. 지원되는 서버에 대한 자세한 정보는 Lenovo OS 상호 운용성 안내서 웹 사이트의 내용을 참조하십시오. • 다음 버전은 ThinkServer 장치 ESXi 6.0u3, 6.5 이상에 지원됩니다.

운영 체제	버전	참고
		• Flex System 섀시의 서버에 ESXi 5.5(모든 업데이트) 또는 6.0을 설치하는 동안 서버가 응답이 없거나 `image.pld` 로드 중 메시지가 표시된 후 즉시 다시 시작될 수 있습니다. • ESXi 5.5를 시스템의 첫 4GB 내에 구성하려면 메모리 매핑된 I/O(MMIO) 공간이 필요합니다. 구성에 따라 특정 시스템은 4GB 이상의 메모리 사용을 시도하여 오류가 발생할 수 있습니다. 문제를 해결하려면 XClarity Administrator 온라인 설명서에서 VMware 배포로 인해 시스템이 정지되거나 재시작됨의 내용을 참조하십시오. • 고정 IPv6 모드를 사용하여 ESXi를 배포하는 경우 XClarity Administrator의 네트워크 설정에 정의된 호스트 이름이 배포된 ESXi 인스턴스에서 구성되지 않습니다. 대신 기본 호스트 이름 `localhost`가 사용됩니다. 배치된 ESXi에서 XClarity Administrator에 정의된 호스트 이름과 일치하도록 호스트 이름을 수동으로 설정해야 합니다. • 관리되는 서버에 ESXi를 배포하는 중인 경우 운영 체제는 운영 체제가 설치되는 드라이브를 명시적으로 부팅 순서 목록의 맨 위로 이동시키지 않습니다. 부팅 가능한 OS 또는 PXE 서버가 포함된 부팅 장치가 ESXi가 포함된 부팅 장치 앞에 지정된 경우 ESXi가 부팅되지 않습니다. ESXi 배포를 위해 XClarity Administrator는 ESXi 부팅 장치가 부팅 순서 목록의 맨 위에 오도록 대부분의 서버에 대한 부팅 순서 목록을 업데이트합니다. 그러나 ThinkServer 서버는 XClarity Administrator에서 부팅 순서 목록을 업데이트하는 방법을 제공하지 않습니다. 운영 체제를 배포하기 전에 설치 드라이브가 아닌 부팅 가능 장치를 제거하거나 PXE 부팅 지원을 사용 안 함으로 설정해야 합니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 ThinkServer 서버에 ESXi를 배치한 후 운영 체제가 부팅되지 않음의 내용을 참조하십시오. **팁:** 각 서버의 Setup Utility를 통해 **MM 구성**를 구성하는 대신 가상화와 관련된 미리 정의된 확장된 UEFI 패턴 중 하나를 사용할 것을 고려하십시오. 이는 MM 구성 옵션을 3GB로 설정하고 PCI 64비트 리소스 할당을 사용 안 함으로 설정합니다. 해당 패턴에 대한 자세한 정보는 확장 UEFI 설정 정의의 내용을 참조하십시오.

운영 체제 이미지 프로필

OS 이미지 리포지토리에 OS 이미지를 가져오는 경우 Lenovo XClarity Administrator가 해당 이미지에 대한 하나 이상의 프로필을 만들고 프로필을 OS 이미지 리포지토리에 저장합니다. 사전 정의된 각 *프로필*에는 해당 이미지에 대한 OS 이미지 및 설치 옵션이 포함됩니다.

OS 이미지 프로필 특성

OS 이미지 프로필 특성은 OS 이미지 프로필에 대한 추가 정보를 제공합니다. 다음 특성이 표시될 수 있습니다.

- kISO. ThinkSystem 서버에 SLES 12 SP2를 배포하려면 kISO 프로필을 사용해야 합니다. Linux 지원 – 다운로드 웹 페이지에서 SLES kISO 이미지를 다운로드할 수 있습니다.

사전 정의 OS 이미지 프로필

다음 표는 운영 체제 이미지를 가져올 때 XClarity Administrator에서 미리 정의한 프로필을 나열합니다. 또한 이 표에는 각 프로파일에 포함된 패키지가 나열됩니다.

기본 운영 체제에 대한 사용자 지정 OS 이미지 프로필을 작성할 수 있습니다. 자세한 정보는 OS 이미지 프로필 사용자 지정의 내용을 참조하십시오.

운영 체제	프로필	프로필에 포함된 패키지	
CentOS Linux	기본	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	최소	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	가상화	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Microsoft® Windows® Azure Stack HCI	Azure	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="Containers" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Client	Enterprise		
	Enterprise N		
	Worksta-tions Pro		
	Worksta-tions_Pro N		

운영 체제	프로필	프로필에 포함된 패키지	
Microsoft Windows Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Server **참고:** Hyper-V 부터 *가상화 프로필*까지 포함됩니다.	데이터 센터	GUI	
	데이터 센터 가상화	GUI Hyper-V role	
	데이터 센터 가상화 코어	Hyper-V role	
	데이터 센터 코어		
	표준	GUI	
	표준 가상화	GUI Hyper-V role	
	표준 가상화 코어	Hyper-V role	
	표준 코어		
사용자 지정 Microsoft Windows Server	데이터센터_사용자 지정		
	기본_사용자 지정		
Red Hat Enterprise Linux(RHEL) **참고:** KVM 포함	기본	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	최소	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	가상화	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm

운영 체제	프로필	프로필에 포함된 패키지	
		@graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Rocky Linux	기본	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	최소	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	가상화	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server(SLES) 15	기본 및 기본	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	

운영 체제	프로필	프로필에 포함된 패키지
	최소 및 최소	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	가상화 –KVM 및 가상화–KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	가상화–Xen 및 가상화 –Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	최소	OpenSSH 서버
	가상화	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor(ESXi)	가상화	기본 VMware vSphere Hypervisor(ESXi) 이미지 및 Lenovo VMware ESXi Custom 이미지가 지원됩니다.

배포된 운영 체제에 대한 포트 가용성

일부 포트는 특정 운영 체제 프로필로 차단됩니다. 다음 테이블은 열려 있어야 하는(차단되지 않은) 포트를 나열합니다.

통신	RHEL, Centos 및 Rocky 가상화 프로필[1]	RHEL, Centos, Rocky 기본 및 최소 프로필[1]	SLES 가상화, 기본 및 최소 프로필[2]	Ubuntu 가상화 및 최소 프로필[3]	VMware ESXi 가상화 프로필[4]	Windows 프로필
아웃바운드 (외부 시스템에서 열리는 포트)	• RHEL KVM 네트워킹 장치와의 통신 – 포트 53 및 67의 TCP 및 UDP • SNMP 에이전트와의 통신 – 포트 161의 UDP • SLP 서비스 에이전트, SLP 디렉토리 에이전트와의 통신 – 포트 427의 TCP 및 UDP • HTTP 통신을 통한 CIM-XML – 포트 15988 및 15989의 TCP • KVM 가상 서버 통신 – 포트 49152 – 49215의 TCP					• SMB 통신 – 포트 445의 TCP
인바운드 (XClarity Administrator 어플라이언스에서 열리는 포트)	• SSH – 포트 22의 TCP • RHEL KVM 네트워킹 장치 – 포트 53 및 67의 TCP 및 UDP • SNMP 에이전트 – 포트 162의 UDP • OS 배포 – 포트 445, 3900 및 8443의 TCP 및 UDP • SLP 서비스 에이전트, SLP 디렉토리 에이전트 – 포트 427	• SSH – 포트 22의 TCP • OS 배포 – 포트 445, 3900 및 8443의 TCP 및 UDP	• OS 배포 – 포트 445, 3900 및 8443의 TCP 및 UDP	• OS 배포 – 포트 445, 3900 및 8443의 TCP 및 UDP	• OS 배포 – 포트 445, 3900 및 8443의 TCP 및 UDP	• OS 배포 – 포트 445, 3900 및 8443의 TCP 및 UDP

통신	RHEL, Centos 및 Rocky 가상화 프로필[1]	RHEL, Centos, Rocky 기본 및 최소 프로필[1]	SLES 가상화, 기본 및 최소 프로필[2]	Ubuntu 가상화 및 최소 프로필[3]	VMware ESXi 가상화 프로필[4]	Windows 프로필
	의 TCP 및 UDP • KVM 가상 서버 – 포트 49152 – 49215의 TCP					

1. 기본적으로 Red Hat Enterprise Linux(RHEL) 프로필은 다음 테이블에 나열된 포트를 제외한 모든 포트를 차단합니다.
2. SUSE Linux Enterprise Server(SLES)의 경우 일부 열린 포트가 운영 체제 버전 및 프로필을 기준으로 동적으로 할당됩니다. 열린 포트 전체 목록은 SUSE Linux Enterprise Server 설명서를 참조하십시오.
3. Ubuntu Linux Server의 경우 일부 열린 포트가 운영 체제 버전 및 프로필을 기준으로 동적으로 할당됩니다. 열린 포트 전체 목록은 Ubuntu Server 설명서를 참조하십시오.
4. VMware vSphere Hypervisor(ESXi)(Lenovo 사용자 지정 포함)에 대한 열린 포트 전체 목록은 VMware 기술 자료 웹 사이트에서 ESXi VMware 설명서를 참조하십시오.

원격 파일 서버 구성

로컬 시스템 또는 원격 파일 서버에서 OS 이미지 리포지토리에 OS 이미지, 장치 드라이버 및 부팅 파일을 가져올 수 있습니다. 원격 파일 서버에서 파일을 가져오려면 먼저 원격 파일 서버 연결을 인증하는 데 사용되는 프로필을 만들어야 합니다.

이 작업 정보

다음은 지원되는 암호화 알고리즘입니다.
- RSA–2048비트
- RSA–4096비트
- ECDSA–521비트(secp521r1 곡선)

다음 프로토콜은 지원되지 않습니다.
- 인증을 사용하는 HTTP.
- 기본 인증을 사용하는 HTTP.
- 기본 인증을 사용하는 HTTPS(인증서 유효성 검증).
- 인증을 사용하지 않는 HTTPS(인증서 유효성 검증).
- 암호 인증을 사용하는 FTP.
- 암호 인증을 사용하는 SFTP(클라이언트 유효성 검증).
- 공개 키 인증을 사용하는 SFTP(클라이언트 유효성 검증)

SFTP 공개 키 인증 및 HTTPS 인증서 유효성 검증의 경우 Lenovo XClarity Administrator가 원격 파일 서버의 인증서를 유효성 검증합니다. 서버 인증서가 신뢰 저장소에 없는 경우 서버 인증서를 승인하고 신뢰 저장소에 추가하라는 메시지가 표시됩니다. 유효성 인증 문제 해결에 대한 정보는 XClarity Administrator 온라인 설명서에서 서버 인증 유효성 검증 실패의 내용을 참조하십시오.

절차

원격 파일 서버를 구성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 구성 대화 상자를 표시합니다.

단계 3. **원격 파일 서버** 프로토콜 목록에서 원격 파일 서버에 대한 프로토콜을 선택하십시오.

단계 4. **만들기**를 클릭하십시오. 원격 파일 서버 구성 대화 상자가 표시됩니다.

참고: 이 대화 상자는 선택한 프로토콜에 따라 다릅니다.

단계 5. 서버 이름, 주소 및 포트를 입력하십시오.

단계 6. 기본 인증을 사용하는 HTTP, HTTPS, FTP 및 SFTP의 경우 서버에 액세스하는 데 인증이 필요한 경우 사용자 이름 및 암호를 입력하십시오.

단계 7. 기본 인증을 사용하는 SFTP의 경우 **서버 인증서 유효성 검사**를 클릭하여 공개 키 서명을 확보하십시오.

참고: OS 배포 프로세스가 SFTP 파일 서버의 공개 키를 신뢰하지 않는다는 내용의 대화 상자가 표시될 수 있습니다. **확인**을 클릭하여 OS 배포 신뢰할 수 있는 키 스토어에서 SFTP 공개 키를 저장하고 신뢰합니다. 성공하면 공개 키 서명이 SFTP **서버 공개 키 서명** 필드에 표시됩니다.

단계 8. 공개 키 인증을 사용하는 SFTP의 경우:

a. 서버에 액세스하는 데 인증이 필요한 경우 키 암호 및 암호를 입력하고 키 유형을 선택하십시오.

b. **관리 서버 키 생성**을 클릭하여 공개 키 서명을 확보하십시오.

c. 생성된 키를 SFTP 원격 파일 서버의 authorized_keys 파일에 복사하십시오.

d. XClarity Administrator에서 **관리 키가 서버에 복사되었습니다** 확인란을 선택하십시오.

e. **서버 인증서 유효성 검사**를 클릭하여 공개 키 서명의 유효성을 검사하십시오.

참고: OS 배포 프로세스가 SFTP 파일 서버의 공개 키를 신뢰하지 않는다는 내용의 대화 상자가 표시될 수 있습니다. **확인**을 클릭하여 OS 배포 신뢰할 수 있는 키 스토어에서 SFTP 공개 키를 저장하고 신뢰합니다. 성공하면 공개 키 서명이 SFTP **서버 공개 키 서명** 필드에 표시됩니다.

f. **저장**을 클릭하십시오.

단계 9. **서버 저장**을 클릭하십시오.

완료한 후에

원격 파일 서버 구성 대화 상자에서 다음 작업을 수행할 수 있습니다.

- **새로 고침** 아이콘()을 클릭하여 원격 파일 서버 목록을 새로 고치십시오.
- **편집** 아이콘()을 클릭하여 선택한 원격 파일 서버를 수정하십시오.

- **삭제** 아이콘()을 클릭하여 선택한 원격 파일 서버를 제거하십시오.

운영 체제 이미지 가져오기

사용이 허가된 운영 체제를 관리 서버로 배치하기 전에, XClarity Administrator OS 이미지 리포지토리로 이미지를 가져와야 합니다.

이 작업 정보

가져와 배포할 수 있는 운영 체제 이미지에 대한 정보는 지원되는 운영 체제의 내용을 참조하십시오.

지원되는 기본 및 사용자 정의 운영 체제 목록은 지원되는 운영 체제Lenovo XClarity Administrator 온라인 설명서에서 지원되는 운영 체제의 내용을 참조하십시오.

이미지를 한 번에 하나만 가져올 수 있습니다. 다른 이미지 가져오기를 시도하기 전에 OS 이미지 리포지토리에 이미지가 표시될 때까지 기다리십시오. 운영 체제 이미지 가져오기는 시간이 걸릴 수 있습니다.

ESXi의 경우에만 주/부 버전이 같은 여러 ESXi 이미지를 OS 이미지 리포지토리로 가져올 수 있습니다.

ESXi의 경우에만 주/부 버전 및 빌드 번호가 같은 여러 개의 사용자 지정된 ESXi 이미지를 OS 이미지 리포지토리로 가져올 수 있습니다.

운영 체제 이미지를 가져오는 경우 XClarity Administrator는 다음과 같이 합니다.

- 운영 체제를 가져오기 전에 OS 이미지 리포지토리에 충분한 공간이 있는지 확인합니다. 이미지를 가져올 충분한 공간이 없는 경우 리포지토리에서 기존 이미지를 삭제하고 다시 새 이미지 가져오기를 시도하십시오.
- 해당 이미지의 프로필을 하나 이상 만들고 그 프로필을 OS 이미지 리포지토리에 저장합니다. 각 *프로필*에는 OS 이미지와 설치 옵션이 포함됩니다. 사전 정의된 OS 이미지 프로필에 대한 자세한 정보는 운영 체제 이미지 프로필의 내용을 참조하십시오.

참고: Internet Explorer 및 Microsoft Edge 웹 브라우저에는 4GB의 업로드 제한이 있습니다. 가져오는 파일의 크기가 4GB보다 큰 경우, 다른 웹 브라우저(예, Chrome 또는 Firefox)의 사용을 고려하거나 파일을 원격 파일 서버에 복사한 다음 **원격 가져오기** 옵션을 사용하여 가져오십시오.

절차

OS 이미지 리포지토리에 운영 체제 이미지를 가져오려면 다음 단계를 완료하십시오.

단계 1. 운영 체제의 라이센스가 부여된 ISO 이미지를 확보하십시오.

참고: 사용자는 운영 체제에 대한 해당 라이센스를 확보할 책임이 있습니다.

단계 2. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 3. **파일 가져오기** 아이콘()을 클릭하여 OS 이미지 및 파일 가져오기 대화 상자를 표시하십시오.

단계 4. **로컬** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.

단계 5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

단계 6. 경로와 ISO 이미지 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 ISO 이미지를 찾으십시오.

*로컬 파일 서버*를 사용하도록 선택한 경우 ISO 이미지 파일의 절대 경로를 입력해야 합니다. *원격 파일 서버*를 사용하도록 선택한 경우 ISO 이미지 파일의 절대 경로(예, /home/user/isos.osimage.iso) 또는 상대 경로(예, /isos.osimage.iso)를 입력해야 합니다(원격 파일 서버의 구성에 따라 다름). 파일을 찾을 수 없으면 파일의 경로가 올바른지 확인한 다음 다시 시도하십시오.

단계 7. **옵션:** OS 이미지에 대한 설명을 입력하십시오.

단계 8. **옵션:** 체크섬 유형을 선택하여 XClarity Administrator에 가져오는 ISO 이미지가 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 OS 이미지의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 이미지가 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 이미지를 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

단계 9. **가져오기**를 클릭하십시오.

팁: ISO 이미지는 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 이미지를 가져오는 시간에 영향을 줍니다. 업로드가 완료되기 전에 운영 체제 이미지가 업로드되는 웹 브라우저 또는 창을 닫는 경우 가져오기가 실패합니다.

결과

XClarity Administrator는 OS 이미지를 업로드하고 OS 이미지 리포지토리에서 이미지 프로필을 만듭니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만듭니다.
- **사용자 지정한 프로필 만들기** 아이콘()을 클릭하여 OS 이미지를 사용자 지정합니다.
- **편집** 아이콘()을 클릭하여 OS 이미지를 수정합니다.
- **프로필 가져오기/내보내기 ➞ 사용자 지정된 프로필 이미지 가져오기**를 클릭하여 사용자 지정 OS 이미지 프로필을 가져와서 기본 OS 이미지에 적용합니다(사용자 지정 OS 이미지 프로필 가져오기 참조).
- **삭제** 아이콘()을 클릭하여 선택한 OS 이미지 또는 사용자 지정 OS 이미지 프로필을 삭제합니다.
- **프로필 가져오기/내보내기 ➞ 사용자 지정된 프로필 이미지 내보내기**를 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 내보냅니다.

참고: Windows Server 이미지를 가져올 때 연관된 번들 파일도 가져와야 합니다. Lenovo는 미리 정의된 WinPE_64.wim 부팅 파일을 장치 드라이버 세트와 함께 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있어, **장치 드라이버** 또는 **부팅 파일** 탭에서 번들 파일을 가져올 수 있습니다..자세한 정보는 부팅 파일 가져오기 및 장치 드라이버 가져오기의 내용을 참조하십시오.

OS 이미지 프로필 사용자 지정

*기본 운영 체제*는 OS 이미지 리포지토리로 가져온 전체 OS 이미지입니다. 가져온 기본 이미지에는 해당 이미지의 설치 구성을 설명하는 미리 정의된 프로필이 들어 있습니다. 특정 구성에 배포할 수 있는 기본 OS 이미지에서 사용자 지정 프로필을 만들 수도 있습니다. 사용자 지정 프로필에는 사용자 지정 파일 및 설치 옵션이 포함됩니다.

참고: 사용자 지정 OS 이미지 프로필에 사용자 지정 Microsoft Windows 서버 이미지를 만들 수 없습니다.

Windows 및 SLES를 비롯하여 OS 이미지를 사용자 지정하고 배포하는 몇 가지 예제 시나리오는 영어로만 제공됩니다. 자세한 정보는 새 장치 설정을 위한 엔드투엔드 시나리오의 내용을 참조하십시오.

다음 유형의 파일을 사용자 지정 OS 이미지 프로필에 추가할 수 있습니다.

- **부팅 파일**

  부팅 파일은 부트스트랩 설치 환경으로 작동합니다. Windows의 경우 부팅 파일은 WinPE(Windows Pre-installation) 파일입니다. Windows를 배포하려면 WinPE 부팅 파일이 필요합니다.

  Lenovo XClarity Administrator는 미리 정의된 부팅 파일 및 사용자 정의 부팅 파일을 지원합니다.

  - **미리 정의된 부팅 파일**. Lenovo는 미리 정의된 OS 이미지 프로필을 배포하는 데 사용할 수 있는 WinPE_64.wim 부팅 파일을 제공합니다.

    Lenovo는 미리 정의된 WinPE_64.wim 부팅 파일을 장치 드라이버 세트와 함께 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있어, **장치 드라이버** 또는 **부팅 파일** 탭에서 번들 파일을 가져올 수 있습니다.

    참고:

    - 미리 정의된 부팅 파일은 XClarity Administrator와 함께 미리 로드되지 않습니다. Windows 프로필을 배포하기 전에 먼저 부팅 파일을 OS 이미지 리포지토리로 가져와야 합니다.
    - XClarity Administrator를 설치할 때 로드된 미리 정의된 부팅 파일은 삭제할 수 없습니다. 그러나 Lenovo 번들에서 가져온 미리 정의된 부팅 파일은 삭제할 수 있습니다.
    - XClarity Administrator에서는 가져온 번들 파일이 Lenovo에서 서명한 파일이어야 합니다. 번들 파일을 가져올 때 .asc 서명 파일도 가져와야 합니다.

– **사용자 지정 부팅 파일**. WinPE 부팅 파일을 만들어 Windows 배포를 위한 부팅 옵션을 사용자 지정할 수 있습니다. 그런 다음 사용자 지정 Windows 프로필에 부팅 파일을 추가할 수 있습니다.

  XClarity Administrator는 올바른 형식으로 부팅 파일을 작성하기 위한 스크립트를 제공합니다. 사용자 지정 부팅 파일을 만드는 방법에 대한 정보는 부팅(WinPE) 파일 만들기 및 Windows PE(WinPE) 소개 웹 사이트의 내용을 참조하십시오.

  사용자 지정 부팅 파일 가져오기에 대해 다음 파일 유형이 지원됩니다.

운영 체제	지원되는 부팅 파일 유형	지원되는 부팅 파일 유형
CentOS Linux	지원되지 않음	지원되지 않음
Microsoft® Windows® Azure Stack HCI	지원되지 않음	지원되지 않음
Microsoft Windows Hyper-V Server	**genimage.cmd** 스크립트를 사용하여 만들어진 WinPE 파일이 포함된 .zip 파일	장치 드라이버 및 부팅 파일이 포함된 .zip 파일
Microsoft Windows Server	**genimage.cmd** 스크립트를 사용하여 만들어진 WinPE 파일이 포함된 .zip 파일	장치 드라이버 및 부팅 파일이 포함된 .zip 파일
Red Hat® Enterprise Linux (RHEL) Server	지원되지 않음	지원되지 않음
Rocky Linux	지원되지 않음	지원되지 않음
SUSE® Linux Enterprise Server(SLES)	지원되지 않음	지원되지 않음
Ubuntu	지원되지 않음	지원되지 않음
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	지원되지 않음	지원되지 않음

- **장치 드라이버**

  배포할 운영 체제 이미지에 적절한 이더넷, Fibre Channel 및 하드웨어의 스토리지 어댑터 장치 드라이버가 포함되어 있어야 합니다. I/O 어댑터 장치 드라이버가 운영 체제 이미지나 프로필에 포함되지 않은 경우 어댑터는 OS 배포에 대해 지원되지 않습니다. 필요한 기본 제공하지 않는 장치 드라이버가 포함된 사용자 지정 OS 이미지 프로필을 만들 수 있습니다.

  Lenovo XClarity Administrator는 기본 제공 장치 드라이버는 물론 사용자 지정 및 미리 정의된 기본 제공하지 않는 장치 드라이버를 지원합니다.

  – **기본 제공 장치 드라이버**. XClarity Administrator는 기본 제공 장치 드라이버를 관리하지 않습니다. 항상 필요한 최신 기본 제공 장치 드라이버가 준비되도록 최신 운영 체제를 설치하십시오.

    참고: 사용자 지정 WinPE 부팅 파일을 만들고 장치 드라이버 파일을 `C:\drivers` 디렉토리의 호스트 시스템에 복사하여 사용자 지정된 Windows 프로필에 기본 제공 장치 드라이버를 추가할 수 있습니다. 사용자 지정 부팅 파일을 사용하는 사용자 지정 OS 이미지 프로필을 만드는 경우 C:\drivers 디렉토리에 있는 장치 드라이버는 WinPE와 최종 OS 둘 다에 포함됩니다. 장치 드라이버는 받은 편지함처럼 취급됩니다. 따라서 사용자 지정 OS 이미지 프로필 작성 시 사용할 장치 드라이버를 지정할 때 이러한 받은 편지함 장치 드라이버를 XClarity Administrator로 가져올 필요가 없습니다.

  – **미리 정의된 장치 드라이버** ThinkSystem 서버의 경우, XClarity Administrator는 최종 운영 체제의 기본 네트워크 및 스토리지 구성은 물론 운영 체제 설치를 가능하게 하는 기본 제공하지 않는 Linux용 장치 드라이버 세트와 함께 미리 로드됩니다. 이러한 미리 정의된 장치 드라이버를 사용자 지정 OS 이미지 프로필에 추가한 다음 프로필을 관리되는 서버에 배포할 수 있습니다.

    Lenovo는 미리 정의된 장치 드라이버 세트를 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 현재 번들 파일은 Windows에서만 사용할 수 있습니다.

번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있으면 **장치 드라이버** 또는 **부팅 이미지** 탭에서 번들을 가져올 수 있습니다.

참고:

- 기본적으로 미리 정의된 OS 이미지 프로필에는 미리 정의된 장치 드라이버가 포함됩니다.
- XClarity Administrator를 설치할 때 로드된 미리 정의된 장치 드라이버는 삭제할 수 없습니다. 그러나 Lenovo 번들에서 가져온 미리 정의된 장치 드라이버는 삭제할 수 있습니다.
- XClarity Administrator에서는 가져온 번들 파일이 Lenovo에서 서명한 파일이어야 합니다. 번들 파일을 가져올 때 .asc 서명 파일도 가져와야 합니다.

- **사용자 지정 장치 드라이버** 기본 제공되지 않는 장치 드라이버를 OS 이미지 리포지토리로 가져온 다음 이러한 장치 드라이버를 사용자 지정 OS 이미지 프로필에 추가할 수 있습니다.

  Lenovo YUM 리포지토리 웹 사이트에서, 공급업체(예, Red Hat)에서 또는 직접 생성한 사용자 지정 장치 드라이버를 통해 장치 드라이버를 확보할 수 있습니다. 일부 Windows 장치 드라이버의 경우 설치 exe에서 로컬 시스템으로 장치 드라이버를 추출하고 .zip 아카이브 파일을 작성하여 사용자 지정 장치 드라이버를 생성할 수 있습니다.

  사용자 지정 장치 드라이버 가져오기에 대해 다음 파일 유형이 지원됩니다.

운영 체제	지원되는 장치 드라이버 파일 유형
CentOS Linux	지원되지 않음
Microsoft® Windows® Azure Stack HCI	지원되지 않음
Microsoft Windows Hyper-V Server	일반적으로 .inf, .cat 및 .dll 파일을 그룹화하는 원시 장치 드라이버 파일이 들어 있는 .zip 파일입니다.
Microsoft Windows Server	일반적으로 .inf, .cat 및 .dll 파일을 그룹화하는 원시 장치 드라이버 파일이 들어 있는 .zip 파일입니다.
Red Hat® Enterprise Linux (RHEL) Server	.rpm 또는 .iso 이미지 형식의 드라이버 업데이트 디스크(DUD) **참고:** DUD .rpm을 사용자 지정 프로필에 적용하면 .rpm이 최종 운영 체제에만 설치됩니다. 설치 환경(initrd)에는 설치되지 않습니다. 사용자 지정 장치 드라이버를 initrd에 설치하려면, DUD .iso를 가져와서 .iso를 사용자 지정 프로필에 적용하십시오.
Rocky Linux	지원되지 않음
SUSE® Linux Enterprise Server(SLES)	.rpm 또는 .iso 이미지 형식의 드라이버 업데이트 디스크(DUD) **참고:** DUD .rpm을 사용자 지정 프로필에 적용하면 .rpm이 최종 운영 체제에만 설치됩니다. 설치 환경(initrd)에는 설치되지 않습니다. 사용자 지정 장치 드라이버를 initrd에 설치하려면, DUD .iso를 가져와서 .iso를 사용자 지정 프로필에 적용하십시오.
Ubuntu	지원되지 않음
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	.vib 이미지 형식의 장치 드라이버

참고: OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

- **사용자 지정 구성 설정**

  구성 설정은 OS 배포 중에 동적으로 수집해야 하는 데이터를 설명합니다. Lenovo XClarity Administrator는 전역, 네트워크 및 스토리지 위치 설정을 포함하여 미리 정의된 구성 설정 세트를 사용합니다. 이러한 미리 정의된 구성 설정을 사용하고 XClarity Administrator를 통해 사용할 수 없는 사용자 정의 구성 설정을 추가할 수 있습니다.

  사용자 정의 구성 설정은 JSON 스키마 형식으로 정의됩니다. 스키마는 JSON 사양을 준수해야 합니다.

사용자 지정 구성 설정을 XClarity Administrator로 가져올 때 XClarity Administrator에서 JSON 스키마의 유효성을 검사합니다. 유효성 검사가 통과되면 XClarity Administrator가 각 설정에 대해 사용자 지정 매크로를 생성합니다.

무인 파일 및 설치 후 스크립트에서 사용자 정의 매크로를 사용할 수 있습니다.

무인 파일의 경우

그런 다음 사용자 정의 구성 파일을 무인 파일과 연결하고 이러한 사용자 정의 매크로(및 미리 정의된 매크로)를 해당 무인 파일에 포함시킬 수 있습니다.

하나 이상의 사용자 지정 구성 설정 파일을 사용자 지정 프로필에 추가할 수 있습니다. OS 프로필을 대상 서버 세트에 배포할 때 사용할 구성 설정 파일을 선택할 수 있습니다. XClarity Administrator는 구성 설정 파일의 JSON 스키마를 기반으로 하여 OS 이미지 배포 대화 상자에서 **사용자 정의 설정** 탭을 렌더링하고 파일에 정의된 각 설정(JSON 오브젝트)에 대한 값을 지정할 수 있습니다.

참고: 필수 사용자 지정 구성 설정을 입력하지 않은 경우 OS 배포가 진행되지 않습니다.

설치 후 스크립트의 경우

OS 배포 중에 데이터가 수집된 후, XClarity Administrator는 설치 후 스크립트에서 사용할 수 있는 호스트 시스템의 구성 설정 파일(선택한 파일의 사용자 정의 설정 및 미리 정의된 설정의 서브세트 포함)의 인스턴스를 만듭니다.

참고:

- 구성 설정 파일은 사용자 지정 OS 이미지 프로필에 고유합니다.
- 미리 정의된 OS 이미지 프로필의 구성 설정은 수정할 수 없습니다.
- 구성 설정은 다음 운영 체제에서만 지원됩니다.
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server(SLES)
  - VMware vSphere® Hypervisor (ESXi)(Lenovo Customization 6.0u3 이상 업데이트 버전 및 6.5 이상 버전 포함)

OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

- **사용자 지정 무인 파일**

  무인 파일을 사용하여 운영 체제의 배포를 자동화하도록 OS 이미지 프로필을 사용자 지정할 수 있습니다.

  사용자 지정 무인 파일에 대해 다음 파일 유형이 지원됩니다.

운영 체제	지원되는 파일 유형	자세한 정보
CentOS Linux	지원되지 않음	
Microsoft® Windows® Azure Stack HCI	지원되지 않음	
Microsoft Windows Hyper-V Server	지원되지 않음	
Microsoft Windows Server	무인(.xml)	무인 파일에 대한 자세한 정보는 무인 Windows 설치 참조 웹 페이지의 내용을 참조하십시오.

운영 체제	지원되는 파일 유형	자세한 정보
Red Hat® Enterprise Linux (RHEL) Server	Kickstart(.cfg)	무인 파일에 대한 자세한 정보는 Red Hat: Kickstart로 설치 자동화 웹 페이지의 내용을 참조하십시오. 파일에 %pre, %post, %firstboot 섹션을 추가할 때 다음을 고려하십시오. – 무인 파일에 %pre, %post, %firstboot 섹션을 여러 개 포함시킬 수 있습니다. 그러나 섹션의 순서에 유의해야 합니다. – 권장 #predefined.unattendSettings.preinstall-Config# 매크로가 무인 파일이 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %pre 섹션 앞에 %pre 섹션을 추가합니다. – 권장 #predefined.unattendSettings.postinstall-Config# 매크로가 무인 파일에 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %post 및 %firstboot 섹션 앞에 %post 및 %firstboot 섹션을 추가합니다.
Rocky Linux	Kickstart (.cfg)	무인 파일에 대한 자세한 정보는 Red Hat: Kickstart로 설치 자동화 웹 페이지의 내용을 참조하십시오. 파일에 %pre, %post, %firstboot 섹션을 추가할 때 다음을 고려하십시오. – 무인 파일에 %pre, %post, %firstboot 섹션을 여러 개 포함시킬 수 있습니다. 그러나 섹션의 순서에 유의해야 합니다. – 권장 #predefined.unattendSettings.preinstall-Config# 매크로가 무인 파일이 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %pre 섹션 앞에 %pre 섹션을 추가합니다. – 권장 #predefined.unattendSettings.postinstall-Config# 매크로가 무인 파일에 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %post 및 %firstboot 섹션 앞에 %post 및 %firstboot 섹션을 추가합니다.
SUSE® Linux Enterprise Server(SLES)	AutoYast(.xml)	무인 파일에 대한 자세한 정보는 SUSE: AutoYaST 웹 페이지의 내용을 참조하십시오.
Ubuntu	지원되지 않음	
Lenovo Customization 을 사용하는 VMware vSphere® Hypervisor(ESXi)	Kickstart(.cfg)	ESXi 6.0u3 이상 업데이트 및 6.5 이상에만 지원됩니다. 무인 파일에 대한 자세한 정보는 VMware: 스크립트를 사용하여 호스트 설치 및 업그레이드 웹 페이지의 내용을 참조하십시오. 파일에 %pre, %post, %firstboot 섹션을 추가할 때 다음을 고려하십시오. – 무인 파일에 %pre, %post, %firstboot 섹션을 여러 개 포함시킬 수 있습니다. 그러나 섹션의 순서에 유의해야 합니다. – 권장 #predefined.unattendSettings.preinstall-Config# 매크로가 무인 파일이 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %pre 섹션 앞에 %pre 섹션을 추가합니다. – 권장 #predefined.unattendSettings.postinstall-Config# 매크로가 무인 파일에 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %post 및

운영 체제	지원되는 파일 유형	자세한 정보
		%firstboot 섹션 앞에 %post 및 %firstboot 섹션을 추가합니다.

주의:

- 미리 정의된 매크로 및 사용자 지정 매크로(구성 설정)를 오브젝트의 고유한 이름을 사용하여 무인 파일에 삽입할 수 있습니다. 미리 정의된 값은 XClarity Administrator 인스턴스에 따라 동적입니다. 사용자 지정 매크로는 OS 배포 중에 지정된 사용자 입력에 따라 동적입니다.

  참고:

  - 매크로 이름을 해시 기호(#)로 묶으십시오.
  - 중첩된 이름 오브젝트의 경우, 마침표를 사용하여 각 오브젝트 이름을 구분합니다(예, #server_settings.server0.locale#).
  - 사용자 정의 매크로의 경우 최상위 오브젝트 이름을 포함하지 마십시오. 미리 정의된 매크로의 경우 매크로 이름 앞에 "predefined"를 붙이십시오.
  - 템플리트에서 오브젝트를 작성할 때, 이름은 0부터 시작하는 고유 번호(예, server0 및 server1)로 추가됩니다.
  - 각 사용자 정의 설정 옆에 있는 도움말 아이콘(?) 위에 놓으면 사용자 정의 설정 탭의 OS 이미지 배포 대화 상자에서 각 매크로의 이름을 볼 수 있습니다.
  - 미리 정의된 매크로 목록은 미리 정의된 매크로의 내용을 참조하십시오. 사용자 지정 구성 설정 및 매크로에 대한 정보는 사용자 정의 매크로의 내용을 참조하십시오.
- XClarity Administrator는 OS 설치 프로그램을 비롯하여 몇 가지 다른 중요한 설치 단계에서 상태를 전달하는 데 사용되는 미리 정의된 매크로를 다음과 같이 제공합니다. 이러한 매크로를 무인 파일에 포함시키는 것이 좋습니다(무인 파일에 미리 정의된 사용자 지정 매크로 삽입 참조).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

- **사용자 지정 설치 스크립트**

  OS 배포가 완료된 후 설치 스크립트를 실행하도록 OS 이미지 프로필을 사용자 지정할 수 있습니다.

  현재 설치 후 스크립트만 지원됩니다.

  다음 표에는 Lenovo XClarity Administrator가 각 운영 체제에 따라 지원하는 설치 스크립트의 파일 유형이 나열되어 있습니다. 특정 운영 체제 버전은 XClarity Administrator가 지원하는 해당 파일 형식을 모두 지원하지는 않습니다(예, 일부 RHEL 버전은 최소 프로파일에 Perl을 포함하지 않을 수 있으므로 Perl 스크립트가 실행되지 않습니다). 배포할 운영 체제 버전에 대해 올바른 파일 유형을 사용해야 합니다.

운영 체제	지원되는 파일 유형	자세한 정보
CentOS Linux	지원되지 않음	
Microsoft® Windows® Azure Stack HCI	지원되지 않음	
Microsoft Windows Hyper-V Server	지원되지 않음	
Microsoft® Windows® Server	명령 파일(.cmd), Power-Shell(.ps1)	기본 사용자 지정 데이터 및 파일 경로는 C:\lxca입니다. 설치 스크립트에 대한 자세한 정보는 Windows 설치에 사용자 지정 스크립트 추가 웹 페이지의 내용을 참조하십시오.

운영 체제	지원되는 파일 유형	자세한 정보
Red Hat® Enterprise Linux (RHEL) Server	Bash(.sh), Perl(.pm or .pl), Python(.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 RHEL: 설치 후 스크립트 웹 사이트의 내용을 참조하십시오.
Rocky Linux	Bash(.sh), Perl(.pm or .pl), Python(.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 RHEL: 설치 후 스크립트 웹 사이트의 내용을 참조하십시오.
SUSE® Linux Enterprise Server(SLES)	Bash(.sh), Perl(.pm or .pl), Python(.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 SUSE: 사용자 정의 사용자 스크립트 웹 페이지의 내용을 참조하십시오.
Ubuntu	지원되지 않음	
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	Bash (.sh), Python (.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 VMware: 스크립트 웹 페이지 설치 및 업그레이드의 내용을 참조하십시오.

- **사용자 지정 소프트웨어**

  OS 배포 및 설치 후 스크립트가 완료된 후 사용자 지정 소프트웨어 페이로드를 설치하도록 OS 이미지 프로필을 사용자 지정할 수 있습니다.

  다음 파일 유형이 사용자 지정 소프트웨어에서 지원됩니다.

운영 체제	지원되는 파일 유형	자세한 정보
CentOS Linux	지원되지 않음	
Microsoft® Windows® Azure Stack HCI	지원되지 않음	
Microsoft Windows Hyper-V Server	지원되지 않음	
Microsoft Windows® Server	소프트웨어 페이로드가 포함된 .zip 파일.	기본 사용자 지정 데이터 및 파일 경로는 C:\lxca입니다.
Red Hat® Enterprise Linux (RHEL) Server	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.
SUSE® Linux Enterprise Server(SLES)	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.
Rocky Linux	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.
Ubuntu	지원되지 않음	
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.

사용자 지정 OS 이미지 프로필 가져오기

사용자 지정 OS 이미지 프로필을 가져와 기존 호환 가능 기본 OS 이미지에 추가할 수 있습니다.

이 작업 정보

사용자 지정 프로필을 가져오기 전에 기본 OS 이미지를 가져와야 합니다.

사용자 지정 OS 이미지 프로필은 동일한 유형의 기본 OS 이미지에만 추가할 수 있습니다. 예를 들어 내보낸 프로필이 Windows 2016 이미지용인 경우 OS 이미지 리포지토리에 있는 Windows 2016 이미지에만 프로필을 가져오고 추가할 수 있습니다.

OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 사용자 지정 프로필을 무제한으로 저장할 수 있습니다.

절차

사용자 지정 OS 이미지 프로필을 가져오려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **OS 이미지** 탭에서 사용자 지정 OS 이미지 프로필에 추가할 기본 OS 이미지를 선택하십시오.

단계 3. **프로필 가져오기/내보내기 → 사용자 지정된 프로필 이미지 가져오기**를 클릭하십시오. 사용자 지정 OS 이미지 프로필 가져오기 대화 상자가 표시됩니다.

단계 4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.

단계 5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

단계 6. 프로필 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 프로필을 찾으십시오.

단계 7. **옵션:** 로컬 가져오기의 경우 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

단계 8. **가져오기**를 클릭하십시오.

팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

사용자 지정 OS 이미지 프로필은 OS 이미지 관리 페이지에서 기본 운영 체제 아래에 나열됩니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- 사용자 지정 OS 이미지 프로필을 만듭니다(사용자 지정 OS 이미지 프로필 만들기 참조).
- **프로필 가져오기/내보내기 → 사용자 지정된 프로필 이미지 내보내기**를 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 내보냅니다.

  중요: FTP 또는 SFTP 프로토콜을 사용하도록 설정된 원격 파일 서버에 사용자 지정 OS 이미지 프로필을 내보낼 수 있습니다. HTTP 또는 HTTPS를 사용하도록 설정된 원격 파일 서버에는 이를 내보낼 수 없습니다.
- **편집** 아이콘( )을 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 수정합니다.
- **삭제** 아이콘( )을 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 제거하십시오.

부팅 파일 가져오기

OS 이미지 리포지토리에 부팅 파일을 가져올 수 있습니다. 그런 다음 이러한 파일을 사용하여 Windows 이미지를 사용자 지정하고 배포할 수 있습니다.

이 작업 정보

부팅 파일은 부트스트랩 설치 환경으로 작동합니다. Windows의 경우 부팅 파일은 WinPE(Windows Pre-installation) 파일입니다. Windows를 배포하려면 WinPE 부팅 파일이 필요합니다.

Lenovo XClarity Administrator는 미리 정의된 부팅 파일 및 사용자 정의 부팅 파일을 지원합니다.

- **미리 정의된 부팅 파일**. Lenovo는 미리 정의된 OS 이미지 프로필을 배포하는 데 사용할 수 있는 WinPE_64.wim 부팅 파일을 제공합니다.

Lenovo는 미리 정의된 WinPE_64.wim 부팅 파일을 장치 드라이버 세트와 함께 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있어, **장치 드라이버** 또는 **부팅 파일** 탭에서 번들 파일을 가져올 수 있습니다.

참고:

- 미리 정의된 부팅 파일은 XClarity Administrator와 함께 미리 로드되지 않습니다. Windows 프로필을 배포하기 전에 먼저 부팅 파일을 OS 이미지 리포지토리로 가져와야 합니다.
- XClarity Administrator를 설치할 때 로드된 미리 정의된 부팅 파일은 삭제할 수 없습니다. 그러나 Lenovo 번들에서 가져온 미리 정의된 부팅 파일은 삭제할 수 있습니다.
- XClarity Administrator에서는 가져온 번들 파일이 Lenovo에서 서명한 파일이어야 합니다. 번들 파일을 가져올 때 .asc 서명 파일도 가져와야 합니다.

- **사용자 지정 부팅 파일**. WinPE 부팅 파일을 만들어 Windows 배포를 위한 부팅 옵션을 사용자 지정할 수 있습니다. 그런 다음 사용자 지정 Windows 프로필에 부팅 파일을 추가할 수 있습니다.

  XClarity Administrator는 올바른 형식으로 부팅 파일을 작성하기 위한 스크립트를 제공합니다. 사용자 지정 부팅 파일을 만드는 방법에 대한 정보는 부팅(WinPE) 파일 만들기 및 Windows PE(WinPE) 소개 웹 사이트의 내용을 참조하십시오.

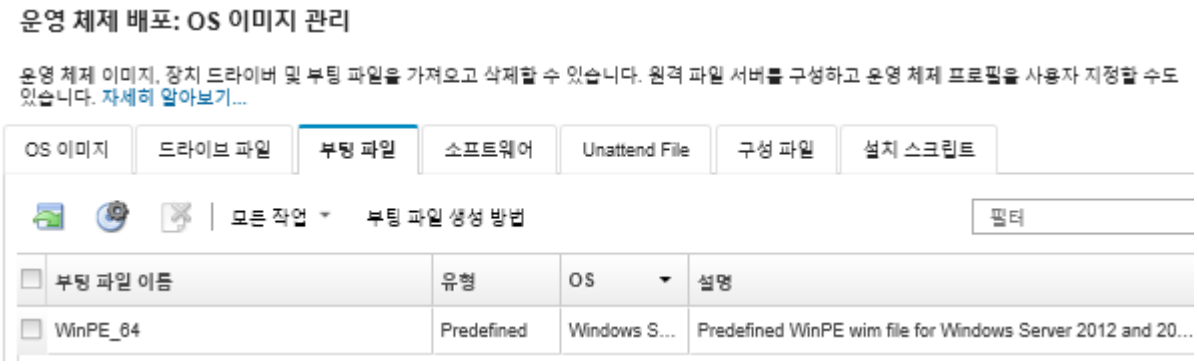
  사용자 지정 부팅 파일 가져오기에 대해 다음 파일 유형이 지원됩니다.

운영 체제	지원되는 부팅 파일 유형	지원되는 부팅 파일 유형
CentOS Linux	지원되지 않음	지원되지 않음
Microsoft® Windows® Azure Stack HCI	지원되지 않음	지원되지 않음
Microsoft Windows Hyper-V Server	genimage.cmd 스크립트를 사용하여 만들어진 WinPE 파일이 포함된 .zip 파일	장치 드라이버 및 부팅 파일이 포함된 .zip 파일
Microsoft Windows Server	genimage.cmd 스크립트를 사용하여 만들어진 WinPE 파일이 포함된 .zip 파일	장치 드라이버 및 부팅 파일이 포함된 .zip 파일
Red Hat® Enterprise Linux (RHEL) Server	지원되지 않음	지원되지 않음
Rocky Linux	지원되지 않음	지원되지 않음
SUSE® Linux Enterprise Server(SLES)	지원되지 않음	지원되지 않음
Ubuntu	지원되지 않음	지원되지 않음
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	지원되지 않음	지원되지 않음

참고: OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

절차

- 부팅 파일이 포함된 Windows 번들 파일을 OS 이미지 리포지토리로 가져오려면 다음 단계를 완료하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
  2. **부팅 파일** 탭을 클릭하십시오.



3. **다운로드 → Windows 번들 파일**을 클릭하여 Lenovo 지원 웹 페이지로 이동한 후 OS 이미지와 관련된 서명 파일과 적절한 번들 파일을 로컬 시스템에 다운로드하십시오.
4. **번들 파일 가져오기** 아이콘()을 클릭하십시오. 번들 파일 가져오기 대화 상자가 표시됩니다.
5. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

   참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.
6. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.
7. 운영 체제 유형 및 릴리스를 선택하십시오.
8. 번들 파일 및 관련 서명 파일의 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 파일을 찾으십시오.
9. **옵션:** 번들 파일에 대한 설명을 입력하십시오.
10. **가져오기**를 클릭하십시오.

    팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

    업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

- OS 이미지 리포지토리에 개별 부팅 파일을 가져오려면 다음 단계를 완료하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
  2. **부팅 파일** 탭을 클릭하십시오.
  3. **파일 가져오기** 아이콘()을 클릭하십시오. 파일 가져오기 대화 상자가 표시됩니다.
  4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

     참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.
  5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.
  6. 운영 체제 유형 및 릴리스를 선택하십시오.
  7. 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 부팅 파일을 찾으십시오.
  8. **옵션:** 부팅 파일에 대한 설명을 입력하십시오.
  9. **옵션:** 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

10. **가져오기**를 클릭하십시오.

    팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

    업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

부팅 파일은 OS 이미지 관리 페이지의 **부팅 파일** 탭에 나열됩니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **파일 서버 구성** 아이콘( )을 클릭하여 원격 파일 서버 프로필을 만듭니다.
- **삭제** 아이콘( )을 클릭하여 선택한 부팅 파일을 제거하십시오.
- 부팅 파일을 사용자 지정 OS 이미지 프로필에 추가하십시오(사용자 지정 OS 이미지 프로필 만들기 참조).

부팅(WinPE) 파일 만들기

Windows 이미지를 사용자 지정하는 데 사용할 수 있는 부팅 파일을 만들 수 있습니다.

시작하기 전에

- 프로비저닝할 운영 체제가 호스트에 설치되어 있는지 확인하십시오. 예를 들어, WinPE 파일을 사용하여 Windows 2016을 프로비저닝하려면 호스트에 Windows 2016을 설치하십시오.
- 설치된 운영 체제와 호환되는 Microsoft ADK도 호스트에 설치되어 있는지 확인하십시오. 예를 들어, Windows 2012R2에는 ADK 버전 8.1 업데이트가 필요합니다.
- 부팅 파일에 추가할 .inf 형식의 장치 드라이버를 확보하십시오.

  Lenovo YUM 리포지토리 웹 사이트에서, 공급업체(예, Red Hat)에서 또는 직접 생성한 사용자 지정 장치 드라이버를 통해 장치 드라이버를 확보할 수 있습니다. 일부 Windows 장치 드라이버의 경우 설치 exe에서 로컬 시스템으로 장치 드라이버를 추출하고 .zip 아카이브 파일을 작성하여 사용자 지정 장치 드라이버를 생성할 수 있습니다.

  Lenovo는 미리 정의된 장치 드라이버 세트를 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 현재 번들 파일은 Windows에서만 사용할 수 있습니다. 번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있으면 **장치 드라이버** 또는 **부팅 이미지** 탭에서 번들을 가져올 수 있습니다.
- `genimage.cmd` 및 `startnet.cmd` 파일을 임시 디렉토리(예, `C:\customwim`)의 호스트로 다운로드하십시오.

  `genimage.cmd` 명령은 WinPE 부팅 파일(.wim 파일 포함)을 생성하는 데 사용됩니다. XClarity Administrator는 `startnet.cmd` 명령을 사용하여 Windows 설치 프로그램을 부트스트랩합니다.
- 장치 드라이버를 부팅 파일에 삽입하는 방법을 결정하십시오. 다음 방법 중 하나로 이를 수행할 수 있습니다.

– 장치 드라이버 파일을 호스트 시스템의 C:\drivers 디렉토리에 복사하여 사용자 지정된 Windows 프로필에 기본 제공 장치 드라이버를 추가하십시오. genimage.cmd가 나중에 실행되면 해당 파일이 부팅 파일에 포함됩니다.

  참고: 사용자 지정 부팅 파일을 사용하는 사용자 지정 OS 이미지 프로필을 만드는 경우 C:\drivers 디렉토리에 있는 장치 드라이버는 WinPE와 최종 OS 둘 다에 포함됩니다. 장치 드라이버는 받은 편지함처럼 취급됩니다. 따라서 사용자 지정 OS 이미지 프로필 작성 시 사용할 장치 드라이버를 지정할 때 이러한 받은 편지함 장치 드라이버를 XClarity Administrator로 가져올 필요가 없습니다.

– 기본 제공하지 않는 장치 드라이버를 부팅 파일에 직접 추가하십시오.

  참고: 이 방법을 사용하는 경우 장치 드라이버는 부팅 파일에만 적용되므로 WinPE 설치 환경에 적용됩니다. 장치 드라이버는 최종 설치된 OS에 적용되지 않습니다. 장치 드라이버를 OS 이미지 장치 드라이버 리포지토리로 수동으로 가져오고 OS 이미지 프로필 사용자 지정의 일부로 장치 드라이버를 선택해야 합니다.

- 부팅 파일에 대한 자세한 정보는 Window PE(WinPE) 소개 웹 사이트의 내용을 참조하십시오.

절차

부팅 파일을 만들려면 다음 단계를 완료하십시오.

단계 1. 관리자 권한이 있는 사용자 ID를 사용하여 Windows ADK 명령 "Deployment and Imaging Tools Environment"를 실행하십시오. 명령 세션이 표시됩니다.

단계 2. 명령 세션에서 `genimage.cmd` 및 `starnet.cmd` 파일이 다운로드된 디렉토리(예, `C:\customwim`)로 변경하십시오.

단계 3. 다음 명령을 실행하여 이전에 탑재된 이미지가 호스트에 없는지 확인하십시오.
```
dism /get-mountedwiminfo
```

탑재된 이미지가 있는 경우 다음 명령을 실행하여 이를 폐기하십시오.

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

단계 4. 사용자 지정된 Windows 프로필에 기본 제공 장치 드라이버를 추가하는 경우 .inf 형식의 원시 장치 드라이버 파일을 호스트 시스템의 `C:\drivers` 디렉토리에 복사하십시오.

단계 5. .wim 형식의 부팅 파일을 생성하려면 다음 명령을 실행하고 명령이 완료될 때까지 몇 분 동안 기다리십시오
```
genimage.cmd amd64 <ADK_Version>
```

여기서, *<ADK_Version>*은 다음 값 중 하나입니다.

- 8.1. Windows 2012 R2의 경우
- 10. Windows 2016의 경우

이 명령은 부팅 파일을 만듭니다. `C:\WinPE_64\media\Boot\WinPE_64.wim`.

단계 6. 다음 명령을 실행하여 부팅 파일을 탑재하십시오.
```
DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
```

단계 7. 기본 제공하지 않는 장치 드라이버를 부팅 파일에 직접 추가하는 경우 다음 단계를 완료하십시오.

1. 다음 디렉토리 구조를 작성하십시오. 여기서, *<os_release>*은(는) `2012`, `2012R2` 또는 `2016`입니다.
   ```
   drivers\<os_release>\
   ```
2. 해당 경로 내의 디렉토리에 .inf 형식의 장치 드라이버를 복사하십시오. 예:
   ```
   drivers\<os_release>\<driver1>\<driver1_files>
   ```
3. `drivers` 디렉토리를 탑재 디렉토리에 복사하십시오. 예:
   ```
   C:\WinPE_64\mount\drivers
   ```

단계 8. 부팅 파일에 추가 사용자 지정을 수행하십시오(예, 폴더, 파일, 시작 스크립트, 언어 팩 및 앱 추가). 부팅 파일 사용자 지정에 대한 자세한 정보는 WinPE: 마운트 및 사용자 지정 웹 사이트의 내용을 참조하십시오.

단계 9. 다음 명령을 실행하여 이미지를 탑재 해제하십시오.
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

단계 10. `C:\WinPE_64\media` 디렉토리의 콘텐츠를 `WinPE_64.zip` 파일로 압축하십시오.

단계 11. .zip 파일을 XClarity Administrator로 가져오십시오(부팅 파일 가져오기 참조).

장치 드라이버 가져오기

개별 장치 드라이버 및 번들 파일을 OS 이미지 리포지토리로 가져올 수 있습니다. 그런 다음 이러한 파일을 사용하여 Linux 및 Windows 이미지를 사용자 지정할 수 있습니다.

이 작업 정보

배포할 운영 체제 이미지에 적절한 이더넷, Fibre Channel 및 하드웨어의 스토리지 어댑터 장치 드라이버가 포함되어 있어야 합니다. I/O 어댑터 장치 드라이버가 운영 체제 이미지나 프로필에 포함되지 않은 경우 어댑터는 OS 배포에 대해 지원되지 않습니다. 필요한 기본 제공하지 않는 장치 드라이버가 포함된 사용자 지정 OS 이미지 프로필을 만들 수 있습니다.

Lenovo XClarity Administrator는 기본 제공 장치 드라이버는 물론 사용자 지정 및 미리 정의된 기본 제공하지 않는 장치 드라이버를 지원합니다.

- **기본 제공 장치 드라이버**. XClarity Administrator는 기본 제공 장치 드라이버를 관리하지 않습니다. 항상 필요한 최신 기본 제공 장치 드라이버가 준비되도록 최신 운영 체제를 설치하십시오.

  참고: 사용자 지정 WinPE 부팅 파일을 만들고 장치 드라이버 파일을 `C:\drivers` 디렉토리의 호스트 시스템에 복사하여 사용자 지정된 Windows 프로필에 기본 제공 장치 드라이버를 추가할 수 있습니다. 사용자 지정 부팅 파일을 사용하는 사용자 지정 OS 이미지 프로필을 만드는 경우 C:\drivers 디렉토리에 있는 장치 드라이버는 WinPE와 최종 OS 둘 다에 포함됩니다. 장치 드라이버는 받은 편지함처럼 취급됩니다. 따라서 사용자 지정 OS 이미지 프로필 작성 시 사용할 장치 드라이버를 지정할 때 이러한 받은 편지함 장치 드라이버를 XClarity Administrator로 가져올 필요가 없습니다.

- **미리 정의된 장치 드라이버** ThinkSystem 서버의 경우, XClarity Administrator는 최종 운영 체제의 기본 네트워크 및 스토리지 구성은 물론 운영 체제 설치를 가능하게 하는 기본 제공하지 않는 Linux용 장치 드라이버 세트와 함께 미리 로드됩니다. 이러한 미리 정의된 장치 드라이버를 사용자 지정 OS 이미지 프로필에 추가한 다음 프로필을 관리되는 서버에 배포할 수 있습니다.

  Lenovo는 미리 정의된 장치 드라이버 세트를 하나의 패키지로 묶어서 번들로 제공합니다. Lenovo Windows 드라이버 및 WinPE 이미지 리포지토리 웹 페이지에서 이 번들을 다운로드한 다음 OS 이미지 리포지토리로 가져올 수 있습니다. 현재 번들 파일은 Windows에서만 사용할 수 있습니다. 번들 파일에 장치 드라이버와 부팅 파일이 모두 포함되어 있으면 **장치 드라이버** 또는 **부팅 이미지** 탭에서 번들을 가져올 수 있습니다.

  참고:

  - 기본적으로 미리 정의된 OS 이미지 프로필에는 미리 정의된 장치 드라이버가 포함됩니다.
  - XClarity Administrator를 설치할 때 로드된 미리 정의된 장치 드라이버는 삭제할 수 없습니다. 그러나 Lenovo 번들에서 가져온 미리 정의된 장치 드라이버는 삭제할 수 있습니다.
  - XClarity Administrator에서는 가져온 번들 파일이 Lenovo에서 서명한 파일이어야 합니다. 번들 파일을 가져올 때 .asc 서명 파일도 가져와야 합니다.

- **사용자 지정 장치 드라이버** 기본 제공되지 않는 장치 드라이버를 OS 이미지 리포지토리로 가져온 다음 이러한 장치 드라이버를 사용자 지정 OS 이미지 프로필에 추가할 수 있습니다.

  Lenovo YUM 리포지토리 웹 사이트에서, 공급업체(예, Red Hat)에서 또는 직접 생성한 사용자 지정 장치 드라이버를 통해 장치 드라이버를 확보할 수 있습니다. 일부 Windows 장치 드라이버의 경

우 설치 exe에서 로컬 시스템으로 장치 드라이버를 추출하고 .zip 아카이브 파일을 작성하여 사용자 지정 장치 드라이버를 생성할 수 있습니다.

사용자 지정 장치 드라이버 가져오기에 대해 다음 파일 유형이 지원됩니다.

운영 체제	지원되는 장치 드라이버 파일 유형
CentOS Linux	지원되지 않음
Microsoft® Windows® Azure Stack HCI	지원되지 않음
Microsoft Windows Hyper-V Server	일반적으로 .inf, .cat 및 .dll 파일을 그룹화하는 원시 장치 드라이버 파일이 들어 있는 .zip 파일입니다.
Microsoft Windows Server	일반적으로 .inf, .cat 및 .dll 파일을 그룹화하는 원시 장치 드라이버 파일이 들어 있는 .zip 파일입니다.
Red Hat® Enterprise Linux (RHEL) Server	.rpm 또는 .iso 이미지 형식의 드라이버 업데이트 디스크(DUD) **참고:** DUD .rpm을 사용자 지정 프로필에 적용하면 .rpm이 최종 운영 체제에만 설치됩니다. 설치 환경(initrd)에는 설치되지 않습니다. 사용자 지정 장치 드라이버를 initrd에 설치하려면, DUD .iso를 가져와서 .iso를 사용자 지정 프로필에 적용하십시오.
Rocky Linux	지원되지 않음
SUSE® Linux Enterprise Server(SLES)	.rpm 또는 .iso 이미지 형식의 드라이버 업데이트 디스크(DUD) **참고:** DUD .rpm을 사용자 지정 프로필에 적용하면 .rpm이 최종 운영 체제에만 설치됩니다. 설치 환경(initrd)에는 설치되지 않습니다. 사용자 지정 장치 드라이버를 initrd에 설치하려면, DUD .iso를 가져와서 .iso를 사용자 지정 프로필에 적용하십시오.
Ubuntu	지원되지 않음
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	.vib 이미지 형식의 장치 드라이버

참고: OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

절차

- 장치 드라이버가 포함된 Windows 번들 파일을 OS 이미지 리포지토리로 가져오려면 다음 단계를 완료하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
  2. **드라이버 파일** 탭을 클릭하십시오.

3. **다운로드 → Windows 번들 파일**을 클릭하여 Lenovo 지원 웹 페이지로 이동한 후 OS 이미지와 관련된 서명 파일과 적절한 번들 파일을 로컬 시스템에 다운로드하십시오.
4. **번들 파일 가져오기** 아이콘()을 클릭하십시오. 번들 파일 가져오기 대화 상자가 표시됩니다.
5. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

   참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.
6. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.
7. 운영 체제 유형 및 릴리스를 선택하십시오.
8. 번들 파일 및 관련 서명 파일의 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 파일을 찾으십시오.
9. **옵션:** 번들 파일에 대한 설명을 입력하십시오.
10. **가져오기**를 클릭하십시오.

    팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

    업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

- 개별 장치 드라이버를 OS 이미지 리포지토리로 가져오려면 다음 단계를 완료하십시오.
  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
  2. **드라이버 파일** 탭을 클릭하십시오.
  3. **파일 가져오기** 아이콘()을 클릭하십시오. 파일 가져오기 대화 상자가 표시됩니다.
  4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

     참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.
  5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

6. 운영 체제 유형 및 릴리스를 선택하십시오.
7. 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 장치 드라이버를 찾으십시오.
8. **옵션:** 장치 드라이버에 대한 설명을 입력하십시오.
9. **옵션:** 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

   체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

   지원되는 체크섬 유형은 다음 세 가지입니다.
   - MD5
   - SHA1
   - SHA256
10. **가져오기**를 클릭하십시오.

    팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

    업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

장치 드라이브 이미지는 OS 이미지 관리 페이지의 **드라이버 파일** 탭에 나열됩니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **파일 서버 구성** 아이콘( )을 클릭하여 원격 파일 서버 프로필을 만듭니다.
- **삭제** 아이콘( )을 클릭하여 선택한 장치 드라이버를 제거하십시오.
- 장치 드라이버를 사용자 지정 OS 이미지 프로필에 추가하십시오(사용자 지정 OS 이미지 프로필 만들기 참조).

사용자 지정 구성 설정 가져오기

구성 설정은 OS 배포 중에 동적으로 수집해야 하는 데이터를 설명합니다. Lenovo XClarity Administrator는 전역, 네트워크 및 스토리지 위치 설정을 포함하여 미리 정의된 구성 설정 세트를 사용합니다. 이러한 미리 정의된 구성 설정을 사용하고 XClarity Administrator를 통해 사용할 수 없는 사용자 정의 구성 설정을 추가할 수 있습니다.

이 작업 정보

사용자 정의 구성 설정은 JSON 스키마 형식으로 정의됩니다. 스키마는 JSON 사양을 준수해야 합니다.

사용자 지정 구성 설정을 XClarity Administrator로 가져올 때 XClarity Administrator에서 JSON 스키마의 유효성을 검사합니다. 유효성 검사가 통과되면 XClarity Administrator가 각 설정에 대해 사용자 지정 매크로를 생성합니다.

무인 파일 및 설치 후 스크립트에서 사용자 정의 매크로를 사용할 수 있습니다.

무인 파일의 경우

그런 다음 사용자 정의 구성 파일을 무인 파일과 연결하고 이러한 사용자 정의 매크로(및 미리 정의된 매크로)를 해당 무인 파일에 포함시킬 수 있습니다.

하나 이상의 사용자 지정 구성 설정 파일을 사용자 지정 프로필에 추가할 수 있습니다. OS 프로필을 대상 서버 세트에 배포할 때 사용할 구성 설정 파일을 선택할 수 있습니다. XClarity Administrator는 구성 설정 파일의 JSON 스키마를 기반으로 하여 OS 이미지 배포 대화 상자에서 **사용자 정의 설정** 탭을 렌더링하고 파일에 정의된 각 설정(JSON 오브젝트)에 대한 값을 지정할 수 있습니다.

참고: 필수 사용자 지정 구성 설정을 입력하지 않은 경우 OS 배포가 진행되지 않습니다.

설치 후 스크립트의 경우

OS 배포 중에 데이터가 수집된 후, XClarity Administrator는 설치 후 스크립트에서 사용할 수 있는 호스트 시스템의 구성 설정 파일(선택한 파일의 사용자 정의 설정 및 미리 정의된 설정의 서브세트 포함)의 인스턴스를 만듭니다.

참고:

- 구성 설정 파일은 사용자 지정 OS 이미지 프로필에 고유합니다.
- 미리 정의된 OS 이미지 프로필의 구성 설정은 수정할 수 없습니다.
- 구성 설정은 다음 운영 체제에서만 지원됩니다.
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server(SLES)
  - VMware vSphere® Hypervisor (ESXi)(Lenovo Customization 6.0u3 이상 업데이트 버전 및 6.5 이상 버전 포함)

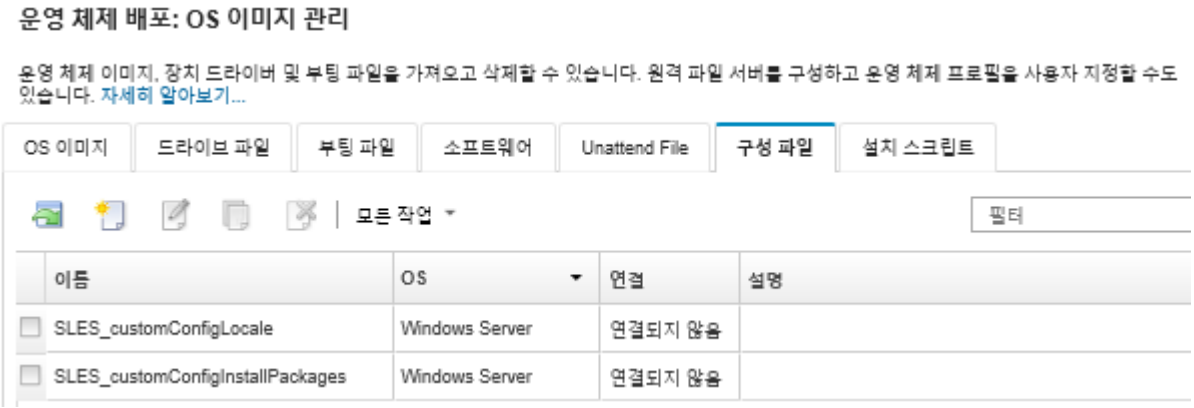
OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

절차

OS 이미지 리포지토리에 구성 설정 파일을 가져오려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **구성 설정** 탭을 클릭하십시오.



단계 3. **파일 가져오기** 아이콁( )을 클릭하십시오. 구성 설정 가져오기 대화 상자가 표시됩니다.

단계 4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콁( )을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.

단계 5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

단계 6. 운영 체제 유형을 선택하십시오.

단계 7. 구성 설정 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 파일을 찾으십시오.

단계 8. **옵션:** 구성 설정에 대한 설명을 입력하십시오.

팁: 설명 필드를 사용하여 같은 이름의 사용자 정의 파일을 구별하십시오.

단계 9. **옵션:** 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

단계 10. **가져오기**를 클릭하십시오. 파일을 가져올 때 JSON 형식의 유효성이 검사됩니다. 오류가 발견되면 오류 메시지 및 위치 정보가 있는 대화 상자가 표시됩니다.

팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

주의: 업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

구성 설정 파일은 OS 이미지 관리 페이지의 **구성 설정** 탭에 나열되어 있습니다.

이 페이지에서 다음 작업을 수행할 수도 있습니다.

- **만들기** 아이콘( )을 클릭한 다음 파일 이름, 설명, OS 유형 및 구성 설정과 값을 지정하여 구성 설정 파일을 만드십시오. 파일을 저장하기 전에 **유효성 검증**을 클릭하여 스키마의 유효성을 검사하십시오.

  편집기는 파일에서 찾은 오류 위치를 식별합니다. 일부 메시지는 영어로만 제공됩니다.
- **편집** 아이콘( )을 클릭하여 구성 설정 파일을 확인하고 수정하십시오.

  무인 파일과 연결된 구성 설정 파일은 편집할 수 없습니다.

  편집기는 파일에서 찾은 오류 위치를 식별합니다. 일부 메시지는 영어로만 제공됩니다.
- **복사** 아이콘( )을 클릭하여 구성 설정 파일을 복사하십시오.

  무인 파일과 연결된 구성 설정 파일을 복사하면 연결된 무인 파일도 복사되고 복사된 두 파일이 자동으로 연결됩니다.
- **삭제** 아이콘( )을 클릭하여 선택한 구성 설정 파일을 제거하십시오.
- **파일 서버 구성** 아이콘( )을 클릭하여 원격 파일 서버 프로필을 만듭니다.

사용자 지정 OS 이미지 프로필에 구성 설정을 추가하는 방법에 대한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

사용자 정의 매크로

*매크로*는 무인 파일이나 설치 후 스크립트에 가변 데이터(구성 설정)를 추가할 수 있는 기능을 제공합니다. Lenovo XClarity Administrator에서 JSON 형식을 사용하여 사용자 지정 구성 설정 파일을 만들어 사용자 정의 설정을 정의할 수 있습니다.

각 사용자 정의 구성 설정의 값은 OS 배포 중에 지정된 사용자 입력에 따라 다릅니다.

사용자 정의 구성 설정을 XClarity Administrator로 가져올 때 XClarity Administrator에서 JSON 스키마의 유효성을 검사합니다. 유효성 검사가 통과되면 XClarity Administrator가 각 설정에 대해 사용자 지정 매크로를 생성합니다.

무인 파일이나 설치 후 스크립트에 사용자 정의 매크로를 삽입하려면, 오브젝트의 고유한 이름을 사용하고 마침표를 사용하여 중첩된 오브젝트를 구분한 다음 매크로 이름을 해시 기호(#)로 묶습니다(예, #server_settings.server0.locale#).

참고:

- 오브젝트 이름을 포함하지 마십시오.
- 템플리트에서 오브젝트를 작성할 때, 이름은 0부터 시작하는 고유 번호(예, server0 및 server1)로 추가됩니다.
- 각 사용자 정의 설정 옆에 있는 **도움말** 아이콘() 위에 놓으면 사용자 정의 설정 탭의 OS 이미지 배포 대화 상자에서 각 매크로의 이름을 볼 수 있습니다.

구성 설정

다음과 같은 사용자 정의 구성 설정을 정의할 수 있습니다.

- 모든 대상 서버에 공통이거나 특정 대상 서버에 고유합니다.
- OS 이미지 프로필을 배포할 때 정적(구성 불가능) 값 또는 동적(구성 가능) 값을 입력합니다.
- 템플릿을 기반으로 다양한 요소를 갖습니다. 예를 들어 배포 중에 0~3 개의 NTP 서버를 지정하는 구성 설정을 정의할 수 있습니다.

일반 설정

OS 배포 중에 OS 이미지 배포 대화 상자의 **일반 설정** 탭에 있는 UI 요소가 content 오브젝트에 표시된 오브젝트를 기반으로 하여 렌더링됩니다. 오브젝트는 모든 대상 서버에서 OS 배포에 필요한 설정 및 값을 설명합니다.

모든 서버에 공통적인 설정을 표시하려면 JSON 파일에 `"common":true` 이름/값 쌍이 포함된 중첩된 오브젝트가 있는 상위 오브젝트가 있어야 합니다.

다음 예제에서는 모든 서버에 동일한 구성 가능(동적) NTP 서버를 사용합니다.

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
      "autoCreateInstance": true,
      "category": "dynamic",
      "common": true,
```

```
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string"
    }],
    "type": "array"
  },
  ...,
}
```

다음 예제에서는 동일한 구성 가능(정적) 설치 후 스크립트 로그 디렉토리를 사용합니다.

```
{
  "category": "dynamic",
  "content": [{
    "category": "static",
    "common": true,
    "description": "Directory location for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
  },
  ...,
}
```

서버 특정 설정

OS 배포 중에 OS 이미지 배포 대화 상자의 **서버 특정 설정** 탭에 있는 UI 요소가 템플릿의 content 오브젝트에 표시된 오브젝트를 기반으로 하여 렌더링됩니다. 오브젝트는 특정 대상 서버에서 OS 배포에 필요한 설정 및 값을 설명합니다.

서버 특정 값이 UI에 수집되면 template 오브젝트를 기반으로 하여 각 대상 서버에 대한 content 오브젝트가 JSON에 생성됩니다. 각 content 오브젝트에는 고유한 name 및 targetServer 필드가 있으며 해당 서버에 대한 값이 입력되어 있습니다.

서버 특정 설정을 표시하려면 JSON 파일에 다음 내용이 포함된 상위 오브젝트가 있어야 합니다.

- "category":"dynamic" 이름/값 쌍.
- "common":false 이름/값 쌍이 포함된 중첩된 오브젝트. 상위 오브젝트의 콘텐츠에서는 한 "common": false 오브젝트만 지원됩니다.
- 내장 콘텐츠 오브젝트가 있는 템플릿 오브젝트. 이 템플릿 배열에는 하나의 객체만 포함될 수 있습니다.

예를 들어 각 대상 서버에 대해 고유한 OS 로케일을 정의하는 경우

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": false,
    "name": "server-settings",
    "optional": false,
    "template": [{
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
```

```
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      }],
      "name": "server",
      "optional": false,
      "type": "assoc_array"
    }],
    "type": "assoc_array"
  },
  ...,
}
```

JSON 사양

다음 표는 JSON 사양에서 허용되는 필드를 설명합니다.

매개변수	필수/옵션	유형	설명
autoCreateInstance	옵션	Boolean	배포 시 템플릿 오브젝트의 인스턴스가 JSON 파일에 자동으로 생성되는지 여부를 나타냅니다. 이는 다음 값 중 하나입니다. • **true**. 배포 시 템플릿 오브젝트의 인스턴스가 JSON 파일에 자동으로 생성됩니다. • **false**. (기본값) 배포 시 템플릿 오브젝트의 인스턴스가 JSON 파일에 자동으로 생성되지 *않습니다*. **참고:** 이 필드는 템플릿 오브젝트에만 배치할 수 있습니다.
category	필수	String	각 설정의 값이 채워지는 방법을 나타냅니다. 이는 다음 값 중 하나입니다. • **dynamic**. 런타임 시 사용자가 값을 입력합니다. Lenovo XClarity Administrator가 OS 배포 중에 이 값을 묻습니다. • **predefined**. Lenovo XClarity Administrator에서 값을 미리 설정합니다. • **static**. 값이 스키마에 지정되며 런타임 시 변경되지 않습니다. 중첩된 오브젝트는 상위 오브젝트에서 이 필드의 값을 상속받습니다. **category**가 상위 오브젝트에서 **static**으로 설정된 경우 모든 중첩된 오브젝트에서도 **static**으로 설정되어야 합니다. **category**가 상위 오브젝트에서 **dynamic**으로 설정된 경우 중첩된 오브젝트에서 **static** 또는 **dynamic**으로 설정될 수 있습니다.
choices	옵션	type 속성과 일치하는 값의 배열	OS 배포(예, ["enabled","disabled"]) 중에 선택할 수 있는 구성 설정의 정적 값(예, string 또는 integer) 배열.

매개변수	필수/옵션	유형	설명
common	옵션	Boolean	이 구성 스키마가 모든 대상 서버에 적용되는지 여부를 나타냅니다. • true. 이 오브젝트는 모든 대상 서버에 적용됩니다. • false. (기본값) 이 오브젝트는 특정 대상 서버에 적용됩니다. 중첩된 오브젝트는 상위 오브젝트에서 이 필드의 값을 상속받습니다. common이 상위 오브젝트에서 true로 설정된 경우 모든 중첩된 오브젝트에서도 true로 설정되어야 합니다. common이 상위 오브젝트에서 false로 설정된 경우 모든 중첩된 오브젝트에서 false로 설정되어야 합니다.
content	옵션	오브젝트 배열	스키마에서 중첩된 오브젝트를 나타내는 패턴입니다. OS 배포 중에 사용자 입력 데이터가 수집되면 이 필드는 배포용으로 생성된 구성 설정 파일의 인스턴스에서 지정된 템플릿의 최종 값을 나타내는 데 사용됩니다.
default	옵션	type에 따라 다름	기본값.
description	옵션	String	오브젝트에 대한 설명입니다.
label	옵션	String	OS 배포 중에 표시되는 사용자 인터페이스의 설정 레이블입니다.
max	옵션	Integer	type이 정수로 설정된 경우 최대값입니다. 기본값은 무제한입니다.
maxElements	옵션	Integer	이 오브젝트에 대한 배열의 최대 항목 수입니다.
-min	옵션	Integer	type이 정수로 설정된 경우 최소값입니다. 기본값은 0입니다.
minElements	옵션	Integer	이 오브젝트에 대한 배열의 최소 항목 수입니다.
name	필수	String	오브젝트의 고유 이름입니다. 이 이름에는 영숫자(az, AZ 및 0-9), 밑줄(_) 및 대시(-)만 사용할 수 있습니다. name을 무인 파일의 사용자 지정 매크로로 참조할 수 있습니다. 중첩된 name 오브젝트를 참조하는 경우 마침표를 사용하여 각 오브젝트를 구분합니다(예, mydeploy.node.locale).
optional	필수	Boolean	오브젝트가 옵션인지 여부를 나타냅니다. 이는 다음 값 중 하나입니다. • true. 이 필드는 옵션입니다. • false. 이 필드는 필수입니다.
regex	옵션	String	값의 유효성을 검사하는 정규 표현식입니다(예, "[\\w\\.]{1,64}$").
script	옵션	문자열 배열	이 오브젝트의 데이터에 대한 종속성이 있는 스크립트 목록(쉼표로 구분)입니다(예, ["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]). **참고:** 스크립트는 설치 스크립트 또는 사용자 지정 소프트웨어로 OS 이미지 프로필에 사용할 수 있어야 합니다.

매개변수	필수/옵션	유형	설명
targetServer	옵션	String	OS 배포의 대상이 되는 서버의 UUID입니다. common이 true인 경우 이 필드는 비어 있거나 널일 수 있으며 대상 서버는 OS 배포 중에 지정됩니다.

template	옵션	오브젝트 배열	재사용 가능한 오브젝트를 나타내는 패턴입니다. OS 배포 중에 이 템플릿은 오브젝트의 여러 인스턴스를 나타낼 수 있습니다. minElements 및 maxElements 필드를 사용하여 인스턴스 수를 제한할 수 있습니다.
			
			다음 예제에서는 템플릿을 사용하여 1 - 3 NTP 서버 배열을 나타냅니다.
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"template": [{
			"autoCreateInstance": true,
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			},
			
			OS 배포 중에 사용자 입력 값이 수집되면 OS가 배포될 각 장치에 대한 특정 콘텐츠가 포함된 구성 설정 파일의 인스턴스가 만들어집니다.
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"content": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver0",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string",
			"value": "192.0.2.1"
			}],
			"template": [{
			"category": "dynamic",

매개변수	필수/옵션	유형	설명

			<pre>"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **참고:**
			• 템플릿은 서버 특정 오브젝트의 최상위 수준에서 *필요*합니다(common = false).
			• category가 static인 경우 템플릿 필드는 무시됩니다.

type	필수	String	오브젝트의 데이터 유형입니다. 이는 다음 값 중 하나입니다. • array • assoc_array • boolean • integer • 암호 • string • user_data
value	옵션	String	구성 설정에 대한 단일 정적 값입니다. **참고:** • default가 설정되면 이 필드는 비어 있거나 널일 수 있습니다. 그렇지 않으면 type이 일치하는 값을 지정하십시오. • type이 password인 경우 암호화되지 않은 문자열을 지정하십시오. • type이 assoc_array 또는 array인 경우 비어 있는 content 필드도 지정해야 합니다. • type이 user_data인 경우 유효한 JSON 형식 value를 지정하십시오. • regex가 설정되면 이 값은 지정된 정규 표현식을 사용하여 유효성이 검사됩니다.

다음 구성 설정 예제에서는 사용자 지정 프로필에 추가될 수 있는 SLES 배포에 대한 로케일 설정을 정의합니다.

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": false,
    "name": "server-settings",
    "optional": false,
    "template": [{
      "autoCreateInstance": true,
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
```

```
      "choices": ["en_US", "pt_BR", "ja_JP"],
      "common": false,
      "description": "This parameter defines the OS language locale to use with this deployment.
                      English, Brazilian Portuguese, and Japanese are supported.",
      "label": "OS Locale",
      "name": "locale",
      "optional": false,
      "type": "string",
      "value": "en_US"
    },
    {
      "category": "dynamic",
      "choices": ["english-us", "pt_BR", "ja_JP"],
      "common": false,
      "description": "This parameter defines the keyboard locale to use with this deployment.
                      English, Brazilian Portuguese, and Japanese are supported.",
      "label": "Keyboard Locale",
      "name": "keyboardLocale",
      "optional": false,
      "type": "string",
      "value": "english-us"
    }],
    "name": "server",
    "optional": false,
    "type": "assoc_array"
  }],
  "type": "assoc_array"
},
{
  "category": "dynamic",
  "common": true,
  "description": "NTP Servers",
  "label": "NTP Servers",
  "maxElements": 3,
  "minElements": 0,
  "name": "common-ntpservers",
  "optional": true,
  "template": [{
    "category": "dynamic",
    "common": true,
    "description": "A NTP Server",
    "label": "NTP Server",
    "name": "ntpserver",
    "optional": true,
    "regex": "[\\w\\.]{1,64}$",
    "type": "string"
  }],
  "type": "array"
},
{
  "category": "static",
  "common": true,
  "description": "Directory for post-installation script logging.",
  "name": "logpath",
  "optional": false,
  "type": "string",
  "value": "/tmp/mylogger.log"
}],
"description": "Custom configuration file for deployment of custom locale, NTP server,
                and directory for post-installation script logs.",
"label": "My Custom Deployment",
```

```
  "name": "myCustomDeploy",
  "optional": false,
  "type": "array"
}
```

다음 예제는 배포 중에 사용자 입력 값이 정의된 후 호스트 시스템에서 생성되는 구성 설정 파일의 인스턴스입니다.

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": false,
    "name": "server-settings",
    "optional": false,
    "content": [{
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                  English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
      {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                  English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server0",
      "optional": false,
      "type": "assoc_array",
      "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
    },
    {
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                  English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
```

```
      {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server1",
      "optional": false,
      "type": "assoc_array",
      "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
      {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server",
      "optional": false,
      "type": "assoc_array"
    }],
    "type": "assoc_array"
  },
  {
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "content": [{
      "category": "dynamic",
```

```
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver0,
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string",
      "value": "192.0.2.1"
    },
    {
      "category": "dynamic",
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver1",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string",
      "value": "192.0.2.2"
    }],
    "template": [{
      "category": "dynamic",
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string"
    }],
    "type": "array"
  },
  {
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logs.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
  }],
  "description": "Custom configuration file for deployment of custom locale, NTP server,
              and directory for post-installation script logs.",
  "label": "My Custom Deployment",
  "name": "myCustomDeploy",
  "optional": false,
  "type": "array"
}
```

미리 정의된 매크로

*매크로*는 무인 파일이나 설치 후 스크립트에 가변 데이터(구성 설정)를 추가할 수 있는 기능을 제공합니다. Lenovo XClarity Administrator에서는 사용할 수 있는 미리 정의된 구성 설정 세트를 제공합니다.

미리 정의된 매크로를 무인 또는 설치 후 스크립트 파일에 삽입하려면, 미리 정의 된 매크로에 대해 "predefined"를 매크로 앞에 붙이고 마침표를 사용하여 중첩된 오브젝트를 구분한 다음 매크로 이름을 해시 기호(#)로 묶습니다(예, # predefined.globalSettings.ipAssignment#).

미리 정의된 각 매크로의 값은 XClarity Administrator 인스턴스에 따라 다릅니다. 예를 들어, **OS 이미지 배포 ➙ 전역 설정 ➙ IP 할당** 필드에서 IP 모드를 지정할 수 있습니다. OS 배포 중에 사용자 입력 값이

수집되면, 값이 미리 정의된 매크로 #predefined.globalSettings.ipAssignment#에 의해 미리 정의된 구성 설정과 ipAssignment 오브젝트 이름의 구성 설정 JSON 파일의 인스턴스에 표시됩니다.

다음 표에서는 XClarity Administrator에서 사용할 수 있는 미리 정의된 매크로(구성 설정)를 나열합니다.

매크로 이름	유형	설명
predefined	Object	모든 미리 정의된 OS 배포 설정에 대한 정보
globalSettings	Object	전역 OS 배포 설정에 대한 정보입니다.
credentials	오브젝트 배열	사용자 자격 증명에 대한 정보
name	String	
type	String	운영 체제 유형. 이는 다음 값 중 하나입니다. • ESXi • LINUX • WINDOWS
ipAssignment	String	운영 체제 배포를 위한 호스트 네트워크 설정 옵션. 이는 다음 값 중 하나입니다. • dhcpv4 • staticv4 • staticv6
isVLANMode	String	VLAN 모드 사용 여부를 나타냅니다. 이는 다음 값 중 하나입니다. • true. VLAN 모드가 사용됩니다. • false. VLAN 모드가 사용되지 않습니다.
hostPlatforms	Object	호스트 플랫폼의 배포 설정
licenseKey	String	Microsoft Windows 또는 VMware ESXi에 사용할 라이센스 키. 라이센스 키가 없으면 이 필드를 null로 설정할 수 있습니다.
networkSettings	Array	네트워크 설정에 대한 정보
dns1	String	운영 체제가 배포된 후 호스트 서버에 사용할 기본 DNS 서버
dns2	String	운영 체제가 배포된 후 호스트 서버에 사용할 대체 DNS 서버
gateway	String	운영 체제가 배포된 후 호스트 서버에 사용할 게이트웨이. 전역 OS 배포 설정에서 네트워크 설정이 정적으로 설정된 경우에 사용됩니다. **팁:** IP 모드를 판별하려면 GET /osdeployment/globalSettings를 사용하십시오.
hostname	String	호스트 서버의 호스트 이름. 호스트 이름을 지정하지 않으면 기본 호스트 이름이 지정됩니다.
ipAddress	String	운영 체제가 배포된 후 호스트 서버에 사용할 IP 주소. 전역 OS 배포 설정에서 네트워크 설정이 정적으로 설정된 경우에 사용됩니다.
mtu	Long	운영 체제가 배포된 후 호스트에 사용할 최대 전송 단위.
prefixLength	String	운영 체제가 배포된 후 호스트 IP 주소에 사용할 접두사 길이. 전역 OS 배포 설정에서 네트워크 설정이 고정 IPv6로 설정된 경우에 사용됩니다.

매크로 이름	유형	설명
selectedMAC	String	IP 주소를 바인딩할 호스트 서버의 MAC 주소. 기본적으로 MAC 주소는 AUTO로 설정됩니다. 이 설정은 배포에 사용하고 구성할 수 있는 이더넷 포트를 자동으로 감지합니다. 기본적으로 감지된 첫 번째 MAC 주소(포트)가 사용됩니다. 다른 MAC 주소에서 연결이 감지되면 새로 감지된 MAC 주소를 배포에 사용하기 위해 XClarity Administrator 호스트가 자동으로 다시 시작됩니다. 및 selectedMAC은 새로 발견된 MAC 주소로 설정됩니다. 인벤터리에 MAC 주소가 있는 서버에 대해서만 VLAN 모드가 지원됩니다. AUTO가 서버에 MAC 주소만 사용가능인 경우라면 해당 서버로 운영 체제를 배포하는 데 VLAN를 사용할 수 없습니다. **팁:** MAC 주소를 얻으려면 GET /hostPlatforms에서 **macaddress** 응답 속성을 사용하십시오.
subnetCIDRNumber	Integer	운영 체제가 배포된 후 사용될 호스트 서버의 서브넷 마스크입니다. CIDR(Classless Inter-Domain Routing) 형식입니다. 전역 OS 배포 설정에서 네트워크 설정이 정적으로 설정된 경우에 사용됩니다. CIDR 번호는 일반적으로 슬래시 "/"로 시작하고 IP 주소 뒤에 옵니다. 예를 들어, 서브넷 마스크가 255.0.0.0(8개의 네트워크 비트 포함)인 IP 주소 131.10.55.70은 131.10.55.70 /8로 표시됩니다. 자세한 정보는 CIDR 표기법 튜토리얼 웹 페이지의 내용을 참조하십시오. **팁:** IP 모드를 판별하려면 GET /osdeployment/globalSettings를 사용하십시오.
subnetMask	String	운영 체제가 배포된 후 사용될 호스트 서버의 서브넷 마스크입니다. 점으로 구분된 10진수 표기법 형식입니다(예: 255.0.0.0). 전역 OS 배포 설정에서 네트워크 설정이 정적으로 설정된 경우에 사용됩니다. **팁:** IP 모드를 판별하려면 GET /osdeployment/globalSettings를 사용하십시오.
vlanId	String	운영 체제 VLAN 태깅에 대한 VLAN ID. 이 매개 변수는 VLAN 모드가 사용으로 설정된 경우에만 유효합니다. VLAN 모드가 사용되는지 판별하려면 XClarity Administrator 온라인 설명서에서 GET /osdeployment/globalSettings를 사용하십시오. **중요:** 네트워크에서 작동하기 위해 VLAN 태그가 필요한 경우에만 VLAN ID를 지정하십시오. VLAN 태그 사용은 호스트 운영 체제와 XClarity Administrator 사이의 네트워크 라우팅에 영향을 미칠 수 있습니다.
selectedImage	String	배포할 운영 체제 이미지의 프로필 ID. **팁:** 운영 체제 이미지 프로파일 ID를 얻으려면 GET /hostPlatforms에서 **availableImages** 응답 속성을 사용하십시오.
storageSettings	Array	운영 체제 이미지를 배포할 기본 스토리지 위치

매크로 이름	유형	설명
targetDevice	String	대상 장치. 이는 다음 값 중 하나입니다. • **localdisk**. 로컬 디스크 드라이브. 관리되는 서버에서 처음에 열거된 로컬 드라이브를 사용합니다. • **M.2 드라이브**. M.2 드라이브. 관리되는 서버에서 처음에 열거된 M.2 드라이브를 사용합니다. • **usbdisk**. 내장 USB 하이퍼바이저. 이 위치는 VMware ESXi 이미지가 관리되는 서버에 배포되는 경우에만 적용됩니다. 2 개의 하이퍼바이저 키가 관리되는 서버에 설치되어 있는 경우 VMware 설치 프로그램이 첫 번째 열거된 배포 키를 선택합니다. • **lunpluswwn=*LUN@WWN***. FC SAN 스토리지(예: `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=*LUN @IQN***. iSCSI SAN 스토리지(예: `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). iSCSI 타겟이 하나만 구성된 경우 *IQN* 지정은 선택 사항이나, *IQN*를 지정하지 않으면 OSDN에 대해 처음 감지된 iSCSI 타겟이 선택됩니다. 지정된 경우 정확히 일치합니다. **참고:** ThinkServer 서버의 경우 이 값은 항상 "localdisk"입니다.
unattendFileId	String	이 배포에 사용할 무인 파일의 ID
uuid	String	운영 체제를 배포할 호스트 서버의 UUID
imageSettings	Object	각 OS 이미지 및 이미지 프로필에 대한 정보
name	String	운영 체제 이미지 이름
프로필	String	이미지 프로필 이름
otherSettings	Object	현재 실행 중인 OS 배포 작업과 관련된 추가 설정
deployDataAndSoft-wareLocation	String	추출된 소프트웨어 페이로드, 사용자 지정 파일 및 배포 데이터(예, 인증서 및 로그)의 경로

installRepoUrl	String	(SLES 15 이상에만 해당) 가져온 패키지 이미지의 URL
		추가 기능 섹션의 media_url에 대한 사용자 지정 무인 모드에서 미리 정의된 이 매크로를 사용할 수 있습니다. 예를 들면 다음과 같습니다.
		`<add-on>`
		`  <add_on_products config:type="list">`
		`  <listentry>`
		`  <media_url>#predefined.otherSettings.installRepoUrl#`
		`  </media_url>`
		`  <product>sle-module-basesystem</product>`
		`  <product_dir>/Module-Basesystem</product_dir>`
		`  </listentry>`
		`  </add_on_products>`
		`</add-on>`

lxcaIp	String	XClarity Administrator 인스턴스의 IP 주소
lxcaRelease	String	XClarity Administrator 릴리스(예, 2.0.0)
jobId	String	현재 실행 중인 OS 배포 작업의 ID
ntpServer	String	XClarity Administrator와 연결된 NTP 서버
statusSettings	Object	OS 배포 상태 설정
urlStatus	String	XClarity Administrator에서 상태를 보고하기 위해 사용하는 HTTPS URL(포트 포함)
certLocation	String	처음 부팅할 때 호스트 OS에서 **urlStatus** 웹 서비스에 액세스하는 데 필요한 인증서가 포함된 폴더

매크로 이름	유형	설명
sdkLocation	String	XClarity Administrator에 액세스하기 위해 XClarity Administrator에서 제공하는 도움 스크립트 및 인터페이스의 위치
timezone	String	XClarity Administrator에 대해 설정된 표준 시간대(예, America/New_York)
unattendSettings	Object	무인 파일을 채우는 데 사용되는 설정. 이 값은 XClarity Administrator의 버전에 따라 다릅니다.
networkConfig	String	(ESXi 및 RHEL만 해당) 무인 설치 시 사용할 XClarity Administrator의 미리 정의된 내용. 이는 운영 체제에 대한 네트워크 설정을 구성합니다.
preinstallConfig	String	설치 전 무인 시간에 사용할 XClarity Administrator의 미리 정의된 내용. 여기에는 설치 전 상태가 포함됩니다. • ESXi 및 RHEL의 경우, %pre 설치 전 스크립트 훅을 사용합니다. • SLES의 경우 <scripts> 설치 전 스크립트 훅을 사용합니다. **주의:** 이 매크로를 사용자 지정 무인 파일에 포함시키는 것이 좋습니다. 무인 파일에서 1라인 뒤(<xml> 태그 뒤)의 아무 위치에나 매크로를 둘 수 있습니다.
postinstallConfig	String	서버를 처음 구성하고 부팅한 후 사용할 XClarity Administrator의 미리 정의된 내용. 여기에는 설치 후 상태가 포함됩니다. • ESXi 및 RHEL의 경우, %post 설치 후 스크립트 훅을 사용합니다. • SLES의 경우 <scripts> 설치 후 스크립트 훅을 사용합니다. • Windows의 경우 "설정 특수화" 섹션을 사용합니다. **주의:** 이 매크로를 사용자 지정 무인 파일에 포함시키는 것이 좋습니다. 무인 파일에서 1라인 뒤(<xml> 태그 뒤)의 아무 위치에나 매크로를 둘 수 있습니다.
reportWorkloadNotComplete	String	이 매크로가 있으면 postinstallConfig 매크로는 OS 설치 완료됨(17) 상태를 보고하지 않습니다. 사용자 지정 프로필은 완료를 보고해야 합니다.
storageConfig	String	(ESXi 및 RHEL만 해당) 무인 설치 시 사용할 XClarity Administrator의 미리 정의된 내용. 이는 운영 체제에 대한 스토리지 설정을 구성합니다.

사용자 지정 무인 파일 가져오기

OS 이미지 리포지토리에 사용자 지정 무인 파일을 가져올 수 있습니다. 그런 다음 이러한 파일을 사용하여 Linux 및 Windows OS 이미지 프로필을 사용자 지정할 수 있습니다.

이 작업 정보

사용자 지정 무인 파일에 대해 다음 파일 유형이 지원됩니다.

운영 체제	지원되는 파일 유형	자세한 정보
CentOS Linux	지원되지 않음	
Microsoft® Windows® Azure Stack HCI	지원되지 않음	
Microsoft Windows Hyper-V Server	지원되지 않음	
Microsoft Windows Server	무인(.xml)	무인 파일에 대한 자세한 정보는 무인 Windows 설치 참조 웹 페이지의 내용을 참조하십시오.

운영 체제	지원되는 파일 유형	자세한 정보
Red Hat® Enterprise Linux (RHEL) Server	Kickstart(.cfg)	무인 파일에 대한 자세한 정보는 Red Hat: Kickstart로 설치 자동화 웹 페이지의 내용을 참조하십시오. 파일에 %pre, %post, %firstboot 섹션을 추가할 때 다음을 고려하십시오. • 무인 파일에 %pre, %post, %firstboot 섹션을 여러 개 포함시킬 수 있습니다. 그러나 섹션의 순서에 유의해야 합니다. • 권장 #predefined.unattendSettings.preinstall-Config# 매크로가 무인 파일이 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %pre 섹션 앞에 %pre 섹션을 추가합니다. • 권장 #predefined.unattendSettings.postinstall-Config# 매크로가 무인 파일에 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %post 및 %firstboot 섹션 앞에 %post 및 %firstboot 섹션을 추가합니다.
Rocky Linux	Kickstart (.cfg)	무인 파일에 대한 자세한 정보는 Red Hat: Kickstart로 설치 자동화 웹 페이지의 내용을 참조하십시오. 파일에 %pre, %post, %firstboot 섹션을 추가할 때 다음을 고려하십시오. • 무인 파일에 %pre, %post, %firstboot 섹션을 여러 개 포함시킬 수 있습니다. 그러나 섹션의 순서에 유의해야 합니다. • 권장 #predefined.unattendSettings.preinstall-Config# 매크로가 무인 파일이 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %pre 섹션 앞에 %pre 섹션을 추가합니다. • 권장 #predefined.unattendSettings.postinstall-Config# 매크로가 무인 파일에 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %post 및 %firstboot 섹션 앞에 %post 및 %firstboot 섹션을 추가합니다.
SUSE® Linux Enterprise Server(SLES)	AutoYast(.xml)	무인 파일에 대한 자세한 정보는 SUSE: AutoYaST 웹 페이지의 내용을 참조하십시오.
Ubuntu	지원되지 않음	
Lenovo Customization 을 사용하는 VMware vSphere® Hypervisor(ESXi)	Kickstart(.cfg)	ESXi 6.0u3 이상 업데이트 및 6.5 이상에만 지원됩니다. 무인 파일에 대한 자세한 정보는 VMware: 스크립트를 사용하여 호스트 설치 및 업그레이드 웹 페이지의 내용을 참조하십시오. 파일에 %pre, %post, %firstboot 섹션을 추가할 때 다음을 고려하십시오. • 무인 파일에 %pre, %post, %firstboot 섹션을 여러 개 포함시킬 수 있습니다. 그러나 섹션의 순서에 유의해야 합니다. • 권장 #predefined.unattendSettings.preinstall-Config# 매크로가 무인 파일이 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %pre 섹션 앞에 %pre 섹션을 추가합니다. • 권장 #predefined.unattendSettings.postinstall-Config# 매크로가 무인 파일에 있는 경우 XClarity Administrator는 파일에 있는 다른 모든 %post 및

운영 체제	지원되는 파일 유형	자세한 정보
		%firstboot 섹션 앞에 %post 및 %firstboot 섹션을 추가합니다.

주의:

- 미리 정의된 매크로 및 사용자 지정 매크로(구성 설정)를 오브젝트의 고유한 이름을 사용하여 무인 파일에 삽입할 수 있습니다. 미리 정의된 값은 XClarity Administrator 인스턴스에 따라 동적입니다. 사용자 지정 매크로는 OS 배포 중에 지정된 사용자 입력에 따라 동적입니다.

  참고:

  - 매크로 이름을 해시 기호(#)로 묶으십시오.
  - 중첩된 이름 오브젝트의 경우, 마침표를 사용하여 각 오브젝트 이름을 구분합니다(예, #server_settings.server0.locale#).
  - 사용자 정의 매크로의 경우 최상위 오브젝트 이름을 포함하지 마십시오. 미리 정의된 매크로의 경우 매크로 이름 앞에 "predefined"를 붙이십시오.
  - 템플리트에서 오브젝트를 작성할 때, 이름은 0부터 시작하는 고유 번호(예, server0 및 server1)로 추가됩니다.
  - 각 사용자 정의 설정 옆에 있는 도움말 아이콘() 위에 놓으면 사용자 정의 설정 탭의 OS 이미지 배포 대화 상자에서 각 매크로의 이름을 볼 수 있습니다.
  - 미리 정의된 매크로 목록은 미리 정의된 매크로의 내용을 참조하십시오. 사용자 지정 구성 설정 및 매크로에 대한 정보는 사용자 정의 매크로의 내용을 참조하십시오.
- XClarity Administrator는 OS 설치 프로그램을 비롯하여 몇 가지 다른 중요한 설치 단계에서 상태를 전달하는 데 사용되는 미리 정의된 매크로를 다음과 같이 제공합니다. 이러한 매크로를 무인 파일에 포함시키는 것이 좋습니다(무인 파일에 미리 정의된 사용자 지정 매크로 삽입 참조).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

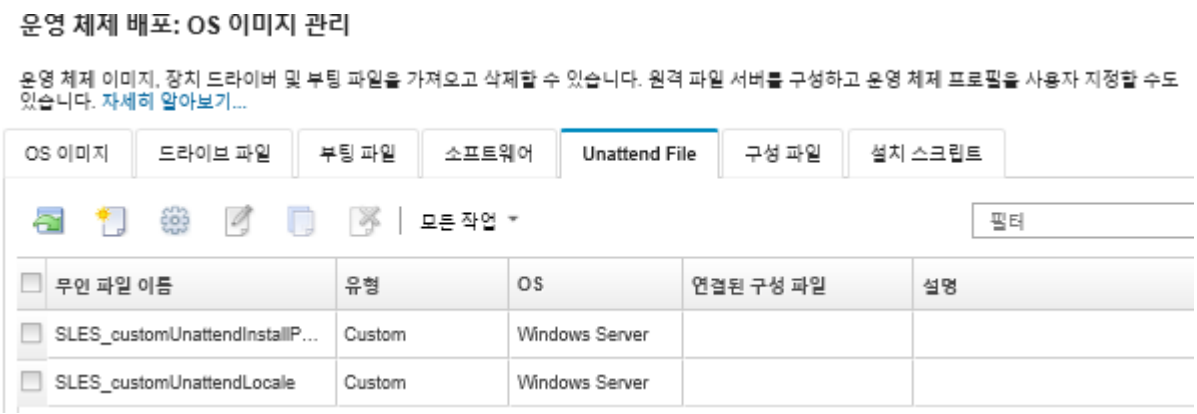
OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

절차

OS 이미지 리포지토리에 무인 파일을 가져오려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **무인 파일** 탭을 클릭하십시오.



단계 3. **파일 가져오기** 아이콘()을 클릭하십시오. 파일 가져오기 대화 상자가 표시됩니다.

단계 4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.

단계 5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

단계 6. 운영 체제 유형을 선택하십시오.

단계 7. 무인 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 파일을 찾으십시오.

단계 8. **옵션:** 무인 파일에 대한 설명을 입력하십시오.

팁: 설명 필드를 사용하여 같은 이름의 사용자 정의 파일을 구별하십시오.

단계 9. **옵션:** 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

단계 10. **가져오기**를 클릭하십시오.

팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

무인 파일 이미지는 OS 이미지 관리 페이지의 **무인 파일** 탭에 나열되어 있습니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **만들기** 아이콘()을 클릭하여 무인 파일을 만드십시오.
  편집기는 파일에서 찾은 오류 위치를 식별합니다. 일부 메시지는 영어로만 제공됩니다.
- 무인 파일을 구성 설정 파일과 연결시키십시오(무인 파일을 구성 설정 파일과 연결 참조).
- **편집** 아이콘()을 클릭하여 무인 파일을 확인하고 수정하십시오.
  편집기는 파일에서 찾은 오류 위치를 식별합니다. 일부 메시지는 영어로만 제공됩니다.
- **복사** 아이콘()을 클릭하여 무인 파일을 복사하십시오.
  구성 설정 파일과 연결된 무인 파일을 복사하면 연결된 구성 설정 파일도 복사되고 복사된 두 파일이 자동으로 연결됩니다.
- **삭제** 아이콘()을 클릭하여 선택한 무인 파일을 제거하십시오.
- **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만듭니다.

사용자 지정 OS 이미지 프로필에 무인 파일을 추가하는 방법에 대한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

무인 파일에 미리 정의된 사용자 지정 매크로 삽입

미리 정의된 사용자 지정 매크로를 무인 파일에 추가할 수 있습니다.

이 작업 정보

*매크로*는 무인 파일에 동적 데이터(구성 설정)를 추가하는 기능을 제공합니다. OS 이미지 프로필이 배포될 때 데이터 값을 제공합니다.

Lenovo XClarity Administrator는 사용자 정의 구성 설정 파일을 연결하지 않고 무인 파일에 추가할 수 있는 *미리 정의된* 매크로 세트를 제공합니다. 미리 정의된 매크로 목록은 미리 정의된 매크로의 내용을 참조하십시오.

다음의 미리 정의된 매크로를 사용자 정의 무인 파일에 포함시키는 것이 좋습니다.

- #predefined.unattendSettings.preinstallConfig# 및 #predefined.unattendSettings postinstallConfig#. OS 설치 프로그램을 비롯하여 몇 가지 다른 중요한 설치 단계에서 상태를 전달하는 데 사용됩니다.

  설치 구성 매크로를 포함하는 방법에 대한 자세한 정보는 다음 예제 OS 배포 시나리오를 참조하십시오.
  - 사용자 정의 무인 파일을 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포
  - 구성 가능한 로케일 및 NTP 서버가 있는 SLES 12 SP3 배포
  - 고정 IP 주소를 사용하여 Lenovo Customization이 있는 VMware ESXi v6.7을 로컬 디스크에 배포
  - 사용자 지정 기능이 있는 Windows 2016 배포
- #predefined.unattendSettings.networkConfig#. (ESXi 및 RHEL의 경우) XClarity Administrator를 사용하여 네트워크를 구성합니다. 이 매크로는 OS 이미지 배포 페이지에서 지정된 네트워크 설정을 사용합니다. 무인 파일에 이 매크로를 포함하지 않거나 네트워크 설정이 XClarity Administrator에서 정의되지 않은 경우, 무인 파일의 일부로 IP 인터페이스를 구성하여 호스트가 다시 XClarity Administrator 이동하는 네트워크 경로를 갖도록 해야 합니다.

  네트워크 구성 매크로를 포함하는 방법에 대한 자세한 정보는 다음 예제 OS 배포 시나리오를 참조하십시오.
  - 사용자 정의 무인 파일을 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포
  - 고정 IP 주소를 사용하여 Lenovo Customization이 있는 VMware ESXi v6.7을 로컬 디스크에 배포
- #predefined.unattendSettings.storageConfig#. (ESXi 및 RHEL의 경우) XClarity Administrator를 사용하여 호스트에서 네트워크를 구성합니다. 이 매크로는 OS 이미지 배포 페이지에서 지정된 스토리지 설정을 사용합니다. 무인 파일에 이 매크로가 포함되어 있지 않거나 스토리지 설정이 XClarity Administrator에서 정의되지 않는 경우, 무인 파일에서 스토리지 구성을 지정해야 합니다.

  스토리지 구성 매크로를 포함하는 방법에 대한 자세한 정보는 다음 예제 OS 배포 시나리오를 참조하십시오.
  - 사용자 정의 무인 파일을 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포
  - 고정 IP 주소를 사용하여 Lenovo Customization이 있는 VMware ESXi v6.7을 로컬 디스크에 배포

구성 설정 파일을 작성한 다음 무인 파일을 사용자 지정 구성 설정 파일과 연결하여 *사용자 지정* 매크로를 만들 수 있습니다. 사용자 지정 구성 설정 파일을 가져올 때 XClarity Administrator는 파일의 각 구성 설정에 대해 매크로를 만듭니다.

절차

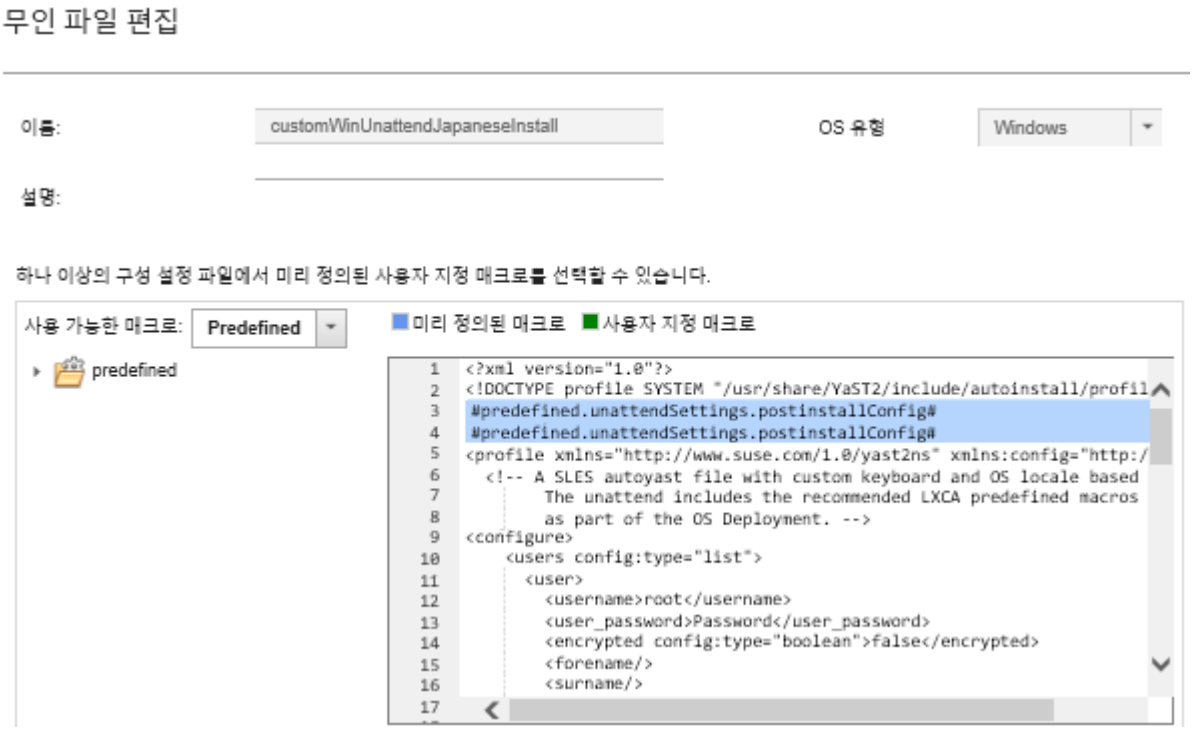
매크로를 무인 파일에 추가하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **무인 파일** 탭을 클릭하십시오.

단계 3. 편집하려는 무인 파일을 선택하십시오.

단계 4. **편집** 아이콘( )을 클릭하여 무인 파일 편집 대화 상자를 표시하십시오.



단계 5. 다음과 같이 권장 사전 정의 매크로를 추가하십시오.

1. 무인 파일에서 1라인 뒤(<xml> 태그 뒤)의 아무 위치에나 커서를 놓으십시오.
2. 사용 가능한 매크로 목록에서 **미리 정의 → unattendSettings** 목록을 펼치십시오.
3. preinstallConfig 및 postinstallConfig를 클릭하여 미리 정의된 필수 매크로를 무인 파일에 추가하십시오.

   다음 코드가 파일에 추가됩니다.

   ```
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
   ```

단계 6. 무인 파일의 올바른 위치에 커서를 놓은 다음 목록에서 매크로를 클릭하여 미리 정의된 매크로 또는 사용자 지정 매크로를 추가하십시오.

단계 7. **저장**을 클릭하십시오.

무인 파일을 구성 설정 파일과 연결

무인 파일에 구성 설정을 연결(바인딩)한 다음 관련 사용자 지정 매크로를 무인 파일에 추가할 수 있습니다.

이 작업 정보

사용자 지정 구성 설정 파일을 연결하지 않고 미리 정의된 매크로를 무인 파일에 추가할 수 있습니다.

무인 파일과 연결된 구성 설정 파일은 편집할 수 없습니다. 그러나 연관된 파일을 복사한 다음 사본을 편집할 수 있습니다.

절차

무인 파일을 구성 설정 파일과 연결하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **무인 파일** 탭을 클릭하십시오.

단계 3. 사용자 지정 무인 파일을 선택하십시오.

단계 4. **구성 파일 연결** 아이콘()을 클릭하여 무인 파일 연결 대화 상자를 표시하십시오.

단계 5. 무인 파일과 연결할 구성 설정 파일을 선택하십시오.

단계 6. 편집기에서 매크로를 추가할 위치에 커서를 놓고 사용 가능한 목록에서 매크로를 클릭하여 미리 정의된 사용자 지정 매크로를 무인 파일에 추가하십시오(무인 파일에 미리 정의된 사용자 지정 매크로 삽입 참조).

오브젝트의 고유한 이름을 사용하여 매크로를 무인 파일에 삽입할 수 있습니다. 중첩된 이름 오브젝트의 경우 마침표를 사용하여 각 오브젝트를 구분합니다(예, `server_specific_settings.server.locale`). 최상위 이름은 포함하지 않습니다.

단계 7. **연결**을 클릭하여 파일을 함께 바인딩하십시오.

사용자 지정 설치 스크립트 가져오기

OS 이미지 리포지토리에 설치 스크립트를 가져올 수 있습니다. 그런 다음 이러한 파일을 사용하여 Linux 및 Windows 이미지를 사용자 지정할 수 있습니다.

이 작업 정보

현재 설치 후 스크립트만 지원됩니다.

다음 표에는 Lenovo XClarity Administrator가 각 운영 체제에 따라 지원하는 설치 스크립트의 파일 유형이 나열되어 있습니다. 특정 운영 체제 버전은 XClarity Administrator가 지원하는 해당 파일 형식을 모두 지원하지는 않습니다(예, 일부 RHEL 버전은 최소 프로파일에 Perl을 포함하지 않을 수 있으므로 Perl 스크립트가 실행되지 않습니다). 배포할 운영 체제 버전에 대해 올바른 파일 유형을 사용해야 합니다.

운영 체제	지원되는 파일 유형	자세한 정보
CentOS Linux	지원되지 않음	
Microsoft® Windows® Azure Stack HCI	지원되지 않음	
Microsoft Windows Hyper-V Server	지원되지 않음	
Microsoft® Windows® Server	명령 파일(.cmd), PowerShell(.ps1)	기본 사용자 지정 데이터 및 파일 경로는 `C:\lxca`입니다. 설치 스크립트에 대한 자세한 정보는 Windows 설치에 사용자 지정 스크립트 추가 웹 페이지의 내용을 참조하십시오.
Red Hat® Enterprise Linux (RHEL) Server	Bash(.sh), Perl(.pm or .pl), Python(.py)	기본 사용자 정의 데이터 및 파일 경로는 `/home/lxca`입니다. 설치 스크립트에 대한 자세한 정보는 RHEL: 설치 후 스크립트 웹 사이트의 내용을 참조하십시오.

운영 체제	지원되는 파일 유형	자세한 정보
Rocky Linux	Bash(.sh), Perl(.pm or .pl), Python(.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 RHEL: 설치 후 스크립트 웹 사이트의 내용을 참조하십시오.
SUSE® Linux Enterprise Server(SLES)	Bash(.sh), Perl(.pm or .pl), Python(.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 SUSE: 사용자 정의 사용자 스크립트 웹 페이지의 내용을 참조하십시오.
Ubuntu	지원되지 않음	
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	Bash (.sh), Python (.py)	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다. 설치 스크립트에 대한 자세한 정보는 VMware: 스크립트 웹 페이지 설치 및 업그레이드의 내용을 참조하십시오.

참고: OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

OS 배포 중에 데이터가 수집된 후, XClarity Administrator는 설치 후 스크립트에서 사용할 수 있는 호스트 시스템의 구성 설정 파일(선택한 파일의 사용자 정의 설정 및 미리 정의된 설정의 서브세트 포함)의 인스턴스를 만듭니다.

미리 정의된 매크로 및 사용자 정의 매크로(구성 설정)를 오브젝트의 고유한 이름을 사용하여 설치 후 스크립트에 삽입할 수 있습니다. 미리 정의된 값은 XClarity Administrator 인스턴스에 따라 동적입니다. 사용자 지정 매크로는 OS 배포 중에 지정된 사용자 입력에 따라 동적입니다.

참고:

- 매크로 이름을 해시 기호(#)로 묶으십시오.
- 중첩된 이름 오브젝트의 경우, 마침표를 사용하여 각 오브젝트 이름을 구분합니다(예, #server_settings.server0.locale#).
- 사용자 정의 매크로의 경우 최상위 오브젝트 이름을 포함하지 마십시오. 미리 정의된 매크로의 경우 매크로 이름 앞에 "predefined"를 붙이십시오.
- 템플리트에서 오브젝트를 작성할 때, 이름은 0부터 시작하는 고유 번호(예, server0 및 server1)로 추가됩니다.
- 각 사용자 정의 설정 옆에 있는 도움말 아이콘( ) 위에 놓으면 사용자 정의 설정 탭의 OS 이미지 배포 대화 상자에서 각 매크로의 이름을 볼 수 있습니다.
- 미리 정의된 매크로 목록은 미리 정의된 매크로의 내용을 참조하십시오. 사용자 지정 구성 설정 및 매크로에 대한 정보는 사용자 정의 매크로의 내용을 참조하십시오.

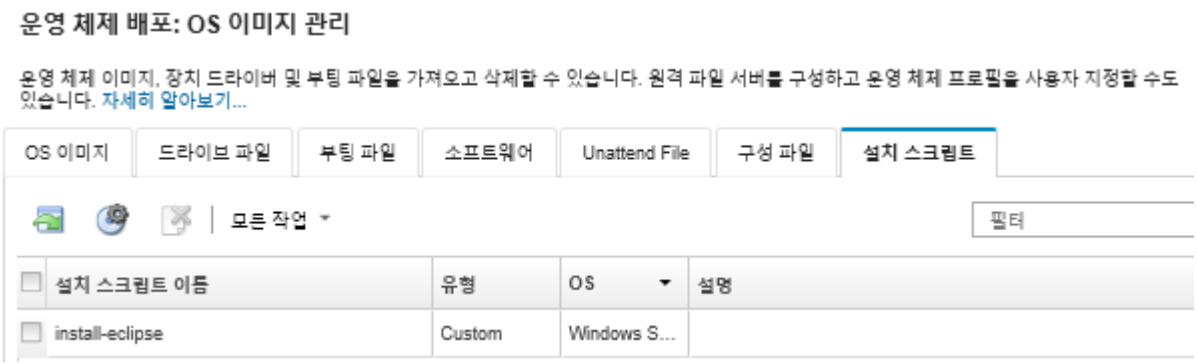
무인 파일에서 권장되는 미리 정의된 매크로는 설치 후 스크립트를 다운로드하고 실행할 때 최종 운영 체제 배포 상태 및 보고 상태를 보고합니다. 대상 운영 체제에 따라 사용자 지정 상태 보고를 포함하도록 설치 후 스크립트를 수정할 수 있습니다. 자세한 정보는 설치 스크립트에 사용자 지정 상태 보고 추가의 내용을 참조하십시오.

절차

OS 이미지 리포지토리에 설치 스크립트를 가져오려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **설치 스크립트** 탭을 클릭하십시오.



단계 3. **파일 가져오기** 아이콘()을 클릭하십시오. 설치 스크립트 가져오기 대화 상자가 표시됩니다.

단계 4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.

단계 5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

단계 6. 운영 체제 유형을 선택하십시오.

단계 7. 설치 스크립트 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 파일을 찾으십시오.

단계 8. **옵션:** 설치 스크립트에 대한 설명을 입력하십시오.

팁: 설명 필드를 사용하여 같은 이름의 사용자 정의 파일을 구별하십시오.

단계 9. **옵션:** 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

단계 10. **가져오기**를 클릭하십시오.

팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

설치 스크립트는 OS 이미지 관리 페이지의 **설치 스크립트** 탭에 나열되어 있습니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만듭니다.
- **삭제** 아이콘()을 클릭하여 선택한 설치 스크립트를 제거하십시오.

사용자 지정 OS 이미지 프로필에 설치 스크립트를 추가하는 방법에 대한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

설치 스크립트에 사용자 지정 상태 보고 추가

무인 파일에서 권장되는 미리 정의된 매크로는 설치 후 스크립트를 다운로드하고 실행할 때 최종 운영 체제 배포 상태 및 보고 상태를 보고합니다. 설치 후 스크립트에 추가 상태 보고를 포함시킬 수 있습니다.

Linux

Linux의 경우 `curl` 명령을 사용하여 상태를 보고할 수 있습니다.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

여기서, *<status_ID>*는 다음 값 중 하나입니다.

- 44. 작업 부하 배포 성공
- 45. 작업 부하 배포 실행 중(경고 있음)
- 46. 작업 부하 배포 실패
- 47. 작업 부하 배포 메시지
- 48. 사용자 지정 설치 후 스크립트 오류

`curl` 명령은 Lenovo XClarity Administrator가 보고 상태에 사용하는 HTTPS URL(predefined.otherSettings.statusSettings.urlStatus) 및 첫 번째 부팅 시 호스트 OS에서 urlStatus 웹 서비스에 액세스하는 데 필요한 인증서가 포함된 폴더(predefined.otherSettings.statusSettings.certLocation)에 대해 미리 정의된 매크로를 사용합니다. 다음 예제에서는 설치 후 스크립트에서 오류가 발생했음을 보고합니다.

다음 예는 설치 후 스크립트에서 오류가 발생했음을 보고합니다.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

Wiindows의 경우, `LXCA.psm1` 스크립트를 가져온 후 다음 명령을 호출하여 상태를 보고할 수 있습니다.

- initializeRestClient

  REST 클라이언트를 초기화합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오. 이 명령은 보고 명령을 실행하기 전에 필요합니다.

  ```
  initializeRestClient
  ```

- testLXCAConnection

  XClarity Administrator가 호스트 서버에 연결할 수 있는지 확인합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오. 이 명령은 선택 사항이지만 보고 명령을 실행하기 전에 설치 스크립트에서 권장됩니다.

  ```
  testLXCAConnection -masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- reportWorkloadDeploymentSucceeded

XClarity Administrator 작업 로그에서 로깅할 완료 성공 메시지를 보고합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오.

팁: #predefined.unattendSettings.reportWorkloadNotComplete# 매크로가 사용자 정의 무인 파일 또는 설치 후 스크립트에 포함된 경우, 설치 후 스크립트에 reportWorkloadDeploymentSucceeded 명령을 포함시켜 성공적인 완료를 알립니다. 그렇지 않으면, XClarity Administrator는 모든 설치 후 스크립트가 실행된 후 완료 상태를 자동으로 보고합니다.

```
reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
-UUID "#predefined.hostPlatforms.uuid#"
```

- reportWorkloadDeploymentRunningWithWarning

  XClarity Administrator 작업 로그에서 로깅할 경고 메시지를 보고합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- reportWorkloadDeploymentFailed

  XClarity Administrator 작업 로그에서 로깅할 실패 메시지를 보고합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- reportCustomPostInstallScriptError

  XClarity Administrator 작업 로그에서 로깅할 설치 후 스크립트 오류 메시지를 보고합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- reportWorkloadDeploymentMessage

  XClarity Administrator 작업 로그에 로깅할 일반 메시지(배포 상태에 영향을 주지 않음)를 보고합니다. 이 명령을 실행하려면 다음 구문을 사용하십시오.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

여기서, *<message_text>*는 각 상태 조건에 대해 XClarity Administrator로 리턴하려는 메시지입니다.

이 명령은 XClarity Administrator 인스턴스의 IP 주소(#predefined.otherSettings.lxcaIp#) 및 운영 체제를 배포할 호스트 서버의 UUID(#predefined.hostPlatforms.uuid#)에 미리 정의된 매크로를 사용합니다.

다음 예제는 Java를 설치하고 설치가 실패할 경우 오류를 보고하는 PowerShell 설치 스크립트입니다.

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
  Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
  [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
```

```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
    -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

사용자 지정 소프트웨어 가져오기

OS 이미지 리포지토리에 소프트웨어를 가져올 수 있습니다. 그런 다음 이러한 파일을 사용하여 Linux 및 Windows 이미지를 사용자 지정할 수 있습니다.

이 작업 정보

사용자 지정 소프트웨어 파일은 운영 체제 배포 및 설치 후 스크립트가 완료된 후에 설치됩니다.

다음 파일 유형이 사용자 지정 소프트웨어에서 지원됩니다.

운영 체제	지원되는 파일 유형	자세한 정보
CentOS Linux	지원되지 않음	
Microsoft® Windows® Azure Stack HCI	지원되지 않음	
Microsoft Windows Hyper-V Server	지원되지 않음	
Microsoft Windows® Server	소프트웨어 페이로드가 포함된 .zip 파일.	기본 사용자 지정 데이터 및 파일 경로는 C:\lxca입니다.
Red Hat® Enterprise Linux (RHEL) Server	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.
SUSE® Linux Enterprise Server(SLES)	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.
Rocky Linux	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.
Ubuntu	지원되지 않음	
Lenovo Customization을 사용하는 VMware vSphere® Hypervisor(ESXi)	소프트웨어 페이로드가 포함된 .tar.gz 파일.	기본 사용자 정의 데이터 및 파일 경로는 /home/lxca입니다.

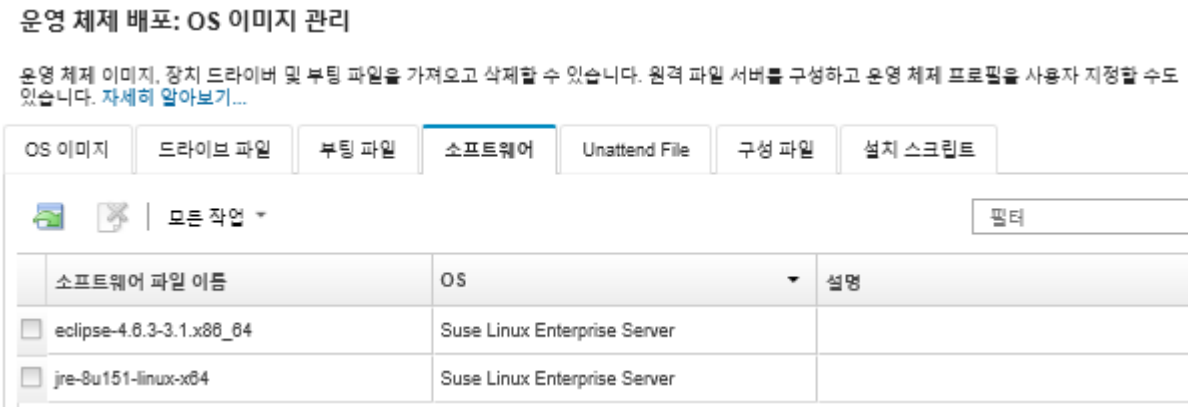
참고: OS 이미지 리포지토리는 파일을 저장할 공간이 있는 한 미리 정의된 파일 및 사용자 정의 파일을 무제한으로 저장할 수 있습니다.

절차

OS 이미지 리포지토리에 소프트웨어를 가져오려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **소프트웨어** 탭을 클릭하십시오.



단계 3. **파일 가져오기** 아이콘()을 클릭하십시오. 설치 스크립트 가져오기 대화 상자가 표시됩니다.

단계 4. **로컬 가져오기** 탭을 클릭하여 로컬 시스템에서 파일을 업로드하거나 **원격 가져오기** 탭을 클릭하여 원격 파일 서버에서 파일을 업로드하십시오.

참고: 원격 파일 서버에서 파일을 업로드하려면 먼저 **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만들어야 합니다. 자세한 정보는 원격 파일 서버 구성 의 내용을 참조하십시오.

단계 5. 원격 파일 서버를 사용하도록 선택한 경우 **원격 파일 서버** 목록에서 사용하려는 서버를 선택하십시오.

단계 6. 운영 체제 유형을 선택하십시오.

단계 7. 소프트웨어 파일 이름을 입력하거나 **찾아보기**를 클릭하여 가져오려는 파일을 찾으십시오.

단계 8. **옵션:** 소프트웨어 파일에 대한 설명을 입력하십시오.

팁: 설명 필드를 사용하여 같은 이름의 사용자 정의 파일을 구별하십시오.

단계 9. **옵션:** 체크섬 유형을 선택하여 업로드하는 파일이 손상되지 않았는지 확인하고 체크섬 값을 복사하여 제공되는 텍스트 필드에 붙여넣으십시오.

체크섬 유형을 선택하는 경우 체크섬 값을 지정하여 업로드된 파일의 무결성과 보안을 확인해야 합니다. 신뢰할 수 있는 조직의 안전한 소스에서 얻은 값이어야 합니다. 업로드된 파일이 체크섬 값과 일치하면 안심하고 배포를 진행할 수 있습니다. 그렇지 않은 경우 파일을 다시 업로드하거나 체크섬 값을 확인해야 합니다.

지원되는 체크섬 유형은 다음 세 가지입니다.
- MD5
- SHA1
- SHA256

단계 10. **가져오기**를 클릭하십시오.

팁: 파일은 보안 네트워크 연결을 통해 업로드됩니다. 따라서 네트워크 안정성 및 성능은 파일을 가져오는 데 걸리는 시간에 영향을 줍니다.

업로드가 완료되기 전에 파일이 로컬에 업로드되는 웹 브라우저 탭 또는 창을 닫는 경우 가져오기가 실패합니다.

완료한 후에

설치 스크립트는 OS 이미지 관리 페이지의 **소프트웨어** 탭에 나열되어 있습니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **파일 서버 구성** 아이콘()을 클릭하여 원격 파일 서버 프로필을 만듭니다.

- **삭제** 아이콘( )을 클릭하여 선택한 소프트웨어 파일을 제거하십시오.

사용자 지정 OS 이미지 프로필에 소프트웨어 파일을 추가하는 방법에 대한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

사용자 지정 OS 이미지 프로필 만들기

OS 이미지 리포지토리에 존재하는 사전 정의된 OS 이미지 프로필에 사용자 지정 장치 드라이버, 부팅 파일(Windows만 해당), 구성 설정, 무인 파일, 설치 스크립트 및 소프트웨어를 추가할 수 있습니다. OS 이미지에 파일을 추가하는 경우 Lenovo XClarity Administrator가 해당 OS 이미지에 대한 사용자 지정 프로필을 만듭니다. 사용자 지정 프로필에는 사용자 지정 파일 및 설치 옵션이 포함됩니다.

시작하기 전에

추가하려는 사용자 지정 파일이 OS 이미지 리포지토리에 있어야 합니다(부팅 파일 가져오기, 장치 드라이버 가져오기, 사용자 지정 구성 설정 가져오기, 사용자 지정 무인 파일 가져오기, 사용자 지정 설치 스크립트 가져오기 및 사용자 지정 소프트웨어 가져오기 참조).

절차

OS 이미지를 사용자 지정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

단계 2. **OS 이미지** 탭을 클릭하십시오.

단계 3. 사용자 지정할 사전 정의된 OS 이미지 프로필을 선택하십시오.

사용자 지정 열은 사용자 지정할 수 있는 OS 이미지를 식별합니다. 특정 OS 이미지에 대한 사용자 지정에 대한 자세한 정보는 **도움말** 아이콘( )을 클릭하십시오.
- **사용자 지정**. OS 이미지 지원 사용자 지정만 사용자 지정되지 않음입니다.
- **사용자 지정 불가능**. OS 이미지는 사용자 지정을 지원하지 않습니다.

참고: 파일 가져오기 아이콘( )을 클릭하여 로컬 또는 원격 시스템에서 추가 기본 OS 이미지(.iso 형식)를 가져올 수 있습니다.

단계 4. **사용자 지정한 프로필 만들기** 아이콘( )을 클릭하십시오. 새 사용자 지정 OS 이미지 대화상자가 표시됩니다.

단계 5. **일반** 탭에서 사용자 지정 파일의 이름, 설명, 경로 및 배포 호스트의 배포 데이터와 새 사용자 지정 OS 이미지 프로필의 사용자 지정 유형을 지정하십시오.

사용자 지정 유형은 다음 중 하나입니다.
- **무인 파일만**
- **구성 파일만**
- **연결되지 않은 무인 및 구성 파일**
- **연결된 무인 및 구성 파일**
- **없음**

단계 6. **다음**을 누르십시오.

단계 7. **장치 드라이버** 탭에서 Linux OS 이미지 프로필에 추가할 장치 드라이버를 선택하십시오.

지원되는 형식 목록은 장치 드라이버 가져오기의 내용을 참조하십시오.

선택한 파일은 구성 마법사를 완료한 후 적용됩니다.

참고: 파일 가져오기 아이콘()을 클릭하여 로컬 또는 원격 시스템에서 추가 장치 드라이버를 가져올 수 있습니다.

단계 8. **다음**을 누르십시오.

단계 9. (Windows만 해당) **부팅 옵션** 탭에서 Windows OS 이미지 프로필에 추가할 부팅 파일을 선택하십시오.

지원되는 형식 목록은 부팅 파일 가져오기의 내용을 참조하십시오.

선택한 파일은 구성 마법사를 완료한 후 적용됩니다.

단계 10. **다음**을 누르십시오.

단계 11. **구성 설정** 탭에서(해당하는 경우) OS 이미지 프로필에 추가할 하나 이상의 사용자 지정 구성 파일을 선택하십시오. 최대 하나의 파일만 선택할 수 있습니다.

단계 12. **다음**을 누르십시오.

단계 13. **무인 파일** 탭에서 다음을 수행하십시오.

a. OS 이미지 프로필에 추가할 무인 파일을 선택하십시오.

   지원되는 형식 목록은 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

   선택한 파일은 구성 마법사를 완료한 후 적용됩니다.

b. **연결된 구성 파일** 열에서 무인 파일과 연결시킬 구성 파일을 선택하십시오.

c. 선택된 구성 파일에 사용 가능한 사용자 지정 매크로를 선택하거나 사용자 지정 매크로를 .xml 형식으로 추가하십시오(옵션).

단계 14. **다음**을 누르십시오.

단계 15. **설치 스크립트** 탭에서(적용 가능한 경우) Windows OS 이미지 프로필에 추가할 설치 스크립트를 선택하십시오. 최대 하나의 설치 후 스크립트를 선택할 수 있습니다.

지원되는 형식 목록은 사용자 지정 설치 스크립트 가져오기의 내용을 참조하십시오.

선택한 파일은 구성 마법사를 완료한 후 적용됩니다.

참고: 파일 가져오기 아이콘()을 클릭하여 로컬 또는 원격 시스템에서 추가 설치 스크립트를 가져올 수 있습니다.

단계 16. **다음**을 누르십시오.

단계 17. **소프트웨어** 탭에서 Linux OS 이미지 프로필에 추가할 소프트웨어를 선택하십시오.

지원되는 형식 목록은 사용자 지정 소프트웨어 가져오기의 내용을 참조하십시오.

선택한 파일은 구성 마법사를 완료한 후 적용됩니다.

참고: 파일 가져오기 아이콘()을 클릭하여 로컬 또는 원격 시스템에서 추가 소프트웨어를 가져올 수 있습니다.

단계 18. **다음**을 누르십시오.

단계 19. **요약** 탭에서 설정을 검토하고 **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

완료한 후에

사용자 지정 OS 이미지 프로필은 OS 이미지 관리 페이지에서 **OS 이미지** 탭의 기본 운영 체제 아래에 나열됩니다.

이 페이지에서 다음 작업을 수행할 수 있습니다.

- **프로필 가져오기/내보내기 → 사용자 지정 프로필 이미지 내보내기**를 클릭하여 사용자 지정 OS 이미지 프로필을 가져와 기본 OS 이미지에 적용합니다(사용자 지정 OS 이미지 프로필 가져오기 참조).
- **프로필 가져오기/내보내기 → 사용자 지정된 프로필 이미지 내보내기**를 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 내보냅니다.
- **편집** 아이콘()을 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 수정하십시오.
- **삭제** 아이콘()을 클릭하여 선택한 사용자 지정 OS 이미지 프로필을 제거하십시오.

전역 OS 배포 설정 구성

운영 체제를 배포하면 전역 설정이 기본 설정으로 사용됩니다.

이 작업 정보

전역 설정 페이지에서 다음 설정을 구성할 수 있습니다.

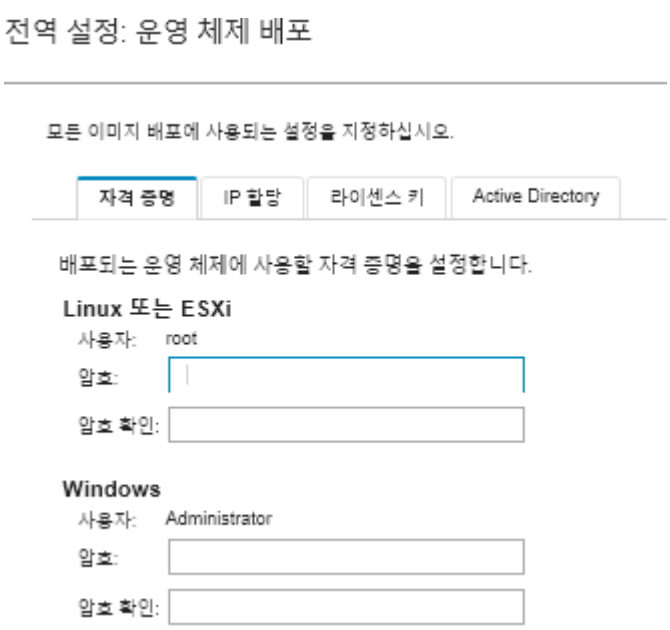
- 운영 체제 배포에 사용할 관리자 사용자 계정의 암호
- 서버에 IP 주소를 지정하는 방법
- 설치된 운영 체제를 활성화하는 데 사용할 라이센스 키
- Active Directory 도메인을 Windows 운영 체제 배포의 일부로 선택적으로 결합

절차

모든 서버에 사용할 전역 설정을 구성하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 OS 이미지 배포 페이지를 표시하십시오.

단계 2. **전역 설정** 아이콘()을 클릭하여 전역 설정: 운영 체제 배포 대화 상자를 표시합니다.



단계 3. **자격 증명** 탭에서 관리자 계정이 운영 체제에 로그인하는 데 사용할 암호를 입력하십시오.

단계 4. **IP 할당** 탭에서 다음 옵션을 선택하십시오.

a. **옵션:** VLAN **사용**을 선택하여 네트워크 설정 대화 상자에서 VLAN 설정을 구성할 수 있습니다(관리되는 서버에 대한 네트워크 설정 구성 참조).

참고: 참고:

- Linux 운영 체제 배포에 대해 VLAN 태깅이 지원되지 않습니다.
- ThinkServer 장치의 운영 체제에 대해서는 VLAN 태깅이 지원되지 않습니다.
- 인벤터리에 MAC 주소가 있는 서버에 대해서만 VLAN 모드가 지원됩니다. AUTO가 서버에 사용 가능한 유일한 MAC 주소인 경우 해당 서버에 운영 체제를 배포하는 데 VLAN을 사용할 수 없습니다.

b. 배포된 운영 체제 구성 시 IP 주소 할당 방법을 선택하십시오.

참고: 관리에 사용되는 XClarity Administrator 네트워크 인터페이스는 전역 설정(운영 체제 배포 대화상자)에서 선택한 것과 동일한 IP 주소 방법을 사용하여 베이스보드 관리 컨트롤러에 연결되도록 구성해야 합니다. 예를 들어 관리를 위해 eth0을 사용하도록 XClarity Administrator을 설정하고, 배포된 OS를 구성할 때 수동으로 할당된 고정 IPv6 주소를 사용하도록 선택한 경우, eth0을 베이스보드 관리 컨트롤러에 연결하는 IPv6 주소로 구성해야 합니다.

- **수동으로 고정 IPv4 주소 할당**. 고정 IPv4 주소를 할당하도록 선택하는 경우 운영 체제를 배포하기 전에 서버에 대한 고정 IPv4 주소, 게이트웨이 주소 및 서브넷 마스크를 구성해야 합니다(관리되는 서버에 대한 네트워크 설정 구성 참조).
- **DHCP(Dynamic Host Configuration Protocol)를 사용하여 주소 할당**. 네트워크에 기존 DHCPv4 인프라스트럭처가 있는 경우 해당 인프라스트럭처를 사용하여 서버에 IP 주소를 할당할 수 있습니다.

  참고: DHCP IPv6 주소는 운영 체제 배포에 지원되지 않습니다.
- **수동으로 고정 IPv6 주소 할당**. 고정 IPv6 주소를 할당하도록 선택하는 경우 운영 체제를 배포하기 전에 서버에 대한 고정 IPv6 주소, 게이트웨이 주소 및 서브넷 마스크를 구성해야 합니다(관리되는 서버에 대한 네트워크 설정 구성 참조).

단계 5. **옵션: 라이센스 키** 탭에서, 설치된 Windows 운영 체제를 활성화할 때 사용할 전역 볼륨 라이센스 키를 지정하십시오.

이 탭에서 전역 볼륨 라이센스 키를 지정하는 경우 OS 이미지 배포 페이지에서 Windows OS 이미지 프로필에 대해 지정된 라이센스 키를 선택할 수 있습니다.

팁: XClarity Administrator는 Windows 설치에 전역 볼륨 라이센스 키를 지원하고 Windows 및 VMware ESXi 둘 다에 소매 라이센스 키를 지원합니다. 개별 소매 라이센스 키를 배포 절차의 일부로 지정할 수 있습니다(운영 체제 이미지 배포 참조).

단계 6. **옵션:** Active Directory 탭에서 Windows 운영 체제 배포에 대한 Active Directory 설정을 구성하십시오. Active Directory와의 통합에 대한 정보는 Windows Active Directory와 통합의 내용을 참조하십시오.

단계 7. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

관리되는 서버에 대한 네트워크 설정 구성

네트워크 설정은 각 서버에 특정한 구성 옵션입니다. 해당 서버에 운영 체제를 배포하려면 먼저 관리 서버에 대한 네트워크 설정을 구성해야 합니다.

이 작업 정보

DHCP를 사용하여 IP 주소를 동적으로 할당하는 경우 MAC 주소를 구성해야 합니다.

고정 IP 주소를 사용하는 경우 특정 서버에 운영 체제를 배포하려면 먼저 해당 서버에 대해 다음 네트워크 설정을 구성해야 합니다. 이러한 설정을 구성하면 서버의 배포 상태가 "준비"로 변경됩니다. (일부 필드에서는 고정 IPv6 주소를 사용할 수 없음.)

- 호스트 이름

  호스트 이름은 다음 규칙을 준수해야 합니다.
  - 관리되는 각 서버의 호스트 이름은 고유해야 합니다.
  - 호스트 이름은 마침표(.)로 구분된 문자열(레이블)을 포함할 수 있습니다.
  - 각 레이블은 ASCII 문자, 숫자 및 대시(-)를 포함할 수 있지만 문자열은 대시로 시작하거나 끝날 수 없으며 모든 숫자를 포함할 수도 없습니다.
  - 첫 번째 레이블의 길이는 2 - 15자일 수 있습니다. 그 다음 레이블의 길이는 2 – 63자일 수 있습니다.
  - 호스트 이름의 총 길이는 255자를 초과해서는 안 됩니다.
- 운영 체제를 설치할 호스트에 있는 포트의 MAC 주소.

  기본적으로 MAC 주소는 AUTO로 설정됩니다. 이 설정은 배포에 사용하고 구성할 수 있는 이더넷 포트를 자동으로 감지합니다. 기본적으로 감지된 첫 번째 MAC 주소(포트)가 사용됩니다. 다른 MAC 주소에서 연결이 감지되면 새로 감지된 MAC 주소를 배포에 사용하기 위해 XClarity Administrator 호스트가 자동으로 다시 시작됩니다..

  OS 배치에 사용되는 MAC 주소 포트의 상태는 네트워크 설정 대화 상자의 **MAC 주소** 드롭다운 메뉴에서 알 수 있습니다. 여러 개의 포트가 사용되었거나 모든 포트가 다운되었을 때, AUTO가 기본값으로 사용됩니다.

  참고:

  - 가상 네트워크 포트는 지원되지 않습니다. 하나의 물리적 네트워크 포트를 사용하여 여러 가상 네트워크 포트를 시뮬레이션하지 마십시오.
  - 서버의 네트워크 설정이 자동으로 설정되어 있으면 슬롯 1 – 16에서 XClarity Administrator이(가) 네트워크 포트를 자동으로 감지할 수 있습니다. 슬롯 1 – 16에서 하나 이상의 포트가 XClarity Administrator에 연결되어 있어야 합니다.
  - MAC 주소에 슬롯 17 이상의 네트워크 포트를 사용하려면 AUTO를 사용할 수 없습니다. 대신 서버의 네트워크 설정을 사용하려는 특정 포트의 MAC 주소로 설정해야 합니다.
  - ThinkServer 서버의 경우 모든 호스트 MAC 주소가 표시되지는 않습니다. 대부분의 경우 AnyFabric 이더넷 어댑터의 MAC 주소가 네트워크 설정 편집 대화 상자에 나열됩니다. 다른 이더

넷 어댑터(예, Lan-On-Motherboard)의 MAC 주소는 나열되지 않습니다. 어댑터에 대한 MAC 주소가 사용 불가능한 경우 비VLAN 배포에 AUTO 방법을 사용하십시오.

- IP 주소 및 서브넷 마스크
- IP 게이트웨이
- 최대 두 개의 DNS(Domain Name System) 서버
- 최대 전송 단위(MTU) 속도
- VLAN ID(VLAN IP 모드를 사용하는 경우)

VLAN을 사용하도록 선택하는 경우 구성 중인 호스트 네트워크 어댑터에 VLAN ID를 할당할 수 있습니다.

절차

하나 이상의 서버에 대한 네트워크 설정을 구성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.

단계 2. 구성할 서버를 하나 이상 선택하십시오. 한 번에 최대 28개의 서버를 구성하도록 선택할 수 있습니다.

단계 3. **선택 항목 변경 → 네트워크 설정**을 클릭하여 네트워크 설정 편집 페이지를 표시하십시오.

단계 4. 테이블에서 각 서버에 대한 필드를 완료하십시오.

팁: 각 행을 입력하는 대체 방법으로 테이블에서 일부 필드의 모든 행을 업데이트할 수 있습니다.

a. **모든 행 변경 → 호스트 이름**을 클릭하여 미리 지정되거나 사용자 지정 이름 지정 체계를 통해 모든 서버에 대한 호스트 이름을 설정하십시오.

b. **모든 행 변경 → IP 주소**를 클릭하여 IP 주소, 서브넷 마스크 및 게이트웨이의 범위를 할당하십시오. IP 주소는 각 서버에 할당되며, 표시되는 첫 번째 IP 주소로 시작해 마지막 IP 주소로 끝납니다. 서브넷 마스크와 게이트웨이 IP 주소가 각 서버에 적용됩니다.

c. **모든 행 변경 → DNS(Domain Name System)**를 클릭하여 운영 체제가 DNS 검색에 사용할 DNS 서버를 설정하십시오. 네트워크가 DNS 서버를 자동으로 정의하는 경우 또는 DNS 서버를 정의하지 않으려는 경우에는 **없음**을 선택하십시오.

d. **모든 행 변경 → MTU(Maximum Transmission Unit)**를 클릭하여 배포된 운영 체제에서 구성된 이더넷 어댑터에 사용할 MTU를 설정하십시오.

e. **모든 행 변경 → VLAN ID**를 클릭하여 운영 체제 VLAN 태깅에 대한 특정 VLAN ID를 설정하십시오.

1에서 4095 사이의 값을 지정할 수 있습니다. 기본값은 1이며, VLAN 모드가 사용되지 않음을 의미합니다.

이 옵션은 전역 설정 대화 상자에서 VLAN 사용이 사용 가능한 경우에만 적용될 수 있습니다 (전역 OS 배포 설정 구성 참조).

중요:

- 네트워크에서 작동하기 위해 VLAN 태그가 필요한 경우에만 VLAN ID를 지정하십시오. VLAN **사용** 태그는 호스트 운영 체제와 XClarity Administrator 사이의 네트워크 라우팅에 영향을 미칠 수 있습니다.
- VLAN 태그 지정된 패킷을 처리하려면 섀시 또는 ToR(top-of-rack) 스위치를 독립적으로 구성하여 해야 합니다. 이러한 패킷을 제대로 처리하도록 XClarity Administrator 및 데이터 네트워크가 구성되었는지 확인하십시오.
- 인벤터리에 MAC 주소가 있는 서버에 대해서만 VLAN 모드가 지원됩니다. AUTO가 서버에 사용 가능한 유일한 MAC 주소인 경우 해당 서버에 운영 체제를 배포하는 데 VLAN을 사용할 수 없습니다.

- VLAN 태깅은 Linux 운영 체제 배포에 지원되지 않지만, 일부 서버에 VLAN으로 배포하고 VLAN이 없는 다른 서버에도 동시에 배포하려는 경우 VLAN ID를 1로 설정하여 VLAN 모드에서 강제로 배포할 수 있습니다.

단계 5. **확인**을 클릭하여 설정을 저장하십시오. 설정은 웹 브라우저의 로컬 스토리지 캐시에서만 저장 및 지속됩니다.

결과

이제 구성된 각 서버에서 운영 체제 배포: OS 이미지 배포 페이지의 배포 상태가 **준비**로 표시됩니다.

관리되는 서버에 대한 스토리지 위치 선택

하나 이상의 서버에 대한 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

시작하기 전에

스토리지 위치를 선택하기 전에 스토리지 및 부팅 옵션 고려 사항을 검토하십시오(운영 체제 배포 고려사항 참조).

다음 유형의 스토리지에 운영 체제를 배포할 수 있습니다.

- **로컬 디스크 드라이브**

  RAID 컨트롤러 또는 SAS/SATA HBA에 연결된 디스크만 지원됩니다.

  Lenovo XClarity Administrator는 관리되는 서버의 첫 번째 열거된 로컬 RAID 디스크에 운영 체제 이미지를 설치합니다.

  서버의 RAID 구성이 올바로 구성되지 않은 경우 또는 비활성인 경우 로컬 디스크는 Lenovo XClarity Administrator에 보이지 않을 수 있습니다. 이 문제를 해결하려면 구성 패턴을 통해(로컬 저장 장치 정의 참조) 또는 서버의 RAID 관리 소프트웨어를 통해 RAID 구성을 사용하도록 설정하십시오.

  참고:

  - M.2 드라이브도 있으면 로컬 디스크 드라이브를 하드웨어 RAID용으로 구성해야 합니다.
  - SATA 어댑터를 사용하는 경우 SATA 모드는 "IDE"로 설정되어 있지 *않아야* 합니다.
  - ThinkServer 서버의 경우 운영 시스템은 로컬 디스크에만 배포할 수 있습니다. SAN 스토리지 및 내장 하이퍼바이저는 지원되지 않습니다.
  - ThinkServer 서버의 경우 구성은 서버의 RAID 관리 소프트웨어를 통해서만 사용할 수 있습니다.

  로컬에 설치한 디스크 드라이브에 VMware ESXi 5.5를 배포하는 예제 시나리오는 로컬 하드 드라이브에 ESXi 배포의 내용을 참조하십시오.

- **(ESXi 전용) 내장 하이퍼바이저(USB 또는 SD 미디어 어댑터)**

  이 위치는 VMware ESXi 이미지가 관리되는 서버에 배포되는 경우에만 적용됩니다.

  내장 하이퍼바이저는 다음 장치 중 하나입니다.

  - 다음 서버 중 하나의 특정 포트에 탑재된 IBM License USB 키(PN 41Y8298) 또는 Lenovo Licensed USB 키:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - 다음 서버에 설치된 SD 미디어 어댑터:

  - Flex System x240 M5
  - System x3500 M5
  - System x3550 M5
  - System x3650 M5

  또한 드라이브는 다음과 같이 구성해야 합니다.
  - 미디어 어댑터에 적합한 드라이브가 정의되어야 합니다.
  - SD 미디어 어댑터의 모드가 **작동 가능**으로 설정되어야 합니다.
  - 소유자는 시스템 또는 시스템 전용으로 설정되어야 합니다.
  - 액세스는 읽기/쓰기로 설정되어야 합니다.
  - 드라이브는 LUN 번호 0이 할당되어야 합니다.

  중요: SD 미디어 어댑터가 올바로 구성되지 않은 경우 Lenovo XClarity Administrator에서 SD 미디어 어댑터에 운영 체제를 배포할 수 없습니다.

  SD 미디어 어댑터의 모드를 **구성**으로 변경하고 `sdraid` 명령을 사용하여 관리 컨트롤러 CLI를 통해 미디어 어댑터를 구성할 수 있습니다. SD 미디어 어댑터의 모드 설정 및 CLI에서 어댑터 구성에 대한 추가 정보는 Integrated Management Module II 온라인 설명서의 내용을 참조하십시오.

2개의 하이퍼바이저 키가 관리되는 서버에 설치되어 있는 경우 VMware 설치 프로그램이 첫 번째 열거된 배포 키를 선택합니다.

참고: 하이퍼바이저 키가 설치된 관리되는 서버에 Microsoft Windows 배포를 시도하면 내장 하이퍼바이저 키를 선택하지 않아도 문제가 발생할 수 있습니다. Windows 배포 오류가 발생하는 경우 관리되는 서버에서 내장 하이퍼바이저 키를 제거하고 해당 서버에 Microsoft Windows 배포를 다시 시도하십시오.

- **M.2 드라이브**

  Lenovo XClarity Administrator는 관리되는 서버에 구성된 첫 번째 M.2 드라이브에 운영 체제 이미지를 설치합니다.

  M.2 스토리지는 ThinkSystem 서버에서만 지원됩니다.

  주의: 관리되는 장치에 하드웨어 RAID용으로 구성되지 않은 로컬 드라이브(SATA, SAS 또는 SSD) 및 M.2 드라이브가 둘 다 있는 경우 M.2 드라이브를 사용하려면 로컬 드라이브를 사용 안 함으로 설정해야 하고 로컬 드라이브를 사용하려면 M.2 드라이브를 사용 안 함으로 설정해야 합니다. 마법사의 로컬 스토리지 탭에서 로컬 디스크 사용 안 함을 선택하거나 기존 서버에서 구성 패턴을 생성한 다음 확장된 UEFI 패턴에서 M.2 장치를 사용 안 함으로 설정하여 구성 패턴에서 온보드 스토리지 컨트롤러 장치와 레거시 및 UEFI 스토리지 옵션 ROM을 사용 안 함으로 설정할 수 있습니다.

- **SAN 스토리지**

  Lenovo XClarity Administrator은(는) 관리되는 서버에 구성된 SAN 부팅 대상에 운영 체제 이미지를 설치합니다.

  다음 프로토콜이 지원됩니다.
  - Fibre Channel
  - 이더넷을 통한 Fibre Channel
  - SAN iSCSI(Emulex VFA5.2 2x10 GbE SFP+ 어댑터 및 FCoE/iSCSI SW 또는 Emulex VFA5.2 ML2 2x10 GbE SFP+ 어댑터 및 FCoE/iSCSI SW 어댑터만 사용)

  관리되는 랙 서버에서는 SAN 스토리지에 Windows 또는 RHEL만 배포할 수 있습니다. SAN 부팅 대상이 관리되는 서버에 구성되어야 합니다. 서버 패턴을 사용하여 SAN 부팅 타겟을 구성할 수도 있습니다(부팅 옵션 정의 참조).

  VMware ESXi를 배포하는 경우:

  - 로컬 하드 디스크는 사용 안 함으로 설정하거나 서버에서 제거해야 합니다. 서버 패턴을 사용하여 로컬 하드 디스크를 사용 안 함으로 설정할 수 있습니다(로컬 저장 장치 정의 참조).
  - 여러 SAN 볼륨을 사용할 수 있는 경우 첫 번째 볼륨만 배포에 사용됩니다.

  설치하는 OS 볼륨이 운영 체제에서 보이는 유일한 볼륨이어야 합니다.

서버에 연결한 SAN 볼륨에 VMware ESXi 5.5를 배포하는 예제 시나리오는 SAN 스토리지에 ESXi 배포의 내용을 참조하십시오.

참고: 각 서버에는 하드웨어 RAID 어댑터 또는 SAS/SATA HBA가 설치되고 구성되어 있어야 합니다. 일반적으로 온보드 Intel SATA 스토리지 어댑터에 있는 소프트웨어 RAID 또는 JBOD로 설정된 스토리지는 지원되지 않습니다. 그러나 하드웨어 RAID 어댑터가 없는 경우 SATA 어댑터를 운영 체제 배포에 대해 사용 설정된 AHCI SATA 모드로 설정하거나 구성되지 않은 정상 디스크를 JBOD로 설정하면 경우에 따라 작동할 수 있습니다. 자세한 정보는 XClarity Administrator 온라인 설명서에서 OS 설치 프로그램이 XClarity Administrator를 설치하려는 디스크를 찾을 수 없음의 내용을 참조하십시오.

절차

하나 이상의 관리되는 서버에 대한 스토리지 위치를 선택하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 OS 이미지 배포 페이지를 표시하십시오.

단계 2. 스토리지 설정을 변경하려는 서버를 선택하십시오.

단계 3. 선택한 모든 서버에 대한 스토리지 위치의 우선순위 순서를 변경하려면 **선택 항목 변경 → 스토리지 위치**를 클릭하십시오. 스토리지 위치가 호환되지 않는 경우 다음 스토리지 위치를 시도합니다.

다음 스토리지 위치의 우선순위를 설정할 수 있습니다.
- **로컬 디스크 드라이브 스토리지 사용**
- **ESXi가 선택된 경우 내장 하이퍼바이저(USB 또는 SD 미디어 어댑터) 사용**
- **M.2 드라이브 사용**
- **SAN 스토리지 사용**

단계 4. 각 서버에 대해 **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오. 이전 단계의 값에 해당하는 다음 값 중에서 선택할 수 있습니다.
- **로컬 디스크 드라이브**
- **내장 하이퍼바이저**
- **M.2 드라이브**
- **SAN 스토리지**

SAN 스토리지를 선택하면 SAN 볼륨을 구성할 수 있는 대화 상자가 표시됩니다. 배치 중에 타겟 SAN 볼륨에 도달할 수 있는지 확인하십시오.

선택한 스토리지 위치가 서버와 호환되지 않는 경우 Lenovo XClarity Administrator는 이전 단계에서 정의된 우선 순위로 다음 스토리지 위치에 운영 체제 배포를 시도합니다.

운영 체제 이미지 배포

Lenovo XClarity Administrator를 사용하여 운영 체제 이미지를 최대 28개의 서버에 동시 배포할 수 있습니다.

시작하기 전에

관리되는 서버에 운영 체제를 배포하기 전에 운영 체제 배포 고려 사항을 읽으십시오(운영 체제 배포 고려사항 참조).

OS 이미지 탭에서 배포할 운영 체제의 **배포 상태**가 "준비"로 설정되어 있는지 확인하십시오. Windows 운영 체제를 배포하려면 WinPE 부팅 파일이 필요합니다. 일치하는 WinPE 파일을 사용할 수 없는 경우 **배포 상태**가 "준비되지 않음"으로 설정되고 운영 체제를 배포할 수 없습니다. WinPE 파일을 수동으로 다운로드하고 가져와야 합니다(부팅 파일 가져오기 참조).

OS 이미지 관리 탭에서 **모두 표시 ➡ 배포 상태**를 클릭하여 OS 이미지 목록을 필터링할 수 있습니다. 상태가 "준비", "준비되지 않음" 및 "경고"인 서버만 표시하도록 목록을 필터링할 수 있습니다. 참고로 운영 체제 이미지의 배포 상태가 "준비되지 않음"인 경우 해당 운영 체제는 배포 가능한 운영 체제 목록에 포함되지 않습니다.

기본적으로 영어 로케일이 지원됩니다. 언어별 로케일을 지정하려면 사용자 지정 구성 파일과 무인 파일을 사용해야 합니다. 자세한 정보는 구성 가능한 로케일 및 NTP 서버가 있는 SLES 12 SP3 배포 및 일본어용 Windows 2016 배포의 내용을 참조하십시오.

비RAID 연결 스토리지에 대한 운영 체제 배포는 지원되지 않습니다.

주의: 서버에 현재 운영 체제가 설치되어 있는 경우 OS 이미지 프로필을 배포하면 현재 운영 체제를 덮어씁니다.

시스템 보호가 사용 설정되고 작업이 **OS 부팅 방지**로 설정된 XCC2가 있는 서버의 경우 시스템 보호가 장치에서 호환되는지 확인하십시오. 시스템 보호가 호환되지 않으면 장치가 부팅 프로세스를 완료할 수 없어 OS 배포에 실패합니다. 이러한 장치를 프로비저닝하려면 시스템 보호 부팅 프롬프트에 수동으로 응답하여 장치가 정상적으로 부팅되도록 하십시오.

절차

하나 이상의 관리되는 서버에 운영 체제 이미지를 배포하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 ➡ OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.

팁: 확장 가능 복합체의 경우 운영 체제가 기본 파티션에 배포됩니다. 따라서 기본 파티션만 서버 목록에 포함됩니다.

단계 2. 운영 체제를 배포할 하나 이상의 서버를 선택하십시오. 한 번에 최대 28개의 서버에 운영 체제를 배포할 수 있습니다.

특정 서버를 더 쉽게 찾을 수 있도록 테이블 열을 정렬할 수 있습니다. 또한 특정 섀시, 랙 또는 그룹에 있는 장치만 나열하도록 **표시** 메뉴에 있는 옵션을 선택하거나 **필터** 필드에 텍스트(예, 이름 또는 IP 주소)를 입력하여 표시되는 장치 목록을 필터링할 수 있습니다.

팁: 모든 컴퓨팅 노드에 동일한 운영 체제를 배포하려는 경우 여러 개의 섀시에서 여러 개의 컴퓨팅 노드를 선택할 수 있습니다.

단계 3. 네트워크 설정을 구성하려면 **선택 항목 변경 → 네트워크 설정**을 클릭하십시오.

자세한 정보는 관리되는 서버에 대한 네트워크 설정 구성의 내용을 참조하십시오.

단계 4. 각 서버에 대해 **배포할 이미지** 열의 드롭 다운 목록에서 배치할 OS 이미지 프로필을 선택하십시오.

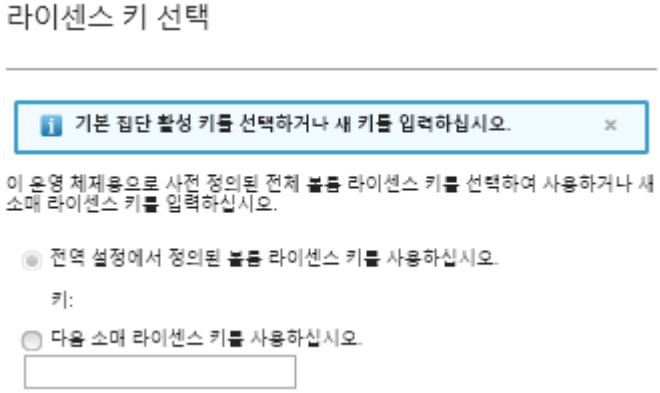
선택한 서버와 호환되는 OS 이미지 프로필을 선택했는지 확인하십시오. OS 이미지 관리 페이지에 **특성**이 나열되는 프로필 특성에서 호환성을 판별할 수 있습니다. 프로필 특성에 대한 정보는 운영 체제 이미지 프로필의 내용을 참조하십시오.

단계 5. 각 서버에 대해 **라이센스 키** 아이콘()을 클릭하고 운영 체제를 설치한 후 활성화하는 데 사용할 라이센스 키를 지정하십시오.

XClarity Administrator는 Windows 설치에 대한 기본 볼륨 라이센스 키 및 Windows와 VMware ESXi에 대한 개별 소매 키를 지원합니다.

전역 설정 대화 상자에서 지정한 전체 볼륨 라이센스 키를 사용하려면 **전역 설정에 정의된 볼륨 라이센스 키 사용**을 선택하십시오. 전체 볼륨 라이센스 키에 대한 자세한 정보는 전역 OS 배포 설정 구성의 내용을 참조하십시오.

개별 소매 라이센스 키를 사용하려면 **다음 소매 라이센스 키 사용**을 선택하고 다음 필드에 키를 입력하십시오.



단계 6. **옵션:** 서버에 대해 Windows 운영 체제를 선택한 경우 운영 시스템 이미지 옆에 표시되는 폴더 아이콘()을 클릭한 다음 Active Directory 이름을 선택하여 운영 체제 배포의 일부로 Windows 운영 시스템을 Active Directory 도메인에 연결할 수 있습니다.

전역 설정 대화 상자에서 지정한 기본 Active Directory를 사용하려면 **전역 설정에 정의된 Active Directory 사용**을 선택하십시오. Active Directory 도메인 연결에 대한 자세한 정보는 Windows Active Directory와 통합의 내용을 참조하십시오.

개별 Active Directory를 사용하려면 **다음 Active Directory 사용**을 선택하고 Active Directory 도메인을 선택하십시오.

단계 7. 각 서버에 대해 **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.
- **로컬 디스크 드라이브**
- **내장 하이퍼바이저**
- **M.2 드라이브**
- **SAN 스토리지**

선택한 스토리지 위치가 서버와 호환되지 않는 경우 XClarity Administrator는 우선 순위로 다음 스토리지 위치에 운영 체제 배포를 시도합니다.

참고: ThinkServer 서버의 경우 **로컬 디스크**만 사용할 수 있습니다.

스토리지 위치를 구성하는 방법에 대한 자세한 정보는 관리되는 서버에 대한 스토리지 위치 선택의 내용을 참조하십시오.

참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

단계 8. 선택한 모든 서버에 대한 배포 상태가 준비인지 확인하십시오.

중요: 선택한 모든 서버에 대한 배포 상태가 준비여야 합니다. 서버의 상태가 준비되지 않음일 경우 해당 서버에 운영 체제 이미지를 배포할 수 없습니다. 문제 해결에 도움이 되는 정보를 가져오려면 **준비되지 않음** 링크를 클릭하십시오. 네트워크 설정이 올바르지 않은 경우 네트워크 설정을 구성하려면 **선택 항목 변경 → 네트워크 설정**을 클릭하십시오.

단계 9. 운영 체제 배포를 시작하려면 **이미지 배포** 아이콘()을 클릭하십시오.

사용자 지정 구성 설정이 OS 이미지 프로필에 추가된 경우 **사용자 정의 설정** 탭이 OS 이미지 배포 대화 상자에 표시됩니다. 사용자 정의 설정, 공통 서버 설정 및 특정 서버 설정을 지정하고 **다음**을 클릭하여 OS 배포를 계속하십시오. 필수 사용자 지정 구성 설정을 입력하지 않은 경우 OS 배포가 진행되지 않습니다.

완료한 후에

작업 로그에서 배포 프로세스의 상태를 모니터링할 수 있습니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오. 작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

또한 서버에 대한 베이스보드 관리 컨트롤러를 통해 설치 진행을 관찰하도록 원격 제어 세션을 설정할 수 있습니다. 원격 제어에 대한 자세한 정보는 원격 제어를 사용하여 Converged, Flex System, NeXtScale 및 System x 서버 관리의 내용을 참조하십시오.

배포 정보는 운영 체제에 대해 저장됩니다. **프로비저닝 → OS 액세스 관리**를 클릭하고 서버 이름 위에 마우스를 갖다 대면 배치 정보를 볼 수 있습니다.

Windows Active Directory와 통합

Lenovo XClarity Administrator를 사용하여 Windows 이미지를 배포하는 경우 Active Directory 도메인을 운영 체제 배포의 일부로 연결할 수 있습니다.

시작하기 전에

Active Directory 도메인을 Windows 이미지 배포의 일부로 연결하려면 영향을 받는 Active Directory 도메인 컨트롤러를 실행 중인 관리 서버와 Windows 서버 모두 구성해야 합니다. 이 구성을 수행하려면 다음 액세스 권한이 필요합니다.

- Active Directory 서버 도메인을 인증 및 연결하는 권한이 있는 관리자 계정. 이 계정은 기본 도메인 관리자 그룹과 유사한 권한이 있어야 하며 이 구성이 이 그룹의 계정을 사용할 수 있습니다.
- 도메인 컨트롤러를 실행하는 Active Directory 서버에 해결하는 도메인 이름 시스템(DNS)에 대한 액세스 권한. 이 DNS는 운영 체제를 배포하는 서버에 대한 **네트워크 설정 → DNS** 옵션에 지정되어 있어야 합니다.
- 운영 체제를 배포하려면 Active Directory 서버 관리자가 도메인 서버에 필요한 컴퓨터 이름을 만들어야 합니다. 연결 시도 시 컴퓨터 이름을 생성하지 않습니다. 이름이 지정되어 있지 않은 경우 연결에 실패합니다.
- Active Directory 서버 관리자는 **네트워크 설정 → 호스트 이름** 필드를 클릭하여 대상 조직 단위에서 이미지가 컴퓨터 이름으로 배포되는 서버의 호스트 이름을 지정해야 합니다.

  지정된 호스트 이름(컴퓨터 이름)은 고유해야 합니다. 다른 Windows 설치가 이미 사용하고 있는 이름을 지정하면 연결에 실패합니다.

다음 방법 중 하나를 사용하여 Active Directory 도메인에 연결할 수 있습니다.

- **Active Directory 도메인 사용**

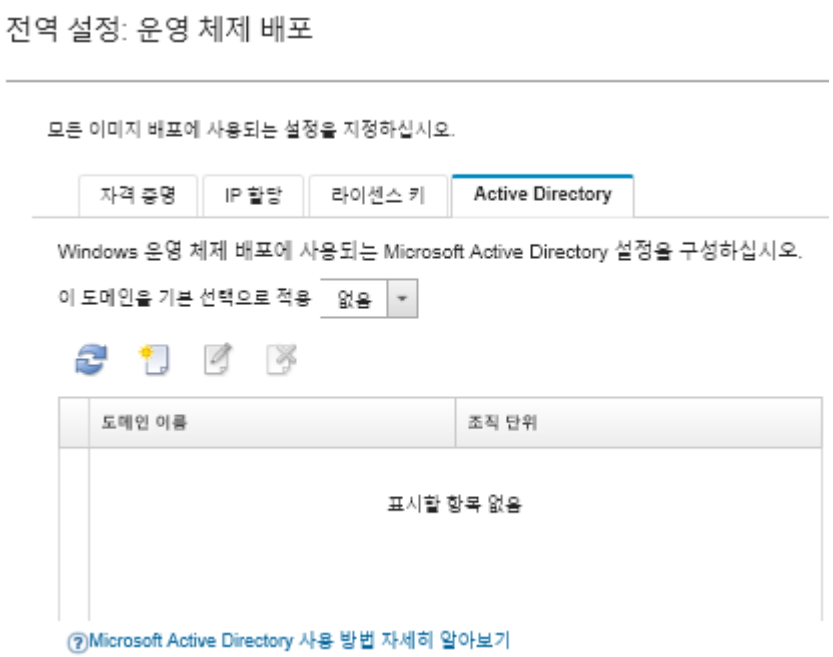
  미리 정의된 도메인 목록에서 특정 Active Directory 도메인을 사용하도록 선택할 수 있습니다. XClarity Administrator에서 Active Directory 도메인을 정의하려면 다음 단계를 완료하십시오. 여러 개의 도메인을 사용하려는 경우 각 도메인 이름에 대해 다음 단계를 반복하십시오.

  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 OS 이미지 배포 페이지를 표시하십시오.
  2. **전역 설정** 아이콘()을 클릭하여 전역 설정: 운영 체제 배포 대화 상자를 표시합니다.
  3. **Active Directory** 탭을 클릭하십시오.
  4. **만들기** 아이콘()을 클릭하여 새 Active Directory 도메인 추가 대화 상자를 표시하십시오.
  5. 도메인 이름 및 조직 단위를 지정하십시오.

     운영 체제 배포는 도메인 연결 및 도메인 내에 중첩 조직 단위 만들기를 지원합니다. 조직 단위를 지정하는 경우 OU를 연결의 일부로 명시적으로 지정할 필요가 없습니다. Active Directory는 도메인 이름 및 컴퓨터 이름을 사용하여 올바른 OU를 추출할 수 있습니다.
  6. **확인**을 누르십시오.
- **기본 Active Directory 도메인 사용**

  전역 설정에서 정의된 기본 Active Directory 도메인을 사용하도록 선택할 수 있습니다. XClarity Administrator에서 기본 Active Directory 도메인을 설정하려면 다음 단계를 완료하십시오.

  1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 OS 이미지 배포 페이지를 표시하십시오.
  2. **전역 설정** 아이콘()을 클릭하여 전역 설정: 운영 체제 배포 대화 상자를 표시하십시오.
  3. **Active Directory** 탭을 클릭하십시오.



4. **이 도메인을 기본 선택 항목으로 적용** 드롭다운 메뉴에서 모든 Windows 배포에 대해 기본적으로 사용할 Active Directory 도메인을 선택하십시오.
5. **확인**을 누르십시오.

- **메타데이터 blob 데이터 사용**

  Active Directory 컴퓨터 계정 메타데이터(Base-64 인코딩 blob 형식)를 사용하여 서버의 Active Directory 도메인에 연결할 수 있습니다. 메타데이터 blob 데이터를 생성하려면 다음 단계를 완료하십시오.

  1. 관리자 계정을 사용하여 컴퓨터에 로그인하십시오. 이 컴퓨터는 연결할 Active Directory 도메인의 일부여야 합니다.
  2. **시작 → 프로그램 → 보조프로그램**을 클릭하십시오. **명령 프롬프트**를 마우스 오른쪽 단추로 클릭한 다음 **관리자로 실행**을 클릭하십시오.
  3. C:\windows\system32 디렉토리로 변경하십시오.
  4. 다음 형식으로 `djoin` 명령을 실행하여 오프라인 도메인 연결을 수행하십시오.
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     여기서,

     – *<AD_domain_name>*은(는) Active Directory 도메인의 이름입니다.
     – *<hostname>*은(는) **네트워크 설정 → 호스트 이름** 필드를 클릭하면 대상 조직 단위의 컴퓨터 이름으로 이미지가 배포될 서버의 호스트 이름입니다.

     이 명령은 메타데이터 blob 데이터가 포함된 `blob`이라는 파일을 작성합니다. 이 파일의 내용은 운영 체제 배포 프로세스에서 Active Directory 연결 세부 정보를 지정하는 데 사용되므로 이 데이터를 가까이에 두십시오.

     메타데이터 blob 데이터는 민감한 데이터입니다.

운영 체제 이미지 배포에 대한 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

절차

Active Directory 도메인을 연결하려면 다음 단계를 완료하십시오.

단계 1. Windows 운영 체제 이미지를 OS 이미지 리포지토리에 가져옵니다(운영 체제 이미지 가져오기 참조).

단계 2. 운영 체제를 배포할 하나 이상의 서버를 선택하십시오. 한 번에 최대 28개의 서버에 운영 체제를 배포할 수 있습니다.

팁: 모든 컴퓨팅 노드에 동일한 운영 체제를 배포하려는 경우 여러 개의 섀시에서 여러 개의 컴퓨팅 노드를 선택할 수 있습니다.

단계 3. 네트워크 설정을 구성하려면 **선택 항목 변경 → 네트워크 설정**을 클릭하십시오.

a. **모든 행 변경 → 도메인 이름 시스템(DNS)**을 클릭하고 최소 Active Directory 도메인에 해결하는 DNS를 지정하십시오.

b. 각 서버에 대해 도메인의 기존 컴퓨터 이름과 일치하는 호스트 이름 및 연결하는 조직 단위를 지정하십시오.

네트워크 설정의 설정에 대한 자세한 정보는 관리되는 서버에 대한 네트워크 설정 구성의 내용을 참조하십시오.

단계 4. 각 서버에 대해 **배포할 이미지** 열에 배치할 Windows 운영 체제 이미지를 선택하십시오. 폴더와 라이센스 키 아이콘이 이미지 이름 옆에 표시됩니다.

단계 5. 각 서버에 대해 **라이센스 키** 아이콘()을 클릭하고 운영 체제를 설치한 후 활성화하는 데 사용할 라이센스 키를 지정하십시오.

단계 6. 각 서버에 대해 **폴더** 아이콘()을 클릭하고 Active Directory 도메인을 지정하십시오. 다음 값 중 하나를 선택할 수 있습니다.

- 기본 도메인을 사용하려면 **전역 설정에 정의된 Active Directory 사용**을 선택하십시오.
- 특정 도메인을 선택하려면 **다음 Active Directory 사용**을 선택하십시오.
- blob 파일의 내용을 지정하려면 **메타데이터 블록 데이터 사용**을 선택하십시오.

  메타데이터 blob 데이터에는 필드에 표시되지 않는 민감한 정보가 포함되어 있습니다. 배포 작업이 완료되기 전까지만 이 정보를 사용할 수 있습니다. 이는 지속적이지 않습니다.

단계 7. 각 서버에 대해 **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.
- **로컬 디스크 드라이브**
- **내장 하이퍼바이저**
- **M.2 드라이브**
- **SAN 스토리지**

선택한 스토리지 위치가 서버와 호환되지 않는 경우 XClarity Administrator는 우선 순위로 다음 스토리지 위치에 운영 체제 배포를 시도합니다.

스토리지 위치를 구성하는 방법에 대한 자세한 정보는 관리되는 서버에 대한 스토리지 위치 선택의 내용을 참조하십시오.

참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

단계 8. 선택한 모든 서버에 대한 배포 상태가 준비인지 확인하십시오.

서버의 상태가 준비되지 않음일 경우 해당 서버에 운영 체제 이미지를 배포할 수 없습니다. 문제 해결에 도움이 되는 정보를 가져오려면 **준비되지 않음** 링크를 클릭하십시오. 네트워크 설정이 올바르지 않은 경우 네트워크 설정을 구성하려면 **선택 항목 변경 → 네트워크 설정**을 클릭하십시오.

단계 9. 운영 체제 배포를 시작하려면 **이미지 배포** 아이콘()을 클릭하십시오.

배포 확인 대화 상자에 Active Directory 서버에 인증하고 도메인을 연결하는 데 사용할 자격 증명을 묻는 메시지가 표시됩니다. 보안상의 이유로 이러한 자격 증명은 XClarity Administrator에 저장되지 않습니다. 도메인을 연결하는 모든 Windows 배포에 대해 자격 증명을 입력해야 합니다.

작업 로그에서 배포 프로세스의 상태를 모니터링할 수 있습니다. XClarity Administrator 메뉴에서 **모니터링 → 작업**을 클릭하십시오. 작업 로그에 대한 자세한 정보는 작업 모니터링의 내용을 참조하십시오.

결과

운영 체제 배포가 완료되면 웹 브라우저를 네트워크 설정 편집 페이지에 지정한 IP 주소로 열고 로그인하여 구성 프로세스를 진행하십시오.

OS 배포 시나리오

이러한 시나리오를 사용하여 운영 체제를 사용자 지정하여 관리되는 서버에 배포할 수 있습니다.

사용자 지정 장치 드라이버와 함께 RHEL 배포

이 시나리오는 Red Hat Enterprise Linux(RHEL) 운영 체제와 기본 운영 체제에서 사용할 수 없는 추가 장치 드라이버를 설치합니다. 추가 장치 드라이버를 포함하는 사용자 지정 프로필이 사용됩니다. 그런 다음 사용자 지정 프로필을 OS 이미지 배포 페이지에서 선택할 수 있습니다.

시작하기 전에

Lenovo XClarity Administrator를 사용하여 운영 체제를 배포하는 경우 운영 체제에는 하드웨어에 적합한 이더넷, Fibre Channel 및 스토리지 어댑터 장치 드라이버가 포함되어야 합니다. 장치 드라이버가 운영 체제에 포함되지 않은 경우 해당 어댑터는 OS 배포에 대해 지원되지 않습니다. XClarity Administrator v1.2.0 이상에서는 장치 드라이버를 추가하여 운영 체제를 사용자 지정할 수 있습니다.

Lenovo YUM 리포지토리 웹 사이트에서, 공급업체(예, Red Hat)에서 또는 직접 생성한 사용자 지정 장치 드라이버를 통해 장치 드라이버를 확보할 수 있습니다. 일부 Windows 장치 드라이버의 경우 설치 exe에서 로컬 시스템으로 장치 드라이버를 추출하고 .zip 아카이브 파일을 작성하여 사용자 지정 장치 드라이버를 생성할 수 있습니다.

참고: .rpm 또는 .iso 이미지 형식에 RHEL 장치 드라이버가 있어야 합니다.

절차

사용자 지정 장치 드라이버와 함께 RHEL을 배포하려면 다음 단계를 완료하십시오.

단계 1. 기본 RHEL 운영 체제를 Red Hat 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘( )을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 RHEL 이미지를 찾아서 선택하십시오(예: RHEL-*<ver>*-*<date>*-Server-x86_64-dvd1.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. 사용자 지정 장치 드라이버를 로컬 시스템에 다운로드하고 파일을 OS 이미지 리포지토리로 가져옵니다. 자세한 정보는 장치 드라이버 가져오기의 내용을 참조하십시오.

1. **장치 드라이버** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 RHEL를 선택하십시오.
5. 운영 체제 버전을 선택하십시오.
6. 장치 유형을 선택하십시오.
7. **찾아보기**를 클릭하여 가져올 장치 드라이버를 찾아서 선택하십시오(예, kmod-i40e-2.0.12-1.el7.x86_64.rpm).
8. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 3. 사용자 지정 장치 드라이버가 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 지정할 OS 이미지 프로필을 선택하십시오(예, Virtualization).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom RHEL with device drivers).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **없음**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 프로필에 포함시킬 사용자 지정 장치 드라이버를 선택하고 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **소프트웨어** 탭에서 **다음**을 클릭하십시오.
7. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 4. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.

b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

   팁: VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.

c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 지정 OS 이미지 프로필을 선택하십시오 (예: *<base_OS>*|*<timestamp>*_Custom RHEL with device drivers).

   참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.

d. (옵션) **라이센스 키** 아이콘()을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.

e. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

   참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

f. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.

3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. **요약** 탭에서 설정을 검토하십시오.
5. **배포**를 클릭하여 운영 체제를 배포하십시오.

사용자 정의 무인 파일을 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포

이 시나리오에서는 사용자 정의 소프트웨어(Apache HTTP, PHP 및 hello-world PHP 응용 프로그램)와 함께 RHEL 운영 체제를 설치합니다. 운영 체제를 내부 Lenovo RHEL 가입 서비스에 등록하여 yum 리포지토리를 사용할 수 있도록 하는 사용자 정의 스크립트를 포함하고 Apache 및 PHP 패키지를 설치하며 Apache를 연결할 수 있도록 방화벽을 구성하고 Hello World PHP 응용 프로그램을 만들어 Apache 웹 서버 디렉토리에 복사한 다음 PHP를 지원하도록 Apache 구성 파일을 구성하는 사용자 정의 OS 이미지 프로파일이 사용됩니다.

시작하기 전에

몇 가지 다른 방법으로 사용자 정의 소프트웨어가 있는 RHEL을 배포할 수 있습니다. 이 예에서는 사용자 정의 OS 이미지 프로필에 포함되는 사용자 정의 무인 파일을 사용합니다. 도한 스토리지로 가져와서 사용자 정의 OS 이미지 프로필에 포함시키는 사용자 정의 소프트웨어를 설치하는 설치 후 스크립트를 사용할 수 있습니다. 설치 후 스크립트를 사용하여 소프트웨어를 설치하려면, 사용자 정의 소프트웨어와 설치 후 스크립트를 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포를 참조하십시오.

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- RHEL_installSoftware_customUnattend.cfg 이 사용자 정의 무인 파일에서는 미리 정의된 사용자 정의 매크로의 값을 사용하며 사용자 정의 소프트웨어를 구성합니다.

절차

사용자 정의 무인 파일을 사용하여 사용자 정의 소프트웨어가 있는 RHEL을 배포하려면 다음 단계를 완료하십시오.

단계 1. 기본 RHEL 운영 체제를 Red Hat 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.

2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 RHEL 이미지를 찾아서 선택하십시오(예: RHEL-*<ver>*-*<date>*-Server-x86_64-dvd1.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. RHEL 무인 (kickstart) 파일을 수정하여 RHEL 위성 가입 서비스에 운영 체제를 등록하고 HTTP (Apache) 및 PHP 패키지를 설치하며 간단한 Hello World PHP 응용 프로그램을 만들고 사전 정의된 필수 매크로 및 기타 사전 정의된 매크로(예, IP 주소, 게이트웨이, DNS 및 호스트 이름 설정)를 추가한 다음 사용자 정의 파일을 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

호스트를 RHEL Satellite에 등록하는 명령 추가하십시오. 예:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

중요: 예제 무인 파일에서 가입 서비스 구성을 기반으로 위성 서버 및 조직의 IP 주소를 지정하십시오.

호스트를 업데이트하고 Apache와 PHP 패키지를 설치 및 구성하기 위한 명령을 추가하십시오. 예:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
```

```
sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

참고: 예제 무인 파일은 킥 스타트 파일과 함께 설치되는 기본 패키지를 수정합니다. Apache 및 PHO 패키지를 %packages 섹션의 일부로 지정합니다.

ESXi 및 RHEL의 경우, XClarity Administrator는 UI에서 정의되는 모든 네트워크 설정을 무인 파일에 추가하는 **#predefined.unattendSettings.networkConfig#** 매크로 및 UI에서 정의되는 모든 스토리지 설정을 무인 파일에 추가하는 **#predefined.unattendSettings.storageConfig#**매크로를 제공합니다. 무인 파일에는 이미 이러한 매크로가 들어 있습니다.

XClarity Administrator는 또한 OOB 드라이버 삽입, 상태 보고, 설치 후 스크립트 및 사용자 정의 소프트웨어와 같은 몇 가지 기본 편의 매크로를 제공합니다. 그러나 이러한 미리 정의된 매크로를 활용하려면 사용자 지정 무인 파일에 다음 매크로를 지정해야 합니다. 예제 파일에는 이미 필수 매크로가 들어 있습니다.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

예제 파일에는 대상 서버 및 표준 시간대에 대한 네트워크 설정을 동적으로 지정하기 위한 필수 매크로 및 미리 정의된 추가 매크로가 이미 포함되어 있습니다. 무인 파일에 매크로를 추가하는 방법에 대한 자세한 정보는 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오.

사용자 정의 메시지를 XClarity Administrator의 작업 로그로 보내는 명령을 추가할 수도 있습니다. 자세한 정보는 설치 스크립트에 사용자 지정 상태 보고 추가의 내용을 참조하십시오.

사용자 지정 설치 스크립트를 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 설치 스크립트 가져오기의 내용을 참조하십시오.

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 RHEL를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 소프트웨어 파일을 찾아서 선택하십시오(예: RHEL_installSoftware_customUnattend.cfg).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 3. 사용자 정의 소프트웨어 및 설치 후 스크립트를 포함하는 사용자 정의 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 OS 이미지 프로필을 선택하십시오(예, Basic).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom RHEL with software using custom unattend).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **무인 파일만**을 선택하십시오.
   d. **다음**을 누르십시오.

5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **소프트웨어** 탭에서 **다음**을 클릭하십시오.
7. **무인 파일** 탭에서 사용자 정의 무인 파일(예: `RHEL_installSoftware_customUnattend.cfg`)을 선택하고 **다음**을 클릭하십시오.
8. **설치 스크립트** 탭에서 **다음**을 클릭하십시오.
9. **요약** 탭에서 설정을 검토하십시오.
10. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 4. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁:

      - VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
      - 네트워크 설정 대화 상자에서 지정한 네트워크 설정은 런타임 시 #predefined.hostPlatforms.networkSettings.*<setting>*# 매크로를 사용하여 무인 파일에 추가됩니다.

   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 정의 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_사용자 정의 무인을 사용하는 소프트웨어가 있는 사용자 정의 RHEL).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.

   d. (옵션) **라이센스 키** 아이콘()을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.
   e. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

   f. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.
3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. 사용자 정의 설정 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 무인 파일을 선택하십시오(예: `RHEL_installSoftware_customUnattend.cfg`).

5. **요약** 탭에서 설정을 검토하십시오.
6. **배포**를 클릭하여 운영 체제를 배포하십시오.

사용자 정의 소프트웨어와 설치 후 스크립트를 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포

이 시나리오에서는 사용자 정의 소프트웨어(Apache HTTP, PHP 및 hello-world PHP 응용 프로그램)와 함께 RHEL 운영 체제를 설치합니다. 사용자 정의 소프트웨어 및 운영 체제를 내부 Lenovo RHEL 가입 서비스에 등록하여 yum 리포지토리를 사용할 수 있도록 하는 설치 후 스크립트를 포함하고 Apache 및 PHP 패키지를 설치하며 Apache를 연결할 수 있도록 방화벽을 구성하고 Hello World PHP 응용 프로그램을 만들어 Apache 웹 서버 디렉토리에 복사한 다음 PHP를 지원하도록 Apache 구성 파일을 구성하는 사용자 정의 OS 이미지 프로파일이 사용됩니다. 사용자 정의 소프트웨어 패키지를 배포 중에 호스트에 내보내고 사용자 정의 설치 후 스크립트에서 사용할 수 있게 합니다.

시작하기 전에

몇 가지 다른 방법으로 RHEL과 Hello World PHP 응용 프로그램을 배포할 수 있습니다. 이 예에서는 스토리지로 가져와서 사용자 정의 OS 이미지 프로필에 포함시키는 사용자 정의 소프트웨어를 설치하는 설치 후 스크립트를 사용합니다. 또한 사용자 정의 OS 이미지 프로필에 포함되는 사용자 정의 무인 파일을 사용할 수 있습니다. 사용자 정의 참석 파일을 사용하여 소프트웨어를 설치하려면, 사용자 정의 무인 파일을 사용하여 RHEL 및 Hello World PHP 응용 프로그램 배포을 참조하십시오.

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- httpd.conf. Apache HTTP의 설치 파일입니다.
- hello_world.php Hello World PHP 응용 프로그램입니다.
- RHEL_installSoftware_customScript.sh 이 사후 설치 스크립트는 사용자 정의 소프트웨어를 설치하고 구성합니다.

참고:

- RHEL 설치 스크립트는 다음 형식 중 하나일 수 있습니다. Bash(.sh), Perl(.pm or .pl), Python(.py)
- 소프트웨어 파일 및 설치 스크립트는 배포 중에 지정한 사용자 지정 데이터 및 파일 경로에서 설치됩니다. 기본 사용자 정의 데이터 및 파일 경로는 `/home/lxca`입니다.

절차

설치 후 스크립트를 사용하여 사용자 정의 소프트웨어와 함께 RHEL을 배포하려면, 다음 단계를 완료하십시오.

단계 1. 기본 RHEL 운영 체제를 Red Hat 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 RHEL 이미지를 찾아서 선택하십시오(예: RHEL-*<ver>*-*<date>*-Server-x86_64-dvd1.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. 사용자 지정 소프트웨어를 로컬 시스템에 다운로드하고 파일을 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 사용자 지정 소프트웨어 가져오기의 내용을 참조하십시오.

팁: 사용자 정의 소프트웨어를 XClarity Administrator로 가져오려면, 파일이 tar.gz 파일에 포함되어야 합니다. 이 예제에서는 다음을 계속하기 전에 예제 소프트웨어 파일 httpd.conf 및 index.php를 RHEL_installSoftware_customsw.tar.gz라고 하는 tar.gz 파일에 압축하십시오.

1. **소프트웨어** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 RHEL를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 소프트웨어 파일을 찾아서 선택하십시오(예: RHEL_installSoftware_customsw.tar.gz).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 3. 사용자 지정 설치 후 스크립트를 만들고 해당 파일을 OS 이미지 리포지토리로 가져오십시오.

호스트를 RHEL Satellite에 등록하는 명령을 추가하십시오. 예:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

호스트를 업데이트하고 아파치와 PHP 패키지를 설치하고 설정하는 명령을 추가하십시오. 예:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

PHP 응용 프로그램을 웹 서버 위성에 추가하는 명령을 추가하십시오. 예:

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php
/var/www/html/index.php
```

Apache HTTP를 구성하는 명령을 추가하십시오. 예:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
```

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf
/etc/httpd/conf/httpd.conf
```

이 명령은 추출된 데이터 및 소프트웨어 파일의 경로에 미리 정의된 매크로를 사용합니다 (predefined.otherSettings.deployDataAndSoftwareLocation).

사용자 정의 메시지를 XClarity Administrator의 작업 로그로 보내는 명령을 추가할 수도 있습니다. 자세한 정보는 설치 스크립트에 사용자 지정 상태 보고 추가의 내용을 참조하십시오.

사용자 지정 설치 스크립트를 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 설치 스크립트 가져오기의 내용을 참조하십시오.

1. **설치 스크립트** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 RHEL를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 설치 후 스크립트를 찾아서 선택하십시오(예: RHEL_installSoftware_customScript.sh).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 4. 사용자 정의 소프트웨어 및 설치 후 스크립트를 포함하는 사용자 정의 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 OS 이미지 프로필을 선택하십시오(예, Basic).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필의 이름을 입력하십시오(예, Custom RHEL with software using post-installation script).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **없음**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **소프트웨어** 탭에서 소프트웨어 설치 파일(예: httpd.conf 및 index.php)을 선택하고 **다음**을 클릭하십시오.
7. **설치 스크립트** 탭에서 설치 스크립트(예: RHEL_installSoftware_customScript.sh)를 선택하고 **다음**을 클릭하십시오.
8. **요약** 탭에서 설정을 검토하십시오.
9. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 5. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

팁: VLAN 설정은 VLAN 모드가 **전역 설정** → **IP 할당** → **VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.

c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 지정 OS 이미지 프로필을 선택하십시오 (예: *<base_OS>*|*<timestamp>*_Custom RHEL with software using post-installation script).

참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.

d. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

e. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.

3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. **요약** 탭에서 설정을 검토하십시오.
5. **배포**를 클릭하여 운영 체제를 배포하십시오.

사용자 지정 패키지 및 시간대가 있는 SLES 12 SP3 배포

이 시나리오에서는 SLES 12 SP3 운영 체제(영문) 및 여러 옵션 SLES 패키지를 설치합니다. 또한 표준 시간대를 묻습니다. 사용자 지정 구성 파일과 사용자 지정 무인 파일이 포함된 사용자 지정 OS 이미지 프로필이 사용됩니다. 이 사용자 지정 프로필은 OS 이미지 배포 페이지에서 선택할 수 있습니다. 그런 다음 배포하려는 SLE 패키지를 선택하고 **사용자 지정 설정** 탭에서 표준 시간대를 지정할 수 있습니다. 사용자 지정 무인 파일의 사용자 지정 매크로가 선택한 값으로 대체되고 SLES autoyast 설치 프로그램은 무인 파일의 해당 값을 사용하여 운영 체제를 구성합니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- SLES_installPackages_customConfig.json. 이 구성 파일은 표준 시간대와 옵션 SLES 패키지(Linux, Apache, MySQL, PHP 소프트웨어 패키지, SLES 메일 서버 패키지 및 SLES 파일 서버 패키지)를 설치하라는 메시지를 표시합니다.
- SLES_installPackages_customUnattend.xml 이 무인 파일은 미리 정의된 매크로와 구성 파일에 정의된 사용자 지정 매크로의 값을 사용합니다.

절차

사용자 지정 OS 이미지 프로필을 사용하여 SLES 12 SP3을 여러 서버에 배포하려면 다음 단계를 완료하십시오.

단계 1. 기본 SLES 운영 체제를 SUSE 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 SLES 12 SP3 이미지를 찾아서 선택하십시오(예, SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. 사용자 지정 구성 설정 파일을 만들고 해당 파일을 OS 이미지 리포지토리로 가져오십시오.

구성 설정 파일은 OS 배포 프로세스 중에 동적으로 수집되어야 하는 데이터를 설명하는 JSON 파일입니다. 이 시나리오에서는 설치할 수 있는 옵션 SLES 패키지(SLES Linux, Apache, MySQL, PHP 소프트웨어 패키지, SLES 메일 서버 패키지 및 SLES 파일 서버 패키지 포함)와 각 OS 배포에 사용할 표준 시간대를 지정하려고 합니다. 구성 설정 파일 만들기에 대한 자세한 정보는 사용자 정의 매크로의 내용을 참조하십시오.

구성 설정 파일을 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 구성 설정 가져오기의 내용을 참조하십시오.

1. **구성 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 SLES를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 구성 설정 파일을 찾아서 선택하십시오(예: SLES_installPackages_customConfig.json).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

   참고: 사용자 지정 구성 설정 파일을 가져올 때 XClarity Administrator는 파일의 각 설정에 대해 사용자 지정 매크로를 생성합니다. 이러한 매크로를 무인 파일에 추가할 수 있습니다. OS 배포 중에 매크로는 실제 값으로 대체됩니다.

단계 3. SLES 무인 파일을 수정하여 옵션 SLES 패키지 및 표준 시간대에 대한 동적 값을 지정한 다음 사용자 지정 파일을 OS 이미지 리포지토리로 가져옵니다. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

<general> 섹션에서 표준 시간대 정보를 추가하십시오. 예:

```
<timezone>
  <hwclock></hwclock>
  <timezone></timezone>
</timezone>
```

<patterns> 섹션에서 3개의 패턴 태그를 추가하십시오. 이러한 태그는 옵션 SLES 패키지 설정의 사용자 지정 매크로에 사용됩니다. 예:

```
<patterns config:type="list">
  <pattern>32bit</pattern>
  <pattern>Basis-Devel</pattern>
  <pattern>Minimal</pattern>
  <pattern>WBEM</pattern>
  <pattern>apparmor</pattern>
  <pattern>base</pattern>
  <pattern>documentation</pattern>
  <pattern>fips</pattern>
  <pattern>gateway_server</pattern>
  <pattern>ofed</pattern>
  <pattern>printing</pattern>
  <pattern>sap_server</pattern>
  <pattern>x11</pattern>
  <pattern></pattern>
  <pattern></pattern>
  <pattern></pattern>
</patterns>
```

참고:

- 이러한 태그는 샘플 무인 파일에 있습니다.
- 사용자 지정 무인 파일을 사용하는 경우 XClarity Administrator는 미리 정의된 무인 파일을 사용할 때 얻을 수 있는 많은 편의 기능을 제공하지 않습니다. 예를 들어 관리자에 대한

대상 <DiskConfiguration>, <ImageInstall>, <ProductKey> 및 <UserAccounts>, 네트워킹에 대한 <Interfaces>, 설치 기능에 대한 <package> 목록이 업로드 중인 사용자 지정 무인 파일에 지정되어야 합니다.

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 SLES를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 무인 파일을 찾아서 선택하십시오(예: SLES_installPackages_customUnattend.xml).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

   참고: 무인 파일에 미리 정의된 매크로가 없다는 경고가 표시됩니다. 이제 경고를 무시할 수 있습니다. 다음 단계에서 미리 정의된 매크로를 추가합니다.
7. 경고 대화 상자에서 **닫기**를 클릭하여 무인 파일 편집 대화 상자를 여십시오.

단계 4. 사용자 지정 무인 파일을 사용자 지정 구성 설정 파일과 연결하고 미리 지정된 필수 사용자 지정 매크로(설정)를 구성 설정 파일에서 무인 파일에 추가하십시오. 자세한 정보는 무인 파일을 구성 설정 파일과 연결 및 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오.

팁: 선택적으로 사용자 정의 무인 파일을 사용자 정의 구성 설정 파일과 연결하고 무인 파일을 가져올 때 매크로를 추가할 수 있습니다.

1. 무인 파일 편집 대화 상자에 있는 **구성 파일 연결** 드롭 다운 목록에서 무인 파일과 연결할 구성 설정 파일을 선택하십시오(예: SLES_installPackages_customConfig).
2. 미리 정의된 필수 매크로를 무인 파일에 추가하십시오.
   a. **사용 가능한 매크로** 드롭 다운 목록에서 **미리 정의됨**을 선택하십시오.
   b. 무인 파일에서 1라인 뒤(<xml> 태그 뒤)의 아무 위치에나 커서를 놓으십시오.
   c. 사용 가능한 미리 정의된 매크로 목록에서 **미리 정의됨** → unattendSettings 목록을 펼치십시오.
   d. preinstallConfig 및 postinstallConfig 매크로를 클릭하여 매크로를 무인 파일에 추가하십시오.

   예를 들어, 다음과 같습니다.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

3. 표준 시간대를 지정하는 사용자 지정 매크로를 추가하십시오.
   a. **사용 가능한 매크로** 드롭 다운 목록에서 **사용자 지정**을 선택하십시오.
   b. 커서를 <hwclock> 태그 뒤에 놓고 timezone을 클릭하여 표준 시간대 매크로를 추가하십시오.
   c. 커서를 <timezone> 태그 뒤에 놓고 timezone을 클릭하여 표준 시간대 매크로를 추가하십시오.

   예를 들어, 다음과 같습니다.

```
<timezone>
  <hwclock>#timezone#</hwclock>
  <timezone>#timezone#</timezone>
</timezone>
```

4. 옵션 SLES 패키지를 지정하는 사용자 지정 매크로를 추가하십시오.

a. 사용 가능한 사용자 지정 매크로 목록에서 **서버 설정 → 노드** 목록을 펼치십시오.
b. 비어 있는 <pattern> 태그 중 하나에 커서를 놓고 fileserver를 클릭하십시오.
c. 비어 있는 <pattern> 태그 중 하나에 커서를 놓고 lampserver를 클릭하십시오.
d. 비어 있는 <pattern> 태그 중 하나에 커서를 놓고 mailserver를 클릭하십시오.

예를 들어, 다음과 같습니다.

```
<patterns config:type="list">
  <pattern>32bit</pattern>
  <pattern>Basis-Devel</pattern>
  <pattern>Minimal</pattern>
  <pattern>WBEM</pattern>
  <pattern>apparmor</pattern>
  <pattern>base</pattern>
  <pattern>documentation</pattern>
  <pattern>fips</pattern>
  <pattern>gateway_server</pattern>
  <pattern>ofed</pattern>
  <pattern>printing</pattern>
  <pattern>sap_server</pattern>
  <pattern>x11</pattern>
  <pattern>#server-settings.node.fileserver#</pattern>
  <pattern>#server-settings.node.lampserver#</pattern>
  <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. **저장**을 클릭하여 파일을 함께 바인딩하고 변경사항을 무인 파일에 저장하십시오.

단계 5. 사용자 지정 구성 설정 및 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 OS 이미지 프로필을 선택하십시오(예, Basic).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom SLES with optional packages).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 정의 유형에 **연결된 무인 및 구성-설정 파일**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **소프트웨어** 탭에서 **다음**을 클릭하십시오.
7. **무인 파일** 탭에서 무인 파일(예: SLES_installPackages_customUnattend.xml)을 선택하고 **다음**을 클릭하십시오.

   연결된 구성 설정 파일이 자동으로 선택됩니다.
8. **설치 스크립트** 탭에서 **다음**을 클릭하십시오.
9. **요약** 탭에서 설정을 검토하십시오.
10. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 6. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.

b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

   팁: VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.

c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 지정 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_Custom SLES with optional packages).

   참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.

d. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

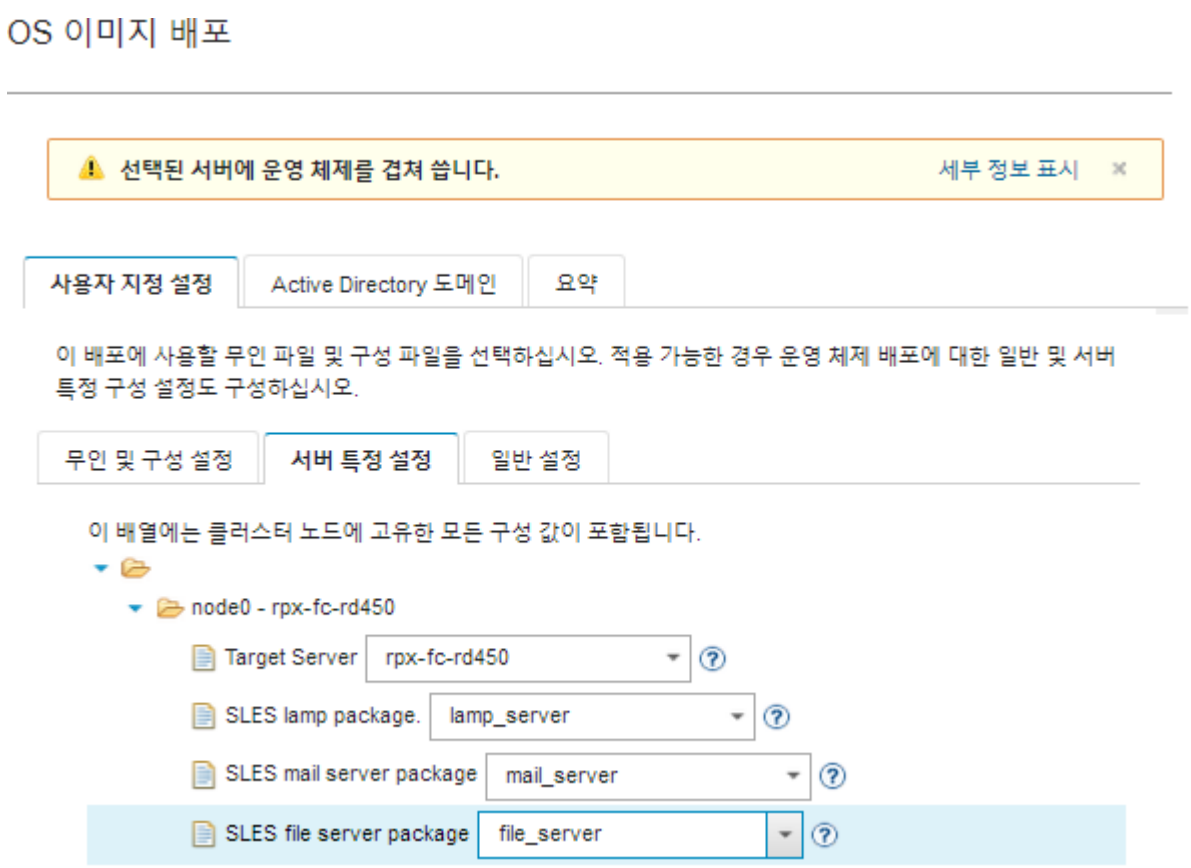
   참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

e. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.

3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘( )을 클릭하십시오.
4. **사용자 정의 설정** 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 구성 설정 파일을 선택하십시오(예: SLES_installPackages_customConfig).

   참고: 연결된 사용자 지정 무인 파일이 자동으로 선택됩니다.

5. **서버 특정 설정** 하위 탭에서 배포하려는 대상 서버와 옵션 SLES 패키지를 선택하십시오.



6. **일반 설정** 하위 탭에서 모든 대상 서버에 설정할 표준 시간대를 선택하십시오.

7. **요약** 탭에서 설정을 검토하십시오.
8. **배포**를 클릭하여 운영 체제를 배포하십시오.

사용자 지정 소프트웨어와 함께 SLES 12 SP3 배포

이 시나리오는 사용자 지정 소프트웨어(Java 및 Eclipse IDE)와 함께 SLES 12 SP3 운영 체제를 설치합니다. 사용자 지정 소프트웨어를 설치하고 구성하기 위한 사용자 지정 소프트웨어 및 설치 후 스크립

트가 포함된 사용자 지정 프로필이 사용됩니다. 사용자 지정 소프트웨어 패키지는 배포 중에 호스트에 복사되고 사용자 지정 설치 후 스크립트에서 사용할 수 있습니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- jre-8u151-linux-x64.tar.gz. Eclipse용 Java의 설치 파일입니다.
- eclipse-4.6.3-3.1.x86_64.tar.gz Eclipse IDE의 설치 파일입니다.
- SLES_installSoftware_customScript.sh 이 설치 후 스크립트는 Eclipse를 실행하는 사용자를 만들고 Eclipse IDE 및 Java를 설치합니다.

참고:

- SLES 설치 스크립트는 다음 형식 중 하나일 수 있습니다. Bash(.sh), Perl(.pm or .pl), Python(.py)
- 소프트웨어 파일 및 설치 스크립트는 배포 중에 지정한 사용자 지정 데이터 및 파일 경로에서 설치됩니다. 기본 사용자 정의 데이터 및 파일 경로는 `/home/lxca`입니다.
- SLES 12 SP3의 경우 Eclipse IDE에는 미리 정의된 기본 프로필에 포함된 GCC 컴파일러가 필요합니다. 이 시나리오는 미리 정의된 기본 프로필을 기본으로 사용하여 사용자 지정 OS 이미지 프로필을 만듭니다. 다른 프로필을 사용하도록 선택한 경우 프로필에 GCC 컴파일러가 포함되어 있는지 확인해야 합니다.

절차

사용자 지정 소프트웨어와 함께 SLES 12 SP3을 배포하려면 다음 단계를 완료하십시오.

단계 1. 기본 SLES 12 SP3 운영 체제를 SUSE 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 SLES 12 SP3 이미지를 찾아서 선택하십시오(예, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. 사용자 지정 소프트웨어를 로컬 시스템에 다운로드하고 파일을 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 사용자 지정 소프트웨어 가져오기의 내용을 참조하십시오.

1. **소프트웨어** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 `SLES`를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 소프트웨어 파일을 찾아서 선택하십시오(예: `jre-8u151-linux-x64.tar.gz`).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.
7. **가져오기** 아이콘()을 다시 클릭하십시오.
8. **로컬 가져오기**를 클릭하십시오.

9. 운영 체제에 SLES를 선택하십시오.
10. **찾아보기**를 클릭하여 가져올 소프트웨어 파일을 찾아서 선택하십시오(예: eclipse-4.6.3-3.1.x86_64.tar.gz).
11. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 3. 사용자 지정 설치 후 스크립트를 만들고 해당 파일을 OS 이미지 리포지토리로 가져오십시오.

이 파일에 Eclipse를 실행하는 사용자를 만드는 명령을 추가하십시오. 예를 들면 다음과 같습니다.

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "PasswOrd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

소프트웨어를 설치하기 위한 명령을 추가하십시오. 예를 들면 다음과 같습니다.

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

이러한 명령은 HTTPS URL에 대해 미리 정의된 매크로를 사용합니다. XClarity Administrator는 이러한 HTTP URL을 보고 상태(predefined.otherSettings.statusSettings.urlStatus), 첫 번째 부팅 시 호스트 OS에서 urlStatus 웹 서비스에 액세스하는 데 필요한 인증서가 포함된 폴더(predefined.otherSettings.statusSettings.certLocation) 및 추출된 데이터 및 소프트웨어 파일에 대한 경로(predefined.otherSettings.deployDataAndSoftwareLocation)에 사용합니다.

샘플 파일에 표시된 대로 사용자 지정 메시지를 XClarity Administrator의 작업 로그로 보내는 명령을 추가할 수도 있습니다. 자세한 정보는 설치 스크립트에 사용자 지정 상태 보고 추가의 내용을 참조하십시오.

사용자 지정 설치 스크립트를 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 설치 스크립트 가져오기의 내용을 참조하십시오.

1. **설치 스크립트** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 SLES를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 설치 후 스크립트를 찾아서 선택하십시오(예: SLES_installSoftware_customScript.sh).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 4. 사용자 정의 소프트웨어 및 설치 후 스크립트를 포함하는 사용자 정의 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.

2. 사용자 정의할 OS 이미지 프로필을 선택하십시오(예, Basic).
3. **만들기** 아이콘()을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom SLES with software).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **없음**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **소프트웨어** 탭에서 소프트웨어 설치 파일(예: jre-8u151-linux-x64.tar.gz 및 eclipse-4.6.3-3.1.x86_64.tar.gz)을 선택하고 **다음**을 클릭하십시오.
7. **설치 스크립트** 탭에서 설치 스크립트(예: SLES_installSoftware_customScript.sh)를 선택하고 **다음**을 클릭하십시오.
8. **요약** 탭에서 설정을 검토하십시오.
9. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 5. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁: VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 정의 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_소프트웨어가 있는 사용자 정의 SLES).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.
   d. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.
   e. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.
3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. **요약** 탭에서 설정을 검토하십시오.
5. **배포**를 클릭하여 운영 체제를 배포하십시오.

구성 가능한 로케일 및 NTP 서버가 있는 SLES 12 SP3 배포

이 시나리오에서는 키보드 및 운영 체제 로케일에 영어, 브라질어 또는 일본어를 사용하는 SLES 12 SP3 운영 체제를 설치합니다. 또한 최대 3개의 NTP 서버에 대한 IP 주소를 구성합니다. 로케일과 NTP 서버 설정을 선택하기 위해 무인 파일(미리 정의된 사용자 지정 매크로 포함)과 구성 설정 파일이 포함된 사용자 지정 OS 이미지 프로필이 사용됩니다. 이 사용자 지정 프로필은 OS 이미지 배포 페이지에서 선택할 수 있습니다. 그런 다음 **사용자 지정 설정** 탭에서 로케일과 NTP 서버 설정을 선택할 수 있습니다. 사용자 지정 무인 파일에 포함된 사용자 지정 매크로가 지정된 값으로 대체되고 SLES autoyast 설치 프로그램은 무인 파일의 해당 값을 사용하여 운영 체제를 구성합니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- SLES_locale_customConfig.json. 이 사용자 지정 구성 파일은 SLES 및 NTP 서버에 대한 OS 로케일 및 키보드용 언어를 설치하라는 메시지를 표시합니다.
- SLES_locale_customUnattend.xml. 이 사용자 지정 무인 파일은 구성 파일에 정의된 사용자 지정 매크로의 값을 사용합니다.

절차

사용자 지정 OS 이미지 프로필을 사용하여 SLES 12 SP3을 배포하려면 다음 단계를 완료하십시오.

단계 1. 기본 SLES 운영 체제를 SUSE 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 SLES 12 SP3 이미지를 찾아서 선택하십시오(예, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오.

단계 2. 사용자 지정 구성 설정 파일을 만들고 해당 파일을 OS 이미지 리포지토리로 가져오십시오.

구성 설정 파일은 OS 배포 프로세스 중에 동적으로 수집되어야 하는 데이터를 설명하는 JSON 파일입니다. 이 시나리오에서는 각 OS 배포에 사용할 운영 체제 로케일(en_US, ja_JP, pt_BR), 키보드 로케일(미국 영어, 일본어 또는 브라질 포르투갈어) 및 최대 3개의 NTP 서버 IP 주소를 지정하려고 합니다. 구성 설정 파일 만들기에 대한 자세한 정보는 사용자 정의 매크로의 내용을 참조하십시오.

구성 설정 파일을 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 구성 설정 가져오기의 내용을 참조하십시오.

1. **구성 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 `SLES`를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 구성 설정 파일을 찾아서 선택하십시오(예: `SLES_locale_customConfig.json`).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

   참고: 사용자 지정 구성 설정 파일을 가져올 때 XClarity Administrator는 파일의 각 설정에 대해 사용자 지정 매크로를 생성합니다. 이러한 매크로를 무인 파일에 추가할 수 있습니다. OS 배포 중에 매크로는 실제 값으로 대체됩니다.

단계 3. SLES 무인 파일을 수정하여 옵션 운영 체제 로케일, 키보드 로케일 및 NTP 서버 IP 주소에 대한 동적 값을 지정한 다음 사용자 지정 파일을 OS 이미지 리포지토리로 가져옵니다. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

<profile> 태그 바로 뒤에 NTP 서버 및 네트워킹 정보를 추가하십시오. 다음 예제에는 두 개의 NTP 서버에 대한 태그가 포함되어 있습니다. IP 주소는 이후 단계에서 매크로로 추가됩니다.

```
<ntp-client>
  <configure_dhcp config:type="boolean">false</configure_dhcp>
  <peers config:type="list">
    <peer>
      <address></address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address></address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
  </peers>
  <start_at_boot config:type="boolean">true</start_at_boot>
  <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

다음 예제에 표시된 대로 <general> 섹션에 OS 및 키보드 로케일 정보를 추가하십시오. 키보드 및 운영 체제 로케일 설정은 이후 단계에서 매크로로 추가됩니다.

```
<keyboard>
  <keymap></keymap>
</keyboard>
<language></language>
```

참고: 사용자 지정 무인 파일을 사용하는 경우 XClarity Administrator는 미리 정의된 무인 파일을 사용할 때 얻을 수 있는 많은 편의 기능을 제공하지 않습니다. 예를 들어 관리자에 대한 대상 <DiskConfiguration>, <ImageInstall>, <ProductKey> 및 <UserAccounts>, 네트워킹에 대한 <Interfaces>, 설치 기능에 대한 <package> 목록이 업로드 중인 사용자 지정 무인 파일에 지정되어야 합니다.

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 SLES를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 무인 파일을 찾아서 선택하십시오(예: SLES_locale_customUnattend.xml).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 4. 사용자 지정 무인 파일을 사용자 지정 구성 설정 파일과 연결하고 미리 지정된 필수 사용자 지정 매크로(설정)를 구성 설정 파일에서 무인 파일에 추가하십시오. 자세한 정보는 무인 파일을 구성 설정 파일과 연결 및 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오.

팁: 선택적으로 사용자 정의 무인 파일을 사용자 정의 구성 설정 파일과 연결하고 무인 파일을 가져올 때 매크로를 추가할 수 있습니다.

1. **무인 파일** 탭에서 사용자 정의 무인 파일을 선택하십시오(예: SLES_locale_customUnattend.xml).
2. **구성 파일 연결** 아이콘()을 클릭하여 무인 파일 연결 대화 상자를 표시하십시오.
3. 무인 파일과 연결시킬 구성 설정 파일을 선택하십시오(예: SLES_locale_customConfig).
4. 미리 정의된 필수 매크로를 무인 파일에 추가하십시오.
   a. **사용 가능한 매크로** 드롭 다운 목록에서 **미리 정의됨**을 선택하십시오.

b. 무인 파일에서 1라인 뒤(<xml> 태그 뒤)의 아무 위치에나 커서를 놓으십시오.

c. 사용 가능한 미리 정의된 매크로 목록에서 **미리 정의됨 → unattendSettings** 목록을 펼치십시오.

d. preinstallConfig 및 postinstallConfig 매크로를 클릭하여 매크로를 추가하십시오.

예를 들어, 다음과 같습니다.

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. 운영 체제 로케일을 지정하는 사용자 지정 매크로를 추가하십시오.

a. **사용 가능한 매크로** 드롭 다운 목록에서 **사용자 지정**을 선택하십시오.

b. 커서를 <language> 태그 뒤에 두십시오.

c. 사용 가능한 사용자 지정 매크로 목록에서 **서버 설정 → 노드**를 펼친 다음 **로케일**을 클릭하여 OS 로케일 매크로를 추가하십시오.

예를 들어, 다음과 같습니다.

```
<language>#server-settings.node.locale#</language>
```

6. 키보드 로케일을 지정하는 사용자 지정 매크로를 추가하십시오.

a. 커서를 <keymap> 태그 뒤에 두십시오.

b. 사용 가능한 사용자 지정 매크로 목록에서 **서버 설정 → 노드**를 펼친 다음 keyboardLocale을 클릭하여 키보드 로케일 매크로를 추가하십시오.

예를 들어, 다음과 같습니다.

```
<keyboard>
  <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. NTP 서버 IP 주소를 지정하는 사용자 지정 매크로를 추가하십시오.

이 시나리오에서 사용자 지정 구성 설정 파일은 템플릿을 사용하여 0 ~ 3개의 NTP 서버를 지정합니다. 구성 설정 파일에서 템플릿을 사용할 때 템플릿과 연결된 매크로는 무인 파일 연결 대화 상자에 표시되지 않습니다. 대신 수동으로 무인 파일을 편집하고 매크로 및 적절한 태그를 추가해야 합니다.

예를 들어, 3개의 NTP 서버를 포함하려면 다음 태그와 매크로를 무인 파일에 추가합니다. 이러한 태그 및 매크로는 이 시나리오의 예제 무인 파일에 이미 있습니다.

```
<ntp-client>
  <configure_dhcp config:type="boolean">false</configure_dhcp>
  <peers config:type="list">
    <peer>
      <address>#server-settings.ntpserver1#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver2#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver3#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
```

```
    <type>server</type>
   </peer>
  </peers>
  <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. **연결**을 클릭하여 파일을 함께 바인딩하고 변경사항을 무인 파일에 저장하십시오.

단계 5. 사용자 지정 구성 설정 및 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 OS 이미지 프로필을 선택하십시오(예, Basic).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필의 이름을 입력하십시오(예, Custom SLES for OS and keyboard locale and NTP server).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 정의 유형에 **연결된 무인 및 구성-설정 파일**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **소프트웨어** 탭에서 **다음**을 클릭하십시오.
7. **무인 파일** 탭에서 무인 파일(예: SLES_locale_customUnattend.xml)을 선택하고 **다음**을 클릭하십시오.

   연결된 구성 설정 파일이 자동으로 선택됩니다.
8. **설치 스크립트** 탭에서 **다음**을 클릭하십시오.
9. **요약** 탭에서 설정을 검토하십시오.
10. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 6. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

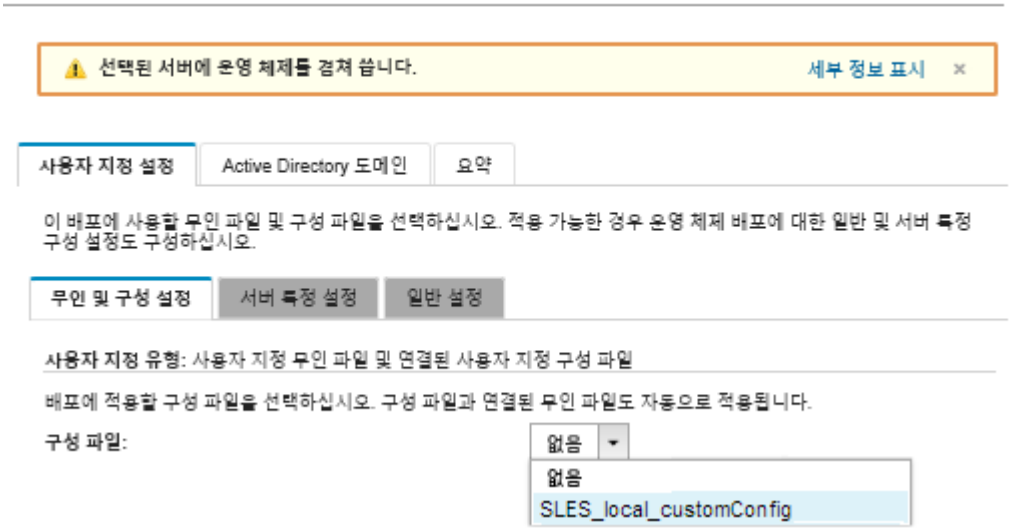
      팁: VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 정의 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_OS의 사용자 정의 SLES, 키보드 로케일 및 NTP 서버).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.
   d. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.
   e. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.
3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘( )을 클릭하십시오.

4. **사용자 정의 설정** 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 구성 설정 파일을 선택하십시오(예: `SLES_locale_customConfig`).

   참고: 연결된 사용자 지정 무인 파일이 자동으로 선택됩니다.



5. **서버 특정 설정** 하위 탭에서 대상 서버, OS 로케일 및 키보드 로케일을 선택하십시오.
6. **일반 설정** 하위 탭에서 **추가**를 클릭하여 최대 3개의 NTP 서버의 IP 주소를 지정하십시오.
7. **요약** 탭에서 설정을 검토하십시오.
8. **배포**를 클릭하여 운영 체제를 배포하십시오.

고정 IP 주소를 사용하여 Lenovo Customization이 있는 VMware ESXi v6.7을 로컬 디스크에 배포

이 시나리오에서는 호스트 서버의 고정 IP 주소를 사용하여 로컬 디스크에 Lenovo Customization 운영 체제가 있는 VMware ESXi v6.7을 설치합니다. 무인 파일(미리 정의된 매크로 포함)을 포함하는 사용자 지정 OS 이미지 프로필이 사용됩니다. 이 사용자 지정 프로필은 OS 이미지 배포 페이지에서 선택할 수 있습니다. 사용자 지정 무인 파일의 미리 정의된 매크로가 알려진 값으로 대체되고 VMware ESXi kickstart 설치 프로그램은 무인 파일의 해당 값을 사용하여 운영 체제를 구성합니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- ESXi_staticIP_customUnattend.cfg. 이 사용자 지정 무인 파일은 미리 정의된 매크로의 값을 사용합니다.

절차

사용자 지정 OS 이미지 프로필을 사용하여 VMware ESXi v6.7을 배포하려면 다음 단계를 완료하십시오.

단계 1. Lenovo Customization 운영 체제가 있는 VMware vSphere® Hypervisor(ESXi)를 VMware 지원 – 다운로드 웹 페이지 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

   1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
   2. **OS 이미지** 탭을 클릭하십시오.

3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 ESXi 이미지를 찾아서 선택하십시오(예, ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오.

단계 2. ESXi 무인(kickstart) 파일을 수정하여 미리 정의된 필수 매크로와 IP 주소, 게이트웨이, DNS 및 호스트 이름 설정과 같은 미리 정의된 기타 매크로를 추가한 다음 사용자 지정 파일을 OS 이미지 리포지토리로 가져옵니다. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

ESXi 및 RHEL의 경우에만, XClarity Administrator가 #predefined.unattendSettings.networkConfig# 매크로를 제공하며 이 매크로는 UI에 정의된 모든 네트워크 설정을 무인 파일에 추가합니다. 이 예제에서는 UI에 정의되지 않은 설정(--addvmportgroup)을 지정하므로 #predefinedunattendSettings.storageConfig# 매크로가 샘플 무인 파일에서 사용되지 않습니다. 대신 네트워크 설정이 개별적으로 파일에 추가되고 #predefined.hostPlatforms.networkSettings.*<setting>*# 매크로가 사용됩니다.

ESXi 및 RHEL의 경우에만, XClarity Administrator는 #predefined.unattendSettings.storageConfig# 매크로도 제공하며 이 매크로는 UI에 정의된 모든 스토리지 설정을 무인 파일에 추가합니다. 이 예제에서는 UI에 정의되지 않은 설정(--novmfsondisk 및 –ignoressd)을 지정하므로 #predefinedunattendSettings.storageConfig# 매크로가 샘플 무인 파일에서 사용되지 않습니다. 대신 스토리지 설정이 개별적으로 추가되고 --firstdisk=local이 파일에 하드코드됩니다.

참고: XClarity Administrator는 OOB 드라이버 삽입, 상태 보고, 설치 후 스크립트, 사용자 지정 소프트웨어와 같은 몇 가지 기본 편의 매크로를 제공합니다. 그러나 이러한 미리 정의된 매크로를 활용하려면 사용자 지정 무인 파일에 다음 매크로를 지정해야 합니다. 예제 파일에는 이미 필수 매크로가 들어 있습니다. %firstboot 섹션이 포함되어 있으므로 이러한 미리 정의된 매크로의 순서가 중요합니다. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
예제 파일에는 대상 서버의 네트워크 설정을 동적으로 지정하기 위한 필수 매크로 및 미리 정의된 추가 매크로가 이미 포함되어 있습니다. 무인 파일에 매크로를 추가하는 방법에 대한 자세한 정보는 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오.

사용 가능한 미리 정의된 매크로에 대한 자세한 정보는 미리 정의된 매크로의 내용을 참조하십시오.

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 ESXi를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 무인 파일을 찾아서 선택하십시오(예: ESXi_staticIP_customUnattend.cfg).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 3. 사용자 지정 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.

2. 사용자 지정할 OS 이미지 프로필을 선택하십시오(예, Virtualization).
3. **만들기** 아이콘()을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom ESXi using static IP).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **무인 파일만**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **무인 파일** 탭에서 무인 파일(예: ESXi_staticIP_customUnattend.cfg)을 선택하고 **다음**을 클릭하십시오.
6. **요약** 탭에서 설정을 검토하십시오.
7. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 4. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁:

      - VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
      - 네트워크 설정 대화 상자에서 지정한 네트워크 설정은 런타임 시 #predefined.hostPlatforms.networkSettings.*<setting>*# 매크로를 사용하여 무인 파일에 추가됩니다.

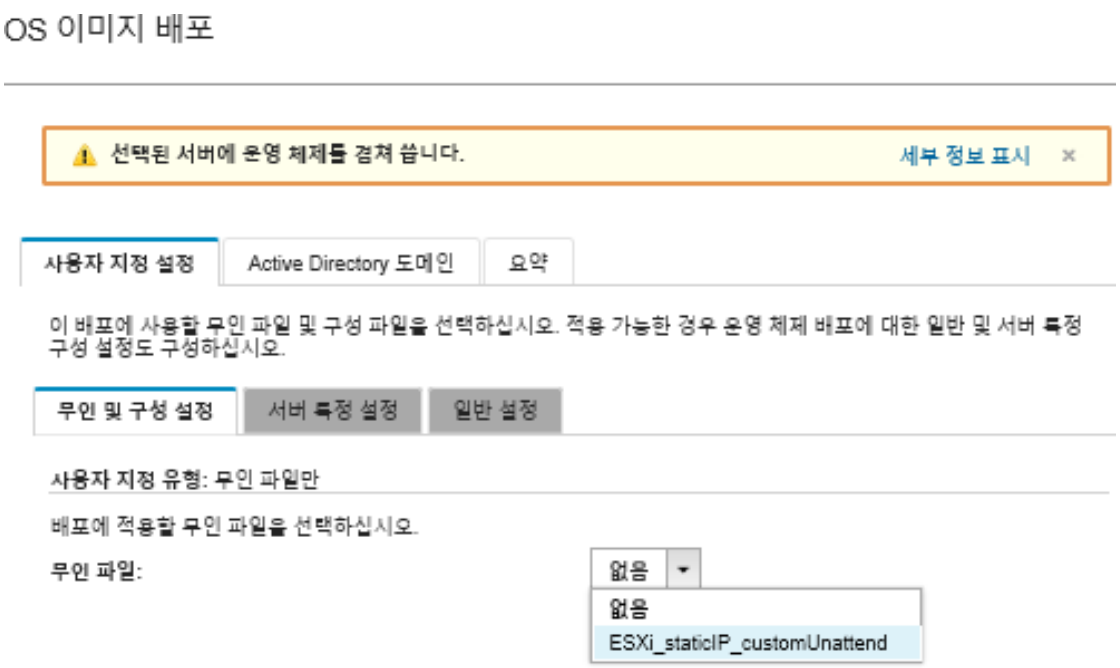
   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 지정 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_Custom ESXi using static IP).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.

   d. (옵션) **라이센스 키** 아이콘()을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.
   e. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.

참고: 무인 파일에 --firstdisk=local이 지정되어 있으므로 **스토리지** 열에 기본 스토리지 위치를 지정할 필요가 없습니다. UI의 설정은 무시됩니다.

3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. **사용자 정의 설정** 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 무인 파일을 선택하십시오(예: ESXi_staticIP_customUnattend.cfg).



5. **요약** 탭에서 설정을 검토하십시오.
6. **배포**를 클릭하여 운영 체제를 배포하십시오.

구성 가능한 로케일 및 두 번째 사용자 자격 증명을 사용하여 Lenovo Customization이 있는 VMware ESXi v6.7 배포

이 시나리오에서는 키보드 로케일에 대해 활성화된 구성 가능한 언어 및 두 번째 ESXi 사용자 자격 증명을 사용하여 Lenovo Customization 운영 체제가 있는 VMware ESXi v6.7을 설치합니다. 또한 이 예에서는 UI에 정의된 기본 네트워크 및 스토리지 설정을 사용합니다. 암호를 선택하기 위해 무인 파일(미리 정의된 사용자 지정 매크로 포함)과 구성 설정 파일이 포함된 사용자 지정 OS 이미지 프로필이 사용됩니다. 이 사용자 지정 프로필은 OS 이미지 배포 페이지에서 선택할 수 있습니다. 그런 다음 암호를 **사용자 지정 설정** 탭에서 지정할 수 있습니다. 사용자 지정 무인 파일의 사용자 지정 매크로는 지정된 값으로 대체되고 ESXi 설치 프로그램은 무인 파일의 해당 값을 사용하여 운영 체제를 구성합니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- ESXi_locale_customConfig.json. 이 사용자 지정 구성 파일은 키보드 로케일 및 두 번째 ESXi 사용자 자격 증명을 요구합니다.
- ESXi_locale_customUnattend.cfg. 이 사용자 지정 무인 파일은 구성 파일에 정의된 미리 정의된 매크로 및 사용자 지정 매크로의 값을 사용합니다.

절차

사용자 지정 OS 이미지 프로필을 사용하여 VMware ESXi v6.7을 배포하려면 다음 단계를 완료하십시오.

단계 1. Lenovo Customization 운영 체제가 있는 VMware vSphere® Hypervisor(ESXi)를 VMware 지원 – 다운로드 웹 페이지 웹 사이트에서 로컬 시스템으로 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.

3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져올 ESXi 이미지를 찾아서 선택하십시오(예, ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오.

단계 2. 사용자 지정 구성 설정 파일을 만들고 해당 파일을 OS 이미지 리포지토리로 가져오십시오.

구성 설정 파일은 OS 배포 프로세스 중에 동적으로 수집되어야 하는 데이터를 설명하는 JSON 파일입니다. 이 시나리오에서는 각 OS 배포에 사용할 키보드 로케일 및 두 번째 ESXi 사용자의 사용자 ID와 암호를 선택하려고 합니다. 구성 설정 파일 만들기에 대한 자세한 정보는 사용자 정의 매크로의 내용을 참조하십시오.

구성 설정 파일을 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 구성 설정 가져오기의 내용을 참조하십시오.

1. **구성 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 ESXi를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 구성 설정 파일을 찾아서 선택하십시오(예: ESXi_locale_customConfig.json).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

   참고: 사용자 지정 구성 설정 파일을 가져올 때 XClarity Administrator는 파일의 각 설정에 대해 사용자 지정 매크로를 생성합니다. 이러한 매크로를 무인 파일에 추가할 수 있습니다. OS 배포 중에 매크로는 실제 값으로 대체됩니다.

단계 3. ESXi 무인(kickstart) 파일을 수정하여 운영 체제 로케일과 키보드 로케일 및 두 번째 ESXi 사용자의 사용자 자격 증명을 지정한 다음 사용자 지정 파일을 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

키보드 로케일을 설정하는 명령을 추가하십시오. 예:

```
# Set the keyboard locale
keyboard ''
```

두 번째 ESXi 사용자를 만드는 명령을 추가하십시오. 다음 예에서 *<user_id>*와 *<password>*는 다음 단계에서 사용자 지정 매크로로 대체됩니다.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 ESXi를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 무인 파일을 찾아서 선택하십시오(예: ESXi_locale_customUnattend.cfg).

6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 4. 사용자 지정 무인 파일을 사용자 지정 구성 설정 파일과 연결하고 미리 지정된 필수 사용자 지정 매크로(설정)를 구성 설정 파일에서 무인 파일에 추가하십시오. 자세한 정보는 무인 파일을 구성 설정 파일과 연결 및 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오.

팁:

- 선택적으로 사용자 지정 무인 파일을 사용자 지정 구성 설정 파일과 연결하고 무인 파일을 가져올 때 매크로를 추가할 수 있습니다.
- XClarity Administrator는 OOB 드라이버 삽입, 상태 보고, 설치 후 스크립트, 사용자 지정 소프트웨어와 같은 몇 가지 기본 편의 매크로를 제공합니다. 그러나 이러한 미리 정의된 매크로를 활용하려면 사용자 지정 무인 파일에 다음 매크로를 지정해야 합니다. 예제 파일에는 이미 필수 매크로가 들어 있습니다. %firstboot 섹션이 포함되어 있으므로 이러한 미리 정의된 매크로의 순서가 중요합니다. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- XClarity Administrator는 UI에 정의된 모든 네트워크 및 스토리지 위치 설정을 주입하는 매크로도 제공합니다. 이러한 매크로는 배포 시 기본 설정만 필요한 경우에 유용합니다. 예제 파일에는 이미 필수 매크로가 들어 있습니다.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

무인 파일에 매크로를 추가하는 방법에 대한 자세한 정보는 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오. 사용 가능한 미리 정의된 매크로에 대한 자세한 정보는 미리 정의된 매크로의 내용을 참조하십시오.

사용자 지정 무인 파일을 사용자 지정 구성 설정 파일과 연결하려면 다음 단계를 완료하십시오.

1. **무인 파일** 탭에서 사용자 정의 무인 파일을 선택하십시오(예: `ESXi_locale_customUnattend.cfg`).
2. **구성 파일 연결** 아이콘( )을 클릭하여 무인 파일 연결 대화 상자를 표시하십시오.
3. 무인 파일과 연결시킬 구성 설정 파일을 선택하십시오(예: `ESXi_locale_customConfig`).
4. **사용 가능한 매크로** 드롭 다운 목록에서 **사용자 지정**을 선택하십시오.
5. 키보드 뒤에 있는 작은 따옴표 사이에 커서를 놓은 다음 keyboard_locale을 클릭하여 키보드 로케일을 지정하는 사용자 지정 매크로를 추가하십시오.

   예를 들어, 다음과 같습니다.

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```

6. 사용자 ID를 추가하려는 각 위치에 커서를 놓은 다음 second_user_id를 클릭하여 두 번째 사용자 ID를 지정하는 사용자 지정 매크로를 추가하십시오. 예제 파일에서 각 *<user_id>* 항목을 사용자 지정 매크로로 대체하십시오.

   예를 들어, 다음과 같습니다.

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

7. 암호를 추가하려는 위치에 커서를 놓은 다음 second_user_password를 클릭하여 두 번째 사용자 암호를 지정하는 사용자 지정 매크로를 추가하십시오. 예제 파일에서 *<password>*를 사용자 지정 매크로로 대체하십시오.

   예를 들어, 다음과 같습니다.

   ```
   #Create second user
   ```

```
/usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
```

8. **연결**을 클릭하여 파일을 함께 바인딩하고 변경사항을 무인 파일에 저장하십시오.

단계 5. 사용자 지정 구성 설정 및 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 지정할 OS 이미지 프로필을 선택하십시오(예, Virtualization).
3. **만들기** 아이콘()을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필의 이름을 입력하십시오(예, Custom ESXi using custom locale and second user credentials).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 정의 유형에 **연결된 무인 및 구성-설정 파일**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **무인 파일** 탭에서 무인 파일(예: ESXi_locale_customUnattend.cfg)을 선택하고 **다음**을 클릭하십시오.

   연결된 구성 설정 파일이 자동으로 선택됩니다.
6. **요약** 탭에서 설정을 검토하십시오.
7. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 6. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁:

      - VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
      - 네트워크 설정 대화 상자에서 지정한 네트워크 설정은 런타임 시 #predefined.hostPlatforms.networkConfig# 매크로를 사용하여 무인 파일에 추가됩니다.

   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 지정 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_Custom ESXi using custom locale and second user credentials).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.

   d. (옵션) **라이센스 키** 아이콘()을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.
   e. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고:

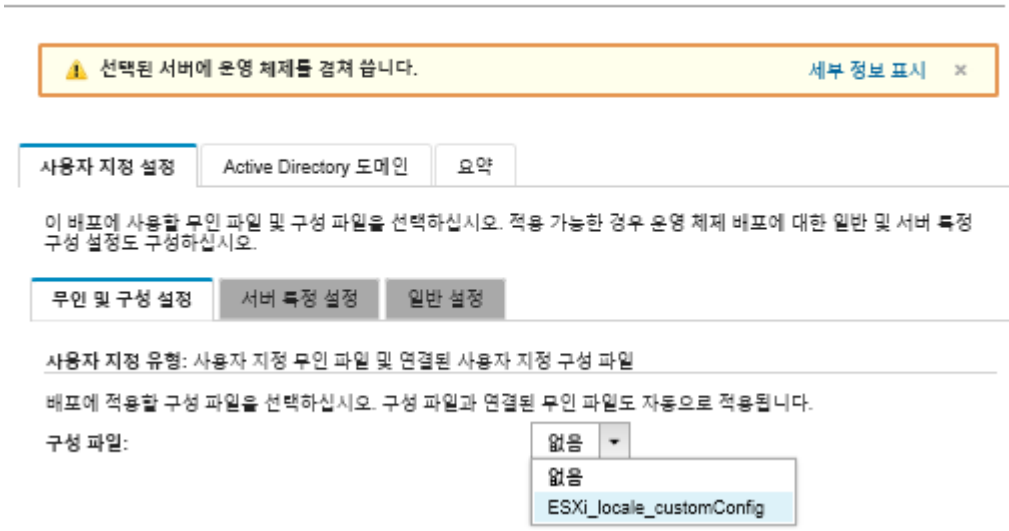
      - 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.

- 스토리지 설정 대화 상자에서 지정한 스토리지 설정은 런타임 시 #predefined.hostPlatforms.storageConfig# 매크로를 사용하여 무인 파일에 추가됩니다.

f. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.

3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘( )을 클릭하십시오.
4. **사용자 정의 설정** 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 구성 설정 파일을 선택하십시오(예: `ESXi_locale_customConfig`).

   참고: 연결된 사용자 지정 무인 파일이 자동으로 선택됩니다.



5. **서버 특정 설정** 하위 탭에서 키보드 로케일 및 두 번째 ESXi 사용자 자격 증명을 선택하십시오.
6. **요약** 탭에서 설정을 검토하십시오.
7. **배포**를 클릭하여 운영 체제를 배포하십시오.

사용자 지정 기능이 있는 Windows 2016 배포

이 시나리오는 Windows 2016 운영 체제와 몇 가지 추가 기능을 설치합니다. 사용자 지정 무인 파일이 포함된 사용자 지정 프로필이 사용됩니다. 그런 다음 사용자 지정 프로필을 OS 이미지 배포 페이지에서 선택할 수 있습니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- Windows_installFeatures_customUnattend.xml. 이 사용자 지정 무인 파일은 WindowsMediaPlayer 및 BitLocker 기능을 설치하고 동적 값에 미리 정의된 매크로를 사용합니다.

절차

사용자 지정 기능과 함께 Windows 2016을 배포하려면 다음 단계를 완료하십시오.

단계 1. 일본어 Windows 2016 운영 체제를 로컬 시스템에 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져오려는 OS 이미지를 찾아서 선택하십시오(예, ja_windows_server_2016_x64_dvd_9720230.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. Windows 2016용 번들 파일을 로컬 시스템에 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 장치 드라이버 가져오기의 내용을 참조하십시오.

번들 파일에는 사용자 지정 OS 이미지 프로필에 추가할 수 있는 최신 장치 드라이버 및 WinPE 부팅 파일이 들어 있습니다. 이 시나리오에서는 사용자 지정 부팅 파일을 사용하므로 번들의 부팅 파일은 사용되지 않습니다.

1. **드라이버 파일** 탭을 클릭하십시오.
2. **다운로드 → Windows 번들 파일**을 클릭하여 Lenovo 지원 웹 사이트로 이동한 후 Windows 2016용 번들 파일을 로컬 시스템에 다운로드하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져오려는 OS 이미지를 찾아서 선택하십시오(예, bundle_win2016_20180126130051.zip).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 3. Windows 무인 파일을 수정하여 추가 기능(예, WindowsMediaPlayer 및 BitLocker)을 설치하고 사용자 정의 파일을 OS 이미지 리포지토리로 가져옵니다.

Windows 무인 파일 "servicing" 섹션에서 설치할 Windows 기능을 추가하십시오. 예를 들면 다음과 같습니다.

```
<servicing>
  <package action="configure">
    <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
              processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
              language=""></assemblyIdentity>
    <selection name="Microsoft-Hyper-V" state="true"></selection>
    <selection name="MultipathIo" state="true"></selection>
    <selection name="FailoverCluster-PowerShell" state="true"></selection>
    <selection name="FailoverCluster-FullServer" state="true"></selection>
    <selection name="FailoverCluster-CmdInterface" state="true"></selection>
    <selection name="FailoverCluster-AutomationServer" state="true"></selection>
    <selection name="FailoverCluster-AdminPak" state="true"></selection>
    <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
    <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
    <selection name="ServerManager-Core-RSAT" state="true"></selection>
    <selection name="WindowsMediaPlayer" state="true"></selection>
    <selection name="BitLocker" state="true"></selection>
  </package>
</servicing>
```

참고:

- 이러한 태그는 샘플 무인 파일에 있습니다.

- 사용자 지정 무인 파일을 사용하는 경우 XClarity Administrator는 미리 정의된 무인 파일을 사용할 때 얻을 수 있는 많은 편의 기능을 제공하지 않습니다. 예를 들어 관리자에 대한 대상 <DiskConfiguration>, <ImageInstall>, <ProductKey> 및 <UserAccounts>, 네트워킹에 대한 <Interfaces> 및 설치 기능에 대한 <package> 목록이 업로드 중인 사용자 지정 무인 파일에 지정되어야 합니다.

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 Windows를 선택하십시오.
5. **찾아보기**를 클릭하여 사용자 정의 무인 파일을 찾아서 선택하십시오(예: Windows_installFeatures_customUnattend.xml).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

XClarity Administrator는 OOB 드라이버 삽입, 상태 보고, 설치 후 스크립트 및 사용자 지정 소프트웨어와 같은 몇 가지 기본 편의 매크로를 제공합니다. 그러나 이러한 미리 정의된 매크로를 활용하려면 사용자 지정 무인 파일에 다음 매크로를 지정해야 합니다.

- #predefined.unattendSettings.preinstallConfig#
- #predefined.unattendSettings.postinstallConfig#

예제 파일에는 추가 기능, 필수 매크로 및 동적 입력에 필요한 기타 매크로를 설치하기 위한 코드가 이미 포함되어 있습니다. 무인 파일에 매크로를 추가하는 방법에 대한 자세한 정보는 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오.

사용 가능한 미리 정의된 매크로에 대한 자세한 정보는 미리 정의된 매크로의 내용을 참조하십시오.

단계 4. 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 프로필을 선택하십시오(예, win2016-x86_64-install-Datacenter_Virtualization).
3. **만들기** 아이콘()을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom Windows with features).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **무인 파일만**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **부팅 옵션** 탭에서 **다음**을 클릭하십시오. 미리 정의된 WinPE 부팅 파일이 기본적으로 선택됩니다.
7. **소프트웨어** 탭에서 **다음**을 클릭하십시오.
8. **무인 파일** 탭에서 사용자 정의 무인 파일(예: Windows_installFeatures_customUnattend.xml)을 선택하고 **다음**을 클릭하십시오.
9. **설치 스크립트** 탭에서 **다음**을 클릭하십시오.
10. **요약** 탭에서 설정을 검토하십시오.
11. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 5. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, 서브넷 마스크, 게이트웨이, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁: VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 정의 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*_*<timestamp>*_기능이 있는 사용자 정의 Windows).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.
   d. (옵션) **라이센스 키** 아이콘( )을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.
   e. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.
   f. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.
3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘( )을 클릭하십시오.
4. **사용자 정의 설정** 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 무인 파일을 선택하십시오(예: `Windows_installFeatures_customUnattend.xml`).
5. (옵션) **Active Directory 도메인** 탭에서 Windows 이미지 배포의 일부로 Active Directory 도메인에 가입하기 위한 정보를 지정하십시오(Windows Active Directory와 통합 참조).
6. **요약** 탭에서 설정을 검토하십시오.
7. **배포**를 클릭하여 운영 체제를 배포하십시오.

사용자 지정 소프트웨어와 함께 Windows 2016 배포

이 시나리오는 사용자 지정 소프트웨어(Java 및 Eclipse IDE)와 함께 Windows 2016 운영 체제를 설치합니다. 사용자 지정 소프트웨어를 설치하고 구성하기 위한 사용자 지정 소프트웨어 및 설치 후 스크립트가 포함된 사용자 지정 프로필이 사용됩니다. 사용자 지정 소프트웨어 패키지는 배포 중에 호스트에 복사되고 사용자 지정 설치 후 스크립트에서 사용할 수 있습니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- jre-8u151-windows-x64-with-configfile.zip. Eclipse용 Java의 설치 파일입니다.
- eclipse-java-oxygen-1a-win32-x86_64.zip Eclipse IDE의 설치 파일입니다.
- Windows_installSoftware_customScript.ps1 이 사후 설치 스크립트는 Eclipse를 시작하는 사용자를 만들고 Eclipse IDE 및 Java를 설치합니다.

참고:

- Windows 설치 스크립트는 다음 형식 중 하나일 수 있습니다. 명령 파일(.cmd), PowerShell(.ps1)

- 소프트웨어 파일 및 설치 스크립트는 배포 중에 지정한 사용자 지정 데이터 및 파일 경로에서 설치됩니다. 기본 사용자 지정 데이터 및 파일 경로는 C:\lxca입니다.

절차

사용자 지정 소프트웨어와 함께 Windows 2016을 배포하려면 다음 단계를 완료하십시오.

단계 1. 일본어 Windows 2016 운영 체제를 로컬 시스템에 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져오려는 OS 이미지를 찾아서 선택하십시오(예, ja_windows_server_2016_x64_dvd_9720230.iso).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. Windows 2016용 번들 파일을 로컬 시스템에 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 장치 드라이버 가져오기의 내용을 참조하십시오.

번들 파일에는 사용자 지정 OS 이미지 프로필에 추가할 수 있는 최신 장치 드라이버 및 WinPE 부팅 파일이 들어 있습니다. 이 시나리오에서는 사용자 지정 부팅 파일을 사용하므로 번들의 부팅 파일은 사용되지 않습니다.

1. **드라이버 파일** 탭을 클릭하십시오.
2. **다운로드 → Windows 번들 파일**을 클릭하여 Lenovo 지원 웹 사이트로 이동한 후 Windows 2016용 번들 파일을 로컬 시스템에 다운로드하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져오려는 OS 이미지를 찾아서 선택하십시오(예, bundle_win2016_20180126130051.zip).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 3. 사용자 지정 소프트웨어를 로컬 시스템에 다운로드하고 파일을 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 사용자 지정 소프트웨어 가져오기의 내용을 참조하십시오.

1. **소프트웨어** 탭을 클릭하십시오.
2. **가져오기** 아이콘()을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 Windows를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 구성 설정 파일을 찾아서 선택하십시오(예: jre-8u151-windows-x64-with-configfile.zip).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.
7. **가져오기** 아이콘()을 다시 클릭하십시오.
8. **로컬 가져오기**를 클릭하십시오.
9. 운영 체제에 Windows를 선택하십시오.

10. **찾아보기**를 클릭하여 가져올 구성 설정 파일을 찾아서 선택하십시오(예: eclipse-java-oxygen-1a-win32-x86_64.zip).
11. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 4. 사용자 지정 설치 후 스크립트를 만들고 해당 파일을 OS 이미지 리포지토리로 가져오십시오.

소프트웨어를 설치하기 위한 명령을 추가하십시오. 예를 들면 다음과 같습니다.

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
    {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
    [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
    /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
    "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
    -DestinationPath $eclipseDir
```

이 명령은 추출된 데이터 및 소프트웨어 파일의 경로에 미리 정의된 매크로를 사용합니다 (predefined.otherSettings.deployDataAndSoftwareLocation).

샘플 파일에 표시된 대로 사용자 지정 메시지를 XClarity Administrator의 작업 로그로 보내는 명령을 추가할 수도 있습니다. 자세한 정보는 설치 스크립트에 사용자 지정 상태 보고 추가의 내용을 참조하십시오.

사용자 지정 설치 스크립트를 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 설치 스크립트 가져오기의 내용을 참조하십시오.

1. **설치 스크립트** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 Windows를 선택하십시오.
5. **찾아보기**를 클릭하여 가져올 무인 파일을 찾아서 선택하십시오(예: Windows_installSoftware_customScript.ps1).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 5. 사용자 지정 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 OS 이미지 프로필을 선택하십시오(예, Datacenter virtualization).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom Windows with software).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **없음**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **부팅 옵션** 탭에서 **다음**을 클릭하십시오. 미리 정의된 WinPE 부팅 파일이 기본적으로 선택됩니다.

7. **소프트웨어** 탭에서 소프트웨어 설치 파일(예: jre-8u151-windows-x64-with-configfile.zip 및 eclipse-java-oxygen-1a-win32-x86_64.zip)을 선택하고 **다음**을 클릭하십시오.
8. **설치 스크립트** 탭에서 설치 스크립트(예: Windows_installSoftware_customScript.ps1)를 선택하고 **다음**을 클릭하십시오.
9. **요약** 탭에서 설정을 검토하십시오.
10. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 6. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝** → **OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경** → **네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁: VLAN 설정은 VLAN 모드가 **전역 설정** → **IP 할당** → **VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 정의 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*|*<timestamp>*_소프트웨어가 있는 사용자 정의 Windows).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.
   d. (옵션) **라이센스 키** 아이콘()을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.
   e. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.
   f. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.
3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. **요약** 탭에서 설정을 검토하십시오.
5. **배포**를 클릭하여 운영 체제를 배포하십시오.

일본어용 Windows 2016 배포

이 시나리오에서는 키보드 및 운영 체제 로케일에 일본어를 사용하는 여러 서버에 Windows 2016 운영 체제를 설치합니다. 사용자 지정 WinPE 부팅 파일 및 무인 파일이 포함된 사용자 지정 프로필이 사용됩니다. 그런 다음 사용자 지정 프로필을 OS 이미지 배포 페이지에서 선택할 수 있습니다.

시작하기 전에

이 시나리오에서는 다음 샘플 파일을 사용합니다.

- WinPE_64_ja.zip. 이 사용자 지정 Windows 부팅(WinPE) 파일은 일본어 로케일을 설치합니다.
- Windows_locale_customUnattend.xml. 이 사용자 지정 무인 파일은 WinPE 파일을 사용하여 일본어를 설치합니다.

참고: 샘플 사용자 지정 무인 파일은 다음을 가정합니다.

- 서버에는 하나의 표시 디스크(디스크 0)만 있으며 시스템 파티션이 아직 없습니다.

- 고정 IPv4 모드가 사용되며 고정 IP를 설정합니다(사용자 지정 무인 모드에서 미리 정의된 매크로로 사용됨).

절차

사용자 지정 OS 이미지 프로필을 사용하여 일본어 Windows 2016을 대상 서버에 배포하려면 다음 단계를 완료하십시오.

단계 1. 일본어 Windows 2016 운영 체제를 로컬 시스템에 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 운영 체제 이미지 가져오기의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 ➡ OS 이미지 관리**를 클릭하여 운영 체제 배포: OS 이미지 관리 페이지를 표시하십시오.
2. **OS 이미지** 탭을 클릭하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져오려는 OS 이미지를 찾아서 선택하십시오(예, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. **가져오기**를 클릭하여 이미지를 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 2. Windows 2016용 번들 파일을 로컬 시스템에 다운로드하고 이미지를 OS 이미지 리포지토리로 가져오십시오. 자세한 정보는 장치 드라이버 가져오기의 내용을 참조하십시오.

번들 파일에는 사용자 지정 OS 이미지 프로필에 추가할 수 있는 최신 장치 드라이버 및 WinPE 부팅 파일이 들어 있습니다. 이 시나리오에서는 사용자 지정 부팅 파일을 사용하므로 번들의 부팅 파일은 사용되지 않습니다.

1. **드라이버 파일** 탭을 클릭하십시오.
2. **다운로드 ➡ Windows 번들 파일**을 클릭하여 Lenovo 지원 웹 사이트로 이동한 후 Windows 2016용 번들 파일을 로컬 시스템에 다운로드하십시오.
3. **가져오기** 아이콘()을 클릭하십시오.
4. **로컬 가져오기**를 클릭하십시오.
5. **찾아보기**를 클릭하여 가져오려는 OS 이미지를 찾아서 선택하십시오(예, `bundle_win2016_20180126130051.zip`).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.
7. 가져오기가 완료될 때까지 기다리십시오. 이 작업은 다소 시간이 걸릴 수 있습니다.

단계 3. WinPE를 설치하는 동안 일본어 로케일을 사용하는 사용자 지정 WinPE 부팅 파일을 만들고 파일을 OS 이미지 리포지토리로 가져오십시오.

XClarity Administrator는 미리 정의된 WinPE(Windows PreInstallation) 부팅 파일을 사용하여 Windows 운영 체제를 설치합니다. 미리 정의된 부팅 파일에서 사용되는 로케일은 영어(en-US)입니다. Windows 설치 중에 사용되는 로케일을 변경하려면 원하는 로케일로 사용자 지정 WinPE 부팅 파일을 만들고 이 사용자 지정 부팅 파일을 사용자 지정 프로필에 할당할 수 있습니다.

WinPE에 로케일을 삽입하는 방법에 대한 정보는 Windows WinPE: 패키지 웹 페이지 추가의 내용을 참조하십시오.

중요: WinPE 부팅 파일에 영어가 아닌 로케일을 지정해도 배포되는 최종 OS의 로케일은 변경되지 않습니다. Windows 설치 및 설정 중에 표시되는 로케일만 변경됩니다.

일본어 로케일이 포함된 사용자 지정 WinPE 부팅 파일을 만들려면 다음 단계를 완료하십시오. 자세한 정보는 부팅(WinPE) 파일 만들기의 내용을 참조하십시오.

1. 관리자 권한이 있는 사용자 ID를 사용하여 Windows ADK 명령 "Deployment and Imaging Tools Environment"를 실행하십시오. 명령 세션이 표시됩니다.
2. 명령 세션에서 `genimage.cmd` 및 `starnet.cmd` 파일이 다운로드된 디렉토리(예, `C:\customwim`)로 변경하십시오.
3. 다음 명령을 실행하여 이전에 탑재된 이미지가 호스트에 없는지 확인하십시오.
   ```
   dism /get-mountedwiminfo
   ```
   탑재된 이미지가 있는 경우 다음 명령을 실행하여 이를 폐기하십시오.
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```
4. 사용자 지정된 Windows 프로필에 기본 제공 장치 드라이버를 추가하는 경우 .inf 형식의 원시 장치 드라이버 파일을 호스트 시스템의 `C:\drivers` 디렉토리에 복사하십시오.
5. .wim 형식의 부팅 파일을 생성하려면 다음 명령을 실행하고 명령이 완료될 때까지 몇 분 동안 기다리십시오
   ```
   genimage.cmd amd64 <ADK_Version>
   ```
   여기서, *<ADK_Version>*은 다음 값 중 하나입니다.
   - 8.1. Windows 2012 R2의 경우
   - 10. Windows 2016의 경우

   이 명령은 `C:\WinPE_64\media\Boot\WinPE_64.wim`이라는 부팅 파일을 만듭니다.
6. 다음 명령을 실행하여 부팅 파일을 탑재하십시오.
   ```
   DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
   ```
7. 기본 제공하지 않는 장치 드라이버를 부팅 파일에 직접 추가하는 경우 다음 단계를 완료하십시오.
   a. 다음 디렉토리를 구조를 만드십시오. 여기서 *<os_release>*은(는) `2012R2` 또는 `2016`입니다.
      ```
      drivers\<os_release>\
      ```
   b. 해당 경로 내의 디렉토리에 .inf 형식의 장치 드라이버를 복사하십시오. 예:
      ```
      drivers\<os_release>\<driver1>\<driver1_files>
      ```
   c. `drivers` 디렉토리를 탑재 디렉토리에 복사하십시오. 예:
      ```
      C:\WinPE_64\mount\drivers
      ```
8. **옵션:** 부팅 파일에 추가 사용자 정의을 수행하십시오(예, 폴더, 파일, 시작 스크립트, 언어 팩 및 앱 추가). 부팅 파일 사용자 지정에 대한 자세한 정보는 WinPE: 마운트 및 사용자 지정 웹 사이트의 내용을 참조하십시오.
9. 예를 들어 일본어 패키지를 추가하십시오.
10. 설치된 패키지를 보고 일본어 전용 패키지가 설치되었는지 확인하십시오.
    ```
    Dism /Add-Package /Image:"C:\WinPE_64\mount"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
    and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
    ```

```
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```

11. 이미지의 국제 설정을 검토하십시오.
    ```
    Dism /Get-Packages /Image:"C:\WinPE_64\mount"
    ```
12. 다음 명령을 실행하여 이미지를 탑재 해제하십시오.
    ```
    DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
    ```
13. C:\WinPE_64\media 디렉토리의 콘텐츠를 WinPE_64_ja.zip 파일로 압축하십시오.
14. .zip 파일을 XClarity Administrator로 가져오십시오(부팅 파일 가져오기 참조).
    a. **부팅 파일** 탭을 클릭하십시오.
    b. **가져오기** 아이콘()을 클릭하십시오.
    c. **로컬 가져오기**를 클릭하십시오.
    d. 운영 체제에 Windows를 선택하십시오.
    e. **찾아보기**를 클릭하여 사용자 정의 부팅 파일을 찾아서 선택하십시오(예: WinPE_64_ja.zip).
    f. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 4. Windows 무인 파일을 수정하여 일본어가 OS 이미지에 포함되도록 지정하고 사용자 지정 파일을 OS 이미지 리포지토리로 가져오십시오.

Windows 설치의 "windowsPE" 단계에서 일본어를 운영 체제 언어 및 로케일로 추가하십시오. 예:

```
<settings pass="windowsPE">
  <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
        publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
        xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SetupUILanguage>
      <UILanguage>ja-JP</UILanguage>
    </SetupUILanguage>
    <SystemLocale>ja-JP</SystemLocale>
    <UILanguage>ja-JP</UILanguage>
    <UserLocale>ja-JP</UserLocale>
    <InputLocale>0411:00000411</InputLocale>
  </component>
</settings>
```

참고: 사용자 지정 무인 파일을 사용하는 경우 XClarity Administrator는 미리 정의된 무인 파일을 사용할 때 얻을 수 있는 많은 편의 기능을 제공하지 않습니다. 예를 들어 관리자에 대한 대상 <DiskConfiguration>, <ImageInstall>, <ProductKey> 및 <UserAccounts>, 네트워킹에 대한 <Interfaces> 및 설치 기능에 대한 <package> 목록이 업로드 중인 사용자 지정 무인 파일에 지정되어야 합니다.

XClarity Administrator는 OOB 드라이버 삽입, 상태 보고, 설치 후 스크립트, 사용자 지정 소프트웨어와 같은 몇 가지 기본 편의 매크로를 제공합니다. 그러나 이러한 미리 정의된 매크로를 활용하려면 사용자 지정 무인 파일에 다음 매크로를 지정해야 합니다.

- #predefined.unattendSettings.preinstallConfig#
- #predefined.unattendSettings.postinstallConfig#

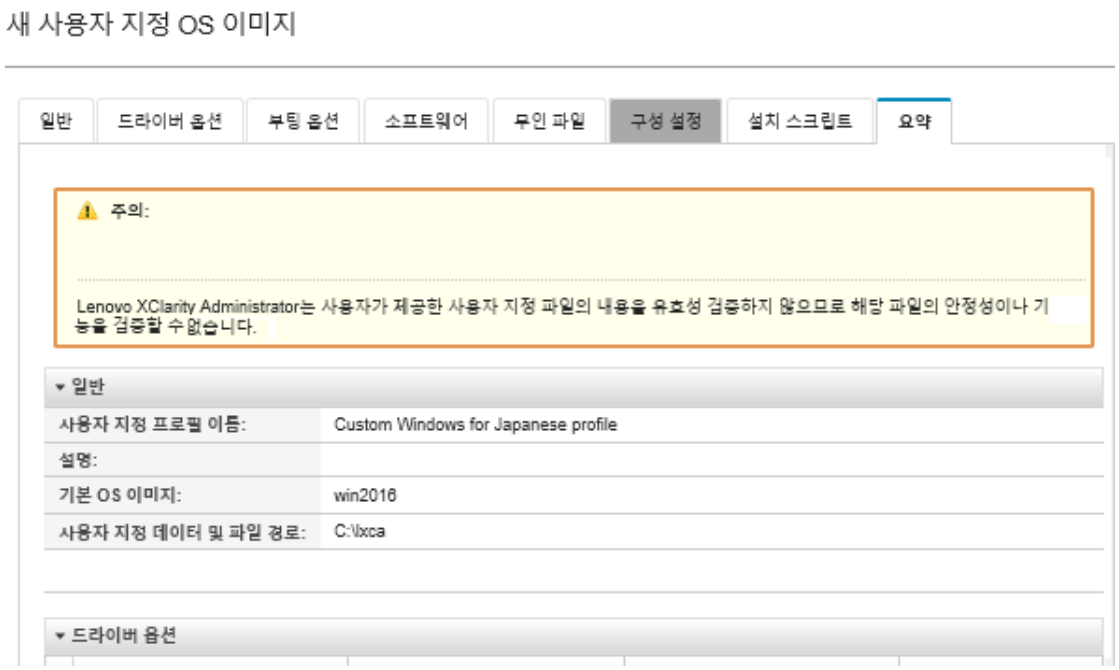
예제 파일에는 이미 필수 매크로가 들어 있습니다. 무인 파일에 매크로를 추가하는 방법에 대한 자세한 정보는 무인 파일에 미리 정의된 사용자 지정 매크로 삽입의 내용을 참조하십시오. 사용 가능한 미리 정의된 매크로에 대한 자세한 정보는 미리 정의된 매크로의 내용을 참조하십시오.

사용자 지정 무인 파일을 가져오려면 다음 단계를 완료하십시오. 자세한 정보는 사용자 지정 무인 파일 가져오기의 내용을 참조하십시오.

1. **무인 파일** 탭을 클릭하십시오.
2. **가져오기** 아이콘( )을 클릭하십시오.
3. **로컬 가져오기**를 클릭하십시오.
4. 운영 체제에 Windows를 선택하십시오.
5. **찾아보기**를 클릭하여 사용자 정의 무인 파일을 찾아서 선택하십시오(예: Windows_locale_customUnattend.xml).
6. **가져오기**를 클릭하여 파일을 OS 이미지 리포지토리로 업로드하십시오.

단계 5. 사용자 지정 부팅(WinPE) 파일 및 무인 파일이 포함된 사용자 지정 OS 이미지 프로필을 만드십시오. 자세한 정보는 사용자 지정 OS 이미지 프로필 만들기의 내용을 참조하십시오.

1. **OS 이미지** 탭을 클릭하십시오.
2. 사용자 정의할 프로필을 선택하십시오(예, win2016-x86_64-install-Datacenter_Virtualization).
3. **만들기** 아이콘( )을 클릭하여 사용자 지정한 프로필 만들기 대화 상자를 표시하십시오.
4. General 탭에서 다음과 같이 하십시오.
   a. 프로필 이름을 입력하십시오(예, Custom Windows for Japanese profile).
   b. **사용자 지정 데이터 및 파일 경로** 필드에 기본값을 사용하십시오.
   c. 사용자 지정 유형에 **무인 파일만**을 선택하십시오.
   d. **다음**을 누르십시오.
5. **드라이버 옵션** 탭에서 **다음**을 클릭하십시오. 기본 제공 장치 드라이버가 기본적으로 포함되어 있습니다.
6. **부팅 파일** 탭에서 사용자 정의 부팅 파일(예, WinPE_64_ja)을 선택하고 **다음**을 클릭하십시오.
7. **소프트웨어** 탭에서 **다음**을 클릭하십시오.
8. **무인 파일** 탭에서 사용자 정의 무인 파일(예: Windows_locale_customUnattend.xml)을 선택하고 **다음**을 클릭하십시오.
9. **설치 스크립트** 탭에서 **다음**을 클릭하십시오.
10. **요약** 탭에서 설정을 검토하십시오.



11. **사용자 지정**을 클릭하여 사용자 지정 OS 이미지 프로필을 만드십시오.

단계 6. 사용자 지정 OS 이미지 프로필을 대상 서버에 배포하십시오. 자세한 정보는 운영 체제 이미지 배포의 내용을 참조하십시오.

1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하여 운영 체제 배포: OS 이미지 배포 페이지를 표시하십시오.
2. 각 대상 서버에 대해 다음을 수행하십시오.
   a. 서버를 선택하십시오.
   b. **선택 항목 변경 → 네트워크 설정**을 클릭하고 서버의 호스트 이름, IP 주소, 서브넷 마스크, 게이트웨이, DNS, MTU 및 VLAN 설정을 지정하십시오.

      팁: VLAN 설정은 VLAN 모드가 **전역 설정 → IP 할당 → VLAN 사용**에 설정된 경우에만 사용할 수 있습니다.
   c. **배포할 이미지** 열의 드롭 다운 목록에서 사용자 정의 OS 이미지 프로필을 선택하십시오(예: *<base_OS>*_*<timestamp>*_일본어 프로필을 위한 사용자 정의 Windows).

      참고: 모든 대상 서버가 동일한 사용자 지정 프로필을 사용하는지 확인하십시오.
   d. (옵션) **라이센스 키** 아이콘()을 클릭하고 운영 체제 설치 후 운영 체제를 정품 인증하는 데 사용할 라이센스 키를 지정하십시오.
   e. **스토리지** 열에서 운영 체제 이미지를 배포할 선호 스토리지 위치를 선택하십시오.

      참고: 운영 체제 배포 성공을 위해 운영 체제 배포에 선택된 스토리지를 제외하고 관리되는 서버에서 모든 스토리지를 분리하십시오.
   f. 선택한 서버에 대한 배포 상태가 **준비** 상태인지 확인하십시오.
3. 운영 체제 배포를 시작하려면 모든 대상 서버를 선택하고 **이미지 배포** 아이콘()을 클릭하십시오.
4. **사용자 정의 설정** 탭에서 **무인 및 구성 설정** 하위 탭을 클릭하고 사용자 정의 무인 파일을 선택하십시오(예: Windows_locale_customUnattend.xml).

5. (옵션) **Active Directory 도메인** 탭에서 Windows 이미지 배포의 일부로 Active Directory 도메인에 가입하기 위한 정보를 지정하십시오(Windows Active Directory와 통합 참조).
6. **요약** 탭에서 설정을 검토하십시오.

7. **배포**를 클릭하여 운영 체제를 배포하십시오.
   Windows 설치 대화 상자가 일본어로 표시됩니다.

설치가 완료되면 Windows 로그인 페이지도 일본어로 표시됩니다.

제 16 장 새 장치 설정을 위한 엔드투엔드 시나리오

이러한 엔드투엔드 시나리오에서는 Lenovo XClarity Administrator를 사용하여 일관되고 쉽게 반복할 수 있는 방식으로 새 장치를 설치하는 방법에 대해 설명합니다.

로컬 하드 드라이브에 ESXi 배포

이러한 절차를 사용하여 VMware ESXi 5.5를 Flex System x240 계산 노드에서 로컬에 설치한 하드 드라이브에 배포하십시오. 기존 서버에서 서버 패턴을 학습하고 해당 서버 패턴에 대해 확장된 UEFI 설정 범주 패턴을 수정하고 VMware ESXi를 설치하는 방법을 보여줍니다.

VMware ESXi 5.5를 시스템의 첫 4GB 내에 구성하려면 메모리 매핑된 I/O(MMIO) 공간이 필요합니다. 구성에 따라 특정 시스템은 4GB 이상의 메모리 사용을 시도하여 오류가 발생할 수 있습니다. 이 문제를 해결하려면 VMware ESXi 5.5를 설치할 각 서버에 대한 Setup Utility를 통해 MM 구성 옵션의 값을 3GB로 늘릴 수 있습니다.

대안은 가상화와 관련된 사전 정의된 확장 UEFI 범주 패턴 중 하나가 포함된 서버 패턴을 배포하는 것인데, 이를 통해 MM 구성 옵션이 설정되고 PCI 64-Bit Resource 할당을 사용 안 함으로 설정합니다.

사전 정의된 가상화 패턴 배포

범주 패턴은 여러 서버 패턴에서 재사용될 수 있는 특정 펌웨어 설정을 정의합니다. 사전 정의된 가상화 패턴을 배포하려면 서버 패턴을 만든 다음 해당 서버 패턴에 사전 정의된 확장된 UEFI 패턴을 적용해야 합니다. 그런 다음 Flex System x240 계산 노드 또는 Flex System x880 X6 계산 노드와 같은 서버 패턴을 동일한 유형의 여러 서버에 적용할 수 있습니다.

이 작업 정보

서버 패턴을 만드는 경우 직접 구성을 완료하거나 이미 설정된 기존 서버에서 패턴 특성을 학습할 수 있습니다. 기존 서버에서 새 패턴을 학습하는 경우 대부분의 패턴 특성이 이미 정의되어 있습니다.

서버 패턴 및 범주 패턴에 대한 자세한 정보는 서버 패턴 작업의 내용을 참조하십시오.

절차

기존 서버에서 새 패턴을 학습하려면 다음 단계를 완료하십시오.

단계 1. XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. **서버 패턴** 탭을 클릭하십시오.

단계 3. **만들기** 아이콘( )을 클릭하십시오. 새 서버 패턴 마법사가 표시됩니다.

새 서버 패턴 마법사

다.

단계 4. **기존 서버에서 새 패턴 만들기**를 클릭하십시오. 처음부터 패턴을 만들 수 있지만 일반적으로 원하는 구성이 있는 기존 서버에서 패턴을 만드는 것이 더 효율적입니다.

기존 서버에서 서버 패턴을 작성하는 경우 XClarity Administrator는 관리되는 서버의 설정(예, 확장된 포트, UEFI 및 베이스보드 관리 컨트롤러 설정)을 가져와서 해당 설정에 대한 범주 패턴을 동적으로 작성합니다. 서버가 새 제품인 경우 XClarity Administrator는 제조 시 설정을 학습합니다. 서버가 사용 중인 경우 XClarity Administrator는 사용자 정의 설정을 학습합니다. 그런 다음 이 패턴을 배포할 서버에 특정하게 설정을 수정할 수 있습니다.

단계 5. 패턴을 만들 때 기본 구성으로 사용할 서버를 선택하십시오.

참고: 선택하는 서버가 서버 패턴을 배포하려는 서버와 모델이 동일해야 합니다. 이 시나리오는 Flex System x240 계산 노드 선택을 기준으로 합니다.

단계 6. 새 패턴의 이름을 입력하고 설명을 제공하십시오.

예를 들어, 다음과 같습니다.

- 이름: x240_ESXi_deployment
- 설명: VMware ESXi 배포에 적절한 확장된 UEFI 설정이 있는 패턴

단계 7. 선택한 서버에서 정보를 로드하려면 **다음**을 클릭하십시오.

단계 8. **로컬 스토리지** 탭에서 **스토리지 구성 지정**을 선택하고 스토리지 유형 중 하나를 선택하십시오. 그런 다음 **다음**을 누르십시오.

로컬 스토리지 설정에 대한 자세한 정보는 로컬 저장 장치 정의의 내용을 참조하십시오.

단계 9. **I/O 어댑터** 탭에서 VMware ESXi를 설치하려는 서버에 있는 어댑터에 대한 정보를 입력하십시오.

기본으로 사용되는 서버에 있었던 모든 어댑터가 표시됩니다.

설치의 모든 Flex System x240 계산 노드에 동일한 어댑터가 있는 경우 이 탭의 어떤 설정도 수정할 필요가 없습니다.

I/O 어댑터 설정에 대한 자세한 정보는 I/O 어댑터 정의의 내용을 참조하십시오.

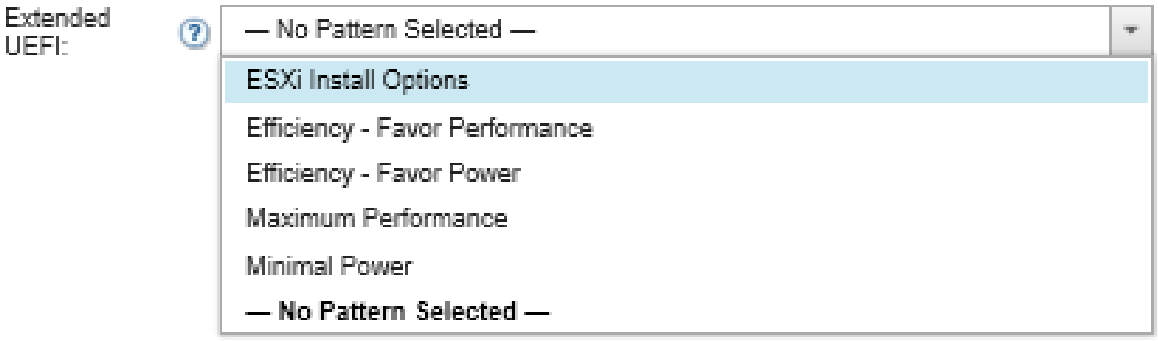
단계 10. **다음**을 클릭하여 계속하십시오.

단계 11. **부팅** 탭에서 legacy-only 부팅 환경 및 SAN 부팅 환경에 대한 설정을 구성하십시오. 이러한 환경 중 하나를 사용하지 않는 한 UEFI Only Boot인 기본 값을 승인하고 **다음**을 클릭하십시오.

부팅 설정에 대한 자세한 정보는 부팅 옵션 정의의 내용을 참조하십시오.

단계 12. **펌웨어 설정** 탭에서 이 패턴이 배포되는 경우 대상 서버에 사용할 관리 컨트롤러 및 UEFI 펌웨어 설정을 지정하십시오(예, x240 **가상화** 선택).

이 탭에서 미리 정의된 확장된 UEFI 패턴 중 하나를 선택할 수 있습니다.



펌웨어 설정에 대한 자세한 정보는 펌웨어 설정 정의의 내용을 참조하십시오.

단계 13. XClarity Administrator에 패턴을 저장하고 VMware ESXi를 설치하려는 서버에 배포하려면 **저장 및 배포**를 클릭하여 패턴을 저장하십시오.

완료한 후에

서버 패턴이 모든 서버에 배포된 후 해당 서버에 운영 체제를 설치할 수 있습니다.

Flex System x240 계산 노드에 VMware ESXi 배포

이 절차를 예제 흐름으로 사용하여 Flex System x240 계산 노드에 ESXi 운영 체제 배포에 대한 프로세스를 설명하십시오.

시작하기 전에

이 절차를 시작하기 전에 Lenovo XClarity Administrator가 Flex System x240 계산 노드가 설치된 섀시를 관리하는지 확인하십시오.

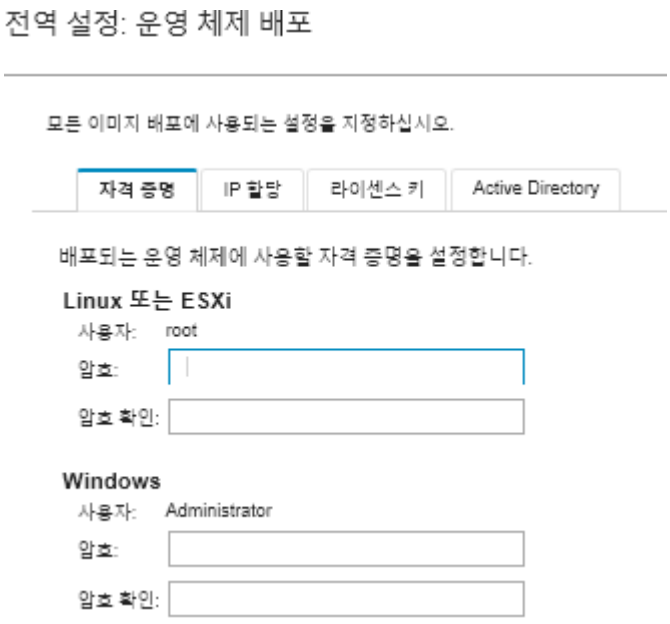
절차

다음 단계를 완료하여 Flex System x240 계산 노드에 ESXi 운영 체제를 배포하십시오.

단계 1. **모든 작업 → OS 이미지 관리**를 클릭하여 사용 가능한 모든 이미지 목록을 표시함으로써 배포할 이미지가 이미 OS 이미지 리포지토리에 로드되었는지 확인하십시오.

단계 2. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하십시오. OS 이미지 배포 페이지가 표시됩니다.

단계 3. **모든 작업 → 전역 설정**을 클릭하여 전역 설정 대화 상자를 표시함으로써 모든 이미지 배포에 대한 기본값으로 사용할 전역 설정을 설정하십시오.



a. **자격 증명** 탭에서 관리자 계정이 운영 체제에 로그인하는 데 사용할 암호를 입력하십시오.

b. **IP 할당** 탭에서 운영 체제의 IP 주소가 서버에 할당되는 방법을 지정하십시오.

DHCP(Dynamic Host Configuration Protocol) **사용**을 선택하여 IP 주소를 할당하는 경우 IP 주소 정보는 네트워크 설정 편집 대화 상자에 표시되지 않습니다(단계 8 9 551페이지단계 참조). **고정 IP 주소(IPv4) 할당**을 선택하는 경우 각 배포에 대한 IP 주소, 서브넷 및 게이트웨이를 지정할 수 있습니다.

c. 원하는 경우 **라이센스 키** 탭에서 다수의 정품 인증 라이센스 키를 입력하십시오.

d. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

단계 4. 운영 체제를 배포할 서버를 선택하여 서버가 운영 체제 배포 준비가 되었는지 확인하십시오. 처음에는 배포 상태가 준비되지 않음으로 표시될 수 있습니다. 서버에 운영 체제를 배포하려면 배포 상태가 준비여야 합니다.

팁: 모든 서버에 동일한 운영 체제를 배포하려는 경우 여러 개의 Flex System 섀시에서 여러 개의 서버를 선택할 수 있습니다. 최대 28개의 서버를 선택할 수 있습니다.

단계 5. **배포할 이미지** 열을 클릭하고 VMware ESXi 5.5를 선택하십시오 (esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization).

단계 6. 동일한 열에서 **라이센스 키** 아이콘()을 클릭하여 이 배포에 대한 라이센스 키를 입력하십시오.

팁: 전역 설정 대화 상자에서 입력한 다수의 정품 인증 키를 사용할 수도 있습니다.

단계 7. 스토리지 열에서 **로컬 디스크**를 선택해야 합니다.

단계 8. 이 배포에 사용할 네트워크 설정을 구성하려면 서버 행의 **네트워크 설정** 열에서 **편집**을 클릭하십시오. 네트워크 설정 편집 페이지가 표시됩니다.

다음 필드를 입력하십시오.

- 호스트 이름
- 운영 체제를 설치할 호스트의 포트 MAC 주소
- 필요한 경우 DNS(Domain Name System) 서버
- 최대 전송 단위(MTU) 속도

참고: 전역 설정 대화 상자(4단계)에서 **고정 IP 주소(IPv4) 할당**을 선택한 경우(단계 3 4 550페이지단계 참조) 다음 정보도 입력하십시오.

- IPv4 주소
- 서브넷 마스크

- 게이트웨이

단계 9. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

OS 이미지 배포 페이지에서 서버에 배포 상태가 준비로 표시되어 있는지 확인하십시오.

단계 10. 모든 **작업 → 이미지 배포**를 클릭하여 운영 체제를 배포하십시오.

단계 11. 이미지를 배포하려면 확인 페이지에서 **배포**를 클릭하십시오.

서버에 현재 운영 체제가 설치되어 있는 경우 이미지를 배포하면 현재 운영 체제를 덮어쓰기한다는 사실에 대한 경고가 표시됩니다.

팁: 설치 진행을 관찰하도록 원격 제어 세션을 설정할 수 있습니다. 서버로 원격 제어 세션을 시작하려면 모든 **작업 → 원격 제어**를 클릭하십시오.

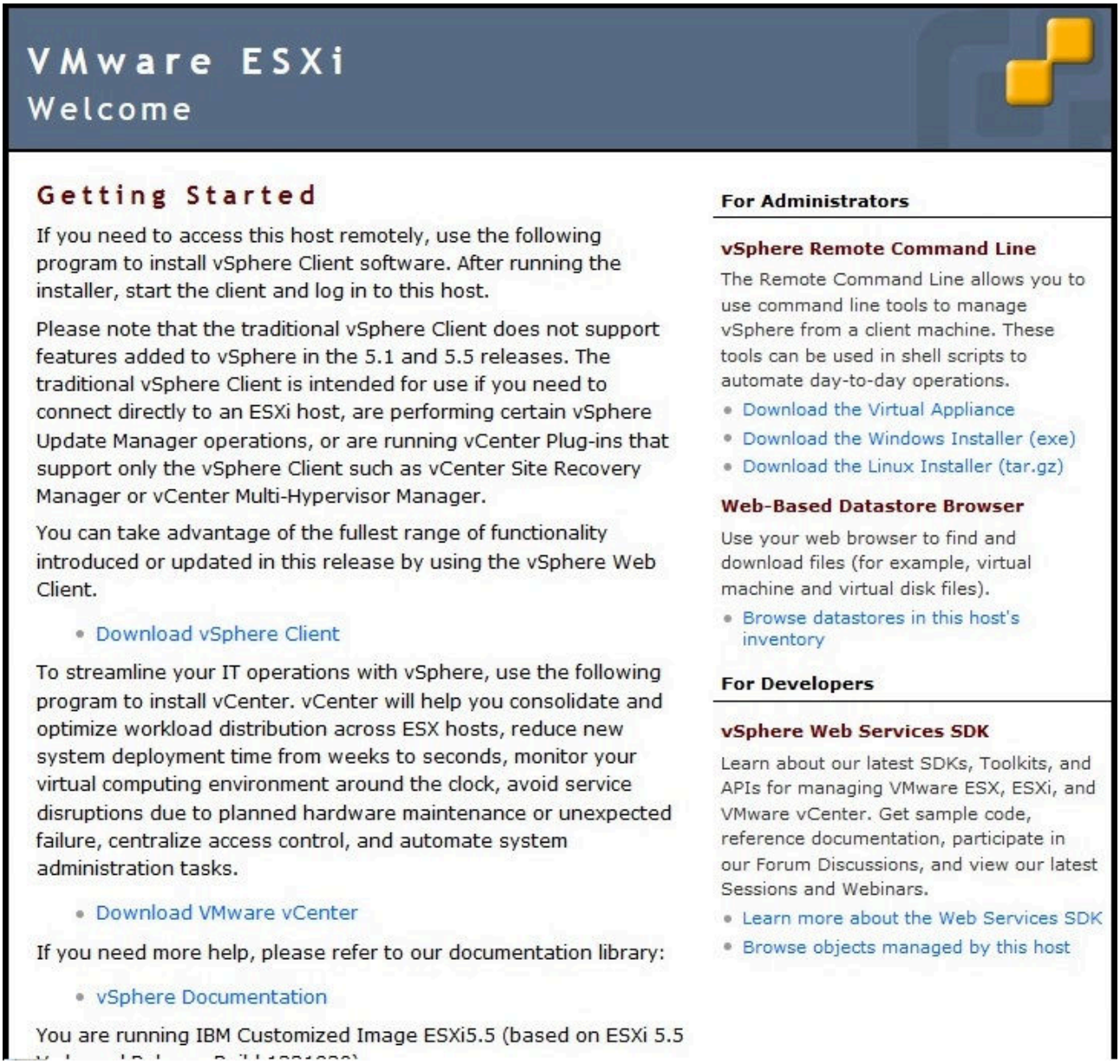
운영 체제를 배포하는 경우 Lenovo XClarity Administrator는 배포를 추적하는 작업을 시작합니다. 배포 작업의 상태를 보려면 Lenovo XClarity Administrator 메뉴 표시줄에서 **작업**을 클릭하십시오. 그런 다음 **실행 중** 탭을 클릭하십시오.

완료된 작업의 비율과 같은 세부 정보를 보려면 실행 중인 작업에 커서를 놓으십시오.

결과

운영 체제 배포가 완료된 후 구성 프로세스를 진행하려면 네트워크 설정 편집 페이지에 지정한 IP 주소에 로그인하십시오.

참고: 이미지에 제공된 라이센스는 60일 무료 평가판입니다. VMware의 모든 라이센싱 요구사항을 충족할 책임이 있습니다.



SAN 스토리지에 ESXi 배포

이러한 절차를 사용하여 서버에 연결한 SAN 볼륨에 VMware ESXi 5.5를 배포하십시오.

SAN에 운영 체제를 배포하는 경우 운영 체제는 서버 패턴을 통해 구성된 첫 번째 SAN 부팅 대상에 배포됩니다. 또한 로컬 하드 드라이브는 SAN에서 부팅되는 서버에서 사용할 수 없습니다. 하드 드라이브가 있는 경우 사용 안 함으로 설정하거나 제거해야 합니다.

SAN 부팅을 지원할 서버 패턴 배포

SAN에서의 시스템 부팅을 지원할 서버 패턴을 만들고 배포하는 경우 SAN 부팅 대상 및 서버의 일부인 어댑터를 식별해야 합니다.

절차

SAN 스토리지에서 운영 체제 배포를 지원하는 서버 패턴을 만들고 배포하려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 패턴**을 클릭하십시오. 구성 패턴: 패턴 페이지가 표시됩니다.

단계 2. 운영 체제를 배포할 스토리지의 WWPN 및 LUN ID를 식별하려면 범주 패턴을 만드십시오.

a. **범주 패턴** 탭을 클릭하십시오.

b. **Fibre Channel 부팅 대상 패턴**을 클릭한 다음 **만들기** 아이콘( )을 클릭하십시오.

c. 스토리지 대상의 WWPN을 입력하십시오.

참고: 동일한 스토리지 볼륨에 여러 개의 LUN ID를 할당하려면 **다중 LUN ID 허용**을 클릭하십시오.

d. 패턴을 만들려면 **만들기**를 클릭하십시오. 대상은 Fibre Channel 부팅 대상 패턴 목록에 표시됩니다.

단계 3. 패턴을 만들려면 **서버 패턴** 탭을 클릭하십시오.

단계 4. **만들기** 아이콘( )을 클릭하십시오. 새 서버 패턴 마법사가 표시됩니다.

새 서버 패턴 마법사

단계 5. **새 패턴 처음부터 새로 만들기**를 클릭하십시오.

단계 6. General 탭에서 다음과 같이 하십시오.

- 폼 팩터에 대한 Flex Compute Node를 선택하십시오.
- 패턴 이름(x240_san_boot) 및 설명을 지정하십시오.
- **다음**을 누르십시오.

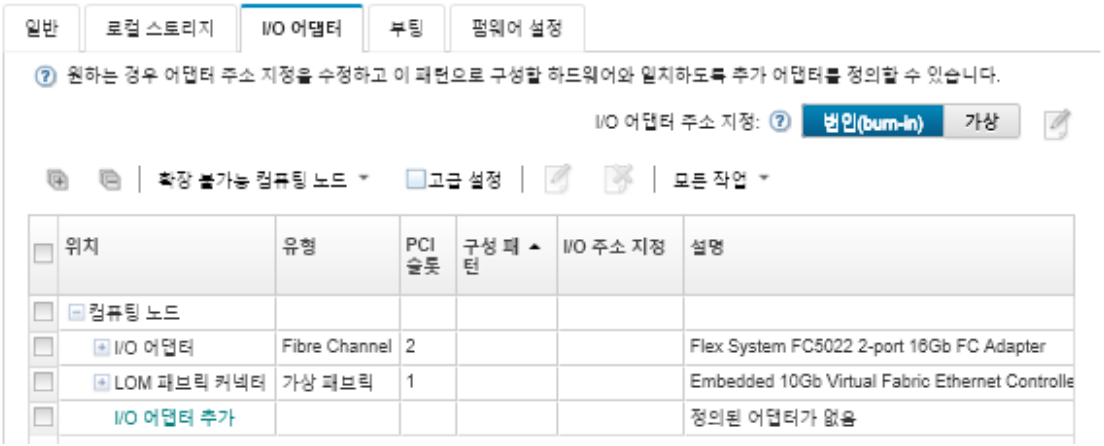
단계 7. 로컬 드라이브 스캔과 관련된 부팅 시간을 개선하기 위해 디스크가 없는 시스템을 사용하는 경우 **로컬 스토리지** 탭에서 로컬 스토리지 어댑터를 사용 안 함으로 설정하는 것을 고려하십시오. 그런 다음, **다음**을 누르십시오.

단계 8. **I/O 어댑터** 탭에서 이더넷 및 Fibre Channel 카드를 추가하십시오. 적절한 PCI 슬롯에 있어야 합니다.

a. 각 카드에 대해 **I/O 어댑터 추가**를 클릭하고 카드가 위치한 PCI 슬롯을 선택하고 카드를 선택하십시오.

참고: 이더넷 카드 및 Fibre Channel 카드를 지정해야 합니다.

서버 패턴 마법사 편집



b. I/O 어댑터 주소 지정은 **가상**으로 설정되어 있어야 합니다. 그런 다음 이더넷(MAC) 가상 주소 지정 및 Fibre Channel(WWN) 가상 주소 지정에 사용할 **편집** 아이콘 을 클릭하십시오.

참고: 가상 주소 지정 편집 페이지에서 가상 주소 지정을 사용하지 않도록 지정하여 이더넷 카드에 대해 번인 MAC 주소를 사용할 수 있습니다. 하지만 Fibre Channel 부팅 대상 패턴을 선택하고 사용하려면 Fibre Channel 어댑터에 대한 가상 주소 지정을 사용해야 합니다.

c. **다음**을 누르십시오.

단계 9. **부팅** 탭에서 이전에 만든 SAN 부팅 대상 패턴을 추가하십시오.

a. SAN **부팅** 탭에서 지정한 부팅 대상 패턴을 선택하십시오.

b. **다음**을 누르십시오.

단계 10. **펌웨어 설정** 탭에서 이 서버 패턴에 포함될 추가 범주 패턴을 정의하십시오. 다음 범주 패턴을 정의할 수 있습니다.

- **시스템 정보**(시스템 정보 설정 정의 참조)
- **관리 인터페이스**(관리 인터페이스 설정 정의 참조)
- **장치 및 I/O 포트**(장치 및 I/O 포트 설정 정의 참조)
- **확장된** BMC. 이전에 학습한 베이스보드 관리 컨트롤러 설정 중에서 선택할 수 있습니다(확장된 관리 컨트롤러 설정 정의 참조).
- **확장된** UEFI. 사전 정의된 설정 또는 이전에 학습한 UEFI 설정 중에서 선택할 수 있습니다(확장 UEFI 설정 정의 참조).

단계 11. Lenovo XClarity Administrator에 패턴을 저장하고 VMware ESXi를 설치하려는 서버에 배포하려면 **저장 및 배포**를 클릭하여 패턴을 저장하십시오.

완료한 후에

서버 패턴이 모든 서버에 배포된 후 다음 단계를 고려하십시오.

1. 서버가 정의된 스토리지 LUN에 접속할 수 있도록 만든 가상화된 WWPN 주소를 스토리지 영역에 추가하십시오.

   팁: 서버 프로필을 배포한 후 서버 프로필을 확인하여 가상화된 WWPN 주소를 찾을 수 있습니다.

   a. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → 서버 프로필**을 클릭하십시오.

   b. 배포된 서버 프로필을 클릭하십시오(예, x240_SAN_boot). **가상 주소 매핑** 탭에는 주소 목록이 표시됩니다.

2. 서버에 운영 체제를 배포하십시오.

SAN 스토리지에 VMware ESXi 배포

이 절차를 예제 흐름으로 사용하여 서버에 연결된 SAN 스토리지에 ESXi 운영 체제 배포에 대한 프로세스를 설명하십시오.

시작하기 전에

이 절차를 시작하기 전에 Lenovo XClarity Administrator가 Flex System x220 계산 노드가 설치된 섀시를 관리하는지 확인하십시오.

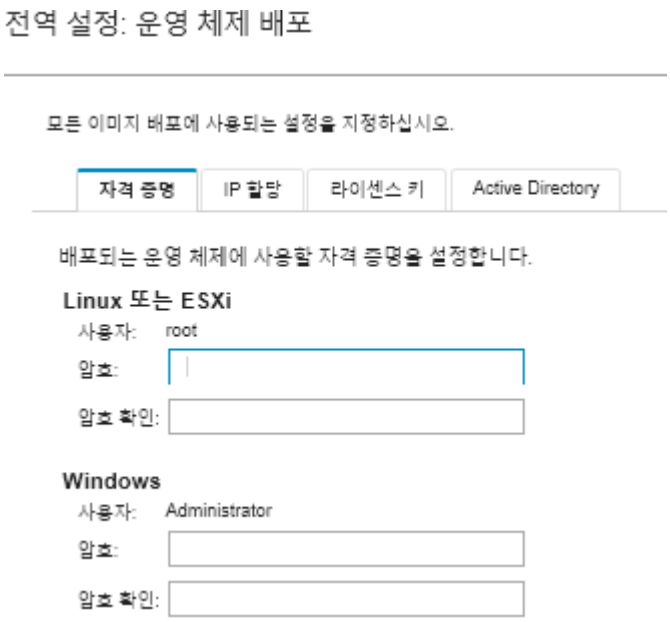
절차

다음 단계를 완료하여 Flex System x222 계산 노드에 ESXi 운영 체제를 배포하십시오.

단계 1. **모든 작업 → OS 이미지 관리**를 클릭하여 배포할 이미지가 이미 OS 이미지 리포지토리에 로드되었는지 확인하십시오.

단계 2. Lenovo XClarity Administrator 메뉴 표시줄에서 **프로비저닝 → OS 이미지 배포**를 클릭하십시오.

단계 3. **모든 작업 → 전역 설정**을 클릭하여 전역 설정: 운영 체제 배포 대화 상자를 표시함으로써 모든 이미지 배포에 대한 기본값으로 사용할 전역 설정을 설정하십시오.



a. **자격 증명** 탭에서 관리자 계정이 운영 체제에 로그인하는 데 사용할 암호를 입력하십시오.

b. IP **할당** 탭에서 운영 체제의 IP 주소가 서버에 할당되는 방법을 지정하십시오.

DHCP(Dynamic Host Configuration Protocol) **사용**을 선택하여 IP 주소를 할당하는 경우 IP 주소 정보는 네트워크 설정 편집 대화 상자에 표시되지 않습니다(단계 8 9 558페이지단계 참조). **고정 IP 주소(IPv4) 할당**을 선택하는 경우 각 배포에 대한 IP 주소, 서브넷 및 게이트웨이를 지정할 수 있습니다.

c. 원하는 경우 **라이센스 키** 탭에서 다수의 정품 인증 라이센스 키를 입력하십시오.

d. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

단계 4. 운영 체제를 배포할 서버를 선택하여 서버가 운영 체제 배포 준비가 되었는지 확인하십시오. 처음에는 배포 상태가 준비되지 않음으로 표시될 수 있습니다. 서버에 운영 체제를 배포하려면 배포 상태가 준비여야 합니다.

팁: 모든 서버에 동일한 운영 체제를 배포하려는 경우 여러 개의 Flex System 섀시에서 여러 개의 서버를 선택할 수 있습니다. 최대 28개의 서버를 선택할 수 있습니다.

단계 5. **배포할 이미지** 열을 클릭하고 VMware ESXi 5.5를 선택하십시오 (esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization).

단계 6. 동일한 열에서 **라이센스 키** 아이콘()을 클릭하여 이 배포에 대한 라이센스 키를 입력하십시오.

팁: 전역 설정: 운영 체제 배포 대화 상자에서 입력한 다수의 정품 인증 키를 사용할 수도 있습니다.

단계 7. **스토리지** 열에서 운영 체제를 배포할 SAN 스토리지를 선택하십시오.

스토리지는
LUN: *<LUN VALUE>* WWPN: *<WWPN_VALUE>*
로 나열됩니다.

단계 8. 이 배포에 사용할 네트워크 설정을 구성하려면 서버 행의 **네트워크 설정** 열에서 **편집**을 클릭하십시오. 네트워크 설정 편집 페이지가 표시됩니다.

다음 필드를 입력하십시오.
- 호스트 이름
- 운영 체제를 설치할 호스트의 포트 MAC 주소
- 필요한 경우 DNS(Domain Name System) 서버
- 최대 전송 단위(MTU) 속도

참고: 전역 설정: 운영 체제 배포 대화 상자(단계 3 4 557페이지단계)에서 **고정 IP 주소(IPv4) 할당**을 선택한 경우 다음 정보도 입력하십시오.
- IPv4 주소

- 서브넷 마스크
- 게이트웨이

단계 9. 대화 상자를 닫으려면 **확인**을 클릭하십시오.

OS 이미지 배포 페이지에서 서버의 배포 상태가 준비로 표시됩니다.

단계 10. **모든 작업 → 이미지 배포**를 클릭하여 운영 체제를 배포하십시오.

단계 11. 이미지를 배포하려면 확인 페이지에서 **배포**를 클릭하십시오.

서버에 현재 운영 체제가 설치되어 있는 경우 이미지를 배포하면 현재 운영 체제를 덮어쓰기한다는 사실에 대한 경고가 표시됩니다.

팁: 설치 진행을 관찰하도록 원격 제어 세션을 설정할 수 있습니다. 서버로 원격 제어 세션을 시작하려면 **모든 작업 → 원격 제어**를 클릭하십시오.

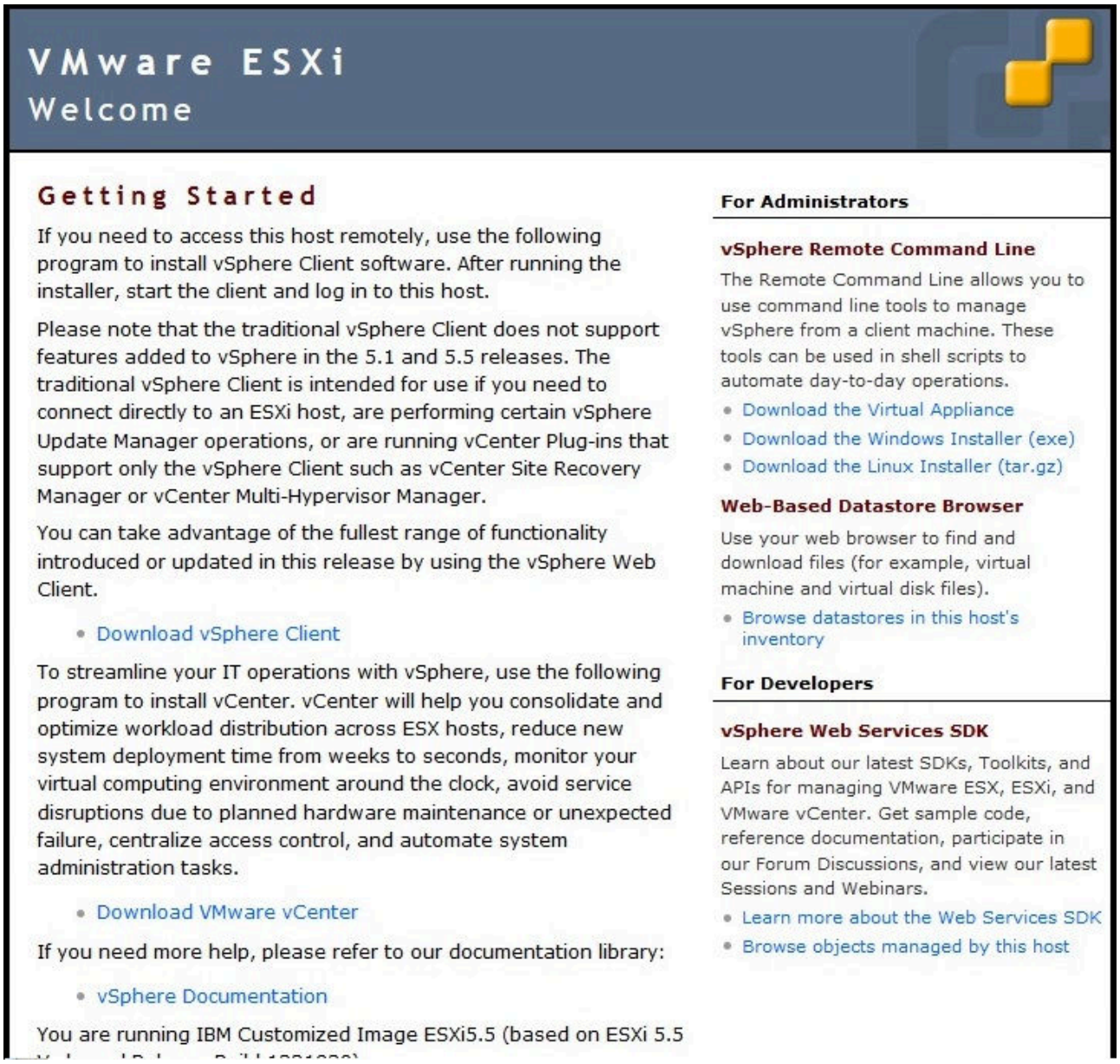
운영 체제를 배포하는 경우 Lenovo XClarity Administrator는 배포를 추적하는 작업을 시작합니다. 배포 작업의 상태를 보려면 Lenovo XClarity Administrator 메뉴 표시줄에서 **작업**을 클릭하십시오. 그런 다음 **실행 중** 탭을 클릭하십시오.

완료된 작업의 비율과 같은 세부 정보를 보려면 실행 중인 작업에 커서를 놓으십시오.

결과

운영 체제 배포가 완료된 후 구성 프로세스를 진행하려면 네트워크 설정 편집 페이지에 지정한 IP 주소에 로그인하십시오.

참고: 이미지에 제공된 라이센스는 60일 무료 평가판입니다. VMware의 모든 라이센싱 요구사항을 충족할 책임이 있습니다.



주의사항

Lenovo가 모든 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하는 것은 아닙니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 Lenovo 담당자에게 문의하십시오.

이 책에서 Lenovo 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 Lenovo 제품, 프로그램 또는 서비스만 사용할 수 있다는 것은 아닙니다. Lenovo의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 기타 제품, 프로그램 또는 서비스의 운영에 대한 평가와 검증은 사용자의 책임입니다.

Lenovo는 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공하는 것은 오퍼링이 아니며 이 책을 제공한다고 해서 특허 또는 특허 응용 프로그램에 대한 라이센스까지 부여하는 것은 아닙니다. 의문사항은 다음으로 문의하십시오.

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

Lenovo는 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현재 상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. Lenovo는 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 책에서 설명한 제품은 오작동으로 인해 인체 상해 또는 사망이 발생할 수 있는 이식 또는 기타 생명 유지 응용 프로그램에서 사용하도록 고안되지 않았습니다. 이 책에 포함된 정보는 Lenovo 제품 사양 또는 보증에 영향을 미치거나 그 내용을 변경하지 않습니다. 이 책의 어떠한 내용도 Lenovo 또는 타사의 지적 재산권 하에서 묵시적 또는 명시적 라이센스 또는 면책 사유가 될 수 없습니다. 이 책에 포함된 모든 정보는 특정 환경에서 얻은 것이며 설명 목적으로만 제공됩니다. 운영 환경이 다르면 결과가 다를 수 있습니다.

Lenovo는 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

이 책에서 언급되는 Lenovo 이외 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 Lenovo 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

본 책에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 운영 환경이 다르면 결과가 현저히 다를 수 있습니다. 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

상표

LENOVO, SYSTEM, NEXTSCALE, SYSTEM X, THINKSERVER, THINKSYSTEM 및 XCLARITY는 Lenovo의 상표입니다.

Intel은 미국 또는 기타 국가에서 사용되는 Intel Corporation의 상표입니다.