Lenovo XClarity Management Hub 설치 및 사용 설명서

버전 2.1

주의

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

제2판 (2024년 7칠월)

목차

제 1 장 Lenovo XClarity Management Hub 계획

Lenovo XClarity Management Hub의 설치를 계획하는 데 유용한 다음 고려사항과 전제조건을 검토하십시오.

지원되는 하드웨어 및 소프트웨어

사용자 환경이 Lenovo XClarity Management Hub에 대한 하드웨어 및 소프트웨어 요구사항을 충족하는지 확인합니다.

호스트 시스템

하이퍼바이저 요구사항

Lenovo XClarity Management Hub 설치에 지원되는 하이퍼바이저는 다음과 같습니다.
- VMware ESXi 7.0, U1, U2 및 U3
- VMware ESXi 6.7, U1, U2[1] 및 U3

VMware ESXi의 경우 가상 어플라이언스는 OVF 템플릿입니다.

중요:

- VMware ESXi 6.7 U2의 경우 ISO 이미지 VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso 이상을 사용해야 합니다.

하드웨어 요구사항

다음 테이블에는 관리되는 에지 클라이언트 장치 수에 따라 XClarity Management Hub에 대한 *최소 권장* 구성이 나열되어 있습니다. 환경에 따라 최적의 성능을 누리려면 추가 리소스가 필요할 수 있습니다.

관리되는 에지 클라이언트 장치 수	프로세서	메모리	스토리지
0~100개의 장치	6	32GB	340GB
100~200개의 장치	8	34GB	340GB
200~400개의 장치	10	36GB	340GB
400~600개의 장치	12	40GB	340GB
600~800개의 장치	14	44GB	340GB
800~1,000개의 장치	16	48GB	340GB

1. 이는 XClarity Management Hub 가상 어플라이언스가 SSD 데이터 저장소로 사용하기 위한 최소 스토리지 용량입니다.

소프트웨어 요구사항

XClarity Management Hub에는 다음 소프트웨어가 필요합니다.

- **NTP 서버**. 리소스 관리자 및 관리되는 장치에서 수신되는 모든 이벤트 및 경고에 대한 타임스탬프가 XClarity Management Hub와 동기화되도록 하려면 NTP(Network Time Protocol) 서버가 필요합니다. NTP 서버는 관리 네트워크(일반적으로 Eth0 인터페이스)로 액세스 가능해야 합니다.

관리 가능 장치

XClarity Management Hub은(는) 최대 10,000 ThinkEdge 클라이언트 장치를 베이스보드 관리 컨트롤러 없이 관리, 모니터링 및 프로비저닝할 수 있습니다.

지원되는 ThinkEdge 클라이언트 장치 및 옵션(예: I/O, DIMM 및 스토리지 어댑터)의 전체 목록, 필수 최소 펌웨어 수준, 제한 및 고려사항은 XClarity Management Hub 서버에서 확인 가능합니다.

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

웹 브라우저

XClarity Management Hub 웹 인터페이스는 다음과 같은 웹 브라우저에서 작동합니다.
- Chrome 80.0 이상
- Firefox ESR 68.6.0 이상
- Microsoft Edge 40.0 이상
- Safari 13.0.4 이상(MacOS 10.13 이상에서 실행)

방화벽 및 프록시 서버

콜 홈 및 보증 상태를 포함한 일부 서비스 및 지원 기능을 사용하려면 인터넷에 액세스해야 합니다. 네트워크에 방화벽이 있는 경우 XClarity Orchestrator 및 리소스 관리자가 이러한 작업을 수행하도록 방화벽을 구성하십시오. Lenovo XClarity Orchestrator 및 리소스 관리자가 인터넷에 직접 액세스할 수 없는 경우 프록시 서버를 사용하도록 구성하십시오.

방화벽

해당하는 경우 XClarity Orchestrator 및 해당 리소스 관리자(Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub, Lenovo XClarity Administrator)의 방화벽에서 다음 DNS 이름과 포트가 공개되어 있는지 확인합니다. 각 DNS는 동적 IP 주소를 사용하여 지리적으로 분산된 시스템을 나타냅니다.

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

DNS 이름	포트	프로토콜
업데이트 다운로드(관리 서버 업데이트, 펌웨어 업데이트, UpdateXpress System Packs(OS 장치 드라이버) 및 리포지토리 팩)		
download.lenovo.com	443	https
support.lenovo.com	443 및 80	https 및 http
Lenovo 지원에 서비스 데이터 보내기(콜 홈) – XClarity Orchestrator 전용		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com(XClarity Orchestrator v2.0 이상) rsgw-eservice.motorola.com(XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx(XClarity Orchestrator v1.5 이하)	443	https
Lenovo에 정기 데이터 보내기 – XClarity Orchestrator 전용		

DNS 이름	포트	프로토콜
esupportwebapi.lenovo.com(XClarity Orchestrator v2.0 이상) rsgw-eservice.motorola.com(XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx(XClarity Orchestrator v1.5 이하)	443	https
보증 정보 검색		
supportapi.lenovo.com	443	https 및 http

프록시 서버

XClarity Orchestrator 또는 리소스 관리자가 인터넷에 직접 액세스할 수 없는 경우 HTTP 프록시 서버를 사용하도록 구성되어 있는지 확인하십시오(네트워크 구성XClarity Orchestrator 온라인 설명서 참조).
- 프록시 서버가 기본 인증을 사용하도록 설정되었는지 확인하십시오.
- 프록시 서버가 비종결 프록시(non-terminating proxy)로 설정되었는지 확인하십시오.
- 프록시 서버가 전달 프록시로 설정되었는지 확인하십시오.
- 로드 밸런서가 한 프록시 서버와의 세션을 유지하고 세션 간을 전환하지 않도록 구성되었는지 확인하십시오.

주의: XClarity Management Hub에서 인터넷에 직접 액세스할 수 있어야 합니다. HTTP 프록시 서버는 현재 지원되지 않습니다.

포트 사용 가능성

Lenovo XClarity Orchestrator 및 리소스 관리자는 통신을 용이하게 하기 위해 특정 포트를 열어야 합니다. 필수 포트가 차단되었거나 다른 프로세스에서 사용되는 경우 일부 기능이 올바르게 수행되지 않을 수 있습니다.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub, Lenovo XClarity Administrator은(는) 포트 443에서 TCP를 통해 안전하게 통신하는 RESTful 응용 프로그램입니다.

XClarity Orchestrator

XClarity Orchestrator는 대기하다가 다음 테이블에 나열된 포트를 통해 응답합니다. XClarity Orchestrator 및 모든 관리되는 리소스가 방화벽 안에 있고 방화벽 *외부*에 있는 브라우저에서 해당 리소스에 액세스하려는 경우 필수 포트가 열려 있어야 합니다.

참고: LDAP, SMTP 또는 syslog와 같은 외부 서비스로의 아웃바운드 연결을 위해 XClarity Orchestrator을(를) 선택적으로 구성할 수 있습니다. 이러한 연결에는 일반적으로 사용자가 구성할 수 있으며 이 목록에 포함되지 않은 추가 포트가 필요할 수 있습니다. 이러한 연결은 외부 서버 이름을 해석하기 위해 TCP 또는 UDP 포트 53에서 도메인 이름 서비스(DNS) 서버에 액세스해야 할 수도 있습니다.

서비스	아웃바운드(외부 시스템에서 열리는 포트)	인바운드(XClarity Orchestrator 어플라이언스에서 열리는 포트)
XClarity Orchestrator 어플라이언스	• DNS – 포트 53의 TCP/UDP	• HTTPS – 포트 443의 TCP
외부 인증 서버	• LDAP– 포트 389[1]의 TCP	해당사항 없음

서비스	아웃바운드(외부 시스템에서 열리는 포트)	인바운드(XClarity Orchestrator 어플라이언스에서 열리는 포트)
이벤트 전달 서비스	• 이메일 서버(SMTP) – 포트 25[1]의 UDP • REST 웹 서비스(HTTP) – 포트 80[1]의 UPD • Splunk – 포트 8088[11], 8089[1]의 UDP • Syslog – 포트 514[1]의 UDP	해당사항 없음
Lenovo Services(콜 홈 포함)	• HTTPS(콜 홈) – 포트 443의 TCP	해당사항 없음

1. 기본 포트입니다. XClarity Orchestrator 사용자 인터페이스에서 이 포트를 구성할 수 있습니다.

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0에서 통신을 용이하게 하려면 특정 포트가 열려 있어야 합니다. 필요한 포트가 차단되었거나 다른 프로세스에서 사용하는 경우 일부 관리 허브 기능이 올바르게 수행되지 않을 수 있습니다.

장치가 방화벽 안에 있고 해당 방화벽 외부에 있는 관리 허브에서 그러한 장치를 관리하려는 경우 관리 허브 및 각 장치의 베이스보드 관리 컨트롤러 간의 통신이 열려 있는 상태에서 모든 포트가 통신에 연결되어야 합니다.

서비스 또는 구성요소	아웃바운드(외부 시스템으로 열리는 포트)	인바운드(대상 장치로 열리는 포트)
XClarity Management Hub 2.0	• DNS – 포트 53의 UDP • NTP – 포트 123의 UDP • HTTPS – 포트 443의 TCP • SSDP – 포트 1900의 UDP • DHCP – 포트 67의 UDP	• HTTPS – 포트 443의 TCP • SSDP 리플로이 – 포트 32768-65535의 UDP
ThinkSystem 및 ThinkAgile 서버	• HTTPS – 포트 443의 TCP • SSDP 검색 – 포트 1900의 UDP	• HTTPS – 포트 443의 TCP

XClarity Management Hub

XClarity Management Hub는 대기하다가 다음 테이블에 나열된 포트를 통해 응답합니다.

서비스 또는 구성요소	아웃바운드(외부 시스템에서 열리는 포트)	인바운드(XClarity Management Hub 어플라이언스에서 열리는 포트)
XClarity Management Hub 어플라이언스[1]	• DNS – 포트 53[2]의 TCP/UDP	• HTTPS – 포트 443의 TCP • MQTT – 포트 8883의 TCP
ThinkEdge 클라이언트 장치[3]	해당사항 없음	• MQTT – 포트 8883의 TCP

1. XClarity Management Hub을(를) 사용하여 XClarity Orchestrator을(를) 통해 장치를 관리하는 경우 통신을 용이하게 하려면 특정 포트가 열려 있어야 합니다. 필요한 포트가 차단되었거나 다른 프로세스에서 사용하는 경우 일부 XClarity Orchestrator 기능이 올바르게 수행되지 않을 수 있습니다.
2. 외부 서비스로의 아웃바운드 연결을 위해 XClarity Management Hub을(를) 선택적으로 구성할 수 있습니다. 이러한 연결은 외부 서버 이름을 해석하기 위해 TCP 또는 UDP 포트 53에서 도메인 이름 서비스(DNS) 서버에 액세스해야 할 수도 있습니다.
3. 관리 가능한 장치가 방화벽 안에 있고 해당 방화벽 외부에 있는 XClarity Management Hub에서 그러한 장치를 관리하려는 경우 XClarity Management Hub 및 에지 장치 간의 통신이 열려 있는 상태에서 모든 포트가 통신에 연결되어야 합니다.

XClarity Administrator

Lenovo XClarity Administrator을(를) 사용하여 Lenovo XClarity Orchestrator을(를) 통해 장치를 관리하는 경우 통신을 용이하게 하려면 특정 포트가 열려 있어야 합니다. 필요한 포트가 차단되었거나 다른 프로세스에서 사용하는 경우 일부 XClarity Orchestrator 기능이 올바르게 수행되지 않을 수 있습니다.

XClarity Administrator에 열려 있어야 하는 포트에 대한 정보는 포트 사용 가능성 XClarity Administrator 온라인 설명서의 내용을 참조하십시오.

네트워크 고려사항

단일 네트워크 인터페이스(eth0) 또는 두 개의 개별 네트워크 인터페이스(eth0 및 eth1)를 통신에 사용하도록 Lenovo XClarity Management Hub을(를) 구성할 수 있습니다.

Lenovo XClarity Management Hub은(는) 다음 네트워크를 통해 통신합니다.

- *관리 네트워크*는 Lenovo XClarity Management Hub 및 관리되는 장치 간의 통신에 사용됩니다.
- *데이터 네트워크*는 서버에 설치된 운영 체제와 회사 인트라넷, 인터넷 또는 두 가지 모두 간의 통신에 사용됩니다.

단일 인터페이스(eth0)

단일 네트워크 인터페이스(eth0)를 사용하면 관리 통신, 데이터 통신 및 운영 체제 배포가 동일한 네트워크를 통해 이루어집니다.

Lenovo XClarity Management Hub을(를) 설정하는 경우 다음 고려사항을 사용하여 eth0 네트워크 인터페이스를 정의하십시오.

- 장치 검색 및 관리(펌웨어 업데이트 포함)를 지원하도록 네트워크 인터페이스를 구성해야 합니다. Lenovo XClarity Management Hub이(가) 관리 네트워크에서 관리할 모든 장치와 통신할 수 있어야 합니다.Lenovo XClarity Management Hub이(가) 네트워크에서 관리할 모든 장치와 통신할 수 있어야 합니다.
- OS 이미지를 배포하려면 eth0 인터페이스에 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결이 있어야 합니다.
- **중요:** 공유 데이터 및 관리 네트워크를 구현하면 네트워크 구성에 따라(예: 서버의 트래픽 우선순위가 높거나 관리 컨트롤러의 트래픽 우선순위가 낮은 경우) 패킷이 중지되거나 관리 네트워크 연결 문제와 같은 트래픽 중단이 발생할 수 있습니다. 관리 네트워크는 추가 TCP에 UDP 트래픽을 사용합니다. 네트워크 트래픽이 높은 경우 UDP 트래픽의 우선 순위가 더 낮을 수 있습니다.

두 개의 개별 인터페이스(eth0 및 eth1)

두 개의 네트워크 인터페이스(eth0 및 eth1)를 사용하는 경우 물리적으로 분리된 네트워크 또는 가상으로 분리된 네트워크로 네트워크를 설정할 수 있습니다.

eth0 및 eth1 네트워크 인터페이스를 정의하는 경우 다음 고려사항을 검토하십시오.

- eth0 네트워크 인터페이스는 관리 네트워크에 연결되어야 하며 장치 검색 및 관리를 지원하도록 구성되어야 합니다. Lenovo XClarity Management Hub이(가) 관리 네트워크에서 관리할 모든 장치와 통신할 수 있어야 합니다.
- eth1 네트워크 인터페이스는 내부 데이터 네트워크, 공개 데이터 네트워크 또는 둘 다와 통신하도록 구성할 수 있습니다.
- 운영 체제 이미지를 배포하려면 eth1 네트워크 인터페이스에 호스트 운영 체제에 액세스하는 데 사용되는 서버 네트워크 인터페이스에 대한 IP 네트워크 연결이 있어야 합니다.
- 기능은 어느 네트워크에서나 수행할 수 있습니다.

- 가상으로 분리된 네트워크의 경우 관리 네트워크의 패킷과 데이터 네트워크의 패킷이 동일한 물리적 연결을 통해 전송됩니다. 모든 관리 네트워크 데이터 패킷의 VLAN 태그 지정을 사용하여 두 네트워크 간의 트래픽을 분리된 상태로 유지합니다.

IP 주소 고려사항

네트워크를 구성하기 전에 다음 IP 주소 고려사항을 검토하십시오.

- 가상 어플라이언스 IP 주소를 XClarity Management Hub이(가) 작동하여 실행한 후 변경하면 XClarity Orchestrator 및 모든 관리되는 장치에 연결 문제가 발생합니다. IP 주소를 변경해야 하는 경우 IP 주소를 변경하기 전에 XClarity Orchestrator에서 XClarity Management Hub 연결을 해제하고 모든 관리되는 장치를 관리 해제한 다음, IP 주소가 변경된 후에 장치를 다시 관리하고 XClarity Management Hub을(를) XClarity Orchestrator에 다시 연결하십시오.
- IP 주소 변경을 최소화하는 방식으로 장치 및 구성 요소를 구성하십시오. DHCP(Dynamic Host Configuration Protocol) 대신에 고정 IP 주소 사용을 고려하십시오. DHCP를 사용하는 경우 MAC 주소를 기반으로 DHCP 주소를 설정하거나 임대가 만료되지 않도록 DHCP를 구성하는 등의 방법으로 IP 주소 변경을 최소화해야 합니다.관리되는 장치(ThinkEdge Client 장치 외)의 IP 주소가 변경되면 장치를 관리 해제한 후 다시 관리해야 합니다.
- 한 IP 주소 공간을 다른 공간으로 재맵핑하는 네트워크 주소 변환(NAT)은 지원되지 않습니다.
- 다음 장치를 관리하려면 네트워크 인터페이스를 IPv4 주소로 구성해야 합니다. IPv6 주소는 지원되지 않습니다.
  - ThinkServer 서버
  - Lenovo Storage 장치
- 데이터 포트 또는 관리 포트를 통해 IPv6 링크 로컬을 사용하는 RackSwitch 장치 관리는 지원되지 않습니다.

고가용성 고려사항

Lenovo XClarity Orchestrator에 대해 고가용성을 설정하려면 호스트 운영 체제의 일부인 고가용성 기능을 사용하십시오.

Microsoft Hyper-V
: Hyper-V 환경에 제공되는 고가용성 기능을 사용하십시오.

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

  VMware High Availability에는 다음 구성 요소가 필요합니다.

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

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

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

제 2 장 에지 클라이언트 장치용 XClarity Management Hub 구성

Lenovo XClarity Management Hub에 처음 액세스하는 경우 처음으로 XClarity Management Hub을(를) 설정하려면 몇 가지 단계를 완료해야 합니다.

절차

다음 단계를 완료하여 XClarity Management Hub을(를) 초기 설정하십시오.

단계 1. XClarity Management Hub 웹 인터페이스에 로그인하십시오.

단계 2. 라이센스 계약을 읽고 동의하십시오.

단계 3. 추가 사용자 계정 만들기.

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

단계 5. 날짜 및 시간을 구성하십시오.

단계 6. Orchestrator 서버로 XClarity Management Hub을(를) 등록하십시오.

에지 클라이언트 장치용 XClarity Management Hub 에 로그인

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

시작하기 전에

다음 지원되는 웹 브라우저 중 하나를 사용하십시오.
- Chrome 80.0 이상
- Firefox ESR 68.6.0 이상
- Microsoft Edge 40.0 이상
- Safari 13.0.4 이상(MacOS 10.13 이상에서 실행)

웹 인터페이스는 보안 연결을 통해 액세스합니다. **https**를 사용하십시오.

XClarity Management Hub를 원격으로 구성하는 경우 동일한 레이어 2 네트워크에 연결할 수 있어야 합니다. 초기 설정이 완료될 때까지 라우팅되지 않은 주소에서 액세스해야 합니다. 따라서 XClarity Management Hub에 연결된 다른 VM에서 XClarity Management Hub에 액세스하는 것을 고려하십시오. 예를 들어 XClarity Management Hub가 설치된 호스트의 다른 VM에서 XClarity Management Hub에 액세스할 수 있습니다.

60분이 지나면 활동 여부와 관계없이 XClarity Management Hub이(가) 사용자 세션에서 자동으로 로그아웃됩니다.

절차

다음 단계를 완료하여 XClarity Management Hub 웹 인터페이스에 로그인하십시오.

단계 1. 브라우저에서 XClarity Management Hub IP 주소를 가리키십시오.

```
https://<IPv4_address>
```

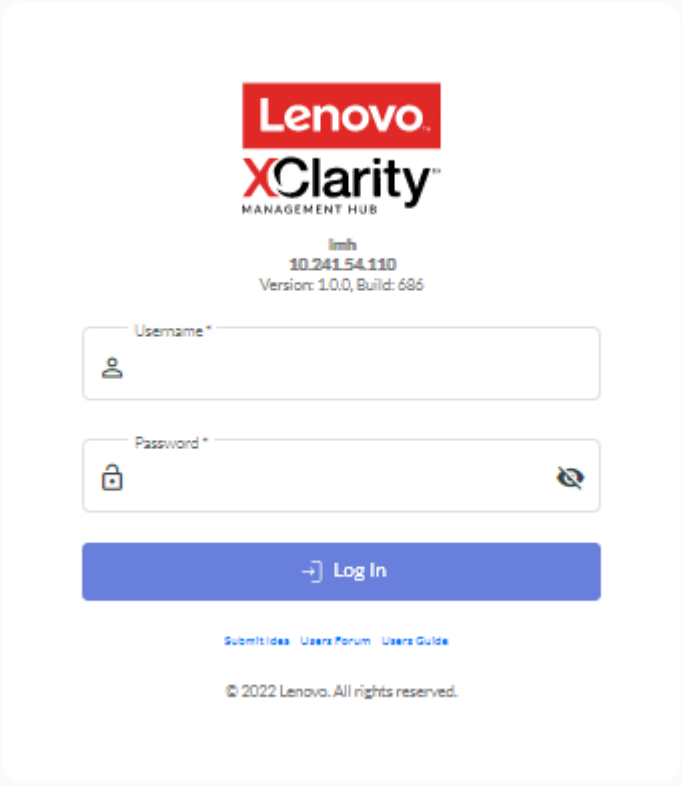
예를 들어, 다음과 같습니다.

```
https://192.0.2.10
```

사용하는 IP 주소는 환경이 설정된 방식에 따라 다릅니다.

- eth0_config에서 IPv4 주소를 지정한 경우 IPv4 주소를 사용하여 XClarity Management Hub에 액세스하십시오.
- DHCP 서버가 XClarity Management Hub과(와) 동일한 브로드캐스트 도메인에서 설정되는 경우 XClarity Management Hub 가상 컴퓨터 콘솔에 표시된 IPv4 주소를 사용하여 XClarity Management Hub에 액세스하십시오.
- 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 Management Hub이(가) 처음 시작되면 eth0 및 eth1은 DHCP 할당 IP 주소를 가져오고 XClarity Management Hub 기본 게이트웨이는 *eth1*의 DHCP 할당 게이트웨이로 설정됩니다.

XClarity Management Hub 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. 사용자 자격 증명을 입력하고 **로그인**을 클릭하십시오.

XClarity Management Hub에 처음 로그인하는 경우 기본 자격 증명인 USERID와 PASSW0RD(여기에서 0은 숫자)를 입력하십시오.

단계 4. 라이센스 계약을 읽고 동의하십시오.

단계 5. 기본 자격 증명을 사용하여 처음 로그인하면 암호를 변경하라는 메시지가 표시됩니다. 기본적으로 암호는 8~256자여야 하며 다음 기준을 충족해야 합니다.

중요: 16자 이상의 안전한 암호를 사용하는 것이 좋습니다.
- (1) 알파벳 대문자를 하나 이상 포함해야 합니다
- (2) 알파벳 소문자를 하나 이상 포함해야 합니다
- (3) 숫자를 하나 이상 포함해야 합니다

- (4) 특수 문자를 하나 이상 포함해야 합니다
- (5) 사용자 이름과 동일하면 안 됩니다.

단계 6. 처음으로 로그인하면 기존의 자체 서명된 인증서를 사용할 것인지 또는 외부 CA 서명 인증서를 사용할 것인지 선택하라는 메시지가 표시됩니다. 외부 서명 인증서를 사용하도록 선택하는 경우 서버 인증서 페이지가 표시됩니다.

주의: 자체 서명된 인증서는 보안이 취약합니다. 직접 외부에서 서명된 인증서를 생성하고 설치하는 것이 좋습니다.

외부 서명 인증서 사용에 대한 자세한 내용은 에지 클라이언트 장치용 XClarity Management Hub 에서 신뢰할 수 있고 외부에서 서명된 서버 인증서 설치에서 확인하십시오.

완료한 후에

XClarity Management Hub 웹 인터페이스 오른쪽 상단에 있는 **사용자 계정** 메뉴(⚙)에서 다음 작업을 수행할 수 있습니다.

- **로그아웃**을 클릭하여 현재 세션에서 로그아웃합니다. XClarity Management Hub 로그 페이지가 표시됩니다.
- 질문하고 Lenovo XClarity 커뮤니티 포럼 웹 사이트의 내용에서 답변을 찾으십시오.
- XClarity Management Hub에 관한 아이디어를 제출하려면 웹 인터페이스 오른쪽 상단 모서리의 **사용자 계정** 메뉴(⚙)에서 **아이디어 제출**을 클릭합니다. Lenovo XClarity 아이디어화 웹 사이트(으)로 바로 이용하는 방법도 있습니다.
- **사용 설명서**를 클릭하여 온라인 설명서를 보십시오.
- **정보**를 클릭하여 XClarity Management Hub 릴리스에 대한 정보를 봅니다.
- **언어 변경**을 클릭하여 사용자 인터페이스의 언어를 변경합니다. 다음과 같은 언어가 지원됩니다.
  - 영어(en)
  - 중국어 간체(zh-CN)
  - 중국어 번체(zh-TW)
  - 프랑스어(fr)
  - 독일어(de)
  - 이탈리아어(it)
  - 일본어(ja)
  - 한국어(ko)
  - 브라질 포르투갈어(pt-BR)
  - 러시아어(ru)
  - 스페인어(es)
  - 태국어(th)

에지 클라이언트 장치용 Lenovo XClarity Management Hub 의 사용자 계정 생성

Lenovo XClarity Management Hub에 대해 최대 10개의 사용자 계정을 생성할 수 있습니다.

절차

사용자 계정을 만들려면 다음 단계를 완료하십시오.

단계 1. Lenovo XClarity Management Hub 메뉴 표시줄에서 **보안**(⚙) → **로컬 사용자**를 클릭하여 로컬 사용자 카드를 표시하십시오.

단계 2. **만들기** 아이콘(⊕)을 클릭하여 사용자를 생성하십시오. 새 사용자 만들기 대화 상자가 표시됩니다.

단계 3. 대화 상자에서 다음 정보를 입력하십시오.

- 중복되지 않는 사용자 이름을 입력하십시오. 영숫자, 마침표(.), 대시(-), 밑줄(_) 문자를 포함하여 최대 32자까지 지정할 수 있습니다.

  참고: 사용자 이름은 대소문자를 구분하지 않습니다.
- 새 암호와 암호 확인을 입력하십시오. 기본적으로 암호는 8~256자여야 하며 다음 기준을 충족해야 합니다.

  중요: 16자 이상의 안전한 암호를 사용하는 것이 좋습니다.
  - (1) 알파벳 대문자를 하나 이상 포함해야 합니다
  - (2) 알파벳 소문자를 하나 이상 포함해야 합니다
  - (3) 숫자를 하나 이상 포함해야 합니다
  - (4) 특수 문자를 하나 이상 포함해야 합니다
  - (5) 사용자 이름과 동일하면 안 됩니다.

단계 4. **만들기**를 클릭하십시오.

사용자 계정이 테이블에 추가됩니다.

완료한 후에

로컬 사용자 카드에서 다음 작업을 수행할 수 있습니다.
- **편집** 아이콘(✎)을 클릭하여 사용자 계정의 암호와 속성을 수정하십시오. 암호는 만료되지 않습니다.
- **삭제** 아이콘(🗑)을 클릭하여 선택된 사용자 그룹을 삭제합니다.

에지 클라이언트 장치용 XClarity Management Hub 의 네트워크 설정 구성

단일 IPv4 네트워크 인터페이스 및 인터넷 라우팅 설정을 구성할 수 있습니다.

시작하기 전에

네트워크를 구성하기 전에 네트워크 고려사항을 검토하십시오(네트워크 고려사항 참조).

절차

네트워크 설정을 구성하려면 XClarity Management Hub메뉴 표시줄에서 **관리**(⚙) → **네트워킹**을 클릭한 후 다음 단계 중 하나 이상을 완료하십시오.

- IP **설정 구성하기**eth0 인터페이스의 경우 Eth0 **인터페이스** 탭을 클릭하고 해당하는 IPv4 주소 설정을 구성한 다음 **적용**을 클릭하십시오.

주의:

- 가상 어플라이언스 IP 주소를 XClarity Management Hub이(가) 작동하여 실행한 후 변경하면 XClarity Orchestrator 및 모든 관리되는 장치에 연결 문제가 발생합니다. IP 주소를 변경해야 하는 경우 IP 주소를 변경하기 전에 XClarity Orchestrator에서 XClarity Management Hub 연결을 해제하고 모든 관리되는 장치를 관리 해제한 다음, IP 주소가 변경된 후에 장치를 다시 관리하고 XClarity Management Hub을(를) XClarity Orchestrator에 다시 연결하십시오.

현재 IPv4 주소만 지원됩니다.

- IPv4 **설정**. IP 할당 방식, IPv4 주소, 네트워크 마스크 및 기본 게이트웨이를 구성할 수 있습니다.IP 할당 방식으로는 할당된 IP 주소를 고정으로 사용하거나 DHCP 서버에서 IP 주소를 얻는 방식이 있습니다. 고정 IP 주소를 사용하는 경우 IP 주소, 네트워크 마스크 및 기본 게이트웨이를 제공해야 합니다.

  기본 게이트웨이는 유효한 IP 주소여야 하고 사용 설정한 인터페이스(eth0)와 동일한 네트워크 마스크(동일한 서브넷)를 사용해야 합니다.

  인터페이스가 DHCP를 사용하여 IP 주소를 얻는 경우 기본 게이트웨이도 DHCP를 사용합니다.

- **인터넷 라우팅 설정 구성하기**필요한 경우 DNS 구성 카드에서 DNS(Domain Name System) 설정을 구성하십시오. 그런 다음 **적용**을 클릭하십시오.

  현재 IPv4 주소만 지원됩니다.

  DNS 서버의 IP 주소를 변경할 수 있습니다.

  DNS 서버의 정규화된 도메인 이름(FQDN)과 호스트 이름은 XClarity Management Hub 서버와 동일하며 변경할 수 없습니다.

에지 클라이언트 장치용 XClarity Management Hub 의 날짜 및 시간 구성

XClarity Management Hub과(와) 모든 관리되는 장치 간에 타임스탬프를 동기화하려면 하나 이상(최대 4개)의 NTP(Network Time Protocol) 서버를 설정해야 합니다.

시작하기 전에

각 NTP 서버는 네트워크를 통해 액세스할 수 있어야 합니다. XClarity Management Hub가 실행 중인 로컬 시스템에 NTP 서버를 설정하도록 고려하십시오.

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

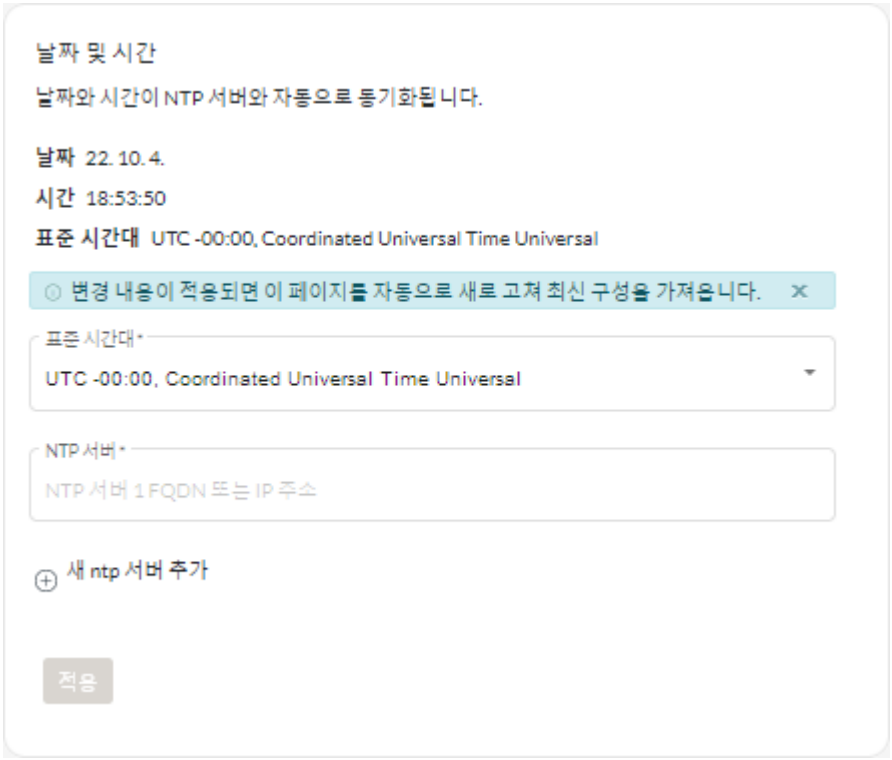
주의: XClarity Management Hub 가상 어플라이언스와 해당 호스트가 동일한 시간 소스와 동기화되도록 설정해야만 XClarity Management Hub와 해당 호스트 간에 부주의하게 수행되는 잘못된 시간 동기화가 방지됩니다. 일반적으로 호스트는 가상 어플라이언스와 시간 동기화를 수행하도록 구성됩니다. XClarity Management Hub이(가) 해당 호스트가 아닌 다른 소스와 동기화하도록 설정된 경우 XClarity Management Hub 가상 어플라이언스와 해당 호스트 간에 호스트 시간 동기화를 사용 안 함으로 설정해야 합니다.

- ESXi의 경우 VMware – 시간 동기화 사용 안 함 웹 페이지의 다음 지시 사항을 참조하십시오.

절차

XClarity Management Hub에 대한 날짜 및 시간을 설정하려면 다음 단계를 완료하십시오.

단계 1. XClarity Management Hub 메뉴 표시줄에서 **관리**(⚙) → **날짜 및 시간**을 클릭하면 날짜 및 시간 카드가 표시됩니다.



단계 2. XClarity Management Hub의 호스트가 있는 시간대를 선택하십시오.

선택한 시간대에서 일광절약시간(DST)를 사용하는 경우 시간이 DST에 맞게 자동으로 조정됩니다.

단계 3. 네트워크에 있는 각 NTP 서버의 호스트 이름 또는 IP 주소를 지정하십시오. 최대 4개의 NTP 서버를 정의할 수 있습니다.

단계 4. **적용**을 클릭하십시오.

에지 클라이언트 장치용 Lenovo XClarity Management Hub 의 보안 인증서 관리

Lenovo XClarity Management Hub은(는) SSL 인증서를 사용하여 Lenovo XClarity Management Hub과(와) 관리되는 장치 간의 신뢰할 수 있는 보안 통신 및 사용자의 Lenovo XClarity Management Hub 또는 다른 서비스와의 통신을 설정합니다. 기본적으로 Lenovo XClarity Management Hub 및 XClarity Orchestrator에서는 내부 인증 기관에서 자체 서명하고 발행한 XClarity Orchestrator에서 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

Lenovo XClarity Management Hub의 모든 인스턴스에서 고유 생성되는 기본 서버 인증서는 여러 환경에서 충분한 보안을 제공합니다. Lenovo XClarity Management Hub가 대신 인증서를 관리하게 하거나 서버 인증서를 사용자 지정 또는 교체함으로써 더 적극적인 역할을 맡을 수 있습니다. Lenovo XClarity Management Hub는 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 Lenovo XClarity Management Hub에 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.

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

Lenovo XClarity Management Hub는 관리 장치 및 외부 서비스와 통신할 때 클라이언트의 역할을 합니다. 이 경우 관리되는 장치 또는 외부 서비스는 Lenovo XClarity Management Hub에서 확인할 수 있도록 서버 인증서를 제공합니다. Lenovo XClarity Management Hub은(는) 신뢰하는 인증서 목록을 유지 관리합니다. 관리되는 장치 또는 외부 서비스에서 제공하는 *신뢰할 수 있는 인증서*가 나열되지 않으면 Lenovo XClarity Management Hub는 관리되는 장치 또는 외부 서비스와의 연결을 끊어 보안에 민감한 정보를 신뢰할 수 없는 출처와 교환하지 않도록 합니다.

다음 인증서 범주는 Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub 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(에지 클라이언트 장치용 XClarity Management Hub 의 자체 서명된 서버 인증서 다시 생성 참고).또한 초기 설정 중에 별도의 키가 생성되고 서버 인증서가 만들어져 내부 인증 기관의 서명을 받습니다. 이 인정서는 기본 Lenovo XClarity Management Hub 서버 인증서로 사용됩니다. 인증서에 서버의 올바른 주소가 포함될 수 있도록 Lenovo XClarity Management Hub에서 네트워킹 주소(IP 또는 DNS 주소)가 변경되었음을 감지할 때마다 자동으로 다시 생성됩니다. 필요 시 사용자 지정 및 생성할 수 있습니다(에지 클라이언트 장치용 XClarity Management Hub 의 자체 서명된 서버 인증서 다시 생성 참조).

  CSR(인증서 서명 요청)을 생성하고, 개인 또는 상업용 인증서 루트 인증 기관에서 CSR에 서명하도록 한 후, 전체 인증서 체인을 Lenovo XClarity Management Hub(으)로 가져와서 기본 자체 서명된 서버 인증서 대신 외부 서명된 서버 인증서를 사용하도록 선택할 수 있습니다(에지 클라이언트 장치용 XClarity Management Hub 에서 신뢰할 수 있고 외부에서 서명된 서버 인증서 설치 참조).

  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(에지 클라이언트 장치용 Lenovo XClarity Management Hub 의 웹 브라우저로 서버 인증서 가져오기 참조).
- **OS 배포 인증서**. 운영 체제 배포 서비스가 별도의 인증서를 사용하여 운영 체제 설치 프로그램이 배포 프로세스 중에 배포 서비스에 안전하게 연결하도록 할 수 있습니다. 키가 유출된 경우 Lenovo XClarity Management Hub을(를) 다시 시작하여 재생성할 수 있습니다.

에지 클라이언트 장치용 XClarity Management Hub 의 자체 서명된 서버 인증서 다시 생성

XClarity Management Hub에서 현재 사용자 지정된 외부 서명 서버 인증서를 사용하는 경우 새 서버 인증서를 생성하여 기존의 자체 서명된 Lenovo XClarity Management Hub 서버 인증서를 교체하거나 XClarity Management Hub에서 생성한 인증서를 복구할 수 있습니다. 자체 서명된 새 서버 인증서는 HTTPS 액세스를 위해 XClarity Management Hub에서 사용됩니다.

시작하기 전에

주의: 새 루트 CA를 사용하여 XClarity Management Hub 서버 인증서를 다시 생성하면 XClarity Management Hub에서 관리되는 장치에 대한 연결이 끊어지고 장치를 다시 관리해야 합니다. 루트 CA를 변경하지 않고 XClarity Management Hub 서버 인증서를 다시 생성하는 경우(예: 인증서가 만료된 경우) 장치를 다시 관리하지 않아도 됩니다.

이 작업 정보

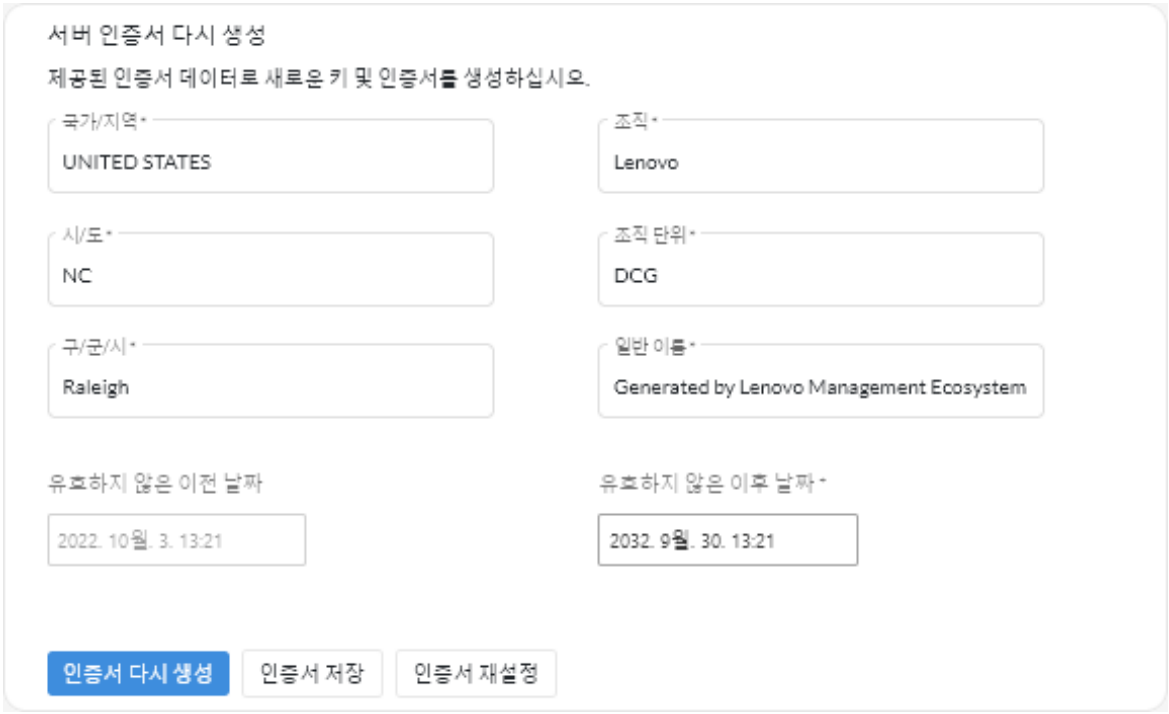
현재 사용 중인 서버 인증서는 자체 서명 또는 외부 서명과는 무관하게 새 서버 인증서가 생성, 서명 및 설치될 때까지 계속 사용됩니다.

중요: 서버 인증서가 수정되면 관리 허브가 다시 시작되고 사용자 세션이 모두 종료됩니다. 웹 인터페이스에서 작업을 계속하려면 사용자가 다시 로그인해야 합니다.

절차

자체 서명된 XClarity Management Hub 서버 인증서를 생성하려면 다음 단계를 완료하십시오.

단계 1. XClarity Management Hub 메뉴 표시줄에서 **보안**(⚙) → **서버 인증서**를 클릭하여 **자체 서명된 서버 인증서 다시 생성** 카드를 표시하십시오.



단계 2. **자체 서명된 서버 인증서 다시 생성** 카드에서 필드를 채워 요청하십시오.

- 인증 기관과 연관시킬 국가 또는 지역의 ISO 3166 코드 2자리(예: 미국의 경우 US).
- 인증서와 연관시킬 주 또는 도의 전체 이름(예: California 또는 New Brunswick).
- 인증서와 연관시킬 도시의 전체 이름(예: San Jose). 필드 값의 길이는 50자 이하여야 합니다.
- 인증서를 소유한 조직(회사). 일반적으로 회사의 법적 명칭입니다. Ltd., Inc. 또는 Corp(예: ACME International Ltd.)와 같은 접미사를 포함해야 합니다. 이 필드 값의 길이는 60자 이하여야 합니다.
- (선택 사항) 인증서를 소유할 조직 단위(예: ABC 부서). 이 필드 값의 길이는 60자 이하여야 합니다.

- 인증서 소유자의 공통 이름. 일반적으로 인증서를 사용하는 서버의 FQDN (충분한 자격을 갖춘 도메인 이름) 또는 IP 주소입니다(예: www.domainname.com 또는 192.0.2.0). 이 필드 값의 길이는 63자 이하여야 합니다.

  참고: 현재 이 특성은 인증서에 영향을 미치지 않습니다.
- 서버 인증서가 더 이상 유효하지 않은 날짜 및 시간

  참고: 현재 이러한 특성은 인증서에 영향을 미치지 않습니다.

참고: 서버 인증서를 재생성할 때는 주체 대체 이름을 변경할 수 없습니다.

단계 3. **자체 서명된 서버 인증서 다시 생성**을 클릭하여 자체 서명된 인증서를 다시 생성한 다음 **인증서 다시 생성**을 클릭하여 확인합니다.관리 허브가 다시 시작되고 연결된 모든 사용자 세션이 종료됩니다.

단계 4. 웹 브라우저에 다시 로그인하십시오.

완료한 후에

자체 서명된 서버 인증서 다시 생성 카드에서 다음 작업을 수행할 수 있습니다.
- **인증서 저장**을 클릭하여 현재 서버 인증서를 로컬 시스템에 PEM 형식으로 저장하십시오.
- **인증서 재설정**을 클릭하고 기본 설정을 사용하여 서버 인증서를 다시 생성하십시오. 메시지가 나오면 Ctrl+F5를 눌러 브라우저를 새로 고친 후 웹 인터페이스에 대한 연결을 다시 설정하십시오.

에지 클라이언트 장치용 XClarity Management Hub 에서 신뢰할 수 있고 외부에서 서명된 서버 인증서 설치

개인 또는 상업용 인증 기관(CA)에서 서명한 신뢰할 수 있는 서버 인증서를 사용할 수 있습니다. 외부 서명된 서버 인증서를 사용하려면 CSR(인증서 서명 요청)을 생성한 다음 나타나는 서버 인증서를 가져와서 기존 서버 인증서를 교체하십시오.

시작하기 전에

주의:

- 새 루트 CA를 사용하여 외부에서 서명된 Lenovo XClarity Management Hub 서버 인증서를 설치하면 XClarity Management Hub에서 관리되는 장치에 대한 연결이 끊어지고 장치를 다시 관리해야 합니다. 루트 CA를 변경하지 않고 외부에서 서명된 Lenovo XClarity Management Hub 서버 인증서를 설치하는 경우(예: 인증서가 만료된 경우) 장치를 다시 관리하지 않아도 됩니다.
- CSR이 생성된 후 서명된 서버 인증서를 가져오기 전에 새 장치를 추가하는 경우 새 서버 인증서를 받으려면 해당 장치를 다시 시작해야 합니다.

이 작업 정보

가장 좋은 방법은 항상 v3 서명 인증서를 사용하는 것입니다.

외부 서명 서버 인증서는 **CSR 파일 생성** 버튼을 사용하여 가장 최근에 생성된 인증서 서명 요청에서 생성되어야 합니다.

외부 서명된 서버 인증서 내용은 CA의 루트 인증서, 모든 중간 인증서 및 서버 인증서를 포함한 전체 CA 서명 체인을 포함하는 인증서 번들이어야 합니다.

새 서버 인증서가 신뢰할 수 있는 타사의 서명을 받지 않은 경우, 다음번 Lenovo XClarity Management Hub에 연결할 때 브라우저에는 보안 메시지와 새 인증서를 브라우저에 허용하도록 하는 대화 상자가 표시됩니다. 보안 메시지를 방지하려면 서버 인증서를 웹 브라우저의 신뢰할 수 있는 인증서 목록에 가져올 수 있습니다(에지 클라이언트 장치용 Lenovo XClarity Management Hub 의 웹 브라우저로 서버 인증서 가져오기 참조).

XClarity Management Hub는 현재 세션을 종료하지 않고 새 서버 인증서를 사용하기 시작합니다. 새 세션은 새 인증서를 사용하여 설정됩니다. 사용 중인 새 인증서를 사용하려면 웹 브라우저를 다시 시작하십시오.

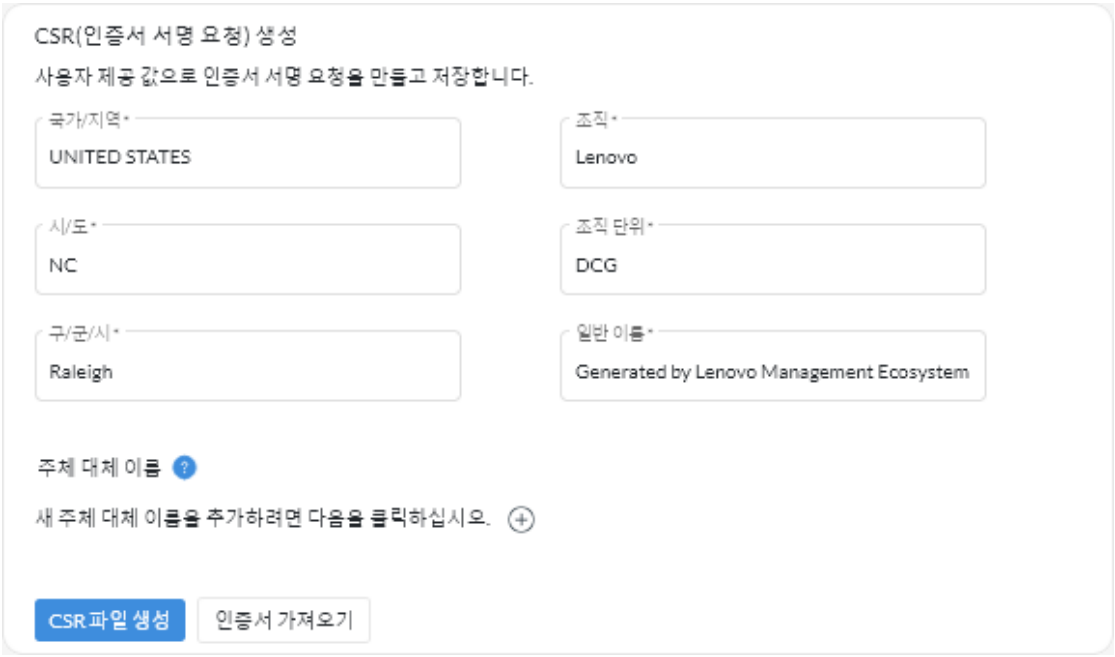
중요: 서버 인증서가 수정되면 모든 사용자 세션은 Ctrl+F5를 클릭하여 웹 브라우저를 새로 고친 다음 XClarity Management Hub 연결을 재설정해야 합니다.

절차

외부 서명된 서버 인증서를 생성하려면 다음 단계를 완료하십시오.

단계 1. 인증서 서명 요청을 작성하고 파일을 로컬 시스템에 저장하십시오.

1. XClarity Management Hub 메뉴 표시줄에서 **보안**() → **서버 인증서**를 클릭하여 인증서 서명 요청 생성 카드를 표시하십시오.



2. 인증서 서명 요청 카드에서 필드를 채워 요청하십시오.
   - 인증 기관과 연관된 국가 또는 지역의 두 자리 ISO 3166 코드(예: 미국의 경우 US).
   - 인증서와 연관시킬 주 또는 도의 전체 이름(예: California 또는 New Brunswick).
   - 인증서와 연관시킬 도시의 전체 이름(예: San Jose). 필드 값의 길이는 50자 이하여야 합니다.
   - 인증서를 소유할 조직(회사). 일반적으로 회사의 법인 명칭입니다. Ltd., Inc. 또는 Corp(예: ACME International Ltd.)와 같은 접미사를 포함해야 합니다. 이 필드 값의 길이는 60자 이하여야 합니다.
   - (선택 사항) 인증서를 소유할 조직 단위(예: ABC 부서). 이 필드 값의 길이는 60자 이하여야 합니다.
   - 인증서 소유자의 공통 이름. 이것은 자격 증명을 사용하는 서버의 호스트 이름이어야 합니다. 이 필드 값의 길이는 63자 이하여야 합니다.

     참고: 현재 이 특성은 인증서에 영향을 미치지 않습니다.
   - (선택 사항) CSR이 생성될 때 X.509 "subjectAltName" 확장자에 추가되는 주체 대체 이름을 사용자 지정합니다. 지정된 대체 대안 이름은 지정된 유형에 따라 검증되고 CSR 생성 후 CSR에 추가됩니다. 기본적으로 XClarity Management Hub는 XClarity

Management Hub 게스트 운영 체제의 네트워크 인터페이스에 의해 검색되는 IP 주소 및 호스트 이름을 기반으로 CSR에 대한 주체 개체 이름을 자동으로 정의합니다.

주의: 주체 대체 이름에는 관리 허브의 IP 주소 또는 FQDN(정규화된 도메인 이름)이 포함되어야 하며 주체 이름은 관리 허브의 FQDN으로 설정되어야 합니다. 결과 인증서가 완전한지 확인하기 위해 CSR 프로세스를 시작하기 전에 이러한 필수 필드가 존재하고 올바른지 확인하십시오. 인증서 데이터가 누락되면 관리 허브를 Lenovo XClarity Orchestrator에 연결하려고 시도할 때 연결이 신뢰할 수 없게 될 수 있습니다.

선택한 유형에 대해 지정한 이름이 유효해야 합니다.
- DNS(FQDN을 사용하십시오. 예: hostname.labs.company.com)
- IP **주소**(예: 192.0.2.0)
- **이메일**(예: example@company.com)

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

단계 3. 외부 서명된 서버 인증서 및 CA 인증서를 XClarity Management Hub에 가져온 다음 현재 서버 인증서를 교체하십시오.

1. 인증서 서명 요청(CSR) 생성 카드에서 **인증서 가져오기**를 클릭하면 인증서 가져오기대화 상자가 나옵니다.
2. 서버 인증서와 CA 인증서를 PEM 형식으로 복사하여 붙여넣습니다. 서버 인증서로 시작하여 루트 CA 인증서로 끝나는 전체 인증서 체인을 제공해야 합니다.
3. **가져오기**를 클릭하여 서버 인증서를 XClarity Management Hub 신뢰 저장소에 보관하십시오.

단계 4. Ctrl + F5를 눌러 브라우저를 새로 고친 후 웹 인터페이스에 대한 연결을 다시 설정하여 새 인증서를 승인하십시오. 이 절차는 설정된 모든 사용자 세션에서 수행되어야 합니다.

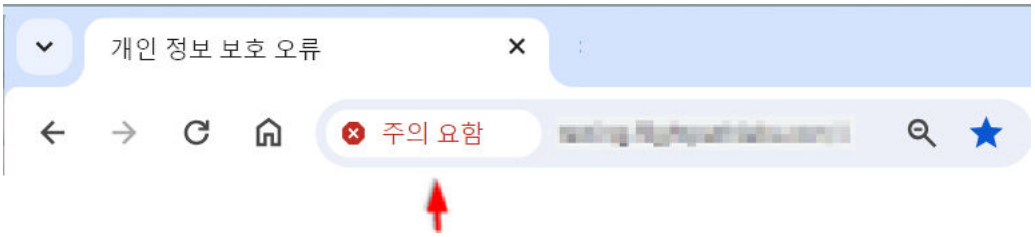
에지 클라이언트 장치용 Lenovo XClarity Management Hub 의 웹 브라우저로 서버 인증서 가져오기

현재 서버 인증서의 사본을 로컬 시스템에 PEM 형식으로 저장할 수 있습니다. 그런 다음 인증서를 웹 브라우저의 신뢰할 수 있는 인증서 목록 또는 다른 응용 프로그램으로 가져오면 Lenovo XClarity Management Hub에 액세스할 때 보안 경고 메시지가 웹 브라우저에 나타나지 않습니다.

절차

서버 인증서를 웹 브라우저로 가져오려면 다음 단계를 완료하십시오.

- Chrome
  1. Lenovo XClarity Management Hub 서버 인증서를 내보냅니다.
     a. 상단 주소 표시줄에서 "안전하지 않음" 경고 아이콘을 클릭합니다. 예를 들면 다음과 같습니다.

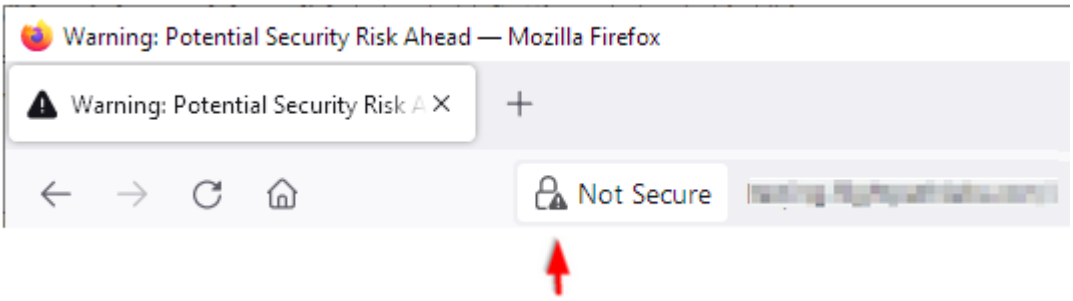


     b. **인증서가 유효하지 않음**을 클릭하여 인증서 대화 상자를 표시합니다.
     c. **세부 정보** 탭을 클릭하십시오.
     d. **내보내기**를 클릭하십시오.
     e. 인증서 파일의 이름과 위치를 지정하고 **저장**을 클릭하여 인증서를 내보냅니다.

f. 인증서 뷰어 대화 상자를 닫습니다.

2. Lenovo XClarity Management Hub 서버 인증서를 브라우저의 신뢰할 수 있는 루트 기관 인증서 목록에 가져오십시오.
   a. Chrome 브라우저에서 창의 오른쪽 상단에 있는 점 3개를 클릭한 다음 **설정**을 클릭하여 설정 페이지를 엽니다.
   b. **개인 정보 및 보안**을 클릭한 다음 **보안**을 클릭하여 보안 페이지를 표시합니다.
   c. **고급** 섹션으로 스크롤한 다음 **장치 인증서 관리**를 클릭합니다.
   d. **가져오기**를 클릭하고 **다음**을 클릭합니다.
   e. 이전에 내보낸 인증서 파일을 선택하고 **다음**을 클릭합니다.
   f. 인증서를 저장할 위치를 선택하고 **다음**을 클릭합니다.
   g. **완료**를 누르십시오.
   h. Chrome 브라우저를 닫았다가 다시 연 다음 Lenovo XClarity Management Hub을(를) 엽니다.

- Firefox
  1. Lenovo XClarity Management Hub 서버 인증서를 내보냅니다.
     a. 상단 주소 표시줄에서 "안전하지 않음" 경고 아이콘을 클릭합니다. 예를 들면 다음과 같습니다.



     b. **연결이 안전하지 않음**을 클릭한 다음 **자세한 정보**를 클릭하십시오.
     c. **인증서 보기**를 클릭하십시오.
     d. **기타** 섹션이 나올 때까지 아래로 스크롤하고 PEM(**인증서**) 링크를 클릭하여 로컬 시스템에 파일을 저장합니다.
  2. Lenovo XClarity Management Hub 서버 인증서를 브라우저의 신뢰할 수 있는 루트 기관 인증서 목록에 가져오십시오.
     a. 브라우저를 열고 **도구** → **설정**을 클릭한 다음 **개인 정보 및 보안**을 클릭합니다.
     b. **보안** 섹션까지 아래로 스크롤합니다.
     c. **인증서 보기**를 클릭하여 인증서 관리자 대화 상자를 표시합니다.
     d. **인증서** 탭을 클릭합니다.
     e. **가져오기**를 클릭하고 인증서가 다운로드된 위치를 살펴보십시오.
     f. 인증서를 선택하고 **열기**를 클릭하십시오.
     g. 인증서 관리자 대화 상자를 닫습니다.

에지 클라이언트 장치용 XClarity Management Hub 을(를) XClarity Orchestrator에 연결

Lenovo XClarity Orchestrator(으)로 Lenovo XClarity Management Hub을(를) 등록(연결)하면 장치 관리 및 모니터링을 시작할 수 있습니다.

시작하기 전에

XClarity Management Hub에서 XClarity Orchestrator의 네트워크에 도달할 수 있고 XClarity Orchestrator에서 XClarity Management Hub의 네트워크에 도달할 수 있어야 합니다.

절차

XClarity Management Hub을(를) 등록하려면 다음 단계를 완료하십시오.

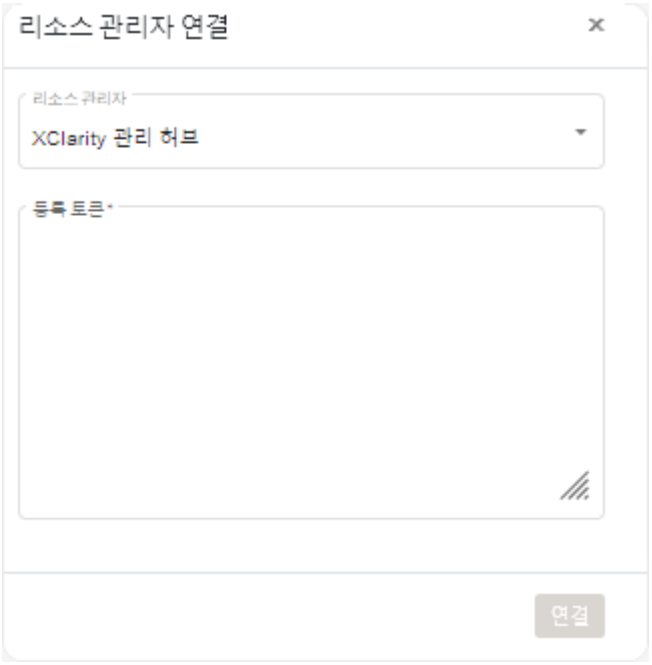
단계 1. 관리 허브 등록 키를 만듭니다.

1. Management Hub 메뉴 표시줄에서 **등록**을 클릭하여 등록 페이지를 표시합니다.

2. **등록 키 만들기**를 클릭합니다.
3. **클립보드에 복사**를 클릭하여 등록 키를 복사한 다음 대화 상자를 닫으십시오.

단계 2. 관리 허브 등록 키를 XClarity Orchestrator에 추가합니다.

1. XClarity Orchestrator 메뉴 표시줄에서 **리소스**() → **리소스 관리자**를 클릭하면 리소스 관리자 카드가 표시됩니다.
2. **연결** 아이콘()을 클릭하면 리소스 관리자가 나옵니다. 리소스 관리자 연결 대화 상자.



3. XClarity Management Hub을(를) 리소스 관리자로 선택하십시오.
4. **등록 토큰** 필드에 등록 키를 복사합니다.
5. **연결**을 클릭하여 XClarity Orchestrator 등록 키가 포함되어 있는 리소스 관리자 연결 대화 상자를 표시합니다.
6. **클립보드에 복사**를 클릭하여 등록 키를 복사한 다음 대화 상자를 닫으십시오.

단계 3. 관리 허브에 XClarity Orchestrator 등록 키를 추가합니다.

1. Management Hub 메뉴 표시줄에서 **등록**을 클릭하여 등록 페이지를 표시합니다.
2. **등록 키 설치**를 클릭합니다.
3. **등록 토큰** 필드에 등록 키를 복사합니다.
4. **연결**을 클릭하십시오.

완료한 후에

- 관리 허브를 사용하여 장치를 관리하십시오(ThinkEdge Client 장치 관리 XClarity Orchestrator 온라인 설명서 참조).
- **등록 재설정**을 클릭하여 현재 관리 허브 등록 키를 삭제합니다.

제 3 장 에지 클라이언트 장치용 XClarity Management Hub 설치 제거

XClarity Management Hub 가상 어플라이언스를 제거하려면 다음 단계를 완료하십시오.

절차

XClarity Management Hub 가상 어플라이언스를 설치 제거하려면 다음 단계를 완료하십시오.

단계 1. 현재 XClarity Management Hub에서 관리하는 모든 장치를 관리 해제하십시오.

단계 2. 운영 체제에 따라 XClarity Management Hub을(를) 제거하십시오.

- ESXi
  1. VMware vSphere Client를 통해 호스트에 연결하십시오.
  2. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 **전원 → 전원 끄기**를 클릭하십시오.
  3. 가상 컴퓨터를 다시 마우스 오른쪽 단추로 클릭하고 **디스크에서 삭제**를 클릭하십시오.