Lenovo XClarity Management Hub Installations- und Benutzerhandbuch

Version 2.1

Anmerkung

Lesen Sie vor der Verwendung dieser Informationen und des entsprechenden Produktes die allgemeinen und rechtlichen Hinweise in der Onlinedokumentation von XClarity Orchestrator.

Zweite Ausgabe (Juli 2024)

Inhaltsverzeichnis

Kapitel 1. Planen von Lenovo XClarity Management Hub

Lesen Sie die folgenden Hinweise und Voraussetzungen, die Ihnen bei der Planung Ihrer Installation von Lenovo XClarity Management Hub helfen.

Unterstützte Hardware und Software

Stellen Sie sicher, dass Ihre Umgebung die Hardware- und Softwarevoraussetzungen für Lenovo XClarity Management Hub erfüllt.

Hostsysteme

Hypervisor-Anforderungen

Die folgenden Hypervisoren werden für die Installation von Lenovo XClarity Management Hub unterstützt.
- VMware ESXi 7.0, U1, U2 und U3
- VMware ESXi 6.7, U1, U2[1] und U3

Bei VMware ESXi ist die virtuelle Einheit eine OVF-Vorlage.

Wichtig:

- Für VMware ESXi 6.7 U2 müssen Sie das ISO-Image VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso oder höher verwenden.

Hardwarevoraussetzungen

In der folgenden Tabelle sind die *empfohlenen Mindestkonfigurationen* für XClarity Management Hub basierend auf der Anzahl der verwalteten Edge-Client-Einheiten aufgeführt. Abhängig von Ihrer Umgebung sind möglicherweise zusätzliche Ressourcen notwendig, um eine optimale Leistung zu erreichen.

Anzahl der verwalteten Edge-Client-Einheiten	Prozessoren	Hauptspeicher	Speicher
0–100 Einheiten	6	32 GB	340 GB
100–200 Einheiten	8	34 GB	340 GB
200–400 Einheiten	10	36 GB	340 GB
400–600 Einheiten	12	40 GB	340 GB
600–800 Einheiten	14	44 GB	340 GB
800–1.000 Einheiten	16	48 GB	340 GB

1. Dies ist die Mindestspeicherkapazität, die von der virtuellen XClarity Management Hub Einheit als SSD-Datenspeicher verwendet wird.

Softwarevoraussetzungen

Die folgende Software wird von XClarity Management Hub benötigt.

- **NTP-Server**. Um sicherzustellen, dass die Zeitstempel für alle Ereignisse und Alerts synchronisiert werden, die mit XClarity Management Hub von Ressourcenmanagern und verwalteten Einheiten empfangen werden, ist ein NTP-Server (Network Time Protocol) erforderlich. Vergewissern Sie sich,

dass der Zugriff über das Verwaltungsnetzwerk (in der Regel über die Eth0-Schnittstelle) auf den NTP-Server funktioniert.

Verwaltbare Einheiten

XClarity Management Hub kann maximal 10,000 ThinkEdge Client-Einheiten verwalten, überwachen und bereitstellen (ohne Baseboard Management Controller).

Sie finden eine vollständige Liste der unterstützten ThinkEdge Client-Einheiten und Zusatzeinrichtungen (z. B. E/A-, DIMM- und Speicheradapter), die mindestens erforderlichen Firmwareversionen und Einschränkungen der Webseite für XClarity Management Hub.

Allgemeine Informationen zu Hardwarekonfigurationen und Optionen für eine bestimmte Einheit finden Sie unter Lenovo Server Proven-Website.

Webbrowser

Die XClarity Management Hub-Webschnittstelle funktioniert mit den folgenden Webbrowsern.
- Chrome 80.0 oder höher
- Firefox ESR 68.6.0 oder höher
- Microsoft Edge 40.0 oder höher
- Safari 13.0.4 oder höher (ausgeführt auf macOS 10.13 oder höher)

Firewalls und Proxy-Server

Einige Service- und Unterstützungsfunktionen, einschließlich Call-Home-Funktion und Garantiestatus, erfordern den Zugriff auf das Internet. Wenn Sie Firewalls in Ihrem Netzwerk haben, konfigurieren Sie die Firewalls so, dass XClarity Orchestrator und Ressourcenmanager diese Vorgänge durchführen können. Wenn Lenovo XClarity Orchestrator und Ressourcenmanager keinen direkten Zugriff auf das Internet hat, konfigurieren Sie sie für die Verwendung eines Proxy-Servers.

Firewalls

Stellen Sie sicher, dass die folgenden DNS-Namen und Ports in der Firewall für XClarity Orchestrator und entsprechende Ressourcenmanager (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub und Lenovo XClarity Administrator) geöffnet sind, falls zutreffend. Jedes DNS stellt ein räumlich verteiltes System mit einer dynamischen IP-Adresse dar.

Anmerkung: Änderungen an IP-Adressen sind vorbehalten. Verwenden Sie die DNS-Namen, wenn möglich.

DNS-Name	Ports	Protokolle
Aktualisierungen herunterladen (Verwaltungsserveraktualisierungen, Firmwareaktualisierungen, UpdateXpress System Packs [BS-Einheitentreiber] und Repository-Pakete)		
download.lenovo.com	443	https
support.lenovo.com	443 und 80	https und http
Servicedatendaten an den Lenovo Support senden (Call Home) – nur XClarity Orchestrator		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 und höher) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 und früher)	443	https

DNS-Name	Ports	Protokolle
Regelmäßig Daten an Lenovo senden – nur XClarity Orchestrator		
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 und höher) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 und früher)	443	https
Informationen zur Garantie abrufen		
supportapi.lenovo.com	443	https und http

Proxy-Server

Wenn XClarity Orchestrator oder Ressourcenmanager keinen direkten Internetzugriff haben, stellen Sie sicher, dass sie für die Verwendung eines HTTP-Proxy-Servers konfiguriert sind (siehe Netzwerk konfigurieren in der Onlinedokumentation zu XClarity Orchestrator).

- Stellen Sie sicher, dass der Proxy-Server für die Verwendung der Basisauthentifizierung eingerichtet ist.
- Stellen Sie sicher, dass der Proxy-Server ein Non-Termination-Proxy ist.
- Stellen Sie sicher, dass der Proxy-Server ein Weiterleitungsproxy ist.
- Achten Sie darauf, dass ein Lastenausgleich konfiguriert ist, damit Sitzungen mit einem Proxy-Server gehalten werden (und kein Wechsel erfolgt).

Achtung: XClarity Management Hub muss über direkten Internetzugriff verfügen. Ein HTTP-Proxy-Server wird derzeit nicht unterstützt.

Portverfügbarkeit

Lenovo XClarity Orchestrator und Ressourcenmanager erfordern, dass bestimmte Ports geöffnet sind, um die Kommunikation zu erleichtern. Wenn die erforderlichen Ports von einem anderen Prozess blockiert oder verwendet werden, können einige Funktionen möglicherweise nicht ordnungsgemäß ausgeführt werden.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub und Lenovo XClarity Administrator sind RESTful-Anwendungen, die sicher über TCP an Port 443 kommunizieren.

XClarity Orchestrator

XClarity Orchestrator überwacht die in der folgenden Tabelle aufgeführten Ports und verwendet sie als Antwortports. Wenn sich der XClarity Orchestrator und alle verwalteten Ressourcen hinter einer Firewall befinden und Sie beabsichtigen, über einen Webbrowser *außerhalb* der Firewall auf diese Ressourcen zuzugreifen, müssen Sie sicherstellen, dass die erforderlichen Ports geöffnet sind.

Anmerkung: XClarity Orchestrator kann optional für ausgehende Verbindungen zu externen Services konfiguriert werden, z. B. LDAP, SMTP oder syslog. Diese Verbindungen erfordern möglicherweise zusätzliche Ports, die in der Regel vom Benutzer konfigurierbar und nicht in dieser Liste enthalten sind. Diese Verbindungen erfordern zudem möglicherweise Zugriff auf einen DNS-Server (Domain Name Service) über TCP oder UDP-Port 53, um externe Servernamen aufzulösen.

Service	Ausgehend (Ports auf externen Systemen geöffnet)	Eingehend (Ports auf der XClarity Orchestrator-Einheit geöffnet)
XClarity Orchestrator-Anwendung	• DNS – TCP/UDP an Port **53**	• HTTPS – TCP an Port **443**
Externe Authentifizierungsserver	• LDAP– TCP an Port **389**[1]	Nicht zutreffend

Service	Ausgehend (Ports auf externen Systemen geöffnet)	Eingehend (Ports auf der XClarity Orchestrator-Einheit geöffnet)
Ereignisweiterleitungsservices	• E-Mail-Server (SMTP) – UDP an Port **25**[1] • REST-Web-Service (HTTP) – UPD an Port **80**[1] • Splunk – UDP an Port **8088**[11], **8089**[1] • Syslog – UDP an Port **514**[1]	Nicht zutreffend
Lenovo Service (einschließlich Call-Home-Funktion)	• HTTPS (Call-Home-Funktion) – TCP an Port **443**	Nicht zutreffend

1. Dies ist der Standard-Port. Sie können diesen Port über die XClarity Orchestrator-Benutzerschnittstelle konfigurieren.

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 erfordert, dass bestimmte Ports geöffnet sind, um die Kommunikation zu erleichtern. Wenn die erforderlichen Ports von einem anderen Prozess blockiert oder verwendet werden, können einige Verwaltungshub-Funktionen möglicherweise nicht ordnungsgemäß ausgeführt werden.

Wenn sich Einheiten hinter einer Firewall befinden und Sie beabsichtigen, diese Einheiten über einen Verwaltungshub außerhalb der Firewall zu verwalten, müssen alle an der Kommunikation zwischen Verwaltungshub und dem Baseboard Management Controller beteiligten Ports in allen Einheiten geöffnet sein.

Service oder Komponente	Ausgehend (Ports zu externen Systemen geöffnet)	Eingehend (Ports auf Zieleinheiten geöffnet)
XClarity Management Hub 2.0	• DNS – UDP an Port **53** • NTP – UDP an Port **123** • HTTPS – TCP an Port **443** • SSDP – UDP an Port **1900** • DHCP – UDP an Port **67**	• HTTPS – TCP an Port **443** • SSDP Reploy – UDP an Ports **32768**-**65535**
ThinkSystem und ThinkAgile Server	• HTTPS – TCP an Port **443** • SSDP-Erkennung – UDP an Port **1900**	• HTTPS – TCP an Port **443**

XClarity Management Hub

XClarity Management Hub überwacht die in der folgenden Tabelle aufgeführten Ports und verwendet sie als Antwortports.

Service oder Komponente	Ausgehend (Ports auf externen Systemen geöffnet)	Eingehend (Ports auf der XClarity Management Hub Einheit geöffnet)
XClarity Management Hub-Einheit[1]	• DNS – TCP/UDP an Port **53**[2]	• HTTPS – TCP an Port **443** • MQTT – TCP an Port **8883**
ThinkEdge Client-Einheiten[3]	Nicht zutreffend	• MQTT – TCP an Port **8883**

1. Bei der Verwendung von XClarity Management Hub zur Verwaltung von Einheiten über XClarity Orchestrator müssen bestimmte Ports geöffnet sein, um die Kommunikation zu erleichtern. Wenn die

erforderlichen Ports von einem anderen Prozess blockiert oder verwendet werden, können einige XClarity Orchestrator-Funktionen möglicherweise nicht ordnungsgemäß ausgeführt werden.

2. XClarity Management Hub kann optional für ausgehende Verbindungen zu externen Services konfiguriert werden. Diese Verbindungen erfordern zudem möglicherweise Zugriff auf einen DNS-Server (Domain Name Service) über TCP oder UDP-Port 53, um externe Servernamen aufzulösen.
3. Wenn sich verwaltbare Einheiten hinter einer Firewall befinden und Sie beabsichtigen, diese Einheiten über einen XClarity Management Hub außerhalb der Firewall zu verwalten, müssen alle an der Kommunikation zwischen XClarity Management Hub und den Edge-Einheiten beteiligten Ports geöffnet sein.

XClarity Administrator

Bei der Verwendung von Lenovo XClarity Administrator zur Verwaltung von Einheiten über Lenovo XClarity Orchestrator müssen bestimmte Ports geöffnet sein, um die Kommunikation zu erleichtern. Wenn die erforderlichen Ports von einem anderen Prozess blockiert oder verwendet werden, können einige XClarity Orchestrator-Funktionen möglicherweise nicht ordnungsgemäß ausgeführt werden.

Informationen zu den Ports, die für XClarity Administrator geöffnet werden müssen, finden Sie unter Portverfügbarkeit in der Onlinedokumentation zu XClarity Administrator.

Hinweise zum Netzwerkbetrieb

Sie können Lenovo XClarity Management Hub so konfigurieren, dass eine einzelne Netzwerkschnittstelle (eth0) oder zwei separate Netzwerkschnittstellen (eth0 und eth1) für die Kommunikation verwendet werden.

Lenovo XClarity Management Hub kommuniziert über die folgenden Netzwerke.

- Das *Verwaltungsnetzwerk* wird für die Kommunikation zwischen Lenovo XClarity Management Hub und den verwalteten Einheiten verwendet.
- Das *Datennetzwerk* wird für die Kommunikation zwischen den Betriebssystemen verwendet, die auf den Servern und im Intranet des Unternehmens und/oder im Internet installiert sind.

Einzelne Schnittstelle (eth0)

Bei Verwendung einer einzelnen Netzwerkschnittstelle (eth0) finden Verwaltungs- und Datenkommunikation und die Betriebssystembereitstellung im selben Netzwerk statt.

Beachten Sie bei der Einrichtung von Lenovo XClarity Management Hub die folgenden Aspekte für die Definition der eth0-Netzwerkschnittstelle.

- Die Netzwerkschnittstelle muss so konfiguriert sein, dass sie die Ermittlung und Verwaltung von Einheiten unterstützt (einschließlich Firmwareaktualisierungen). Lenovo XClarity Management Hub muss mit allen Einheiten kommunizieren können, die es aus diesem Verwaltungsnetzwerk verwaltet.Lenovo XClarity Management Hub muss mit allen Einheiten kommunizieren können, die es aus dem Netzwerk verwaltet.
- Zum Implementieren von BS-Images muss die eth0-Schnittstelle über eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle verfügen, die für den Zugriff auf das Hostbetriebssystem verwendet wird.
- **Wichtig:** Das Implementieren eines gemeinsamen Daten- und Verwaltungsnetzwerks kann zu Unterbrechungen im Datenverkehr führen. Zum Beispiel können je nach Netzwerkkonfiguration Pakete verloren gehen oder es können Netzwerkkonnektivitätsprobleme auftreten (wenn etwa die Priorität des Serverdatenverkehrs hoch und die Priorität des von Management-Controllern ausgehenden Datenverkehrs gering ist). Das Verwaltungsnetzwerk verwendet neben TCP- auch UDP-Datenverkehr. UDP-Datenverkehr kann bei hohem Netzwerkverkehrsaufkommen eine niedrigere Priorität haben.

Zwei separate Schnittstellen (eth0 und eth1)

Wenn Sie zwei Netzwerkschnittstellen (eth0 und eth1) verwenden, können Sie die Netzwerke als physisch getrennte oder logisch getrennte Netzwerke einrichten.

Lesen Sie die folgenden Hinweise, bevor Sie die eth0- und eth1-Netzwerkschnittstellen definieren.

- Die eth0-Netzwerkschnittstelle muss mit dem Verwaltungsnetzwerk verbunden und so konfiguriert sein, dass Einheitenermittlung und -verwaltung unterstützt werden. Lenovo XClarity Management Hub muss mit allen Einheiten kommunizieren können, die es aus dem Verwaltungsnetzwerk verwaltet.
- Die eth1-Netzwerkschnittstelle kann so konfiguriert werden, dass eine Kommunikationsverbindung mit einem internen Datennetzwerk, einem öffentlichen Datennetzwerk oder mit beiden möglich ist.
- Zur Implementierung von Betriebssystem-Images muss die eth1-Netzwerkschnittstelle eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle haben, die für den Zugriff auf das Hostbetriebssystem verwendet wird.
- Funktionen können in beiden Netzwerken ausgeführt werden.
- Für logisch getrennte Netzwerke werden Pakete aus dem Verwaltungsnetzwerk und Pakete aus dem Datennetzwerk über dieselbe physische Verbindung übertragen. Verwenden Sie VLAN-Tagging bei allen Datenpaketen des Verwaltungsnetzwerks, um den Datenverkehr zwischen den beiden Netzwerken getrennt zu halten.

Hinweise zur IP-Adresse

Lesen Sie vor der Netzwerkkonfiguration die folgenden Hinweise zur IP-Adresse.

- Das Ändern der IP-Adresse der virtuellen Einheit, nachdem XClarity Management Hub betriebsbereit ist, verursacht Verbindungsprobleme mit XClarity Orchestrator und allen verwalteten Einheiten. Wenn Sie die IP-Adresse ändern müssen, trennen Sie XClarity Management Hub vom XClarity Orchestrator und heben Sie die Verwaltung aller verwalteten Einheiten auf, bevor Sie die IP-Adresse ändern. Verwalten Sie die Einheiten erneut und verbinden Sie XClarity Management Hub wieder mit XClarity Orchestrator, nachdem die IP-Adressänderung abgeschlossen ist.
- Konfigurieren Sie die Einheiten und die Gehäusekomponenten so, dass möglichst wenige IP-Adressen geändert werden. Ziehen Sie in Betracht, statische IP-Adressen anstelle des Dynamic Host Configuration Protocol (DHCP) zu verwenden. Stellen Sie bei Verwendung von DHCP sicher, dass die IP-Adressänderungen minimiert werden, z. B. durch Basieren der DHCP-Adresse auf einer MAC-Adresse oder dem Konfigurieren von DHCP ohne Ablauf der Zugangsberechtigung.Wenn sich die IP-Adresse einer verwalteten Einheit (außer einer ThinkEdge Client-Einheit) ändert, müssen Sie die Verwaltung der Einheit aufheben und sie anschließend erneut verwalten.
- Network Address Translation (NAT), die einen IP-Adressraum in einen anderen neu zuordnet, wird nicht unterstützt.
- Zur Verwaltung der folgenden Einheiten müssen die Netzwerkschnittstellen mit einer IPv4-Adresse konfiguriert werden. IPv6-Adressen werden nicht unterstützt.
  - ThinkServer-Server
  - Lenovo Storage-Einheit
- Verwaltung von RackSwitch-Einheiten mit IPv6-Link-Local über einen Daten- oder Verwaltungsanschluss wird nicht unterstützt.

Hinweise zu hoher Verfügbarkeit

Um hohe Verfügbarkeit für Lenovo XClarity Orchestrator zu konfigurieren, verwenden Sie die Hochverfügbarkeitsfunktionen, die Bestandteil des Hostbetriebssystems sind.

Microsoft Hyper-V

Verwenden Sie die Hochverfügbarkeitsfunktion, die für die Hyper-V-Umgebung bereitgestellt wird.

VMware ESXi

In einer VMware-Umgebung mit hoher Verfügbarkeit werden mehrere Hosts als Cluster konfiguriert. Durch gemeinsam genutzten Speicher wird das Datenträgerimage einer virtuellen Maschine (Virtual Machine, VM) für die Hosts im Cluster verfügbar gemacht. Die VM wird nur auf einem Host zur gleichen Zeit ausgeführt. Bei einem Problem mit der VM wird eine weitere Instanz dieser VM auf einem Sicherungshost gestartet.

VMware High Availability erfordert die folgenden Komponenten.

- Mindestens zwei Hosts, auf denen ESXi installiert ist. Diese Hosts werden Teil des VMware-Clusters.
- Einen dritten Host, auf dem VMware vCenter installiert ist.

  Tipp: Stellen Sie sicher, dass Sie eine VMware vCenter-Version installieren, die mit den ESXi-Versionen kompatibel ist, die auf den im Cluster genutzten Hosts installiert sind.

  VMware vCenter kann auf einem der Hosts installiert werden, die im Cluster verwendet werden. Wenn dieser Host allerdings ausgeschaltet oder nicht einsetzbar ist, geht auch der Zugriff auf die VMware vCenter-Schnittstelle verloren.
- Gemeinsam genutzter Speicher (Datenspeicher), auf den von allen Hosts im Cluster zugegriffen werden kann. Sie können jeden Typ gemeinsam genutzten Speicher verwenden, der von VMware unterstützt wird. Der Datenspeicher wird von VMware verwendet, um zu bestimmen, ob eine VM einen Failover zu einem anderen Host ausführen soll (Taktsignale).

Kapitel 2. XClarity Management Hub für Edge-Client-Einheiten konfigurieren

Wenn Sie zum ersten Mal auf den Lenovo XClarity Management Hub zugreifen, müssen Sie bestimmte Schritte für die Erstkonfiguration des XClarity Management Hub ausführen.

Vorgehensweise

Gehen Sie bei der Erstkonfiguration von XClarity Management Hub wie folgt vor.

Schritt 1. Melden Sie sich bei der XClarity Management Hub-Webschnittstelle an.

Schritt 2. Lesen und akzeptieren Sie die Lizenzvereinbarung.

Schritt 3. Erstellen Sie zusätzliche Benutzeraccounts.

Schritt 4. Konfigurieren Sie den Netzwerkzugriff einschließlich der IP-Adressen für Daten- und Verwaltungsnetzwerke.

Schritt 5. Stellen Sie das Datum und die Uhrzeit ein.

Schritt 6. Registrieren Sie den XClarity Management Hub beim Orchestrator-Server.

Bei XClarity Management Hub für Edge-Client-Einheiten anmelden

Sie können die XClarity Management Hub-Webschnittstelle von jedem Computer aus starten, der über eine Netzwerkverbindung zur virtuellen XClarity Management Hub-Maschine verfügt.

Vorbereitende Schritte

Vergewissern Sie sich, dass Sie einen der folgenden unterstützten Webbrowser verwenden:
- Chrome 80.0 oder höher
- Firefox ESR 68.6.0 oder höher
- Microsoft Edge 40.0 oder höher
- Safari 13.0.4 oder höher (ausgeführt auf macOS 10.13 oder höher)

Der Zugriff auf die Webschnittstelle erfolgt über eine sichere Verbindung. Stellen Sie sicher, dass Sie **https** verwenden.

Wenn Sie XClarity Management Hub über Fernzugriff konfigurieren, muss eine Verbindung zum selben Layer-2-Netzwerk bestehen. Darauf muss von einer nicht gerouteten Adresse zugegriffen werden, bis die Erstkonfiguration abgeschlossen ist. Sie sollten daher möglicherweise von einer anderen VM auf XClarity Management Hub zugreifen, die eine Verbindung zu XClarity Management Hub aufweist. Beispielsweise können Sie über eine andere VM auf dem Host, auf der XClarity Management Hub installiert ist, auf XClarity Management Hub zugreifen.

Nach 60 Minuten werden Benutzersitzungen von XClarity Management Hub unabhängig von der Benutzeraktivität automatisch beendet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um sich bei der XClarity Management Hub-Webschnittstelle anzumelden.

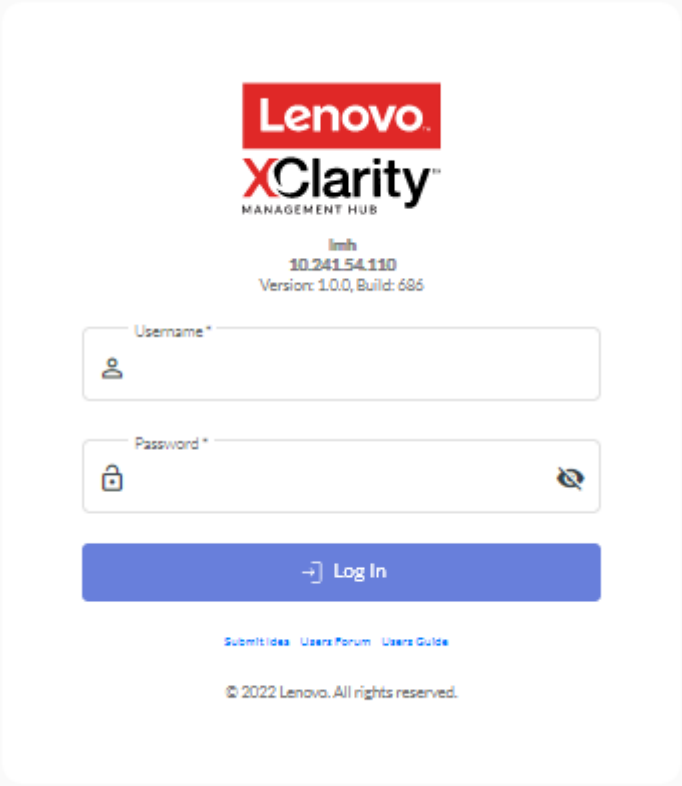
Schritt 1. Öffnen Sie im Browser die IP-Adresse von XClarity Management Hub.
`https://<IPv4_address>`

Beispiel:
`https://192.0.2.10`

Die verwendete IP-Adresse hängt davon ab, wie Ihre Umgebung eingerichtet ist.

- Wenn Sie eine IPv4-Adresse in eth0_config angegeben haben, verwenden Sie diese, um auf XClarity Management Hub zuzugreifen.
- Wenn ein DHCP-Server in derselben Übertragungsdomäne wie XClarity Management Hub eingerichtet ist, verwenden Sie die IPv4-Adresse, die in der Konsole der virtuellen Maschine von XClarity Management Hub angezeigt wird, für Zugriff auf den XClarity Management Hub.
- Wenn Sie eth0- und eth1-Netzwerke auf separaten Subnetzen haben und DHCP auf beiden Subnetzen verwendet wird, verwenden Sie die IP-Adresse von *eth1* für den Zugriff auf die Webschnittstelle bei der Erstkonfiguration. Beim ersten Starten von XClarity Management Hub wird eth0 und eth1 eine von DHCP zugeordnete IP-Adresse zugewiesen und das Standard-Gateway XClarity Management Hub wird für *eth1* auf das von DHCP zugeordnete Gateway festgelegt.

Die Seite für die erste Anmeldung bei XClarity Management Hub wird angezeigt:



Schritt 2. Wählen Sie die gewünschte Sprache aus der Dropdown-Liste **Sprache** aus.

Anmerkung: Die Konfigurationseinstellungen und Werte, die von den verwalteten Einheiten bereitgestellt werden, sind möglicherweise nur in Englisch verfügbar.

Schritt 3. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie auf **Anmelden**.

Wenn Sie sich zum ersten Mal bei XClarity Management Hub anmelden, geben Sie die Standard-Anmeldeinformationen **USERID** und **PASSW0RD** (wobei 0 = NULL ist) ein.

Schritt 4. Lesen und akzeptieren Sie die Lizenzvereinbarung.

Schritt 5. Wenn Sie sich zum ersten Mal mit den Standard-Anmeldeinformationen angemeldet haben, werden Sie aufgefordert, das Kennwort zu ändern. Standardmäßig müssen Kennwörter **8–256** Zeichen enthalten und die folgenden Kriterien erfüllen.

Wichtig: Es wird empfohlen, sichere Kennwörter mit mindestens 16 Zeichen zu verwenden.
- (1) Muss mindestens einen Großbuchstaben enthalten
- (2) Muss mindestens einen Kleinbuchstaben enthalten
- (3) Muss mindestens eine Zahl enthalten
- (4) Muss mindestens ein Sonderzeichen enthalten
- (5) Darf nicht identisch mit dem Benutzernamen sein

Schritt 6. Wenn Sie sich zum ersten Mal angemeldet haben, müssen Sie auswählen, ob das aktuelle selbst signierte Zertifikat oder ein extern von einer Zertifizierungsstelle signiertes Zertifikat verwendet werden soll. Wenn Sie ein extern signiertes Zertifikat auswählen wird die Seite „Serverzertifikat“ angezeigt.

Achtung: Das selbst signierte Zertifikat ist nicht sicher. Es wird empfohlen, ein eigenes extern signiertes Zertifikat zu generieren und zu installieren.

Informationen zur Verwendung eines extern signierten Zertifikats finden Sie unter Vertrauenswürdiges, extern signiertes Serverzertifikat für XClarity Management Hub für Edge-Client-Einheiten installieren.

Nach dieser Aufgabe

Sie können die folgenden Aktionen über das Menü **Benutzerkonto** ( ) oben rechts in der XClarity Management Hub-Webschnittstelle durchführen.

- Sie können sich durch Klicken auf **Abmelden** von der aktuellen Sitzung abmelden. Die XClarity Management Hub-Anmeldeseite wird angezeigt.
- Stellen Sie Fragen und erhalten Sie Antworten auf der Community-Forumswebsite für Lenovo XClarity.
- Senden Sie Ideen zu XClarity Management Hub, indem Sie im Menü **Benutzeraktionen** ( ) rechts oben in der Webschnittstelle auf **Ideen einreichen** klicken oder direkt zur Website für Lenovo XClarity Ideation navigieren.
- Die Onlinedokumentation finden Sie mit einem Klick auf **Benutzerhandbuch**.
- Sie können Informationen zur XClarity Management Hub-Version durch Klicken auf **Info** anzeigen.
- Sie können die Sprache der Benutzerschnittstelle durch Klicken auf **Sprache ändern** ändern. Die folgenden Sprachen werden unterstützt.
  - Englisch (en)
  - Vereinfachtes Chinesisch (zh-CN)
  - Traditionelles Chinesisch (zh-TW)
  - Französisch (fr)
  - Deutsch (de)
  - Italienisch (it)
  - Japanisch (ja)
  - Koreanisch (ko)
  - Portugiesisch, Brasilien (pt-BR)
  - Russisch (ru)
  - Spanisch (es)
  - Thailändisch (th)

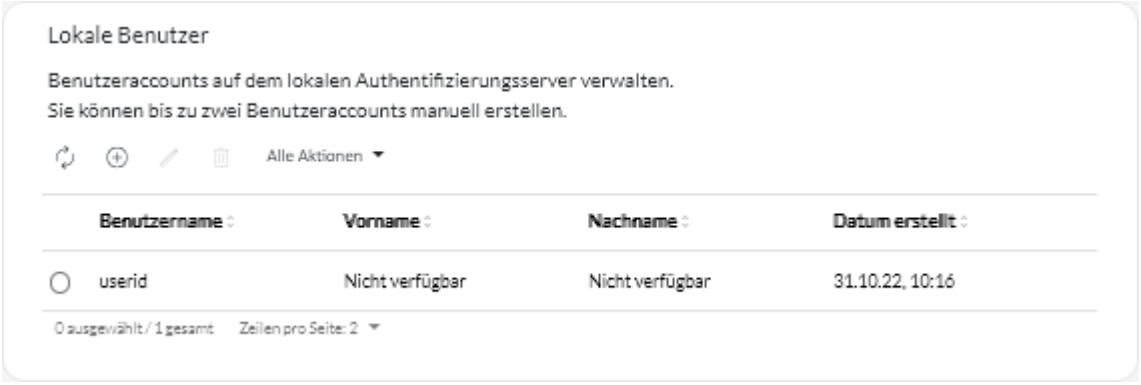
Benutzeraccounts für Lenovo XClarity Management Hub für Edge-Client-Einheiten erstellen

Sie können bis zu 10 Benutzeraccounts für Lenovo XClarity Management Hub erstellen.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Benutzeraccount zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Management Hub auf **Sicherheit (⚙) → Lokale Benutzer**, um die Übersicht Lokale Benutzer anzuzeigen.



Schritt 2. Klicken Sie auf das Symbol **Erstellen** (⊕), um einen Benutzer zu erstellen. Das Dialogfenster Neuen Benutzer erstellen wird angezeigt.

Schritt 3. Tragen Sie die folgenden Informationen ein.

- Geben Sie einen eindeutigen Benutzernamen ein. Sie können bis zu 32 Zeichen angeben, darunter alphanumerische Zeichen, Punkt (.), Bindestrich (-) und Unterstrich (_).

  Anmerkung: Bei Benutzernamen wird keine Groß-/Kleinschreibung beachtet.

- Geben Sie das neue Kennwort ein und bestätigen Sie es. Standardmäßig müssen Kennwörter **8**–**256** Zeichen enthalten und die folgenden Kriterien erfüllen.

  Wichtig: Es wird empfohlen, sichere Kennwörter mit mindestens 16 Zeichen zu verwenden.
  - (1) Muss mindestens einen Großbuchstaben enthalten
  - (2) Muss mindestens einen Kleinbuchstaben enthalten
  - (3) Muss mindestens eine Zahl enthalten
  - (4) Muss mindestens ein Sonderzeichen enthalten
  - (5) Darf nicht identisch mit dem Benutzernamen sein

Schritt 4. Klicken Sie auf **Erstellen**.

Der Benutzeraccount wird zur Tabelle hinzugefügt.

Nach dieser Aufgabe

In der Übersicht Lokale Benutzer können Sie die folgenden Aktionen ausführen.

- Ändern Sie das Kennwort und die Eigenschaften für Ihren Benutzeraccount, indem Sie auf das Symbol **Bearbeiten** (✎) klicken. Beachten Sie, dass Kennwörter nicht ablaufen.
- Sie löschen einen ausgewählten Benutzer über das Symbol **Löschen** (🗑).

Netzwerkeinstellungen für XClarity Management Hub für Edge-Client-Einheiten konfigurieren

Sie können eine einzelne IPv4-Netzwerkschnittstelle und Internet-Routingeinstellungen konfigurieren.

Vorbereitende Schritte

Lesen Sie vor der Netzwerkkonfiguration die Hinweise zum Netzwerkbetrieb (siehe Hinweise zum Netzwerkbetrieb).

Vorgehensweise

Um die Netzwerkeinstellungen zu konfigurieren, klicken Sie auf **Verwaltung (⚙) → Netzwerk** auf der Menüleiste von XClarity Management Hub und führen Sie einen oder mehrere der folgenden Schritte aus.

- **IP-Einstellungen konfigurieren**Klicken Sie für die eth0-Schnittstelle auf die Registerkarte **Eth0-Schnittstelle**, konfigurieren Sie die entsprechenden IPv4-Adresseinstellungen und klicken Sie auf **Übernehmen**.

  Achtung:

  – Das Ändern der IP-Adresse der virtuellen Einheit, nachdem XClarity Management Hub betriebsbereit ist, verursacht Verbindungsprobleme mit XClarity Orchestrator und allen verwalteten Einheiten. Wenn Sie die IP-Adresse ändern müssen, trennen Sie XClarity Management Hub vom XClarity Orchestrator und heben Sie die Verwaltung aller verwalteten Einheiten auf, bevor Sie die IP-Adresse ändern. Verwalten Sie die Einheiten erneut und verbinden Sie XClarity Management Hub wieder mit XClarity Orchestrator, nachdem die IP-Adressänderung abgeschlossen ist.

  Momentan werden nur Adressen im Format IPv4 unterstützt.

  – **IPv4-Einstellungen**. Sie können die IP-Zuordnungsmethode, die IPv4-Adresse, die Netzwerkmaske und das Standard-Gateway konfigurieren.Für die IP-Zuordnungsmethode können Sie eine statisch zugewiesene IP-Adresse verwenden oder eine IP-Adresse von einem DHCP-Server abrufen. Wenn Sie eine statische IP-Adresse verwenden, müssen Sie eine IP-Adresse, eine Netzwerkmaske und ein Standard-Gateway angeben.

    Das Standard-Gateway muss eine gültige IP-Adresse aufweisen und dieselbe Netzwerkmaske (dasselbe Subnetz) wie die aktivierte Schnittstelle (eth0) verwenden.

    Wenn eine der beiden Schnittstellen eine IP-Adresse über DHCP abruft, verwendet das Standard-Gateway ebenfalls DHCP.

- **Internet-Routingeinstellungen konfigurieren**Konfigurieren Sie in der Übersicht DNS-Konfiguration optional die Einstellungen für DNS (Domain Name System). Klicken Sie dann auf **Übernehmen**.

  Momentan werden nur Adressen im Format IPv4 unterstützt.

  Sie können die IP-Adresse für den DNS-Server ändern.

  Der vollständig qualifizierte Domänenname (FQDN) und Hostname für den DNS-Server sind dieselben wie beim XClarity Management Hub-Server und können nicht geändert werden.

Datum und Uhrzeit für XClarity Management Hub für Edge-Client-Einheiten konfigurieren

Sie müssen mindestens einen (und maximal vier) NTP-Server (Network Time Protocol) einrichten, um die Zeitstempel zwischen XClarity Management Hub und allen verwalteten Einheiten zu synchronisieren.

Vorbereitende Schritte

Es muss möglich sein, über das Netzwerk auf jeden NTP-Server zuzugreifen. Ziehen Sie in Betracht, den NTP-Server auf dem lokalen System einzurichten, auf dem auch XClarity Management Hub ausgeführt wird.

Wenn Sie die Uhrzeit auf dem NTP-Server ändern, kann es einige Zeit dauern, bis die neue Uhrzeit in XClarity Management Hub synchronisiert ist.

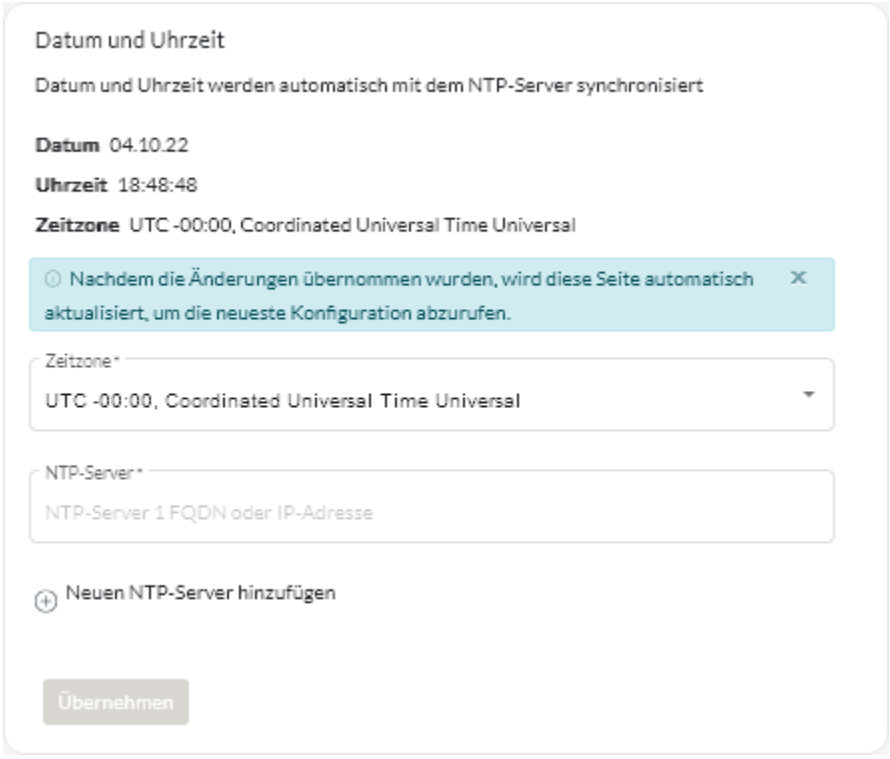
Achtung: Die virtuelle XClarity Management Hub-Einheit und ihr Host müssen mit derselben Zeitquelle synchronisiert werden, um eine unbeabsichtigte fehlerhafte Zeitsynchronisation zwischen XClarity Management Hub und dem Host zu verhindern. In der Regel ist der Host so konfiguriert, dass eine Zeitsynchronisation mit seiner virtuellen Einheit erfolgt. Wenn bei XClarity Management Hub für die Synchronisation eine andere Quelle als die des Hosts festgelegt ist, müssen Sie die Host-Zeitsynchronisation zwischen der virtuellen XClarity Management Hub-Einheit und ihrem Host deaktivieren.

- Befolgen Sie für ESXi die Anweisungen auf der VMware – Website zur Deaktivierung der Zeitsynchronisation.

Vorgehensweise

Gehen Sie wie folgt vor, um das Datum und die Uhrzeit für XClarity Management Hub festzulegen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Management Hub auf **Verwaltung (⚙) → Datum und Uhrzeit**, um die Übersicht Datum und Uhrzeit anzuzeigen.



Schritt 2. Wählen Sie die Zeitzone für den Host von XClarity Management Hub aus.

Sofern in der ausgewählten Zeitzone die Sommerzeit gilt, wird die Uhrzeit automatisch angepasst.

Schritt 3. Geben Sie den Hostnamen oder die IP-Adresse für jeden NTP-Server im Netzwerk an. Sie können bis zu vier NTP-Server definieren.

Schritt 4. Klicken Sie auf **Übernehmen**.

Sicherheitszertifikate für Lenovo XClarity Management Hub für Edge-Client-Einheiten verwalten

Lenovo XClarity Management Hub verwendet SSL-Zertifikate für die Einrichtung von sicheren und vertrauenswürdigen Kommunikationsverbindungen zwischen Lenovo XClarity Management Hub und den verwalteten Einheiten sowie für die Herstellung von Kommunikationsverbindungen mit Lenovo XClarity Management Hub durch Benutzer oder verschiedenen Services. Standardmäßig verwenden Lenovo XClarity Management Hub und XClarity Orchestrator selbst signierte, von XClarity Orchestrator generierte Zertifikate, die von einer internen Zertifizierungsstelle ausgestellt wurden.

Vorbereitende Schritte

Dieser Abschnitt richtet sich an Administratoren mit einem grundlegenden Verständnis der SSL-Standards und SSL-Zertifikate, einschließlich ihrer Art und Verwaltung. Allgemeine Informationen zu Zertifikaten mit öffentlichen Schlüsseln finden Sie unter X.509-Webseite in Wikipedia und Webseite „Internet X.509 Public Key-Infrastrukturzertifikat und Zertifikatsperrliste (CRL) Profil (RFC5280)“.

Zu dieser Aufgabe

Das eindeutige Standardserverzertifikat, das in jeder Instanz von Lenovo XClarity Management Hub generiert wird, bietet eine ausreichende Sicherheit für viele Umgebungen. Sie können die Zertifikate wahlweise von Lenovo XClarity Management Hub verwalten lassen oder eine aktivere Rolle übernehmen und die Serverzertifikate selbst anpassen und ersetzen. Lenovo XClarity Management Hub bietet verschiedene Optionen zum Anpassen von Zertifikaten an Ihre Umgebung. Beispielsweise können Sie Folgendes auswählen:

- Generieren Sie ein neues Schlüsselpaar, indem Sie die interne Zertifizierungsstelle und/oder das Endserverzertifikat erneut generieren, das spezifische Werte für Ihre Organisation verwendet.
- Generieren Sie eine Zertifikatssignieranforderung (CSR), die an eine Zertifizierungsstelle Ihrer Wahl gesendet werden kann. Hier wird ein benutzerdefiniertes Zertifikat signiert, das zu Lenovo XClarity Management Hub hochgeladen und als Endserverzertifikat für alle gehosteten Services verwendet werden kann.
- Laden Sie das Serverzertifikat in Ihr lokales System herunter und importieren Sie es in die Liste mit vertrauenswürdigen Zertifikaten im Webbrowser.

Lenovo XClarity Management Hub bietet verschiedene Services, die eingehende SSL/TLS-Verbindungen akzeptieren. Wenn sich ein Client, z. B. ein Webbrowser, mit einem dieser Services verbindet, stellt Lenovo XClarity Management Hub sein *Serverzertifikat* bereit, das vom Client identifiziert wird, der eine Verbindung herstellen will. Der Client muss über eine Liste mit Zertifikaten verfügen, denen er vertraut. Wenn das Serverzertifikat von Lenovo XClarity Management Hub nicht in der Liste des Client enthalten ist, trennt der Client die Verbindung mit Lenovo XClarity Management Hub, damit keine vertraulichen Informationen mit einer nicht vertrauenswürdigen Quelle ausgetauscht werden.

Lenovo XClarity Management Hub fungiert bei der Kommunikation mit verwalteten Einheiten und externen Services als Client. In diesem Fall stellen die verwaltete Einheit oder der externe Service ihr jeweiliges Serverzertifikat für ihre Authentifizierung bei Lenovo XClarity Management Hub bereit. Lenovo XClarity Management Hub hält eine Liste von vertrauenswürdigen Zertifikaten vor. Wenn das *vertrauenswürdige Zertifikat*, das von der verwalteten Einheit oder dem externen Service bereitgestellt wird, nicht in der Liste vorhanden ist, trennt Lenovo XClarity Management Hub die entsprechende Verbindung, damit keine vertraulichen Informationen mit einer nicht vertrauenswürdigen Quelle ausgetauscht werden.

Die folgende Zertifikatskategorie wird von Lenovo XClarity Management Hub Services verwendet und sollte von allen Clients, die eine Verbindung herstellen, als vertrauenswürdig gekennzeichnet werden.

- **Serverzertifikat**. Während des ersten Boots werden ein eindeutiger Schlüssel und ein selbst signiertes Zertifikat generiert. Diese werden als die Standard-Stammzertifizierungsstelle verwendet, die auf der Seite „Zertifizierungsstelle“ in den Sicherheitseinstellungen von Lenovo XClarity Management Hub verwaltet wird. Es ist nicht notwendig, das Stammzertifikat neu zu generieren, sofern kein Schlüssel kompromittiert wurde oder eine Unternehmensrichtlinie besteht, nach der alle Zertifikate regelmäßig ersetzt werden müssen (siehe Selbst signiertes Serverzertifikat für XClarity Management Hub für Edge-Client-Einheiten neu generieren).Bei der Erstkonfiguration wird auch ein separater Schlüssel generiert und es wird ein Serverzertifikat erstellt, das durch die interne Zertifizierungsstelle signiert wird. Dieses Zertifikat dient als standardmäßiges Lenovo XClarity Management Hub-Serverzertifikat. Es wird automatisch jedes Mal neu generiert, wenn Lenovo XClarity Management Hub ermittelt, dass seine Netzwerkadressen (IP- oder DNS-Adressen) sich geändert haben. So wird sichergestellt, dass das Zertifikat die korrekten Adressen für den Server enthält. Das Zertifikat kann nach Bedarf angepasst und generiert werden (siehe Selbst signiertes Serverzertifikat für XClarity Management Hub für Edge-Client-Einheiten neu generieren).

  Sie können festlegen, dass ein extern signiertes Serverzertifikat anstelle des standardmäßig selbst signierten Serverzertifikats verwendet wird, indem Sie eine Zertifikatssignieranforderung (CSR) generieren, die CSR von einer privaten oder kommerziellen Stammzertifizierungsstelle signieren lassen und dann die vollständige Zertifikatskette in Lenovo XClarity Management Hub importieren (siehe Vertrauenswürdiges, extern signiertes Serverzertifikat für XClarity Management Hub für Edge-Client-Einheiten installieren).

  Wenn Sie das standardmäßig selbst signierte Serverzertifikat verwenden möchten, wird empfohlen, das Serverzertifikat in Ihren Webbrowser als vertrauenswürdige Stammzertifizierungsstelle zu importieren, um Fehlernachrichten im Browser zu vermeiden (siehe Serverzertifikat in einen Webbrowser für Lenovo XClarity Management Hub für Edge-Client-Einheiten importieren).
- **Vom Betriebssystem implementiertes Zertifikat**. Der Betriebssystem-Implementierungsservice verwendet ein separates Zertifikat, um zu gewährleisten, dass der Betriebssystem-Installer während des Implementierungsprozesses eine sichere Verbindung mit dem Implementierungsservice herstellen kann. Wenn der Schlüssel kompromittiert wurde, können Sie ihn neu generieren, indem Sie Lenovo XClarity Management Hub neu starten.

Selbst signiertes Serverzertifikat für XClarity Management Hub für Edge-Client-Einheiten neu generieren

Sie können ein neues Serverzertifikat generieren, um das aktuelle selbst signierte Lenovo XClarity Management Hub-Serverzertifikat zu ersetzen oder ein von XClarity Management Hub generiertes Zertifikat wiederherzustellen, wenn XClarity Management Hub aktuell ein angepasstes extern signiertes Serverzertifikat verwendet. Das neue selbst signierte Serverzertifikat wird von XClarity Management Hub für den HTTPS-Zugriff verwendet.

Vorbereitende Schritte

Achtung: Wenn Sie das XClarity Management Hub-Serverzertifikat mithilfe einer neuen Stamm-Zertifizierungsstelle erneut generieren, verliert XClarity Management Hub die Verbindung zu den verwalteten Einheiten und Sie müssen die Einheiten erneut verwalten. Wenn Sie das XClarity Management Hub-Serverzertifikat erneut generieren, ohne die Stamm-Zertifizierungsstelle zu ändern (z. B. bei einem abgelaufenen Zertifikat), müssen die Einheiten nicht erneut verwaltet werden.

Zu dieser Aufgabe

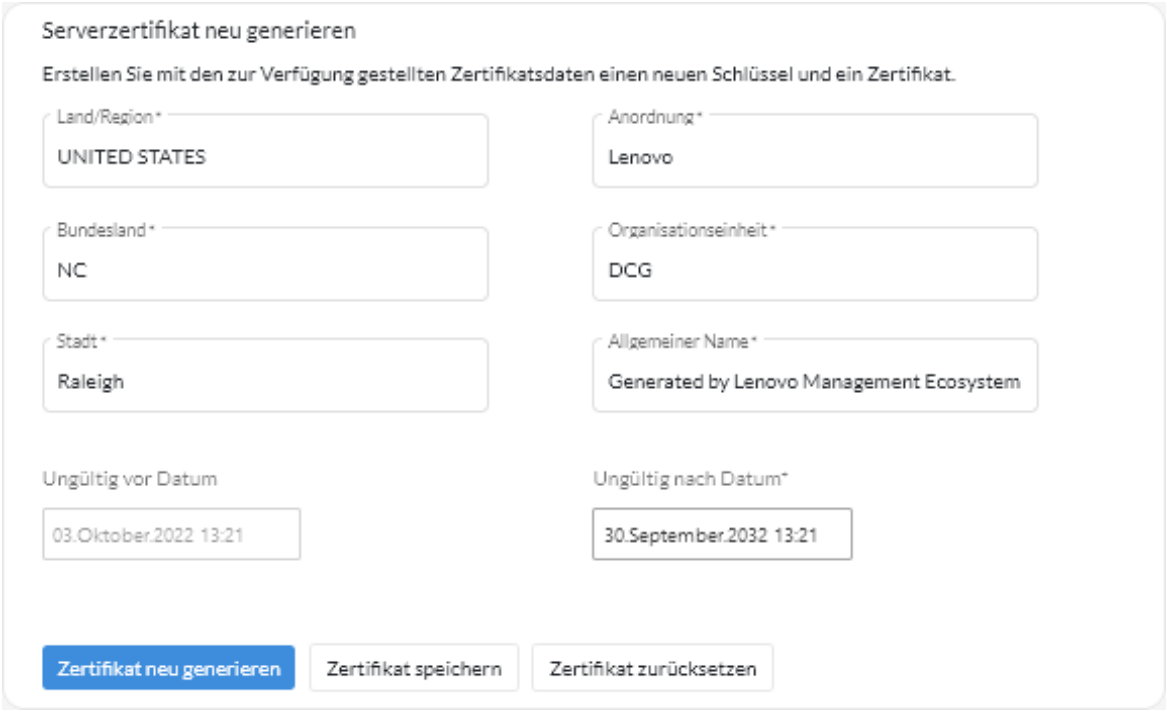
Das derzeit verwendete Serverzertifikat, ob selbst oder extern signiert, wird weiterhin genutzt, bis ein neues Serverzertifikat generiert, signiert und installiert wurde.

Wichtig: Wenn das Serverzertifikat geändert wird, wird der Verwaltungshub neu gestartet und alle Benutzersitzungen werden beendet. Benutzer müssen sich erneut anmelden, um weiter in der Webschnittstelle zu arbeiten.

Vorgehensweise

Gehen Sie wie folgt vor, um ein selbst signiertes XClarity Management Hub-Serverzertifikat zu generieren.

Schritt 1. Navigieren Sie in der Menüleiste von XClarity Management Hub zu **Sicherheit (⚙) → Serverzertifikat**, um die Übersicht **Selbst signiertes Serverzertifikat neu generieren** anzuzeigen.



Schritt 2. Geben Sie in der Übersicht **Selbst signiertes Serverzertifikat neu generieren** Daten in die Felder für die Anforderung ein.

- Zweistelliger ISO 3166-Code für das ursprüngliche Land oder die ursprüngliche Region, der der Zertifizierungsorganisation zugeordnet werden soll (z. B. US für die Vereinigten Staaten).
- Vollständiger Name des Bundesstaats/-lands, das dem Zertifikat zugeordnet werden soll (z. B. Kalifornien oder New Brunswick)
- Vollständiger Name der Stadt, die dem Zertifikat zugeordnet werden soll (z. B. San Jose). Die Länge des Werts darf 50 Zeichen nicht überschreiten.
- Unternehmen, dem das Zertifikat gehören soll. In der Regel handelt es sich hierbei um den eingetragenen Namen eines Unternehmens. Dies sollte alle Suffixe umfassen wie etwa Ltd., Inc. oder GmbH (z. B. ACME International Ltd.). Die Länge des Werts darf 60 Zeichen nicht überschreiten.
- (Optional) Organisationseinheit, der das Zertifikat gehören soll (z. B. Sparte ABC). Die Länge des Werts darf 60 Zeichen nicht überschreiten.
- Allgemeiner Name des Zertifikatsinhabers. In der Regel handelt es sich hierbei um den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Servers, der das Zertifikat verwendet (z. B. `www.domainname.com` oder `192.0.2.0`). Die Länge des Werts darf 63 Zeichen nicht überschreiten.

  Anmerkung: Derzeit hat dieses Attribut keine Auswirkungen auf das Zertifikat.
- Datum und Uhrzeit, ab wann das Serverzertifikat nicht mehr gültig ist

  Anmerkung: Derzeit haben diese Attribute keine Auswirkungen auf das Zertifikat.

Anmerkung: Sie können die alternativen Namen bei der Neugenerierung des Serverzertifikats nicht ändern.

Schritt 3. Klicken Sie auf **Selbst signiertes Serverzertifikat neu generieren**, um das selbst signierte Zertifikat neu zu generieren. Klicken Sie zur Bestätigung dann auf **Zertifikat neu generieren**.Der Verwaltungshub wird neu gestartet und alle aktiven Benutzersitzungen werden beendet.

Schritt 4. Melden Sie sich wieder im Webbrowser an.

Nach dieser Aufgabe

In der Übersicht Selbst signiertes Serverzertifikat neu generieren können Sie die folgenden Aktionen ausführen.

- Speichern Sie das aktuelle Serverzertifikat im PEM-Format auf Ihrem lokalen System, indem Sie auf **Zertifikat speichern** klicken.
- Generieren Sie das Serverzertifikat mithilfe der Standardeinstellung erneut, indem Sie auf **Zertifikat zurücksetzen** klicken. Wenn Sie dazu aufgefordert werden, drücken Sie Strg+F5, um den Browser zu aktualisieren und die Verbindung zur Webschnittstelle wiederherzustellen.

Vertrauenswürdiges, extern signiertes Serverzertifikat für XClarity Management Hub für Edge-Client-Einheiten installieren

Sie können ein von einer privaten oder einer kommerziellen Zertifizierungsstelle (Certificate Authority, CA) signiertes, vertrauenswürdiges Serverzertifikat verwenden. Wenn Sie ein extern signiertes Serverzertifikat verwenden möchten, generieren Sie eine Zertifikatssignieranforderung (CSR). Importieren Sie das daraus resultierende Serverzertifikat, um das vorhandene Serverzertifikat zu ersetzen.

Vorbereitende Schritte

Achtung:

- Wenn Sie ein extern signiertes Lenovo XClarity Management Hub-Serverzertifikat mithilfe einer neuen Stamm-Zertifizierungsstelle installieren, verliert XClarity Management Hub die Verbindung zu den verwalteten Einheiten und Sie müssen die Einheiten erneut verwalten. Wenn Sie ein extern signiertes Lenovo XClarity Management Hub-Serverzertifikat installieren, ohne die Stamm-Zertifizierungsstelle zu ändern (z. B. bei einem abgelaufenen Zertifikat), müssen die Einheiten nicht erneut verwaltet werden.
- Wenn neue Einheiten hinzugefügt werden, nachdem die CSR generiert wurde und bevor das signierte Serverzertifikat importiert wird, müssen diese Einheiten neu gestartet werden, um das neue Serverzertifikat zu erhalten.

Zu dieser Aufgabe

Es hat sich bewährt, immer v3-signierte Zertifikate zu verwenden.

Das extern signierte Serverzertifikat muss von der Zertifikatssignieranforderung erstellt werden, die als letzte mithilfe der Schaltfläche **CSR-Datei generieren** generiert wurde.

Der Inhalt des extern signierten Serverzertifikats muss ein Zertifikatspaket sein, das die gesamte Signierungskette der Zertifizierungsstelle enthält, einschließlich des Stammzertifikats der Zertifizierungsstelle, eventueller Zwischenzertifikate und des Serverzertifikats.

Wenn das neue Serverzertifikat nicht von einem vertrauenswürdigen Drittanbieter signiert wurde, wird das nächste Mal, wenn Sie eine Verbindung mit Lenovo XClarity Management Hub herstellen, im Webbrowser eine Sicherheitsnachricht angezeigt. In einem Dialogfeld werden Sie aufgefordert, das neue Zertifikat im Browser zu akzeptieren. Sie können das Serverzertifikat in die Liste vertrauenswürdiger Zertifikate Ihres

Webbrowsers importieren, um die Sicherheitsnachrichten zu vermeiden (siehe Serverzertifikat in einen Webbrowser für Lenovo XClarity Management Hub für Edge-Client-Einheiten importieren).

XClarity Management Hub beginnt, das neue Serverzertifikat zu verwenden, ohne die aktuelle Sitzung zu beenden. Neue Sitzungen werden mit dem neuen Zertifikat gestartet. Um das neue verwendete Zertifikat zu verwenden, starten Sie den Webbrowser neu.

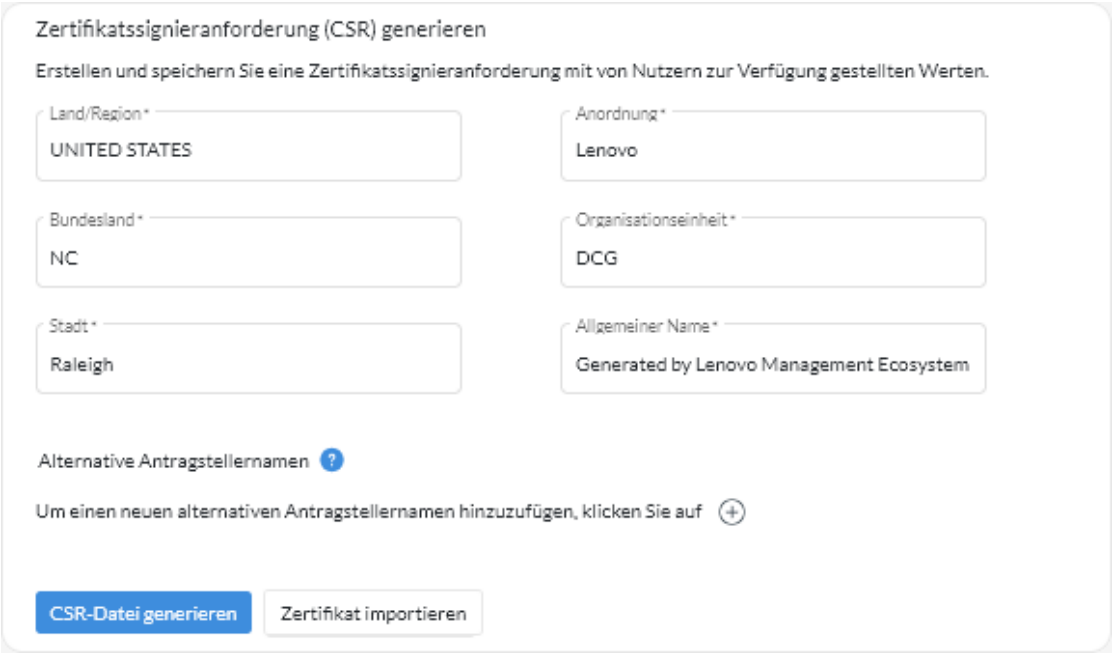
Wichtig: Wenn das Serverzertifikat geändert wird, müssen alle bestehenden Benutzersitzungen das neue Zertifikat durch Klicken auf Strg+F5 akzeptieren. Dadurch wird der Webbrowser aktualisiert und die Verbindung zu XClarity Management Hub wird wiederhergestellt.

Vorgehensweise

Gehen Sie wie folgt vor, um ein extern signiertes Serverzertifikat zu generieren und zu installieren.

Schritt 1. Erstellen Sie eine Zertifikatssignieranforderung und speichern Sie die Datei auf Ihrem lokalen System.

1. Klicken Sie in der Menüleiste von XClarity Management Hub auf **Sicherheit (⚙) → Serverzertifikat**, um die Übersicht Zertifikatssignieranforderung (CSR) generieren anzuzeigen.



2. Geben Sie in der Übersicht „Zertifikatssignieranforderung (CSR) generieren“ Daten in die Felder für die Anforderung ein.
   - Zweistelliger ISO 3166-Code für das ursprüngliche Land oder die ursprüngliche Region, der der Zertifizierungsorganisation zugeordnet ist (z. B. US für die Vereinigten Staaten).
   - Vollständiger Name des Bundesstaats/-lands, das dem Zertifikat zugeordnet werden soll (z. B. Kalifornien oder New Brunswick).
   - Vollständiger Name der Stadt, die dem Zertifikat zugeordnet werden soll (z. B. San Jose). Die Länge des Werts darf 50 Zeichen nicht überschreiten.
   - Unternehmen, dem das Zertifikat gehören soll. In der Regel handelt es sich hierbei um den eingetragenen Namen eines Unternehmens. Dies sollte alle Suffixe umfassen wie etwa Ltd., Inc. oder GmbH (z. B. ACME International Ltd.). Die Länge des Werts darf 60 Zeichen nicht überschreiten.

- (Optional) Organisationseinheit, der das Zertifikat gehören soll (z. B. Sparte ABC). Die Länge des Werts darf 60 Zeichen nicht überschreiten.
- Allgemeiner Name des Zertifikatsinhabers. Dies muss der Hostname des Servers sein, der das Zertifikat verwendet. Die Länge des Werts darf 63 Zeichen nicht überschreiten.

  Anmerkung: Derzeit hat dieses Attribut keine Auswirkungen auf das Zertifikat.
- (Optional) Alternative Namen, die beim Generieren der CSR angepasst, gelöscht und zur Erweiterung X.509 „subjectAltName“ hinzugefügt werden. Die angegebenen alternativen Namen werden validiert (basierend auf dem angegebenen Typ) und erst zur CSR hinzugefügt, nachdem Sie die CSR generiert haben. Standardmäßig definiert XClarity Management Hub automatisch alternative Namen für die Zertifikatssignieranforderung auf Basis der IP-Adresse und des Hostnamens, die von den Netzwerkschnittstellen des Gastbetriebssystems von XClarity Management Hub erkannt werden.

  Achtung: Die alternativen Namen müssen den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Verwaltungshubs enthalten und der Name muss auf den FQDN des Verwaltungshubs festgelegt sein. Prüfen Sie vor Beginn des CSR-Prozesses, dass diese erforderlichen Felder vorhanden und korrekt sind, um sicherzustellen, dass das daraus resultierende Zertifikat vollständig ist. Fehlende Zertifikatsdaten können zu nicht vertrauenswürdigen Verbindungen führen, wenn Sie versuchen, den Verwaltungshub mit Lenovo XClarity Orchestrator zu verbinden.

  Der von Ihnen angegebene Name muss für den ausgewählten Typ gültig sein.
  - **DNS** (FQDN verwenden, z. B. hostname.labs.company.com)
  - **IP-Adresse** (z. B. 192.0.2.0)
  - **E-Mail** (z. B. example@company.com)

Schritt 2. Übermitteln Sie die Zertifikatssignieranforderung an eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA). Die Zertifizierungsstelle signiert die Zertifikatssignieranforderung und gibt ein Serverzertifikat zurück.

Schritt 3. Importieren Sie das extern signierte Serverzertifikat und das Zertifizierungsstellenzertifikat in XClarity Management Hub und ersetzen Sie das aktuelle Serverzertifikat.

1. Klicken Sie in der Übersicht „Zertifikatssignieranforderung (CSR) generieren“ auf **Zertifikat importieren**, um das Dialogfeld Zertifikat importieren anzuzeigen.
2. Kopieren Sie das Serverzertifikat und das Zertifizierungsstellenzertifikat im PEM-Format und fügen Sie sie ein. Sie müssen die gesamte Zertifikatskette angeben, beginnend mit dem Serverzertifikat und endend mit dem Zertifizierungsstellenzertifikat.
3. Klicken Sie auf **Importieren**, um das Serverzertifikat im XClarity Management Hub-Truststore zu speichern.

Schritt 4. Akzeptieren Sie das neue Zertifikat, indem Sie Strg + F5 drücken, um den Browser zu aktualisieren, und dann die Verbindung zur Webschnittstelle wiederherstellen. Dies muss von allen bestehenden Benutzersitzungen durchgeführt werden.

Serverzertifikat in einen Webbrowser für Lenovo XClarity Management Hub für Edge-Client-Einheiten importieren

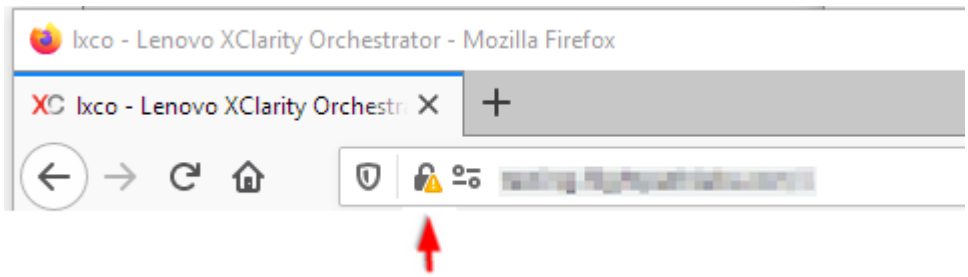
Sie können eine Kopie des aktuellen Serverzertifikats im PEM-Format auf dem lokalen System speichern. Anschließend können Sie das Zertifikat in die Liste vertrauenswürdiger Zertifikate des Webbrowsers oder in andere Anwendungen importieren, um beim Zugriff auf Lenovo XClarity Management Hub Sicherheitswarnungen des Webbrowsers zu vermeiden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das Serverzertifikat in einen Webbrowser zu importieren.

- **Chrome**
  1. Exportieren Sie das Lenovo XClarity Management Hub-Serverzertifikat.
     a. Klicken Sie oben in der Adressleiste auf das Warnsymbol „Nicht sicher“, z. B.:

     b. Klicken Sie auf **Zertifikat ist ungültig**, um das gleichnamige Dialogfeld anzuzeigen.
     c. Klicken Sie auf die Registerkarte **Details**.
     d. Klicken Sie auf **Exportieren**.
     e. Geben Sie Name und Speicherort der Zertifikatsdatei an und klicken Sie dann auf **Speichern**, um das Zertifikat zu exportieren.
     f. Schließen Sie den Dialog „Zertifikat-Viewer“.
  2. Importieren Sie das Lenovo XClarity Management Hub-Serverzertifikat in die Liste der vertrauenswürdigen Stammzertifizierungsstellen für Ihren Browser.
     a. Klicken Sie im Chrome-Browser auf die drei Punkte in der oberen rechten Ecke des Fensters und klicken Sie dann auf **Einstellungen**, um die Seite Einstellungen zu öffnen.
     b. Klicken Sie auf **Datenschutz und Sicherheit** und anschließend auf **Sicherheit**, um die Seite Sicherheit anzuzeigen.
     c. Blättern Sie zum Abschnitt **Erweitert** und klicken Sie auf **Einheitenzertifikate verwalten**.
     d. Klicken Sie auf **Importieren** und dann auf **Weiter**.
     e. Wählen Sie die Zertifikatsdatei aus, die Sie zuvor exportiert haben. Klicken Sie dann auf **Weiter**.
     f. Wählen Sie aus, wo das Zertifikat gespeichert werden soll, und klicken Sie auf **Weiter**.
     g. Klicken Sie auf **Fertig stellen**.
     h. Schließen Sie den Chrome-Browser, öffnen Sie ihn erneut und öffnen Sie Lenovo XClarity Management Hub.
- **Firefox**
  1. Exportieren Sie das Lenovo XClarity Management Hub-Serverzertifikat.
     a. Klicken Sie oben in der Adressleiste auf das Warnsymbol „Nicht sicher“, z. B.:



     b. Klicken Sie auf **Verbindung nicht sicher** und dann auf **Weitere Informationen**.
     c. Klicken Sie auf **Zertifikat anzeigen**.
     d. Blättern Sie abwärts zum Abschnitt **Verschiedene** und klicken Sie auf den Link **PEM (Zert)**, um die Datei auf dem lokalen System zu speichern.

2. Importieren Sie das Lenovo XClarity Management Hub-Serverzertifikat in die Liste der vertrauenswürdigen Stammzertifizierungsstellen für Ihren Browser.
   a. Öffnen Sie den Browser, navigieren Sie zu **Werkzeuge → Einstellungen** und klicken Sie dann auf **Datenschutz & Sicherheit**.
   b. Blättern Sie abwärts zum Abschnitt **Sicherheit**.
   c. Klicken Sie auf **Zertifikate anzeigen**, um den Dialog Zertifikatsverwaltung anzuzeigen.
   d. Wählen Sie die Registerkarte **Ihre Zertifikate** aus.
   e. Wählen Sie **Importieren** aus und navigieren Sie zur Position des heruntergeladenen Zertifikats.
   f. Markieren Sie das Zertifikat und klicken Sie auf **Öffnen**.
   g. Schließen Sie den Dialog Zertifikatsverwaltung.

XClarity Management Hub für Edge-Client-Einheiten mit XClarity Orchestrator verbinden

Nach der Registrierung (Verbindung) von Lenovo XClarity Management Hub bei Lenovo XClarity Orchestrator können Sie mit der Verwaltung und Überwachung Ihrer Einheiten beginnen.

Vorbereitende Schritte

Stellen Sie sicher, dass XClarity Management Hub im Netzwerk für XClarity Orchestrator erreichbar ist und XClarity Orchestrator im Netzwerk für XClarity Management Hub erreichbar ist.

Vorgehensweise

Gehen Sie zum Registrieren von XClarity Management Hub wie folgt vor.

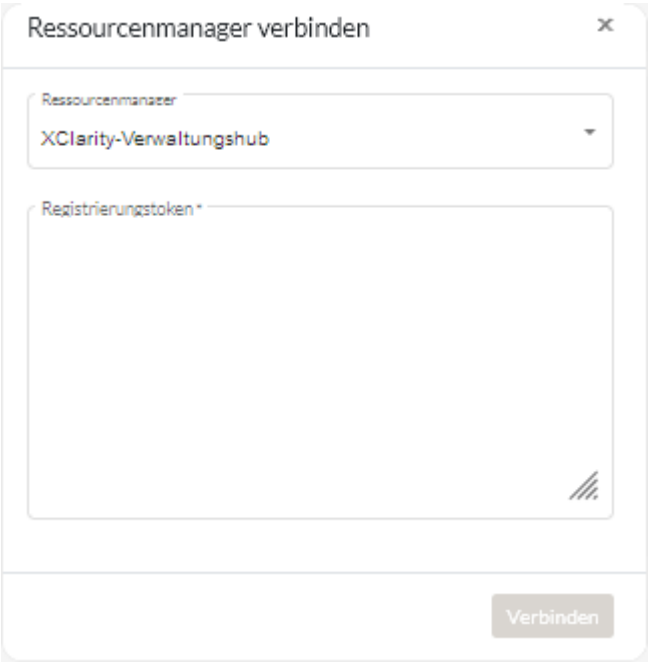
Schritt 1. Erstellen Sie den Verwaltungshub-Registrierungsschlüssel.

1. Navigieren Sie in der Menüleiste des Management Hub zu **Registrierung**, um die Seite Registrierung anzuzeigen.

2. Klicken Sie auf **Registrierungsschlüssel erstellen**.
3. Klicken Sie auf **In Zwischenablage kopieren**, um den Registrierungsschlüssel zu kopieren, und schließen Sie anschließend das Dialogfenster.

Schritt 2. Fügen Sie den Registrierungsschlüssel des Verwaltungshubs zu XClarity Orchestrator hinzu.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen (⚙) → Ressourcenmanager**, um die Übersicht Ressourcenmanager anzuzeigen.
2. Klicken Sie auf das Symbol **Verbinden** (+), um den Ressourcenmanager anzuzeigen. Das Dialogfenster Ressourcenmanager verbinden wird angezeigt.



3. Wählen Sie **XClarity Management Hub** als Ressourcenmanager aus.
4. Kopieren Sie den Registrierungsschlüssel und fügen Sie ihn im Feld **Registrierungstoken** ein.
5. Klicken Sie auf **Verbinden**, um das Dialogfenster Ressourcenmanager verbinden anzuzeigen, das den XClarity Orchestrator-Registrierungsschlüssel enthält.
6. Klicken Sie auf **In Zwischenablage kopieren**, um den Registrierungsschlüssel zu kopieren, und schließen Sie anschließend das Dialogfenster.

Schritt 3. Fügen Sie den XClarity Orchestrator-Registrierungsschlüssel zum Verwaltungshub hinzu.

1. Navigieren Sie in der Menüleiste des Management Hub zu **Registrierung**, um die Seite Registrierung anzuzeigen.
2. Klicken Sie auf **Registrierungsschlüssel installieren**.
3. Kopieren Sie den Registrierungsschlüssel und fügen Sie ihn im Feld **Registrierungstoken** ein.
4. Klicken Sie auf **Verbinden**.

Nach dieser Aufgabe

- Verwalten Sie die Einheiten mit dem Verwaltungshub (siehe ThinkEdge Client-Einheiten verwalten in der Onlinedokumentation zu XClarity Orchestrator).
- Löschen Sie den aktuellen Verwaltungshub-Registrierungsschlüssel, indem Sie auf **Registrierung zurücksetzen** klicken.

Kapitel 3. XClarity Management Hub für Edge-Client-Einheiten deinstallieren

Gehen Sie wie folgt vor, um eine virtuelle XClarity Management Hub-Einheit zu deinstallieren.

Vorgehensweise

Gehen Sie wie folgt vor, um die virtuelle XClarity Management Hub-Einheit zu deinstallieren.

Schritt 1. Heben Sie die Verwaltung aller Einheiten auf, die derzeit von XClarity Management Hub verwaltet werden.

Schritt 2. Deinstallieren Sie XClarity Management Hub, je nach Betriebssystem.

- **ESXi**
  1. Stellen Sie über VMware vSphere Client eine Verbindung zum Host her.
  2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Ein/Aus → Ausschalten**.
  3. Klicken Sie erneut mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Von Datenträger löschen**.

Lenovo