Lenovo XClarity Administrator Planungs- und Installationshandbuch für Docker-Umgebungen

Version 4.0.0

Anmerkung

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

Erste Ausgabe (Februar 2023)

Inhaltsverzeichnis

Abbildungen

Tabellen

Zusammenfassung der Änderungen

Nachfolgeversionen der Lenovo XClarity Administrator-Verwaltungssoftware bieten Unterstützung für neue Hardware, Softwareverbesserungen und Fixes.

Informationen zu Fixes finden Sie in der Änderungsprotokolldatei (*.chg), die im Aktualisierungspaket enthalten ist.

Ausführliche Informationen zur unterstützten Hardware (einschließlich Server, Gehäuse und Flex-Switches) finden Sie unter Voraussetzungen bei Hardware und Software.

Weitere Informationen zu Änderungen in früheren Versionen finden Sie unter Neuerungen in der Onlinedokumentation zu XClarity Administrator.

Die folgende Hardware wird ab diesem Release unterstützt.

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

- **Speichereinheiten**
  - ThinkSystem DE6400F All Flash Array (7DB6)
  - ThinkSystem DE6400H Hybrid Flash Array (7DB6)
  - ThinkSystem DE6600F All Flash Array (7DB7)
  - ThinkSystem DE6600H Hybrid Flash Array (7DB7)
- **Switches**
  - ThinkSystem DB730S FC SAN Switch (7D9J)
  - ThinkSystem DB400D FC SAN Director (6684)
  - ThinkSystem DB800D FC SAN Director (6682)

Diese Version unterstützt die folgenden Verbesserungen für Planung und Installation der Verwaltungssoftware.

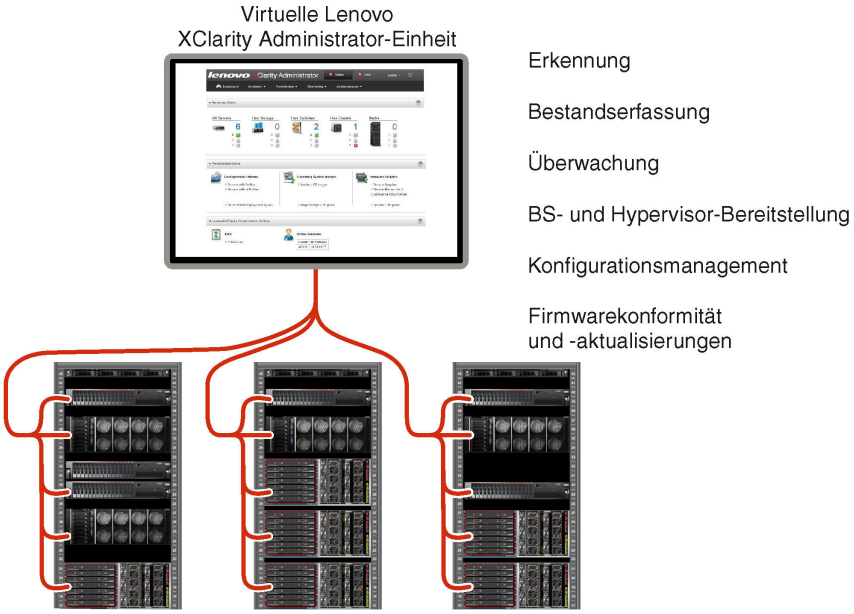
Funktion	Beschreibung
Planung und Installation	ssh-rsa wurde entfernt, und ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 und ecdsa-sha2-nistp521 wurden zur Liste der unterstützten Hostschlüsselalgorithmen hinzugefügt (siehe Verschlüsselungsverwaltung).

Kapitel 1. Lenovo XClarity Administrator – Übersicht

Lenovo XClarity Administrator ist eine Lösung für die zentrale Ressourcenverwaltung und sorgt für eine einfachere Infrastrukturverwaltung, schnellere Antworten und eine bessere Verfügbarkeit der Serversysteme und Lösungen von Lenovo®. Sie wird als virtuelle Einheit ausgeführt, welche die Ermittlung, die Inventarverfolgung, die Überwachung und die Bereitstellung von Server-, Netzwerk- und Speicherhardware in einer sicheren Umgebung automatisiert.

Weitere Informationen:

- XClarity Administrator: Hardware wie Software verwalten
- XClarity Administrator: Übersicht



XClarity Administrator enthält eine zentrale Schnittstelle, um die folgenden Funktionen für alle verwalteten Einheiten auszuführen.

Hardwareverwaltung

XClarity Administrator bietet Agent-freie Hardwareverwaltung. Sie kann verwaltbare Einheiten, einschließlich Server-, Netzwerk- und Speicherhardware, automatisch erkennen. Bestandsdaten der verwalteten Einheiten werden erfasst, sodass eine schnelle Übersicht des verwalteten Hardwarebestands und Status möglich ist.

Es gibt verschiedene Verwaltungstasks für jede unterstützte Einheit, einschließlich des Anzeigens von Status und Eigenschaften und des Konfigurierens der System- und Netzwerkeinstellungen, des Startens der Verwaltungsschnittstellen, des Ein- und Ausschaltens und der Fernsteuerung. Weitere Informationen über das Verwalten von Einheiten finden Sie unter Gehäuse verwalten, Server verwalten und Switches verwalten in der Onlinedokumentation von XClarity Administrator.

Tipp: Server-, Netzwerk- und Speicherhardware, die von XClarity Administrator verwaltet wird, wird als *Einheiten* bezeichnet. Hardware, die unter XClarity Administrator verwaltet wird, wird als *verwaltete Einheiten* bezeichnet.

Sie können die Rack-Ansicht in XClarity Administrator verwenden, um Ihre verwalteten Einheiten zu gruppieren, damit Sie die physische Rack-Konfiguration in Ihrem Rechenzentrum widerspiegeln. Weitere Informationen zu Racks finden Sie unter Racks verwalten in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen:

- XClarity Administrator: Ermittlung
- XClarity Administrator: Bestand
- XClarity Administrator: Fernsteuerung

Hardwareüberwachung

XClarity Administrator enthält eine zentrale Ansicht aller Ereignisse und Alerts, die von verwalteten Einheiten generiert werden. Ein Ereignis oder Alert wird an den XClarity Administrator weitergegeben und im Ereignis- oder Alertprotokoll dargestellt. Eine Zusammenfassung aller Ereignisse und Alerts ist im Dashboard und in der Statusleiste zu sehen. Ereignisse und Alerts für eine bestimmte Einheit sind auf der Alert- und Ereignisdetailseite für diese Einheit verfügbar.

Weitere Informationen über das Verwalten von Hardware finden Sie unter Ereignisse handhaben und Mit Alerts arbeiten in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen: XClarity Administrator: Überwachung

Konfigurationsmanagement

Mithilfe einer konsistenten Konfiguration können Sie alle Server bereitstellen und vorab bereitstellen. Konfigurationseinstellungen (wie lokaler Speicher, E/A-Adapter, Booteinstellungen, Firmware, Ports und die Management-Controller- und UEFI-Einstellungen) werden als Servermuster gespeichert, das auf einen oder mehrere verwaltete Server angewendet werden kann. Wenn die Servermuster aktualisiert werden, werden die entsprechenden Änderungen automatisch auf den entsprechenden Servern implementiert.

Servermuster integrieren außerdem eine Unterstützung für das Virtualisieren von E/A-Adressen, sodass Sie Flex System Fabric-Verbindungen virtualisieren oder Server ohne Unterbrechung für den Fabric umfunktionieren können.

Weitere Informationen zum Konfigurieren von Servern finden Sie unter Server mithilfe von XClarity Administrator konfigurieren in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen:

- XClarity Administrator: Bare Metal zu Cluster
- XClarity Administrator: Konfigurationsmuster

Firmwarekonformität und -aktualisierungen

Die Firmwareverwaltung wird vereinfacht, indem verwaltete Einheiten Firmwarekonformitätsrichtlinien zugeordnet werden. Wenn Sie eine Konformitätsrichtlinie erstellen und verwalteten Einheiten zuordnen, überwacht XClarity Administrator Änderungen im Bestand für diese Einheiten und markiert alle Einheiten, die nicht konform sind.

Wenn eine Einheit nicht konform ist, können Sie XClarity Administrator verwenden, um Firmwareaktualisierungen aus einem Repository von Firmwareaktualisierungen, die Sie verwalten, für alle Einheiten in dieser Einheit anzuwenden und zu aktivieren.

Anmerkung: Für die Aktualisierung des Repositorys und das Herunterladen von Firmwareaktualisierungen ist eine Internetverbindung erforderlich. Wenn XClarity Administrator keine Internetverbindung hat, können Sie Firmwareaktualisierungen manuell in das Repository importieren.

Weitere Informationen zum Aktualisieren von Firmware finden Sie unter Firmware auf verwalteten Einheiten aktualisieren in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen:

- XClarity Administrator: Bare Metal zu Cluster
- XClarity Administrator: Firmwareaktualisierungen
- XClarity Administrator: Firmwaresicherheitsaktualisierungen bereitstellen

Betriebssystemimplementierung

Sie können XClarity Administrator verwenden, um ein Repository von Betriebssystem-Images zu verwalten und um Betriebssystem-Images für bis zu 28 verwaltete Server gleichzeitig zu implementieren.

Weitere Informationen zum Implementieren von Betriebssystemen finden Sie unter Betriebssystem-Image implementieren in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen:

- XClarity Administrator: Bare Metal zu Cluster
- XClarity Administrator: Betriebssystemimplementierung

Benutzerverwaltung

XClarity Administrator enthält einen zentralen Authentifizierungsserver, um Benutzeraccounts zu erstellen und zu verwalten sowie Benutzeranmeldeinformationen zu verwalten und zu authentifizieren. Der Authentifizierungsserver wird automatisch erstellt, wenn Sie den Verwaltungsserver zum ersten Mal starten. Die Benutzeraccounts, die Sie für XClarity Administrator erstellen, werden auch für die Anmeldung beim verwalteten Gehäuse und den Servern im verwalteten Authentifizierungsmodus verwendet. Weitere Informationen zu Benutzern finden Sie unter Benutzeraccounts verwalten in der Onlinedokumentation von XClarity Administrator.

XClarity Administrator unterstützt drei Arten von Authentifizierungsservern:

- **Lokaler Authentifizierungsserver**. Standardmäßig wird XClarity Administrator so konfiguriert, dass der lokale Authentifizierungsserver verwendet wird, der sich auf dem Verwaltungsknoten befindet.
- **Externer LDAP-Server**. Derzeit wird nur Microsoft Active Directory unterstützt. Dieser Server muss sich auf einem externen Microsoft Windows-Server befinden, der mit dem Verwaltungsnetzwerk verbunden ist.Wenn ein externer LDAP-Server verwendet wird, ist der lokale Authentifizierungsserver deaktiviert.
- **Externe SAML 2.0 Identity Provider**. Derzeit wird nur Microsoft Active Directory Federation Services (AD FS) unterstützt. Zusätzlich zur Eingabe eines Benutzernamens und Kennworts kann eine mehrstufige Authentifizierung konfiguriert werden, um zusätzliche Sicherheit zu aktivieren, indem ein PIN-Code, das Lesen einer Smartcard und ein Clientzertifikat erforderlich sind.

Weitere Informationen zum Authentifizierungstypen finden Sie unter Authentifizierungsserver verwalten in der Onlinedokumentation von XClarity Administrator.

Wenn Sie einen Benutzeraccount erstellen, weisen Sie diesem eine vordefinierte oder angepasste Rollengruppe zu, um die Zugriffsebene für diesen Benutzer zu steuern. Weitere Informationen zu Rollengruppen finden Sie unter Rollengruppe verwalten in der Onlinedokumentation von XClarity Administrator.

XClarity Administrator umfasst ein Prüfprotokoll, das eine historische Aufzeichnung aller Benutzeraktionen bietet, z. B. Anmelden, Erstellen neuer Benutzer oder Ändern der Benutzerkennwörter. Weitere Informationen zum Prüfprotokoll finden Sie unter Ereignisse handhaben in der Onlinedokumentation von XClarity Administrator.

Einheitenauthentifizierung

XClarity Administrator nutzt die folgenden Methoden zur Authentifizierung bei den verwalteten Gehäusen und Servern.

- **Verwaltete Authentifizierung**. Bei aktivierter verwalteter Authentifizierung werden die Benutzeraccounts, die Sie in XClarity Administrator erstellen, verwendet, um das verwaltete Gehäuse und die Server zu authentifizieren.

  Weitere Informationen zu Benutzern finden Sie unter Benutzeraccounts verwalten in der Onlinedokumentation von XClarity Administrator.

- **Lokale Authentifizierung**. Bei deaktivierter verwalteter Authentifizierung werden die Anmeldeinformationen, die in XClarity Administrator definiert sind, zur Authentifizierung verwalteter Server verwendet. Die gespeicherten Anmeldeinformationen müssen einem aktiven Benutzeraccount auf der Einheit oder im Active Directory entsprechen.

  Weitere Informationen zu gespeicherten Anmeldeinformationen finden Sie im Abschnitt Gespeicherte Anmeldeinformationen verwalten in der XClarity Administrator Onlinedokumentation.

Sicherheit

Wenn Ihre Umgebung den Standard NIST SP 800-131A erfüllen muss, kann XClarity Administrator Ihnen helfen, eine vollständig kompatible Umgebung zu erreichen.

XClarity Administrator unterstützt selbstsignierte SSL-Zertifikate (die von einer internen Zertifizierungsstelle ausgegeben werden) und externe SSL-Zertifikate (die durch eine private oder gewerbliche Zertifizierungsstelle ausgegeben werden).

Firewalls auf Gehäusen und Servern können so konfiguriert werden, dass sie eingehende Anforderungen nur von XClarity Administrator akzeptieren.

Weitere Informationen zur Sicherheit finden Sie unter Eine sichere Umgebung implementieren in der Onlinedokumentation von XClarity Administrator.

Service und Support

XClarity Administrator kann so installiert werden, dass Diagnosedateien automatisch gesammelt und an Ihren bevorzugten Service Provider gesendet werden, wenn bestimmte wartungsfähige Ereignisse in XClarity Administrator und den verwalteten Einheiten auftreten. Sie können auswählen, ob die Diagnosedateien über Call-Home-Funktion an den Lenovo-Support oder mit SFTP an einen anderen Service Provider gesendet werden. Sie können Diagnosedateien auch manuell sammeln, einen Problemdatensatz öffnen und Diagnosedateien an das Lenovo-Support Center senden.

Weitere Informationen:  XClarity Administrator: Service und Support

Taskautomatisierung mithilfe von Scripts

XClarity Administrator kann in externe Verwaltungs- und Automatisierungsplattformen auf höherer Ebene über offene REST-Anwendungsprogrammierschnittstellen (APIs) integriert werden. Mithilfe der REST-APIs kann XClarity Administrator einfach in Ihre bestehende Verwaltungsinfrastruktur integriert werden.

Das PowerShell-Toolkit enthält eine Bibliothek mit Cmdlets, um die Bereitstellung und Ressourcenverwaltung von einer Microsoft-PowerShell-Sitzung zu automatisieren. Das Python-Toolkit enthält eine Bibliothek von Python-basierten Befehlen und APIs, um die Bereitstellung und Ressourcenverwaltung von einer OpenStack-Umgebung, wie Ansible oder Puppet, zu automatisieren. Beide Toolkits bilden eine Schnittstelle zu XClarity Administrator REST-APIs und ermöglichen die Automatisierung von Funktionen wie:

- Bei XClarity Administrator anmelden
- Verwalten und Beenden der Verwaltung von Gehäusen, Servern, Speichereinheiten und Top-of-Rack-Switches (Einheiten)

- Erfassen und Anzeigen von Bestandsdaten für Einheiten und Komponenten
- Implementieren eines Betriebssystemimages in einem oder mehreren Servern
- Konfigurieren von Servern mithilfe von Konfigurationsmustern
- Anwenden von Firmwareaktualisierungen auf Einheiten

Integration in andere verwaltete Software

XClarity Administrator-Module integrierten XClarity Administrator mit Verwaltungssoftware von Drittanbietern für Ermittlungs-, Überwachungs-, Konfigurations- und Verwaltungsfunktionen, um die Kosten und die Komplexität der Routinesystemverwaltung für unterstützte Einheiten zu reduzieren.

Weitere Informationen zu XClarity Administrator finden Sie in den folgenden Dokumenten:
- Lenovo XClarity Integrator für Microsoft System Center
- Lenovo XClarity Integrator für VMware vCenter

Weitere Hinweise finden Sie unter Verwaltungshinweise.

Weitere Informationen:
-  Lenovo XClarity Integrator für Microsoft System Center Übersicht
-  Lenovo XClarity Integrator für VMware vCenter

Dokumentation

Die XClarity Administrator Dokumentation wird regelmäßig online in Englisch aktualisiert. Aktuelle Informationen und Verfahren finden Sie in XClarity Administrator Onlinedokumentation.

Die Onlinedokumentation ist in den folgenden Sprachen verfügbar:
- Deutsch (de)
- Englisch (en)
- Spanisch (es)
- Französisch (fr)
- Italienisch (it)
- Japanisch (ja)
- Koreanisch (ko)
- Portugiesisch, Brasilien (pt_BR)
- Russisch (ru)
- Thailändisch (th)
- Vereinfachtes Chinesisch (zh_CN)
- Traditionelles Chinesisch (zh_TW)

Sie können die Sprache der Onlinedokumentation folgendermaßen ändern:

- Ändern Sie die Spracheinstellungen in Ihrem Webbrowser
- Fügen Sie `?lang=`*<language_code>* ans Ende der URL an, z. B. zur Anzeige der Onlinedokumentation in vereinfachtem Chinesisch:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Kapitel 2. Planen für XClarity Administrator

Bevor Sie Lenovo XClarity Administrator installieren, lesen Sie die folgenden Hinweise; diese helfen Ihnen bei der Planung Ihrer Installationen und täglichen Verwaltungsaufgaben.

Lizenzen und die kostenlose 90-Tage-Testversion

Lenovo XClarity Administratorbietet eine kostenlose, 90-tägige Testlizenz, die eine vollständige Nutzung aller verfügbaren Funktionen für einen begrenzten Zeitraum ermöglicht.

Sie können den Lizenzstatus und die Anzahl der verbleibenden Tage der Testlizenz bestimmen, indem Sie auf das Benutzeraktionen-Menü (

) in der XClarity Administrator-Titelleiste und anschließend auf **Info** klicken.

XClarity Administrator unterstützt die folgende Lizenz.

- **Lenovo XClarity Pro**. Jede Lizenz bietet die folgenden Nutzungsrechte für eine einzelne Einheit.
  - Service und Unterstützung für Lenovo XClarity Integrator
  - Service und Unterstützung für XClarity Administrator
  - Erweiterte Funktionen in XClarity Administrator:
    - Server mithilfe von Konfigurationsmustern konfigurieren
    - Betriebssysteme implementieren
    - XClarity Administrator-Probleme mithilfe der Call-Home-Funktion melden (Call-Home-Funktion für Hardware-Alerts ist nicht betroffen)

Sie müssen für jede verwaltete Einheit, die die erweiterten Funktionen unterstützt, eine Lizenz erwerben. Eine Lizenz ist nicht an eine bestimmte Einheit gebunden.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt, die die verwalteten Funktionen unterstützen. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen gültigen Lizenzschlüsseln nicht überschreiten. Wenn XClarity Administrator nicht den installierten Lizenzen entspricht (z. B. wenn Lizenzen ablaufen oder wenn die Verwaltung zusätzlicher Einheiten die Gesamtanzahl der aktiven Einheiten überschreitet), haben Sie eine Kulanzzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Jedes Mal, wenn XClarity Administrator nicht konform ist, wird die Kulanzzeit auf 90 Tage zurückgesetzt. Wenn die Kulanzzeit (einschließlich der kostenlosen Testversion) endet, bevor die Lizenzen konform sind, werden die erweiterten Funktionen für alle Geräte deaktiviert.

Anmerkungen:

- Funktionen für Serverkonfiguration und Betriebssystembereitstellung werden mit Ablauf der Kulanzzeit deaktiviert.
- Die Call-Home-Funktion für Probleme mit XClarity Administrator (Software für die Call-Home-Funktion) ist deaktiviert, wenn die Lizenzen nicht konform sind. Für diese Funktion gibt es keine Kulanzzeit. Die Call-Home-Funktion für Hardware-Alerts ist jedoch nicht betroffen.

Wenn bereits Lizenzen installiert sind, sind *keine* neuen Lizenzen erforderlich, wenn Sie eine Aktualisierung auf eine neue Version von XClarity Administrator ausführen.

Informationen zum Kauf von Lenovo XClarity Pro-Lizenzen erhalten Sie von Ihrem Lenovo Ansprechpartner oder autorisierten Business Partner.

Informationen zum Installieren der Lizenz finden Sie unter Lizenz für den vollständigen Funktionsumfang installieren in der Onlinedokumentation von XClarity Administrator.

Voraussetzungen bei Hardware und Software

Die virtuelle Lenovo XClarity Administrator-Verwaltungseinheit wird auf einer virtuellen Maschine auf einem Hostsystem ausgeführt.

Hypervisor-Anforderungen

Containerumgebungen

Die folgenden Containerumgebungen werden für die Ausführung von XClarity Administrator als Container unterstützt.

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

Hypervisoren

Die folgenden Hypervisoren werden für die Ausführung von XClarity Administrator als virtuelle Einheit unterstützt.

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 7 und 8[1]
- Microsoft Windows Server 2022 mit installiertem Hyper-V
- Microsoft Windows Server 2019 mit installiertem Hyper-V
- Microsoft Windows Server 2016 mit installiertem Hyper-V
- Microsoft Windows Server 2012 R2 mit installiertem Hyper-V
- Microsoft Windows Server 2012 mit installiertem Hyper-V
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat v8.x mit installiertem KVM v2.12.0 (Kernel-based Virtual Machine)
- Red Hat v7.x mit installiertem KVM v1.2.17
- Ubuntu 20.04.2 LTS mit installiertem KVM v4.2.3
- VMware ESXi 7.0, U1, U2 und U3
- VMware ESXi 6.7, U1, U2[2] und U3

Anmerkungen:

1. CentOS Linux wird nicht mehr von Red Hat aktualisiert. Ziehen Sie in Betracht, stattdessen zu Red Hat Enterprise Linux zu migrieren (siehe Website zu Red Hat: Konvertieren von CentOS oder Oracle Linux zu RHEL).
2. Für VMware ESXi 6.7 U2 müssen Sie das ISO-Image VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso (oder höher) verwenden.

Für VMware und Citrix ist die virtuelle Maschine als OVF-Vorlage verfügbar. Für Hyper-V und Nutanix AHV ist die virtuelle Maschine ein virtuelles Festplatten-Image (VHD). Für CentOS und KVM steht die virtuelle Maschine im qcow2-Format zur Verfügung.

Wichtig: Für Hyper-V-Umgebungen, die auf Linux-Gastsystemen mit einer 2.6-Kernel-Basis ausgeführt werden und hohe Speicherkapazitäten für die virtuelle Einheit nutzen, müssen Sie in den Hyper-V-Einstellungen im Hyper-V-Manager die Verwendung von Non-Uniform Memory Access (NUMA) deaktivieren. Nach der Änderung dieser Einstellung müssen Sie den Hyper-V-Service neu starten, wodurch auch alle ausgeführten virtuellen Maschinen neu gestartet werden. Wenn diese Einstellung nicht deaktiviert ist, können beim ersten Starten der virtuellen XClarity Administrator-Einheit u. U. Probleme auftreten.

Hardwarevoraussetzungen

Für XClarity Administrator gelten die unten stehenden *Mindestanforderungen*. Je nach Größe Ihrer Umgebung und Ihrer Verwendung von Konfigurationsmuster sind möglicherweise zusätzliche Ressourcen notwendig, um eine optimale Leistung zu erreichen.

- Zwei virtuelle Mikroprozessoren
- 8 GB Speicher
- 192 GB Speicher zur Nutzung durch die virtuelle XClarity Administrator-Einheit.
- Mit minimaler Auflösung bei Breite von 1024 Pixel (XGA) anzeigen

In der folgenden Tabelle sind die empfohlenen Mindestkonfigurationen für eine bestimmte Anzahl Einheiten aufgeführt. Beachten Sie, dass bei der Mindestkonfiguration die Ausführung von Verwaltungsaufgaben möglicherweise länger dauert als erwartet. Für Bereitstellungsaufgaben wie beispielsweise Betriebssystemimplementierung, Firmwareaktualisierungen und Serverkonfigurationen müssen Sie ggf. die Ressourcen vorübergehend erhöhen.

Anzahl der verwalteten Einheiten	Konfiguration virtuelle CPU/Hauptspeicher
0–100 Einheiten	2 vCPUs, 8 GB RAM
100–200 Einheiten	4 vCPUs, 10 GB RAM
200–400 Einheiten	6 vCPUs, 12 GB RAM
400–600 Einheiten	8 vCPUs, 16 GB RAM
600–800 Einheiten	10 vCPUs, 20 GB RAM
800–1.000 Einheiten	12 vCPUs, 24 GB RAM

Anmerkungen:

- Eine einzelne XClarity Administrator-Instanz kann maximal 1.000 Einheiten unterstützen.
- Aktuelle Empfehlungen und zusätzliche Leistungsaspekte finden Sie im Whitepaper zur Leistung von XClarity Administrator.
- Je nach der Größe Ihrer verwalteten Umgebung und dem Nutzungsmuster in Ihrer Installation müssen Sie möglicherweise Ressourcen hinzufügen, um für eine akzeptable Leistung zu sorgen. Wenn im Dashboard für die Systemressourcen oft eine hohe oder sehr hohe Prozessorauslastung angezeigt wird, kann es sinnvoll sein, ein bis zwei virtuelle Prozessorkerne hinzuzufügen. Wenn die Speicherauslastung bei Inaktivität weiterhin über 80 % beträgt, sollten Sie 1–2 GB RAM hinzufügen. Wenn das System mit einer wie in der Tabelle definierten Konfiguration gut reagiert, sollten Sie die VM für einen längeren Zeitraum ausführen, um die Systemleistung zu beurteilen.
- Mehr Informationen dazu, wie Sie Speicherplatz freigeben, indem Sie nicht länger benötigte XClarity Administrator-Ressourcen löschen, erhalten Sie unter Plattenspeicher verwalten in der XClarity Administrator-Onlinedokumentation.

Softwarevoraussetzungen

- **Orchestrator-Server**

  Wenn Sie eine große Anzahl von Einheiten über mehrere XClarity Administrator-Instanzen verwalten, können Sie die Überwachung, Verwaltung, Bereitstellung und Analyse mithilfe von Lenovo XClarity Orchestrator zentralisieren. XClarity Orchestrator kann eine unbegrenzte Anzahl von XClarity Administrator-Instanzen unterstützen, die zusammen maximal **10.000** Einheiten verwalten, die keine ThinkEdge Clients sind.

  Zum Verwalten von XClarity Administrator v4.0 oder höheren Instanzen mit Lenovo XClarity Orchestrator ist XClarity Orchestrator v2.0 oder höher erforderlich.

- **Authentifizierungsserver**

Bei Verwendung eines externen Authentifizierungsservers wird nur Microsoft Active Directory unter Windows Server 2008 oder höher unterstützt.

Wenn Sie einen SAML-Identitätsanbieter nutzen möchten, wird nur Microsoft Active Directory Federation Services (AD FS) Version 2.0 oder höher unter Windows Server 2012 unterstützt.

- **NTP-Server**

  Um sicherzustellen, dass die Zeitstempel für alle Ereignisse und Alerts synchronisiert werden, die mit XClarity Administrator von 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.

  Tipp: Überlegen Sie, das Hostsystem, auf dem XClarity Administrator installiert ist, als NTP-Server zu verwenden. Wenn Sie sich dafür entscheiden, stellen Sie sicher, dass über das Verwaltungsnetzwerk auf das Hostsystem zugegriffen werden kann.

Verwaltbare Ressourcen

Eine einzelne XClarity Administrator-Instanz kann maximal **1.000** physische Einheiten verwalten, überwachen und bereitstellen.

Eine vollständige Liste der unterstützten Einheiten und Optionen (z. B. E/A-, DIMM- und Speicheradapter), die mindestens erforderlichen Firmwareversionen und Einschränkungen von Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator finden Sie, indem Sie auf die Registerkarte **Kompatibilität** klicken und dann auf den Link für die entsprechenden Einheitentypen klicken.

Allgemeine Informationen zur Konfiguration der Hardware und zu den Optionen für eine bestimmte Einheit finden Sie unter Lenovo Server Proven-Website.

Einschränkung: Wenn das Hostsystem, auf dem XClarity Administrator installiert ist, ein verwalteter Rack-Server oder Rechenknoten ist, können Sie XClarity Administrator nicht verwenden, um auf diesem Hostsystem oder dem gesamten Gehäuse gleichzeitig Firmwareaktualisierungen auszuführen. Das Hostsystem muss nach einer Aktualisierung seiner Firmware neu gestartet werden. Durch den Neustart des Hostsystems wird auch XClarity Administrator neu gestartet. Somit ist XClarity Administrator nicht verfügbar, um die Aktualisierungen auf dem Hostsystem abzuschließen.

Unterstützte Webbrowser

Die XClarity Administrator-Webschnittstelle funktioniert mit den folgenden Webbrowsern.
- Chrome™ 48.0 oder höher (55.0 oder höher für Ferne Konsole)
- Firefox® ESR 38.6.0 oder höher
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 oder höher (IOS7 oder höher und OS X)

Firewalls und Proxy-Server

Einige Funktionen von Lenovo XClarity Administrator, einschließlich Verwaltungsserveraktualisierungen, Firmwareaktualisierungen, Service und Support, erfordern den Zugriff auf das Internet. Wenn Sie Firewalls in Ihrem Netzwerk haben, konfigurieren Sie die Firewalls so, dass XClarity Administrator Verwaltungsserver diese Vorgänge durchführen können. Wenn der Verwaltungsserver keinen direkten Zugriff auf das Internet hat, konfigurieren Sie XClarity Administrator für die Verwendung eines Proxy-Servers.

Firewalls

Überprüfen Sie, ob die folgenden DNS-Namen und Ports in der Firewall geöffnet sind.

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

Tabelle 1. Erforderliche Internetverbindungen

DNS-Name	IPv4-Adresse	IPv6-Adresse	Ports	Protokolle
Lizenzaktivierungsschlüssel herunterladen				
fod.lenovo.com	Nicht zutreffend	Nicht zutreffend	443	https
Service-Bulletins herunterladen				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	Nicht zutreffend	Nicht zutreffend	443 und 80	https
Aktualisierungen herunterladen (Verwaltungsserveraktualisierungen, Firmwareaktualisierungen, UpdateXpress System Packs [Betriebssystem-Einheitentreiber] und Repository-Pakete)				
datacentersupport.lenovo.com	Nicht zutreffend	Nicht zutreffend	443 und 80	https
download.lenovo.com	Nicht zutreffend	Nicht zutreffend	443 und 80	https
filedownload.lenovo.com	Nicht zutreffend	Nicht zutreffend	443 und 80	https
support.lenovo.com	Nicht zutreffend	Nicht zutreffend	443 und 80	https und http
supportapi.lenovo.com	Nicht zutreffend	Nicht zutreffend	443 und 80	https
Firmware (nur Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, einige Flex-Switches und CMMs der ersten Generation) herunterladen				
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.19-7	Nicht zutreffend	443 und 80	https und http
www-03.ibm.com	204.146.30.17	Nicht zutreffend	443 und 80	https und http
download3.boulder.ibm.com	170.225.126.2-4	Nicht zutreffend	443	https
download4.boulder.ibm.com	170.225.126.4-3	Nicht zutreffend	443 und 80	https und http
delivery04-bld.dhe.ibm.com	170.225.126.4-5	Nicht zutreffend	443 und 80	https und http
delivery04-mul.dhe.ibm.com	170.225.126.4-6	Nicht zutreffend	443 und 80	https und http
delivery04.dhe.ibm.com	170.225.126.4-4	Nicht zutreffend	443 und 80	https und http
Servicedatendaten zu Lenovo Unterstützung hochladen (Call-Home-Funktion)				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	Nicht zutreffend	443	https
logupload.lenovo.com/BLL/Logupload.ashx	Nicht zutreffend	Nicht zutreffend	443 und 80	https

Tabelle 1. Erforderliche Internetverbindungen (Forts.)

DNS-Name	IPv4-Adresse	IPv6-Adresse	Ports	Protokolle
Servicedaten zu Lenovo Update Facility hochladen				
logupload.lenovo.com/BLL/Logupload.ashx	Nicht zutreffend	Nicht zutreffend	443 und 80	https
Informationen zur Garantie herunterladen				
ibase.lenovo.com (weltweit)	Nicht zutreffend	Nicht zutreffend	443 und 80	https und http
service.lenovo.com.cn (nur China)	114.247.140.2-12 (nur China)	Nicht zutreffend	83	http
supportapi.lenovo.com	Nicht zutreffend	Nicht zutreffend	443 und 80	https und http

Achtung: Benutzer in China, die Informationen zur Garantie für ihre verwalteten Einheiten mithilfe von XClarity Administrator abrufen wollen, müssen auf XClarity Administrator v1.3.1 oder höher aktualisieren.

Proxy-Server

Wenn der Verwaltungsserver keinen direkten Zugriff auf das Internet hat, stellen Sie sicher, dass der Verwaltungsserver für die Verwendung eines HTTP-Proxy-Servers konfiguriert ist (siehe Netzwerkzugriff konfigurieren).

- 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).

Portverfügbarkeit

Je nachdem, wie die Firewalls in Ihrer Umgebung implementiert sind, müssen verschiedene Ports verfügbar sein. Wenn die erforderlichen Ports von einem anderen Prozess blockiert oder verwendet werden, können einige Lenovo XClarity Administrator-Funktionen möglicherweise nicht ausgeführt werden.

Lesen Sie die folgenden Abschnitte, um herauszufinden, welche Ports je nach Umgebung offen sein müssen. Die Tabellen in diesen Abschnitten enthalten Informationen darüber, wie die einzelnen Ports in XClarity Administrator verwendet werden, zur betroffenen verwalteten Einheit, zum Protokoll (TCP oder UDP) und zur Richtung des Verkehrsflusses. *Eingehender* Netzwerkverkehr fließt von der verwalteten Einheit zu XClarity Administrator, daher müssen die Ports auf der XClarity Administrator-Appliance geöffnet werden. *Ausgehender* Netzwerkverkehr fließt von XClarity Administrator zur verwalteten Einheit.

- Zugriff auf den XClarity Administrator-Server
- Zugriff von XClarity Administrator auf verwaltete Einheiten
- Zugriff von XClarity Administrator auf Datennetzwerk für BS-Implementierung und Einheitentreiberaktualisierungen

Zugriff auf den XClarity Administrator-Server

Wenn sich der XClarity Administrator-Server und alle verwalteten Einheiten hinter einer Firewall befinden und Sie beabsichtigen, über einen Browser außerhalb der Firewall auf diese Einheiten zuzugreifen, müssen Sie sicherstellen, dass alle XClarity Administrator-Ports geöffnet sind. Wenn Sie SNMP und SMTP für die Ereignisverwaltung verwenden, müssen zudem die Ports, die der XClarity Administrator-Server für die Ereignisweiterleitung verwendet, geöffnet sein.

Der XClarity Administrator-Server überwacht die in der folgenden Tabelle aufgeführten Ports und verwendet sie als Antwortports.

Anmerkungen:

- XClarity Administrator ist eine RESTful-Anwendung, die sicher über TCP an Port 443 kommuniziert.
- XClarity Administrator 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.

Kommunikation	**XClarity Administrator-Anwendung**	**Externe Authentifizierungsserver**	**Ereignisweiterleitungsservices**	**Lenovo Service (einschließlich Call-Home-Funktion)**
Ausgehend (Ports auf externen Systemen geöffnet)	• DNS – TCP/UDP an Port **53**	• LDAP– TCP an Port **389**[1] • LDAPS – TCP an Port **636** • SAML-Authentifizierung – TCP an den Ports **3268, 3269**	• FTP-Server – TCP an Port **21**[1] • E-Mail-Server (SMTP) – UDP an Port **25**[1] • REST-Web-Service (HTTP) – UDP an Port **80**[1] • SNMP-Manager – UDP an Port **161**[2], **162**[1] • MS Azure – UDP an Port **443**[1] • Syslog – UDP an Port **514**[1] • Apple-Push[3] – TCP an Ports **443, 2195, 5223** • Google-Push[4] – TCP an Ports **443, 5288, 5299, 5230**	• Warranty (Garantie) (nur China) – TCP an Port **83**[5] • HTTPS (Call-Home-Funktion) – TCP an Port **443**
Eingehend (Ports auf der XClarity Administrator Einheit geöffnet)	• HTTPS – TCP an Port **443**	Nicht zutreffend	• SNMP – UDP an Port **161**	Nicht zutreffend

1. Dies ist der Standard-Port. Sie können diesen Port über die Benutzerschnittstelle konfigurieren.
2. Er wird verwendet, wenn die SNMP-Ereignisweiterleitung mit Benutzerauthentifizierung konfiguriert ist.
3. Öffnen Sie diesen Port, wenn sich das WLAN hinter einer Firewall oder einem privaten Zugriffspunktnamen (Access Point Name, APN) für Mobildaten befindet. An diesem Port ist für die APN-Server eine direkte Verbindung erforderlich, die nicht über einen Proxy läuft. Dieser Port wird nur dann als Failback für das WLAN verwendet, wenn die Einheiten den Apple-Push-Benachrichtigungsservice über Port 5223 nicht erreichen können. Der IP-Adressbereich ist 17.0.0.0/8.

4. IP-Adressbereich: siehe Google-ASN 15169. Domäne: android.googleapis.com.
5. Zwar ist dies außerhalb Chinas nicht erforderlich, dennoch versucht XClarity Administrator möglicherweise auch in anderen Ländern, eine Verbindung zu diesem Service herzustellen.

Zugriff von XClarity Administrator auf verwaltete Einheiten

Wenn verwaltete Einheiten (z. B. Rechenknoten oder Rack-Server) sich hinter einer Firewall befinden und Sie diese Einheiten über einen XClarity Administrator-Server außerhalb der Firewall verwalten, müssen in allen verwalteten Einheit alle an der Kommunikation zwischen XClarity Administrator und dem Baseboard Management Controller beteiligten Ports geöffnet sein.

Wenn Sie Betriebssysteme auf verwalteten Einheiten mithilfe von XClarity Administrator installieren möchten, prüfen Sie die Liste der Ports unter Zugriff von XClarity Administrator auf Datennetzwerk für BS-Implementierung und Einheitentreiberaktualisierungen.

- **Flex-Gehäuse CMM**

Kommunikation	Flex-Gehäuse CMMs
Ausgehend (Ports auf externen Systemen geöffnet)	– SLP – UDP/TCP an Port **427** – CIM HTTP – TCP an Port **5988**[2] – CIM HTTPS – TCP an Port **5989** – TCP-Befehl – TCP an Port **6090**[2] – Sicherer TCP-Befehl – TCP an Port **6091**
Eingehend (Ports auf der XClarity Administrator Einheit geöffnet)	– SFTP – TCP an Port **22**[1] – CIM-Meldungen über HTTPS – TCP **9090** – LDAPS – TCP an Ports **50637**

1. Dieser Port wird zur Übermittlung von Firmwareaktualisierungen mit SFTP verwendet.
2. Standardmäßig wird die Verwaltung über sichere Ports ausgeführt. Die nicht sicheren Ports sind optional.

- **Server und Rechenknoten**

Kommunikation	ThinkSystem und ThinkAgile	System x	Flex System	ThinkServer
Ausgehend (Ports auf externen Systemen geöffnet)	– SFTP – TCP an Port **115** – SLP – UDP/TCP an Port **427** – HTTPS – TCP an Port **443** – SSDP-Erkennung – UDP an Port **1900** – Fernsteuerung – TCP an Port **3888**[4] – Remote-KVM – TCP an Port **3889**[4] – CIM HTTPS – TCP an Port **5989** – Firmwareaktualisierungen – TCP an Port **6990**[5]	– SLP – UDP/TCP an Port **427** – HTTPS – TCP an Port **443** – IPMI – TCP an Port **623** – Fernsteuerung – TCP an Port **3888**[4] – Remote-KVM – TCP an Port **3889**[4] – CIM HTTP – TCP an Port **5988**[3] – CIM HTTPS – TCP an Port **5989**[3] – Firmwareaktualisierungen – TCP an Port **6990**[5]	– SLP – UDP/TCP an Port **427** – Fernsteuerung – TCP an Port **3888**[4] – Remote-KVM – TCP an Port **3889**[1, 4] – CIM HTTP – TCP an Port **5988**[3] – CIM HTTPS – TCP an Port **5989**[3] – Firmwareaktualisierungen – TCP an Port **6990**[5]	– SNMP-Traps – UDP an Port **162** – IPMI – UDP an Port **623**
Eingehend (Ports auf der XClarity Administrator Einheit geöffnet)	– SFTP – TCP an Port **22**[2] – HTTPS – TCP an Port **443** – SSDP-Erkennung – UDP an Port **1900** – Firmwareaktualisierungen – TCP an Port **6990**[5] – CIM-Meldungen über HTTPS – TCP **9090** – LDAPS – TCP an Ports **50636**[6]**, 50637**	– SFTP – TCP an Port **22**[2] – HTTPS – TCP an Port **443** – Firmwareaktualisierungen – TCP an Port **6990**[5] – CIM-Meldungen über HTTPS – TCP **9090** – LDAPS – TCP an Ports **50636**[6]**, 50637**	– SFTP – TCP an Port **22**[2] – HTTPS – TCP an Port **443** – Firmwareaktualisierungen – TCP an Port **6990**[5] – CIM-Meldungen über HTTPS – TCP **9090** – LDAPS – TCP an Ports **50636**[6]**, 50637**	– SNMP-Traps – UDP an Port **162**

1. Dieser Port muss nur für Server mit IMM2 geöffnet sein.
2. Dieser Port wird zur Übermittlung von Firmwareaktualisierungen mit SFTP verwendet.
3. Standardmäßig wird die Verwaltung über sichere Ports ausgeführt. Die nicht sicheren Ports sind optional.
4. Fernsteuerung und Remote-KVM werden über den Webbrowser und nicht über den XClarity Administrator-Server gestartet.
5. Dieser Port wird verwendet, um eine Verbindung mit dem BMU-BS zur Dateiübertragung und zum Ausführen von Aktualisierungsbefehlen herzustellen.
6. Dieser Port ist erforderlich für die Konfiguration von Servern mithilfe von Konfigurationsmustern.

- **Rack- und Flex-Switches**

Kommunikation	Rack-Switches	Flex-Switches
Ausgehend (Ports auf externen Systemen geöffnet)	– SSH – TCP an Port **22**[1, 3] – SNMP – UDP an Port **161**[2] – SLP – UDP/TCP an Port **427**[6] – HTTPS – TCP an Port **443**[7]	– SSH – TCP an Port **22**[3] – SNMP – UDP an Port **161**[5]
Eingehend (Ports auf der XClarity Administrator Einheit geöffnet)	– SFTP – TCP an Port **22**[4] – SNMP-Traps – TCP an Port **162**[2]	– SFTP – TCP an Port **22**[4] – SNMP-Traps – TCP an Port **162**[2]

1. Bei ENOS-Rack-Switches wird dieser Port verwendet, um Head of Stack(HoS)-Anmeldeinformationen zu konfigurieren, die zwischen CMM und Flex-Switches verwendet werden, den Firmware-Slot zu aktivieren und SSH-Hostschlüssel vor SFTP-Dateiübertragungen zu löschen.
2. Dieser Port muss auf der XClarity Administrator Einheit (eingehend) geöffnet sein, wenn sich Switches in einem anderen Netzwerk befinden als XClarity Administrator, sodass XClarity Administrator Ereignisse für diese Geräte erhalten kann.
3. Dieser Port wird für die Verwaltung (SSH) verwendet.
4. Dieser Port wird zur Übermittlung von Firmwareaktualisierungen mit SFTP verwendet.
5. Bei ENOS-Rack-Switches wird dieser Port zum Übertragen von Bestandsdaten verwendet.
6. Dieser Port wird für die Ermittlung verwendet.
7. Dieser Port wird zur Anwendung von Firmwareaktualisierungen verwendet.

- **Speichereinheiten**

Kommunikation	Speichereinheiten
Ausgehend (Ports auf externen Systemen geöffnet)	– FTP – TCP an Port **21** – SFTP – TCP an Port **22**[2] – SLP – UDP/TCP an Port **427** – HTTPS – TCP an Port **443**[1]
Eingehend (Ports auf der XClarity Administrator Einheit geöffnet)	– HTTPS – TCP an Port **443**[2] – SNMP-Traps – UDP an Port **115**

1. Dieser Port wird zur Übermittlung von Firmwareaktualisierungen verwendet.
2. Dieser Port wird zur Übermittlung und Anwendung von Firmwareaktualisierungen verwendet.

Zugriff von XClarity Administrator auf Datennetzwerk für BS-Implementierung und Einheitentreiberaktualisierungen

Kommunikation	BS-Implementierung[1, 2, 3]	BS-Einheitentreiberaktualisierungen[2]
Ausgehend (Ports auf externen Systemen geöffnet)		• WinRM über HTTP – TCP an Port **5985**[5] • WinRM über HTTPS – TCP an Port **5986**[6]
Eingehend (Ports auf der XClarity Administrator Einheit geöffnet)	• SMB-Kommunikation – TCP an Port **445**[4] • HTTPS (außer ThinkServer) – TCP an Port **8443**[6]	• SMB-Kommunikation – TCP an Port **445**[4]

1. Wenn Sie XClarity Administrator so konfiguriert haben, dass ein Betriebssystemimplementierungs-Netzwerk verwendet wird, müssen die Ports in diesem Netzwerk geöffnet sein.
2. Für eine Liste der Ports, die für die Betriebssystemimplementierung verfügbar sein müssen, siehe Portverfügbarkeit für implementierte Betriebssysteme in der XClarity Administrator Onlinedokumentation. Wenn die Betriebssystemimplementierung beispielsweise für die Verwendung des Datennetzwerks (eth1) konfiguriert ist, müssen diese Ports in diesem Netzwerk geöffnet sein.
3. Jede XClarity Administrator-Instanz hat eine eindeutige Zertifizierungsstelle, die nur für die BS-Implementierung verwendet wird. Diese Zertifizierungsstelle signiert ein Zertifikat, das für den Zielserver an Port 8443 verwendet wird. Wenn die BS-Implementierung gestartet wird, ist das Zertifizierungsstellenzertifikat im BS-Image enthalten, das an den Zielserver weitergeleitet wird. Beim Implementierungsprozess stellt dieser Server wieder eine Verbindung mit Port 8443 her und überprüft das Zertifikat, das Port 8443 beim Handshake bereitstellen, da sie das Zertifizierungsstellenzertifikat haben.
4. Dieser Port wird zur Übertragung von Windows-Treiberdateien verwendet.
5. Dieser Port wird zur Verbindung mit dem Zielserver-WinRM verwendet.
6. Dieser Port wird zum Austausch von Daten zwischen dem Ziel-BS und XClarity Administrator, einschließlich BS-Images und Status.

Verwaltungshinweise

Bei der Verwaltung von Einheiten stehen verschiedene Möglichkeiten zur Wahl. Abhängig von den Einheiten, die verwaltet werden, benötigen Sie möglicherweise mehrere Verwaltungslösungen gleichzeitig.

Eine Einheit kann nur von einer Instanz von Lenovo XClarity Administrator verwaltet werden. Sie können jedoch andere Verwaltungssoftware (z. B. VMware vRealize Operations Manager) zusammen mit Lenovo XClarity Administrator verwenden, um von XClarity Administrator verwaltete Einheiten zu *überwachen*.

Achtung: Bei der Verwendung mehrerer Verwaltungstools zur Verwaltung Ihrer Einheiten muss besondere Vorsicht walten gelassen werden, um unvorhersehbare Konflikte zu vermeiden. Beispielsweise könnte das Übermitteln von Änderungen an der Stromversorgung mit einem anderen Tool zu einem Konflikt mit Konfigurations- oder Aktualisierungsjobs, die in XClarity Administrator ausgeführt werden. führen.

ThinkSystem-, ThinkServer- und System x-Einheiten

Wenn Sie beabsichtigen, eine andere Verwaltungssoftware zu verwenden, um Ihre verwalteten Einheiten zu überwachen, erstellen Sie einen neuen lokalen Benutzer mit den richtigen SNMP- oder IPMI-Einstellungen aus der IMM-Schnittstelle. Stellen Sie sicher, dass Sie SNMP- oder IPMI-Berechtigungen erteilen, abhängig von Ihren Anforderungen.

Flex System-Einheiten

Wenn Sie planen, eine andere Verwaltungssoftware zur Überwachung der verwalteten Einheiten zu nutzen und diese Verwaltungssoftware über SNMPv3 oder IPMI kommuniziert, müssen Sie die Umgebung vorbereiten. Führen Sie für jeden verwalteten CMM folgende Schritte aus:

1. Melden Sie sich bei der Management-Controller-Webschnittstelle für das Gehäuse mit dem `RECOVERY_ID`-Benutzernamen und dem Kennwort an.
2. Wenn für die Sicherheitsrichtlinie **Sicher** festgelegt wurde, ändern Sie das Benutzerauthentifizierungsverfahren.
   a. Klicken Sie auf **Mgt Modulverwaltung → Benutzeraccounts**.
   b. Wechseln Sie auf die Registerkarte **Konten**.
   c. Klicken Sie auf **Globale Anmeldeeinstellungen**.
   d. Klicken Sie auf die Registerkarte **Allgemein**.
   e. Wählen Sie für das Benutzerauthentifizierungsverfahren die Option **Erst externe, danach lokale Authentifizierung** aus.
   f. Klicken Sie auf **OK**.
3. Erstellen Sie über die Management-Controller-Webschnittstelle einen neuen lokalen Benutzer mit den richtigen SNMP- oder IPMI-Einstellungen.
4. Wenn für die Sicherheitsrichtlinie **Sicher** festgelegt wurde, melden Sie sich bei der Management-Controller-Webschnittstelle ab und anschließend mit dem neuen Benutzernamen und dem Kennwort an. Ändern Sie das Kennwort für den neuen Benutzer, wenn Sie dazu aufgefordert werden.

Sie können den neuen Benutzer jetzt als aktiven SNMP- oder IPMI-Benutzer verwenden.

Anmerkung: Wenn Sie die Verwaltung des Gehäuses aufheben und dann wieder aufnehmen, wird dieser neue Benutzeraccount gesperrt und deaktiviert. In diesem Fall müssen Sie diese Schritte wiederholen und einen neuen Benutzeraccount erstellen.

Hinweise zum Netzwerkbetrieb

Berücksichtigen Sie bei der Planung der Lenovo XClarity Administrator-Installation die Netzwerktopologie, die in Ihrer Umgebung implementiert ist, und wie XClarity Administrator in diese Topologie passt.

Wichtig: 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. Wenn Sie DHCP nutzen, stellen Sie sicher, dass die IP-Adressenänderungen minimiert werden.

IP-Konfigurationseinschränkungen

Für die folgenden Funktionen und verwalteten Einheiten müssen die Netzwerkschnittstellen mit einer IPv4-Adresse konfiguriert werden. IPv6-Adressen werden nicht unterstützt.

- Firmwareaktualisierungen für Lenovo Storage-Einheiten
- ThinkServer-Server
- Lenovo Storage-Einheit

Verwaltung von RackSwitch-Einheiten mit IPv6-Link-Local über einen Daten- oder Verwaltungsanschluss wird nicht unterstützt.

Network Address Translation (NAT), die einen IP-Adressraum in einen anderen neu zuordnet, wird nicht unterstützt.

Netzwerktypen

Im Allgemeinen werden in den meisten Umgebungen die folgenden Netzwerktypen implementiert. Je nach Anforderungen können Sie eines oder alle drei Netzwerke implementierten.

- **Verwaltungsnetzwerk**

  Das Verwaltungsnetzwerk ist in der Regel für die Kommunikation zwischen Lenovo XClarity Administrator und den Verwaltungsprozessoren für verwaltete Einheiten reserviert. Beispielsweise kann das Verwaltungsnetzwerk so konfiguriert werden, dass es XClarity Administrator, die CMMs für alle verwalteten Gehäuse und den Baseboard Management Controller für alle Server enthält, die von XClarity Administrator verwaltet werden.

- **Datennetzwerk**

  Das Datennetzwerk wird in der Regel für die Kommunikation zwischen den Betriebssystemen verwendet, die auf den Servern und im Intranet des Unternehmens und/oder im Internet installiert sind.

- **Betriebssystem-Bereitstellungsnetzwerk**

  Mit der Einrichtung von Betriebssystem-Bereitstellungsnetzwerken kann die Kommunikation, die für die Bereitstellung von Betriebssystemen auf Servern erforderlich ist, ausgelagert werden. Dieses Netzwerk enthält nach der Bereitstellung in der Regel XClarity Administrator und alle Serverhosts.

  Sie können diese Funktion aber auch in das Verwaltungs- oder Datennetzwerk integrieren, anstatt ein separates Betriebssystem-Bereitstellungsnetzwerk zu implementieren.

Netzwerkkonfigurationen

Sie können Lenovo XClarity Administrator für die Verwendung von ein oder zwei Netzwerkschnittstellen konfigurieren.

Achtung:

- Das Ändern der IP-Adresse von XClarity Administrator nach der Verwaltung von Einheiten kann dazu führen, dass die Einheiten in XClarity Administrator in den Offlinestatus versetzt werden. Stellen Sie sicher, dass die Verwaltung aller Einheiten aufgehoben wurde, bevor Sie die IP-Adresse ändern.
- Sie können die Prüfung auf doppelte IP-Adressen im selben Subnetz aktivieren oder deaktivieren, indem Sie auf die Umschalt-Schaltfläche **Doppelte IP-Adressen prüfen** klicken. Die Option ist standardmäßig deaktiviert. Bei Aktivierung löst XClarity Administrator einen Alert aus, wenn Sie versuchen, die IP-Adresse von XClarity Administrator zu ändern oder eine Einheit zu verwalten, die dieselbe IP-Adresse wie eine andere verwaltete Einheit oder eine andere Einheit im selben Subnetz hat.

  Anmerkung: Wenn diese Option aktiviert ist, führt XClarity Administrator einen ARP-Scan aus, um aktive IPv4-Komponenten im selben Subnetz zu finden. Wenn Sie den ARP-Scan verhindern möchten, deaktivieren Sie **Doppelte IP-Adressen prüfen**.
- Wenn XClarity Administrator als eine virtuelle Einheit ausgeführt wird und die Netzwerkschnittstelle für das Verwaltungsnetzwerk für die Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert ist, ändert sich möglicherweise die IP-Adresse der Verwaltungsschnittstelle, wenn die DHCP-Zugangsberechtigung abläuft. Ist das der Fall, müssen Sie die Gehäuse-, Rack- und Tower-Server-Verwaltung zunächst aufheben und anschließend erneut aufnehmen. Sie können dieses Problem vermeiden, indem Sie entweder für die Verwaltungsschnittstelle eine statische IP-Adresse angeben oder den DHCP-Server so konfigurieren, dass die DHCP-Adresse auf einer MAC-Adresse basiert oder die DHCP-Zugangsberechtigung nicht abläuft.
- Wenn Sie *nicht* beabsichtigen, XClarity Administrator zum Implementieren des Betriebssystems oder Aktualisieren von BS-Einheitentreibern zu verwenden, können Sie Samba- und Apache-Server deaktivieren, indem für die Netzwerkschnittstelle die Option **Nur Hardware ermitteln und verwalten** konfigurieren. Beachten Sie, dass der Verwaltungsserver nach dem Ändern der Einstellungen für die Netzwerkschnittstelle neu gestartet wird.

- Wenn XClarity Administrator als Container ausgeführt wird.
  - Sie können nur die Überprüfung auf doppelte IP-Adressen aktivieren oder deaktivieren, die Netzwerkschnittstellenrollen ändern und Proxyeinstellungen ändern. Alle anderen Netzwerkeinstellungen (einschließlich IP-Adresse, Gateway und DNS) werden in der Containerkonfiguration definiert.
  - Stellen Sie sicher, dass ein macvlan-Netzwerk auf dem Hostsystem eingerichtet ist.

XClarity Administrator verfügt über zwei separate Netzwerkschnittstellen, die je nach implementierter Netzwerktopologie für Ihre Umgebung definiert werden können. Bei virtuellen Einheiten werden diese Netzwerke als „eth0“ und „eth1“ bezeichnet. Sie können benutzerdefinierte Namen für Container festlegen.

- Wenn nur eine Netzwerkschnittstelle (Eth0) vorhanden ist:
  - Die Schnittstelle muss für die Ermittlung und Verwaltung (z. B. Serverkonfiguration und Firmwareaktualisierungen) konfiguriert werden. Sie muss mit CMMs und Flex-Switches in allen verwalteten Gehäusen, den Baseboard Management Controllern in sämtlichen verwalteten Servern und mit allen RackSwitch-Switches kommunizieren können.
  - Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.
  - Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
  - Wenn Sie Betriebssystem-Images implementieren und BS-Einheitentreiber aktualisieren möchten, muss die Schnittstelle eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle haben, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

    Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.
- Wenn zwei Netzwerkschnittstellen (Eth0 und Eth1) vorhanden sind:
  - Die erste Netzwerkschnittstelle (in der Regel die Eth0-Schnittstelle) muss mit dem Verwaltungsnetzwerk verbunden und für die Unterstützung der Einheitenermittlung und -verwaltung (einschließlich Serverkonfiguration und Firmwareaktualisierungen) konfiguriert sein. Sie muss mit CMMs und Flex-Switches in sämtlichen verwalteten Gehäusen, den Management-Controllern in allen verwalteten Servern und mit sämtlichen RackSwitch-Switches kommunizieren können.
  - Die zweite Netzwerkschnittstelle (in der Regel die Eth1-Schnittstelle) kann so konfiguriert werden, dass eine Kommunikationsverbindung mit einem internen Datennetzwerk, einem öffentlichen Datennetzwerk oder mit beiden möglich ist.
  - Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.
  - Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss

mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.

– Wenn Sie beabsichtigen, Betriebssystem-Images zu implementieren und Einheitentreiber zu aktualisieren, können Sie entweder die Eth1- oder die Eth0-Schnittstelle verwenden. Die Schnittstelle, die Sie verwenden, muss jedoch über eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle verfügen, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

  Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.

In der folgenden Tabelle werden Konfigurationsmöglichkeiten für die XClarity Administrator-Netzwerkschnittstellen auf Basis des Typs der in Ihrer Umgebung implementierten Netzwerktopologie beschrieben. Verwenden Sie diese Tabelle, um zu bestimmen, wie Sie jede Netzwerkschnittstelle definieren.

Tabelle 2. Rolle jeder Netzwerkschnittstelle auf Basis der Netzwerktopologie

Netzwerktopologie	**Rolle von Schnittstelle1 (eth0)**	**Rolle von Schnittstelle2 (eth1)**
Konvergentes Netzwerk (Verwaltungs- und Datennetzwerk mit Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen)	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten • BS-Implementierung • BS-Einheitentreiberaktualisierungen	Keine Angabe
Separates Verwaltungsnetzwerk mit Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen sowie Datennetzwerk	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten • BS-Implementierung • BS-Einheitentreiberaktualisierungen	Datennetzwerk • Keine Angabe

Tabelle 2. Rolle jeder Netzwerkschnittstelle auf Basis der Netzwerktopologie (Forts.)

Netzwerktopologie	Rolle von Schnittstelle1 (eth0)	Rolle von Schnittstelle2 (eth1)
Separates Verwaltungsnetzwerk und Datennetzwerk mit Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten	Datennetzwerk • BS-Implementierung • BS-Einheitentreiberaktualisierungen
Separates Verwaltungsnetzwerk und Datennetzwerk ohne Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten	Datennetzwerk • Keine Angabe
Nur-Verwaltungsnetzwerk (ohne Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen)	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten	Keine Angabe

Einzelne Daten und Verwaltungsnetzwerk

In dieser Netzwerktopologie befinden sich Verwaltungs- und Datenkommunikationsverbindungen und die Betriebssystembereitstellung im selben Netzwerk. Diese Topologie nennt man *konvergentes* Netzwerk.

Wichtig: Die Bereitstellung eines gemeinsamen Daten- und Verwaltungsnetzwerks, enthält, kann zu Unterbrechungen im Datenverkehr führen. Zum Beispiel können je nach Netzwerkkonfiguration (wenn etwa die Priorität des Serverdatenverkehrs hoch und die Priorität des von Management-Controllern ausgehenden Datenverkehrs gering ist) Pakete verloren gehen oder es können Netzkonnektivitätsprobleme auftreten. Das Verwaltungsnetzwerk verwendet neben TCP- auch UDP-Datenverkehr. UDP-Datenverkehr kann bei hohem Netzwerkverkehrsaufkommen eine niedrigere Priorität haben.

Beachten Sie bei der Installation von Lenovo XClarity Administrator die folgenden Aspekte für die Definition der Eth0-Netzwerkschnittstelle:

- Die Schnittstelle muss für die Ermittlung und Verwaltung (z. B. Serverkonfiguration und Firmwareaktualisierungen) konfiguriert werden. Sie muss mit CMMs und Flex-Switches in allen verwalteten Gehäusen, den Baseboard Management Controllern in sämtlichen verwalteten Servern und mit allen RackSwitch-Switches kommunizieren können.
- Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.

- Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
- Wenn Sie Betriebssystem-Images implementieren und BS-Einheitentreiber aktualisieren möchten, muss die Schnittstelle eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle haben, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

  Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.
- Sie können XClarity Administrator auf jedem System installieren, das die Anforderungen für XClarity Administrator erfüllt, darunter auch verwaltete Server, wenn Sie entweder ein gemeinsames Daten- und Verwaltungsnetzwerk oder ein logisch getrenntes Daten- und Verwaltungsnetzwerk bereitstellen; Sie können jedoch mit XClarity Administrator keine Firmwareaktualisierungen für diesen verwalteten Server durchführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator Hosts installiert.

Zur Unterstützung der Redundanz können Sie auch eine zweite Netzwerkschnittstelle für eine Verbindung mit demselben Netzwerk über XClarity Administrator konfigurieren.

Die folgende Abbildung zeigt ein Beispiel für die Bereitstellung einer konvergenten Netzwerktopologie.

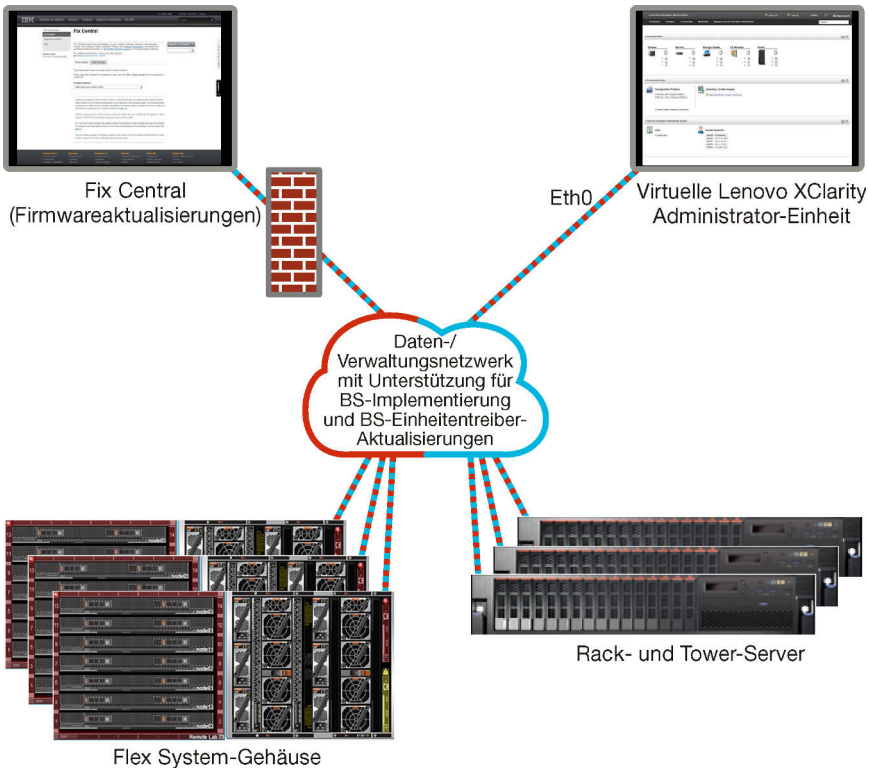


Abbildung 1. Beispiel für die Bereitstellung eines gemeinsamen Netzwerks für Verwaltung, Daten und die Betriebssystembereitstellung

Physisch getrennte Daten und Verwaltungsnetzwerk

In dieser Netzwerktopologie sind das Verwaltungsnetzwerk und das Datennetzwerk physische Einzelnetze und das Betriebssystem-Bereitstellungsnetzwerk wird entweder als Teil des Verwaltungsnetzwerks oder als Teil des Datennetzwerks konfiguriert.

Beachten Sie bei der Installation von Lenovo XClarity Administrator folgenden Aspekte für die Definition der Netzwerkeinstellungen:

- Die erste Netzwerkschnittstelle (in der Regel die Eth0-Schnittstelle) muss mit dem Verwaltungsnetzwerk verbunden und für die Unterstützung der Einheitenermittlung und -verwaltung (einschließlich Serverkonfiguration und Firmwareaktualisierungen) konfiguriert sein. Sie muss mit CMMs und Flex-Switches in sämtlichen verwalteten Gehäusen, den Management-Controllern in allen verwalteten Servern und mit sämtlichen RackSwitch-Switches kommunizieren können.
- Die zweite Netzwerkschnittstelle (in der Regel die Eth1-Schnittstelle) kann so konfiguriert werden, dass eine Kommunikationsverbindung mit einem internen Datennetzwerk, einem öffentlichen Datennetzwerk oder mit beiden möglich ist.
- Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.
- Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
- Wenn Sie beabsichtigen, Betriebssystem-Images zu implementieren und Einheitentreiber zu aktualisieren, können Sie entweder die Eth1- oder die Eth0-Schnittstelle verwenden. Die Schnittstelle, die Sie

verwenden, muss jedoch über eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle verfügen, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.

Abbildung 2 „Beispiel für die Bereitstellung eines physisch getrennten Daten- und Verwaltungsnetzwerks, in dem das Betriebssystemnetzwerk Teil des Datennetzwerks ist“ auf Seite 25 zeigt ein Beispiel für die Bereitstellung von getrennten Verwaltungs- und Datennetzwerken, in denen das Betriebssystem-Implementierungsnetzwerk als Teil des Datennetzwerks konfiguriert ist.

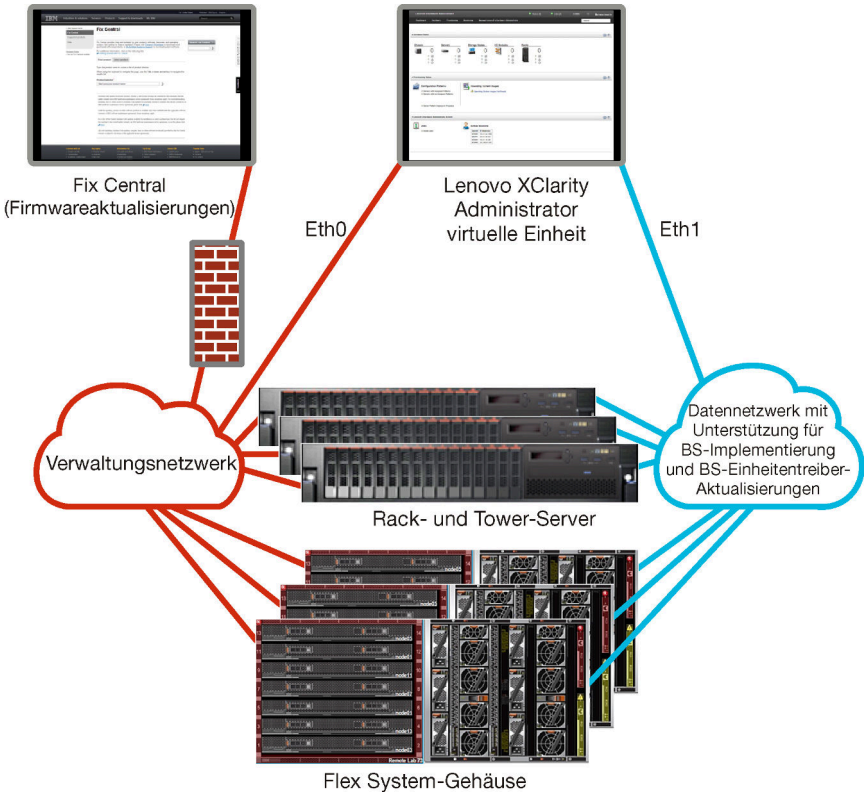


Abbildung 2. Beispiel für die Bereitstellung eines physisch getrennten Daten- und Verwaltungsnetzwerks, in dem das Betriebssystemnetzwerk Teil des Datennetzwerks ist

Abbildung 3 „Beispiel für die Bereitstellung eines physisch getrennten Daten- und Verwaltungsnetzwerks, in dem das Betriebssystemnetzwerk Teil des Verwaltungsnetzwerks ist“ auf Seite 26 zeigt ein weiteres Beispiel für die Bereitstellung von getrennten Verwaltungs- und die Datennetzwerken, in denen das Betriebssystem-Implementierungsnetzwerk als Teil des Verwaltungsnetzwerks konfiguriert ist. In dieser Implementierung benötigt XClarity Administrator keine Verbindung zum Datennetzwerk.

Anmerkung: Wenn das Betriebssystem-Bereitstellungsnetzwerk keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem auf dem Server zum Datennetzwerk bereitzustellen, falls erforderlich.

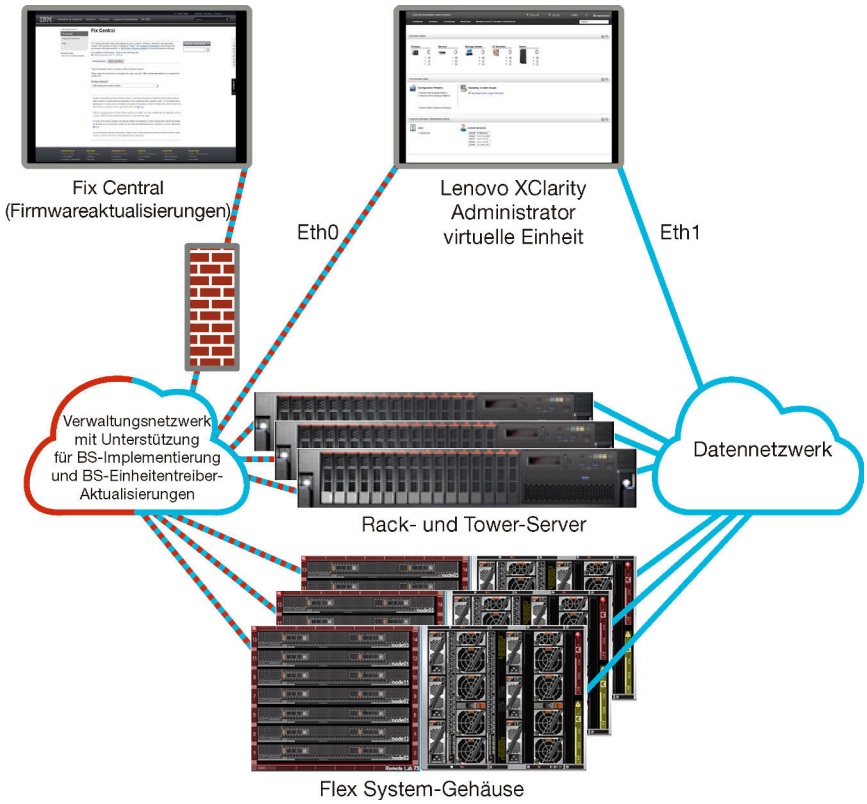


Abbildung 3. Beispiel für die Bereitstellung eines physisch getrennten Daten- und Verwaltungsnetzwerks, in dem das Betriebssystemnetzwerk Teil des Verwaltungsnetzwerks ist

Virtuell getrennte Daten und Verwaltungsnetzwerk

In dieser Topologie sind Daten- und Verwaltungsnetzwerk logisch getrennt. Die Pakete aus dem Datennetzwerk und die Pakete aus dem Verwaltungsnetzwerk werden über dieselbe physische Verbindung übertragen. Mithilfe von VLAN-Tagging in allen Verwaltungsnetzwerkdatenpaketen wird der Datenverkehr zwischen den beiden Netzwerken getrennt.

Anmerkung: Wenn Lenovo XClarity Administrator auf einem Host in einem verwalteten Server in einem Gehäuse installiert ist, können Sie mit XClarity Administrator keine Firmwareaktualisierungen auf das gesamte Gehäuse anwenden. Wenn Firmwareaktualisierungen durchgeführt werden, muss das Hostsystem neu gestartet werden.

Beachten Sie bei der Installation von XClarity Administrator folgenden Aspekte für die Definition der Netzwerkeinstellungen:

- Die erste Netzwerkschnittstelle (in der Regel die Eth0-Schnittstelle) muss mit dem Verwaltungsnetzwerk verbunden und für die Unterstützung der Einheitenermittlung und -verwaltung (einschließlich Serverkonfiguration und Firmwareaktualisierungen) konfiguriert sein. Sie muss mit CMMs und Flex-Switches in sämtlichen verwalteten Gehäusen, den Management-Controllern in allen verwalteten Servern und mit sämtlichen RackSwitch-Switches kommunizieren können.
- Die zweite Netzwerkschnittstelle (in der Regel die Eth1-Schnittstelle) kann so konfiguriert werden, dass eine Kommunikationsverbindung mit einem internen Datennetzwerk, einem öffentlichen Datennetzwerk oder mit beiden möglich ist.
- Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.

- Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
- Wenn Sie beabsichtigen, Betriebssystem-Images zu implementieren und Einheitentreiber zu aktualisieren, können Sie entweder die Eth1- oder die Eth0-Schnittstelle verwenden. Die Schnittstelle, die Sie verwenden, muss jedoch über eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle verfügen, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

  Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.
- Sie können XClarity Administrator auf jedem System installieren, das die Anforderungen für XClarity Administrator erfüllt, darunter auch verwaltete Server, wenn Sie entweder ein gemeinsames Daten- und Verwaltungsnetzwerk oder ein logisch getrenntes Daten- und Verwaltungsnetzwerk bereitstellen; Sie können jedoch mit XClarity Administrator keine Firmwareaktualisierungen für diesen verwalteten Server durchführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator Hosts installiert.

Abbildung 4 „Beispiel für die Bereitstellung eines logisch getrennten Daten- und Verwaltungsnetzwerks, in dem das Betriebssystemnetzwerk Teil des Datennetzwerks ist“ auf Seite 28 zeigt ein Beispiel für die Bereitstellung von virtuell getrennten Verwaltungs- und Datennetzwerken, in denen das Betriebssystem-Implementierungsnetzwerk als Teil des Datennetzwerks konfiguriert ist. In diesem Beispiel wird XClarity Administrator auf einem verwalteten Server in einem Gehäuse installiert.

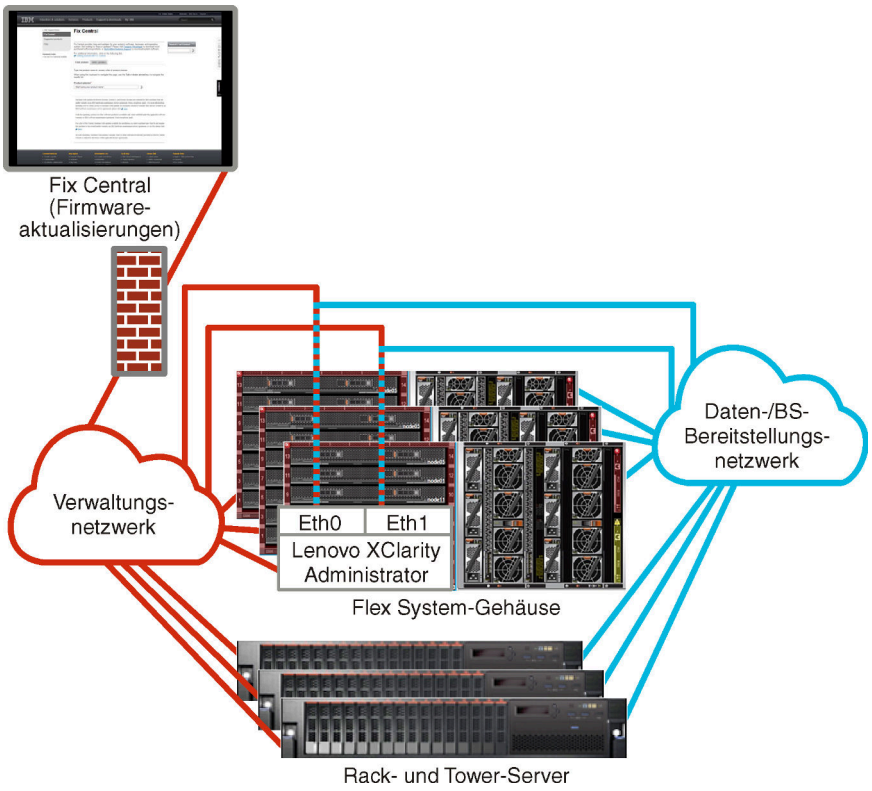


Abbildung 4. Beispiel für die Bereitstellung eines logisch getrennten Daten- und Verwaltungsnetzwerks, in dem das Betriebssystemnetzwerk Teil des Datennetzwerks ist

Abbildung 5 „Beispiel für die Bereitstellung eines logisch getrennten Verwaltungs- und Datennetzwerks, in dem das Betriebssystemnetzwerk Teil des Verwaltungsnetzwerks ist“ auf Seite 29 zeigt ein Beispiel für die Bereitstellung von virtuell getrennten Verwaltungs- und Datennetzwerken, in denen das Betriebssystem-Bereitstellungsnetzwerk als Teil des Verwaltungsnetzwerks konfiguriert und XClarity Administrator auf einem verwalteten Server in einem Gehäuse installiert ist. In dieser Implementierung benötigt XClarity Administrator keine Verbindung zum Datennetzwerk.

Anmerkung: Wenn das Betriebssystem-Bereitstellungsnetzwerk keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem auf dem Server zum Datennetzwerk bereitzustellen, falls erforderlich.

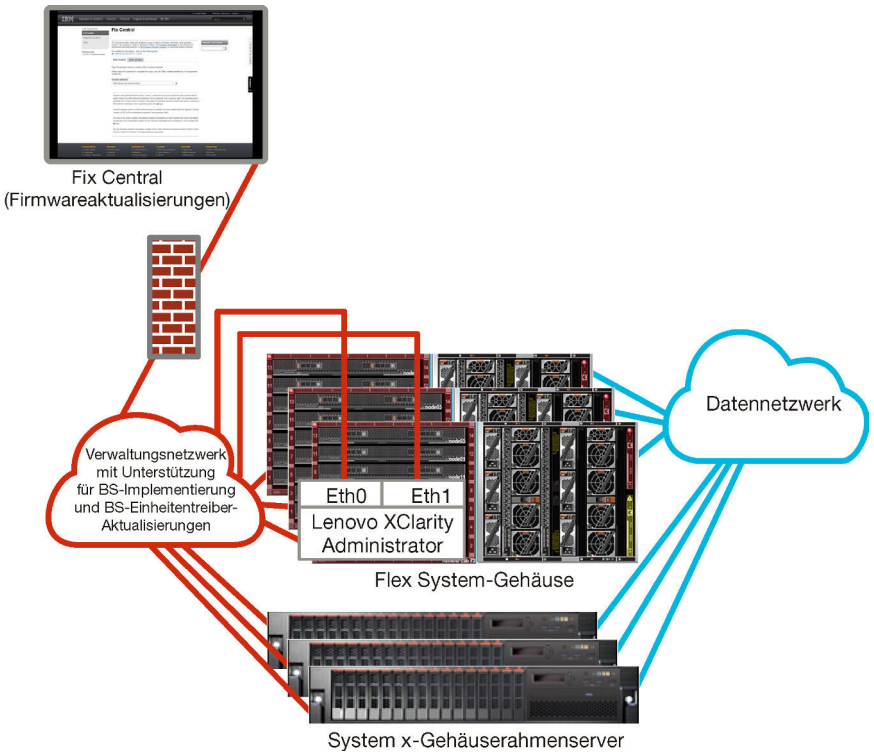


Abbildung 5. Beispiel für die Bereitstellung eines logisch getrennten Verwaltungs- und Datennetzwerks, in dem das Betriebssystemnetzwerk Teil des Verwaltungsnetzwerks ist

Nur-Verwaltungsnetzwerk

In dieser Topologie hat Lenovo XClarity Administrator nur Zugriff auf das Verwaltungsnetzwerk, nicht auf das Datennetzwerk. XClarity Administrator muss allerdings über Zugriff auf das Betriebssystembereitstellungsnetzwerk verfügen, wenn Sie Betriebssystem-Images für verwaltete Server mit XClarity Administrator implementieren möchten.

Wenn Sie XClarity Administrator installieren und Netzwerkeinstellungen definieren, muss die eth0-Netzwerkschnittstelle folgendermaßen konfiguriert werden:

- Die Schnittstelle muss für die Ermittlung und Verwaltung (z. B. Serverkonfiguration und Firmwareaktualisierungen) konfiguriert werden. Sie muss mit CMMs und Flex-Switches in allen verwalteten Gehäusen, den Baseboard Management Controllern in sämtlichen verwalteten Servern und mit allen RackSwitch-Switches kommunizieren können.
- Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.
- Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
- Wenn Sie Betriebssystem-Images implementieren und BS-Einheitentreiber aktualisieren möchten, muss die Schnittstelle eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle haben, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

  Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das

Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.

Zur Unterstützung der Redundanz können Sie auch eine zweite Netzwerkschnittstelle für eine Verbindung mit demselben Netzwerk über XClarity Administrator konfigurieren.

In Abbildung 6 „Beispiel für die Implementierung eines Nur-Verwaltungsnetzwerks ohne Unterstützung von Betriebssystembereitstellungen“ auf Seite 30 wird eine Beispielimplementierung für ein Nur-Verwaltungsnetzwerk dargestellt. In diesem Beispiel wird keine Betriebssystembereitstellung über XClarity Administrator unterstützt.

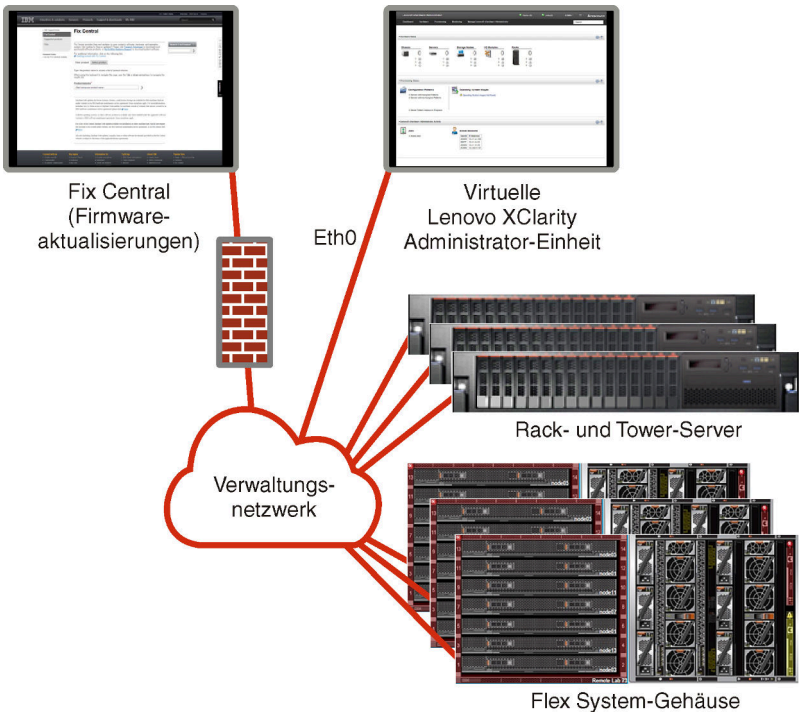


Abbildung 6. Beispiel für die Implementierung eines Nur-Verwaltungsnetzwerks ohne Unterstützung von Betriebssystembereitstellungen

In Abbildung 6 „Beispiel für die Implementierung eines Nur-Verwaltungsnetzwerks ohne Unterstützung von Betriebssystembereitstellungen“ auf Seite 30 wird eine Beispielimplementierung für ein Nur-Verwaltungsnetzwerk mit Unterstützung für Betriebssystembereitstellungen über XClarity Administrator gezeigt.

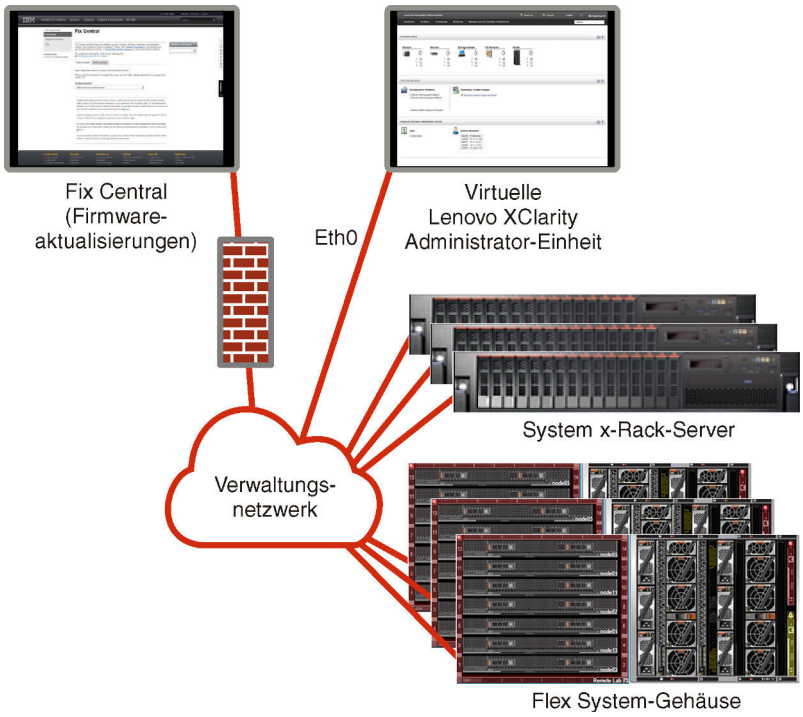


Abbildung 7. Beispiel für die Implementierung eines Nur-Verwaltungsnetzwerks mit Unterstützung von Betriebssystembereitstellungen

Sicherheitsaspekte

Plan für die Sicherheit von Lenovo XClarity Administrator und allen verwalteten Einheiten.

Kapselungsverwaltung

Wenn Sie Lenovo Gehäuse und Server in Lenovo XClarity Administrator verwalten, können Sie über Lenovo XClarity Administrator die Firewallregeln für Einheiten so konfigurieren, dass nur eingehende Anforderungen von Lenovo XClarity Administrator akzeptiert werden. Dies wird als *Kapselung* bezeichnet. Sie können die Kapselung auch für Gehäuse und Server aktivieren und deaktivieren, die bereits von Lenovo XClarity Administrator verwaltet werden.

Wenn die Kapselung auf Einheiten aktiviert ist, die Kapselung unterstützen, ändert Lenovo XClarity Administrator den Kapselungsmodus für die Einheiten in „encapsulationLite“. Außerdem werden die Firewallregeln auf der Einheit so eingestellt, dass eingehende Anforderungen nur von diesem Lenovo XClarity Administrator akzeptiert werden.

Ist die Kapselung deaktiviert, ist der Kapselungsmodus auf „Normal“ festgelegt. Wenn die Kapselung zuvor auf den Einheiten aktiviert war, werden die Firewallregeln für die Kapselung entfernt.

Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Gehäuseverwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen und Rack- oder Tower-Serververwaltung nach einem Verwaltungsserverausfall wiederherstellen in der Onlinedokumentation von XClarity Administrator.

Anmerkungen:

- Die Kapselung wird für Switches, Speichereinheiten und Gehäuse bzw. Server anderer Hersteller (nicht Lenovo) nicht unterstützt.

- Wenn die Verwaltungsnetzwerkschnittstelle zur Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert ist und die Kapselung aktiviert ist, kann die Verwaltung eines Rack-Servers sehr viel Zeit in Anspruch nehmen.

Weitere Informationen zur Kapselung finden Sie unter Kapselung aktivieren in der Onlinedokumentation von XClarity Administrator.

Verschlüsselungsverwaltung

Die Verschlüsselungsverwaltung besteht aus Kommunikationsmodi und -protokollen, die die Methode für eine sichere Kommunikation zwischen Lenovo XClarity Administrator und den verwalteten Systemen (wie Gehäusen, Servern und Flex-Switches) steuern.

Verschlüsselungsalgorithmen

XClarity Administrator unterstützt TLS 1.2 und stärkere Verschlüsselungsalgorithmen für sichere Netzwerkverbindungen.

Für eine höhere Sicherheit werden nur hohe Verschlüsselungsgrade unterstützt. Die Clientbetriebssysteme und Ihre Webbrowser müssen eines der folgenden Verschlüsselungssysteme unterstützen.
- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

Verschlüsselungsmodi für den Verwaltungsserver

Diese Einstellung legt fest, welche Methode für eine sichere Kommunikation vom Verwaltungsserver verwendet werden soll.

- **Kompatibilität**. Dies ist der Standardmodus. Er ist kompatibel mit älteren Firmwareversionen, Browsern und anderen Netzwerkclients, auf denen nicht die strengeren Sicherheitsstandards implementiert werden, die für die Konformität mit NIST SP 800-131A erforderlich sind.
- **NIST SP 800-131A**. Dieser Modus entspricht dem NIST SP 800-131A-Standard. XClarity Administrator ist so konzipiert, dass intern immer eine starke Verschlüsselung und, sofern verfügbar, stark verschlüsselte Netzwerkverbindungen verwendet werden. Allerdings sind in diesem Modus Netzverbindungen unzulässig, die eine von NIST SP 800-131A nicht genehmigte Verschlüsselung verwenden; so werden z. B. Transport Layer Security (TLS)-Zertifikate zurückgewiesen, die mit SHA-1 oder schwächerem Hash signiert sind.

  Beachten Sie bei Auswahl dieses Modus Folgendes:

  – Für alle Ports außer Port 8443 sind alle TLS-CBC-Codierschlüssel und alle Codierschlüssel deaktiviert, die kein Perfect Forward Secrecy unterstützen.

  – Ereignisbenachrichtigungen werden möglicherweise nicht erfolgreich an einige Mobilgeräteabonnements weitergeleitet (siehe Ereignisse an mobile Einheiten weiterleiten in der XClarity Administrator Onlinedokumentation). Externe Services wie Android und iOS legen SHA-1-signierte Zertifikate vor; dieser Algorithmus entspricht nicht den strikten Anforderungen von NIST SP 800-131A. Dementsprechend können bei Verbindungen zu diesen Services Zertifikatsausnahmen oder Handshakefehler auftreten.

Weitere Informationen über die Konformität mit NIST SP 800-131A finden Sie unter NIST 800-131A-Konformität implementieren in der XClarity Administrator Onlinedokumentation.

Weitere Informationen zum Festlegen der Sicherheitsmodi auf dem Verwaltungsserver finden Sie unter Verschlüsselungsmodus und Kommunikationsprotokolle festlegen in der Onlinedokumentation von XClarity Administrator.

Sicherheitsmodi für verwaltete Server

Diese Einstellung legt fest, welche Methode für eine sichere Kommunikation von den verwalteten Servern verwendet werden soll.

- **Kompatibilität für Sicherheit**. Wählen Sie diesen Modus aus, wenn Services und Clients eine Verschlüsselung erfordern, die nicht CNSA/FIPS entspricht. Dieser Modus unterstützt eine Vielzahl von Verschlüsselungsalgorithmen und ermöglicht die Aktivierung aller Services.
- **NIST SP 800-131A**. Wählen Sie diesen Modus aus, um die Einhaltung des Standards NIST SP 800-131A sicherzustellen. Eingeschlossen sind hier einschränkende RSA-Schlüssel bis 2048 Bit oder höher und einschränkende Hashwerte für digitale Signaturen für SHA-256 oder länger. Des Weiteren muss sichergestellt werden, dass nur NIST-zertifizierte, symmetrische Verschlüsselungsalgorithmen verwendet werden. Für diesen Modus muss der SSL/TLS-Modus auf **TLS 1.2 Server Client** festgelegt werden.

  Dieser Modus wird *nicht* für Server mit XCC2 unterstützt.
- **Standardsicherheit**. (Nur Server mit XCC2) Dies ist der Standardsicherheitsmodus für Server mit XCC2. Wählen Sie diesen Modus aus, um die Einhaltung des Standards FIPS 140-3 sicherzustellen. Damit XCC im überprüften FIPS 140-3-Modus betrieben wird, können nur Services aktiviert werden, die eine Verschlüsselung auf FIPS 140-3-Ebene unterstützen. Services, die keine Verschlüsselung auf FIPS 140-2/140-3-Ebene unterstützen, werden standardmäßig deaktiviert, aber können bei Bedarf aktiviert werden. Wenn ein Service aktiviert ist, der eine Verschlüsselung verwendet, die nicht auf FIPS 140-3-Ebene ist, kann XCC nicht im überprüften FIPS 140-3-Modus betrieben werden. Dieser Modus erfordert Zertifikate auf FIPS-Ebene.
- **„Enterprise Strikt“-Sicherheit**. (Nur Server mit XCC2) Dies ist der sicherste Modus. Wählen Sie diesen Modus aus, um die Einhaltung des CNSA-Standards sicherzustellen. Es sind nur Services zulässig, die die Verschlüsselung auf CNSA-Ebene unterstützen. Unsichere Services sind standardmäßig deaktiviert und können nicht aktiviert werden. Dieser Modus erfordert Zertifikate auf CNSA-Ebene.

  XClarity Administrator verwendet RSA-3072/SHA-384-Zertifikatsignaturen für Server im Modus **„Enterprise Strikt“-Sicherheit**.

  Wichtig:

  – Der XCC2 FoD-Schlüssel (Feature On Demand) muss bei jedem ausgewählten Server mit XCC2 installiert sein, damit dieser Modus verwendet werden kann.

  – Wenn XClarity Administrator ein selbst signiertes Zertifikat nutzt, muss XClarity Administrator in diesem Modus ein RSA-3072/SHA-384-basiertes Stammzertifikat und Serverzertifikat verwenden. Wenn XClarity Administrator ein extern signiertes Zertifikat verwendet, muss XClarity Administrator eine RSA-3072/SHA-384-basierte Zertifikatssignieranforderung generieren und die externe Zertifizierungsstelle kontaktieren, um ein neues Serverzertifikat auf Basis von RSA-3072/SHA-384 zu signieren.

  – Wenn XClarity Administrator ein RSA-3072/SHA-384-basiertes Zertifikat verwendet, trennt XClarity Administrator möglicherweise Einheiten mit Ausnahme von Flex System Gehäusen (CMMs) und Servern, ThinkSystem Servern, ThinkServer Servern, System x M4 und M5 Servern, Switches der Lenovo ThinkSystem DB Serie, Lenovo RackSwitch, Flex System Switches, Mellanox Switches, Speichereinheiten der ThinkSystem DE/DM Serie, IBM Bandbibliotheksspeicher und ThinkSystem SR635/SR655 Server, auf denen Firmware vor 22C geflasht ist. Um die getrennten Einheiten weiterhin zu verwalten, müssen Sie eine weitere XClarity Administrator-Instanz mit einem RSA-2048/SHA-384-basierten Zertifikat einrichten.

Beachten Sie die folgenden Auswirkungen, die eine Änderung des Verschlüsselungsmodus mit sich bringt.

- Der Wechsel vom Modus **Kompatibilität für Sicherheit** oder **Standardsicherheit** zum Modus **„Enterprise Strikt“-Sicherheit** wird nicht unterstützt.
- Wenn Sie ein Upgrade vom Modus **Kompatibilität für Sicherheit** zu **Standardsicherheit** ausführen, werden Sie gewarnt, wenn importierte Zertifikate oder öffentliche SSH-Schlüssel nicht konform sind. Sie können trotzdem ein Upgrade auf den Modus **Standardsicherheit** durchführen.
- Bei einem Herunterstufen vom Modus **„Enterprise Strikt“-Sicherheit** zum Modus **Kompatibilität für Sicherheit** oder **Standardsicherheit**:
  - Der Server wird automatisch neu gestartet, damit der Sicherheitsmodus in Kraft tritt.
  - Wenn der FoD-Schlüssel für den strikten Modus auf dem XCC2 fehlt oder abgelaufen ist und XCC2 ein selbst signiertes TLS-Zertifikat verwendet, generiert XCC2 das selbst signierte TLS-Zertifikat auf Basis des konformen Algorithmus „Standard Strikt“. XClarity Administrator zeigt aufgrund eines Zertifikatsfehlers einen Verbindungsfehler an. Informationen zum Beheben des Fehlers mit nicht vertrauenswürdigen Zertifikaten finden Sie unter Ein nicht vertrauenswürdiges Serverzertifikat beheben in der Onlinedokumentation von XClarity Administrator. Wenn XCC2 ein angepasstes TLS-Zertifikat verwendet, gestattet XCC2 das Herabstufen und warnt Sie, dass Sie ein Serverzertifikat importieren müssen, das auf dem Verschlüsselungsmodus **Standardsicherheit** basiert.
- Der Modus **NIST SP 800-131A** wird nicht für Server mit XCC2 unterstützt.
- Wenn der Verschlüsselungsmodus für XClarity Administrator auf „TLS v1.2“ festgelegt ist und bei einem verwalteten Server mit verwalteter Authentifizierung der Sicherheitsmodus „TLS v1.2“ festgelegt ist, führt das Ändern des Serversicherheitsmodus zu „TLS v1.3“ mit XClarity Administrator oder XCC dazu, der Server dauerhaft offline ist.
- Wenn der Verschlüsselungsmodus für XClarity Administrator auf „TLS v1.2“ festgelegt ist und Sie versuchen, einen Server mit XCC zu verwalten, dessen Sicherheitsmodus auf „TLS v1.3“ festgelegt ist, kann der Server nicht mit verwalteter Authentifizierung verwaltet werden.

Sie können die Sicherheitseinstellungen für die folgenden Einheiten ändern.
- Lenovo ThinkSystem Server mit Intel oder AMD Prozessoren (außer SR635/SR655)
- Lenovo ThinkSystem V2 Server
- Lenovo ThinkSystem V3 Server mit Intel oder AMD Prozessoren
- Lenovo ThinkEdge SE350/SE450 Server
- Lenovo System x Server

Weitere Informationen zum Festlegen der Sicherheitsmodi auf dem verwalteten Server finden Sie unter Sicherheitseinstellungen für einen Server konfigurieren in der Onlinedokumentation von XClarity Administrator.

Sicherheitszertifikate

Lenovo XClarity Administrator verwendet SSL-Zertifikate für die Einrichtung von sicheren und vertrauenswürdigen Kommunikationsverbindungen zwischen XClarity Administrator und den verwalteten Einheiten (z. B. Gehäuse und Serviceprozessoren in System x Servern) sowie für die Herstellung von Kommunikationsverbindungen mit XClarity Administrator durch Benutzer oder mit anderen Services. Standardmäßig verwenden XClarity Administrator, CMMs und Management-Controller selbst signierte, von XClarity Administrator generierte Zertifikate, die von einer internen Zertifizierungsstelle (Certificate Authority, CA) ausgestellt wurden.

Das eindeutige, selbst signierte Standardserverzertifikat, das in jeder Instanz von XClarity Administrator generiert wird, bietet eine ausreichende Sicherheit für vielen Umgebungen. Sie können die Zertifikate wahlweise von XClarity Administrator verwalten lassen oder eine aktivere Rolle übernehmen und die Serverzertifikate selbst anpassen oder ersetzen. XClarity Administrator 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 XClarity Administrator 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.

Weitere Informationen über Zertifikate finden Sie unter Mit Sicherheitszertifikaten arbeiten in der Onlinedokumentation von XClarity Administrator.

Authentifizierung

Unterstützte Authentifizierungsserver

Der *Authentifizierungsserver* ist ein Benutzerregistry, das zum Authentifizieren von Benutzeranmeldeinformationen verwendet wird. Lenovo XClarity Administrator unterstützt die folgenden Typen von Authentifizierungsservern:

- **Lokaler Authentifizierungsserver**. XClarity Administrator ist standardmäßig für die Verwendung des eingebetteten LDAP-Servers (Lightweight Directory Access Protocol) konfiguriert, der sich auf dem Verwaltungsserver befindet.
- **Externer LDAP-Server**. Derzeit werden nur Microsoft Active Directoryund OpenLDAP unterstützt. Dieser Server muss sich auf einem externen Microsoft Windows-Server befinden, der mit dem Verwaltungsnetzwerk verbunden ist. Wenn ein externer LDAP-Server verwendet wird, ist der lokale Authentifizierungsserver deaktiviert.

  Achtung: Um die Bindungsmethode für Active Directory so zu konfigurieren, dass Anmeldeinformationen verwendet werden, muss im Baseboard Management Controller für jeden verwalteten Server Firmware ab September 2016 (oder später) ausgeführt werden.
- **Externes Identitätsverwaltungssystem**. Derzeit wird nur CyberArk unterstützt.

  Wenn Benutzeraccounts für einen ThinkSystem oder ThinkAgile Server auf CyberArk integriert werden, können Sie wählen, dass XClarity Administrator die Anmeldeinformationen für die Anmeldung beim Server bei der Ersteinrichtung der Server zur Verwaltung (mit verwalteter oder lokaler Authentifizierung) von CyberArk abruft. Bevor Anmeldeinformationen von CyberArk abgerufen werden können, müssen die CyberArk-Pfade in XClarity Administrator definiert werden und es muss eine gegenseitige Vertrauensstellung zwischen CyberArk Und XClarity Administrator mithilfe von TLS für gegenseitige Authentifizierung über Clientzertifikate hergestellt werden.
- **Externe SAML Identity Provider**. Derzeit wird nur Microsoft Active Directory Federation Services (AD FS) unterstützt. Zusätzlich zur Eingabe eines Benutzernamens und Kennworts kann eine mehrstufige Authentifizierung konfiguriert werden, um zusätzliche Sicherheit zu aktivieren, indem ein PIN-Code, das Lesen einer Smartcard und ein Clientzertifikat erforderlich sind. Bei Verwendung eines SAML-Servers Identity Provider ist der lokale Authentifizierungsserver nicht deaktiviert. Zur direkten Anmeldung an einem verwalteten Gehäuse oder einem Server (es sei denn, dass in dieser Einheit Encapsulation aktiviert ist), für die PowerShell- und REST-API-Authentifizierung und für die Wiederherstellung bei nicht verfügbarer externer Authentifizierung sind lokale Benutzeraccounts erforderlich.

  Sie können sowohl einen externen LDAP-Server als auch einen externen Identity Provider verwenden. Wenn beide aktiviert sind, wird der externe LDAP-Server für die direkte Anmeldung an den verwalteten Einheiten und der Identity Provider für die Anmeldung am Verwaltungsserver verwendet.

Weitere Informationen zu Authentifizierungsservern finden Sie unter Authentifizierungsserver verwalten in der Onlinedokumentation von XClarity Administrator.

Einheitenauthentifizierung

Standardmäßig werden Einheiten anhand der verwalteten XClarity Administrator Authentifizierung verwaltet, um sich bei den Einheiten anzumelden. Bei der Verwaltung von Rack-Servern und Lenovo Gehäusen können Sie auswählen, ob Sie die lokale Authentifizierung oder die verwaltete Authentifizierung zur Anmeldung bei den Einheiten verwenden möchten.

- Wenn die *lokale Authentifizierung* für Rack-Server, Lenovo Gehäuse und Lenovo Rack-Switches verwendet wird, verwendet XClarity Administrator gespeicherte Anmeldeinformationen zur Authentifizierung der Einheit. Bei den *gespeicherten Anmeldeinformationen* kann es sich um einen aktiven Benutzeraccount auf der Einheit oder um einen Benutzeraccount auf dem Active Directory-Server handeln.

  Sie müssen gespeicherte Anmeldeinformationen in XClarity Administrator erstellen, die mit einem aktiven Benutzeraccount auf der Einheit oder mit einem Benutzeraccount auf einem Active Directory-Server übereinstimmen, bevor Sie die Einheit über die lokale Authentifizierung verwalten können (siehe Gespeicherte Anmeldeinformationen verwalten in der Onlinedokumentation von XClarity Administrator).

  Anmerkungen:

  – RackSwitch-Einheiten unterstützen nur gespeicherte Anmeldeinformationen für die Authentifizierung. Benutzeranmeldeinformationen für XClarity Administrator werden nicht unterstützt.
- Mit der *verwalteten Authentifizierung* können Sie mehrere Einheiten mithilfe von Anmeldeinformationen auf dem XClarity Administrator-Authentifizierungsserver anstatt lokaler Anmeldeinformationen verwalten und überwachen. Wenn die verwaltete Authentifizierung für eine Einheit (außer ThinkServer-Server, System x M4-Servern und Switches) verwendet wird, konfiguriert XClarity Administrator die Einheit und deren installierte Komponenten zur Verwendung eines bestimmten XClarity Administrator-Authentifizierungsservers für eine zentrale Verwaltung.

  – Wenn die verwaltete Authentifizierung aktiviert ist, können Sie Einheiten entweder über manuell eingegebene oder gespeicherte Anmeldeinformationen verwalten (siehe Benutzeraccounts verwalten und in der Onlinedokumentation zu XClarity Administrator).

    Die gespeicherten Anmeldeinformationen werden nur verwendet, bis XClarity Administrator die LDAP-Einstellungen auf dem Gerät konfiguriert. Danach haben Änderungen an den gespeicherten Anmeldeinformationen keine Auswirkungen auf die Verwaltung oder Überwachung dieser Einheit.

    Anmerkung: Wenn die verwaltete Authentifizierung für ein Gerät aktiviert ist, können Sie mit XClarity Administrator keine gespeicherten Anmeldeinformationen für dieses Gerät bearbeiten.

  – Wenn Sie den lokalen oder externen LDAP-Server als XClarity Administrator-Authentifizierungsserver nutzen, werden auf diesem Authentifizierungsserver definierte Benutzeraccounts für die Anmeldung bei XClarity Administrator, CMMs und BMCs (Baseboard Management Controllern) in der XClarity Administrator-Domäne verwendet. Lokale CMM- und Management-Controller-Benutzeraccounts werden deaktiviert.

  – Bei Verwendung eines SAML 2.0 Identity Provider als XClarity Administrator-Authentifizierungsserver sind SAML-Accounts für verwaltete Einheiten nicht zugänglich. Wenn Sie jedoch einen SAML Identitiy Provider und einen LDAP-Server zusammen verwenden und der Identity Provider Konten nutzt, die sich auf dem LDAP-Server befinden, können LDAP-Benutzeraccounts zur Anmeldung bei den verwalteten Einheiten und gleichzeitig modernere von SAML 2.0 bereitgestellte Authentifizierungsmethoden (z. B. mehrstufige Authentifizierung und Single Sign-on) zur Anmeldung bei XClarity Administrator verwendet werden.

  – Mit Single Sign-On kann sich ein Benutzer, der bereits bei XClarity Administrator angemeldet ist, automatisch beim Baseboard Management Controller anmelden. Single Sign-On ist standardmäßig aktiviert, wenn ein ThinkSystem oder ThinkAgile Server von XClarity Administrator verwaltet wird (es sei denn, der Server wird mit CyberArk-Kennwörtern verwaltet). Sie können global konfigurieren, dass Single Sign-On für alle verwalteten ThinkSystem und ThinkAgile Server aktiviert oder deaktiviert ist. Das Aktivieren von Single Sign-On für einen bestimmten ThinkSystem und ThinkAgile Server überschreibt

die globale Einstellung für alle ThinkSystem und ThinkAgile Server (siehe Server verwalten in der XClarity Administrator Onlinedokumentation).

Anmerkung: Single Sign-On ist automatisch deaktiviert, wenn das CyberArk Identitätsverwaltungssystem zur Authentifizierung verwendet wird.

- Wenn die verwaltete Authentifizierung für ThinkSystem SR635 und SR655 Server aktiviert ist:
  - Die Baseboard Management Controller-Firmware unterstützt bis zu fünf LDAP-Benutzerrollen. XClarity Administrator fügt diese LDAP-Benutzerrollen während der Verwaltung zu den Servern hinzu: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** und **lxc-os-admin**.

    Benutzern muss mindestens eine der angegebenen LDAP-Benutzerrollen zugeordnet werden, damit sie mit den ThinkSystem SR635 und SR655 Servern kommunizieren können.
  - Die Management-Controller-Firmware unterstützt keine LDAP-Benutzer mit demselben Benutzernamen wie der lokale Benutzer des Servers.
- Für ThinkServer- und System x M4-Server wird der XClarity Administrator-Authentifizierungsserver nicht verwendet. Stattdessen wird ein IPMI-Account in der Einheit mit dem Präfix „LXCA_“ erstellt, auf das eine willkürliche Zeichenfolge folgt. (Die vorhandenen lokalen IPMI-Benutzeraccounts werden nicht deaktiviert.) Wenn Sie die Verwaltung eines ThinkServer-Servers beenden, wird der Benutzeraccount „LXCA_“ deaktiviert und das Präfix „LXCA_“ wird durch das Präfix „DISABLED_“ ersetzt. Um festzustellen, ob ein ThinkServer-Server durch eine andere Instanz verwaltet wird, sucht XClarity Administrator nach IPMI-Accounts mit dem Präfix „LXCA_“. Wenn Sie sich dazu entschließen, die Verwaltung eines verwalteten ThinkServer-Servers zu erzwingen, werden alle IPMI-Accounts in der Einheit mit dem Präfix „LXCA_“ deaktiviert und umbenannt. IPMI-Konten, die nicht mehr verwendet werden, sollten Sie manuell löschen.

  Wenn Sie manuell eingegebene Anmeldeinformationen verwenden, werden in XClarity Administrator automatisch gespeicherte Anmeldeinformationen erstellt und zur Verwaltung der Einheit verwendet.

  Anmerkungen: Wenn die verwaltete Authentifizierung für ein Gerät aktiviert ist, können Sie mit XClarity Administrator keine gespeicherten Anmeldeinformationen für dieses Gerät bearbeiten.
  - Jedes Mal, wenn Sie ein Gerät mit manuell eingegebenen Anmeldeinformationen verwalten, werden auch dann neue gespeicherte Anmeldeinformationen für dieses Gerät erstellt, wenn bei einem vorherigen Verwaltungsprozess andere gespeicherte Anmeldeinformationen für dieses Gerät erstellt wurden.
  - Wenn Sie die Verwaltung eines Geräts aufheben, löscht XClarity Administrator keine gespeicherten Anmeldeinformationen, die während des Verwaltungsprozesses automatisch für dieses Gerät erstellt wurden.

Benutzeraccount für Wiederherstellung

Wenn Sie ein Kennwort für die Wiederherstellung angeben, deaktiviert XClarity Administrator den Benutzeraccount für das lokale CMM oder den Management-Controller und erstellt einen neuen Benutzeraccount für die Wiederherstellung (`RECOVERY_ID`) auf der Einheit für die künftige Authentifizierung. Wenn der Verwaltungsserver ausfällt, können Sie sich, bis der Verwaltungsknoten wieder verfügbar ist oder ausgetauscht wurde, über den Account `RECOVERY_ID` an der Einheit anmelden, um Aktionen zum Wiederherstellen der Accountverwaltungsfunktionen auf der Einheit durchzuführen.

Wenn Sie die Verwaltung einer Einheit aufheben, die über einen Benutzeraccount `RECOVERY_ID` verfügt, werden alle lokalen Benutzeraccounts aktiviert und der Account `RECOVERY_ID` wird gelöscht.

- Wenn Sie Änderungen an den deaktivierten lokalen Benutzeraccounts vornehmen (z. B. ein Kennwort ändern), haben diese Änderungen keinerlei Auswirkungen auf den Account `RECOVERY_ID`. Im Modus „Verwaltete Authentifizierung“ ist der Account `RECOVERY_ID` der einzige aktive und betriebsbereite Benutzeraccount.

- Verwenden Sie den Account `RECOVERY_ID` nur in Notfällen, z. B. bei Ausfall des Verwaltungsserver oder wenn ein Netzwerkproblem verhindert, dass die Einheit zur Benutzerauthentifizierung mit XClarity Administrator kommuniziert.
- Das Kennwort `RECOVERY_ID` wird angegeben, wenn Sie das Gerät erkennen. Notieren Sie sich das Kennwort für die spätere Verwendung.

Informationen zum Wiederherstellen einer Einheitenverwaltung erhalten Sie in den Abschnitten Gehäuseverwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen und Rack- oder Tower-Serververwaltung nach einem Verwaltungsserverausfall wiederherstellen in der XClarity Administrator Onlinedokumentation.

Benutzeraccounts und Rollengruppen

Benutzeraccounts werden zur Anmeldung und zur Verwaltung von Lenovo XClarity Administrator und allen verwalteten Gehäusen und Servern verwendet. Die Benutzeraccounts von XClarity Administrator sind zwei voneinander abhängigen Prozessen ausgesetzt: Authentifizierung und Autorisierung.

Authentifizierung ist ein Sicherheitsmechanismus, durch den die Anmeldeinformationen eines Benutzers überprüft werden. Beim Authentifizierungsprozess werden die im konfigurierten Authentifizierungsserver gespeicherten Anmeldeinformationen verwendet. Die Authentifizierung hindert nicht berechtigte Verwaltungsserver oder Anwendungen auf fehlerhaft verwalteten Systemen am Zugriff auf die Ressourcen. Nach der Authentifizierung kann ein Benutzer auf XClarity Administrator zugreifen. Damit ein Benutzer jedoch auf eine bestimmte Ressource zugreifen oder eine bestimmte Task ausführen kann, muss er auch über die geeignete Berechtigung verfügen.

Bei der *Autorisierung* werden die Berechtigungen des authentifizierten Benutzers überprüft und der Zugriff auf Ressourcen wird abhängig von den Rollen gesteuert, die dem Benutzer zugeordnet sind. *Rollengruppen* werden verwendet, um einer Gruppe von Benutzeraccounts bestimmte Rollen zuzuweisen, die im Authentifizierungsserver definiert und verwaltet werden. Wenn ein Benutzer beispielsweise Mitglied einer Rollengruppe mit der Berechtigung „Supervisor“ ist, darf er Benutzeraccounts in XClarity Administrator erstellen, bearbeiten und löschen. Wenn ein Benutzer über die Berechtigung „Operator“ verfügt, darf er die Informationen zum Benutzeraccount nur anzeigen.

Weitere Informationen zu Benutzeraccounts und Rollengruppen finden Sie unter Benutzeraccounts verwalten in der Onlinedokumentation von XClarity Administrator.

Benutzeraccountsicherheit

Benutzeraccounteinstellungen steuern die Komplexität von Kennwörtern, die Sperrung von Accounts und das Sitzungszeitlimit bei Webdeaktivität. Sie können die Werte für die Accountsicherheitseinstellungen ändern.

Weitere Informationen zu den Einstellungen für die Accountsicherheit finden Sie unter Die Sicherheitseinstellungen eines Benutzeraccounts ändern in der Onlinedokumentation von Lenovo XClarity Administrator.

Hinweise zu hoher Verfügbarkeit

Konfigurieren Sie eine hohe Verfügbarkeit für Lenovo XClarity Administrator, indem Sie die Hochverfügbarkeitsfunktionen verwenden, die Bestandteile des Hostbetriebssystems oder der Containerumgebung sind.

Docker

Mit Docker Datacenter können Sie eine Hochverfügbarkeitsumgebung für XClarity Administrator Container einrichten, die in der Docker Engine ausgeführt werden. Weitere Informationen über Hochverfügbarkeit mit Docker Datacenter finden Sie unter Webseite „Hochverfügbarkeitsarchitektur und Apps mit Docker Datacenter“.

Citrix

Verwenden Sie die Hochverfügbarkeitsfunktion, die für eine Citrix-Umgebung bereitgestellt wird. Weitere Informationen hierzu finden Sie unter Hochverfügbarkeit implementieren (Citrix) in der Onlinedokumentation von XClarity Administrator.

KVM (CentOS, RedHat und Ubuntu)

Sie können OpenStack oder – sofern Sie bereits eine Hochverfügbarkeitsumgebung haben – weiterhin Ihre internen Prozesse verwenden. Weitere Informationen zur Hochverfügbarkeit mit OpenStack finden Sie im Abschnitt Hochverfügbarkeit implementieren (KVM) in der Onlinedokumentation zu XClarity Administrator.

Microsoft Hyper-V

Verwenden Sie die Hochverfügbarkeitsfunktion, die für eine ESXi-Umgebung bereitgestellt wird. Weitere Informationen finden Sie unter Hochverfügbarkeit implementieren (Microsoft Hyper-V) in der Onlinedokumentation zu XClarity Administrator.

Nutanix AHV

Verwenden Sie die Hochverfügbarkeitsfunktion der virtuellen Maschine, die für die Nutanix AHV-Umgebung bereitgestellt wird. Weitere Informationen finden Sie unter Hochverfügbarkeit implementieren (Nutanix) in der Onlinedokumentation zu XClarity Administrator.

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 auf einen anderen Host ausführen soll (Taktsignale).

Details zum Einrichten eines VMware High Availability-Clusters finden Sie unter Hochverfügbarkeit implementieren (VMware ESXi) in der Onlinedokumentation zu XClarity Administrator.

Features on Demand

Mit Features on Demand werden Funktionen aktiviert, ohne dass eine Installation von Hardware oder der Kauf neuer Geräte erforderlich ist. Zur Aktivierung benötigen Sie den entsprechenden Features on Demand-Schlüssels und installieren diesen.

Um die Fernsteuerungs- und Betriebssystemimplementierungsvorgänge in Lenovo XClarity Administrator zu verwenden, müssen Sie für Server, auf denen diese Funktionen nicht bereits standardmäßig aktiviert sind, XClarity Controller Enterprise-Stufe oder MM Advance Upgrade aktivieren. Auf ThinkSystem-, Converged- und System x-Servern muss für diese Vorgänge außerdem ein Features on Demand-Schlüssel für Fernpräsenz installiert sein. Auf der Seite „Server“ sehen Sie, ob die Fernpräsenz-Funktion auf einem Server aktiviert, deaktiviert oder nicht installiert ist (siehe Den Status eines verwalteten Servers anzeigen in der Onlinedokumentation von XClarity Administrator).

Einige erweiterte Serverfunktionen werden mithilfe von Features on Demand-Schlüsseln aktiviert. Wenn Funktionen konfigurierbare Einstellungen haben, auf die während der UEFI-Konfiguration zugegriffen werden kann, können Sie die Einstellungen mit Konfigurationsmuster festlegen. Die daraus resultierende Konfiguration wird jedoch erst durch die Installation des entsprechenden Features on Demand-Schlüssels aktiviert.

Anmerkung: In XClarity Administrator ist keine Installation oder Verwaltung von Features on Demand-Schlüsseln möglich. Sie können allerdings eine Liste mit den derzeit auf verwalteten Servern installierten Features on Demand-Schlüsseln aufrufen. Weitere Informationen zum Anzeigen von installierten Features on Demand-Schlüsseln finden Sie unter FoD-Schlüssel (Feature on Demand) anzeigen in derXClarity Administrator-Onlinedokumentation.

So erhalten und installieren Sie Features on Demand-Schlüssel

1. Kaufen Sie die Features on Demand-Aktualisierung mithilfe der entsprechenden Teilenummer.

   Sie können Schlüssel auf der Features on Demand-Webportal kaufen. Nach Abschluss des Kaufs erhalten Sie per E-Mail einen Berechtigungscode.
2. Geben Sie auf Features on Demand-Webportal den erhaltenen Autorisierungscode und die eindeutige Systemkennung des zu aktualisierenden Servers ein.
3. Laden Sie den Aktivierungsschlüssel in Form einer .key-Datei herunter.
4. Laden Sie den Aktivierungsschlüssel auf den Management-Controller für den Server hoch.
5. Starten Sie den Server erneut. Nach dem Neustart ist die Funktion aktiviert.

Weitere Informationen zu Features on Demand-Schlüsseln finden Sie unter Verwendung von „Lenovo Features on Demand“.

Kapitel 3. Lenovo XClarity Administrator

Es gibt viele verschiedene Möglichkeiten, um verwaltbare Einheiten mit dem Netzwerk zu verbinden und die virtuelle Lenovo XClarity Administrator-Einheit zur Verwaltung dieser Einheiten einzurichten. Verwenden Sie die Informationen in diesem Abschnitt als Anleitung, um verwaltbare Einheiten einzurichten und XClarity Administrator

In diesem Abschnitt wird die Einrichtung von häufig verwendeten Topologien beschrieben. Es kann jedoch nicht jede mögliche Netzwerktopologie vorgestellt werden.

Achtung: Für die Einheitenverwaltung benötigt XClarity Administrator Zugriff auf das Verwaltungsnetzwerk.

Weitere Informationen:

-  Installation von Lenovo XClarity Administrator unter VMware vCenter
-  Installation von Lenovo XClarity Administrator unter VMware vSphere
-  Installation von Lenovo XClarity Administrator unter Windows Hyper-V
-  Installation von Lenovo XClarity Administrator unter Red Hat KVM

Gemeinsames Daten- und Verwaltungsnetzwerk

In dieser Netzwerktopologie sind das Datennetzwerk und das Verwaltungsnetzwerk dasselbe Netzwerk.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jeder Einheit installiert ist, die Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Wichtig: 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. Wenn Sie DHCP nutzen, stellen Sie sicher, dass die IP-Adressenänderungen minimiert werden.

Zu dieser Aufgabe

Bei virtuellen Einheiten erfolgt die gesamte Kommunikation zwischen XClarity Administrator und dem Netzwerk über die Eth0-Netzwerkschnittstelle auf dem Host. Für Container können Sie einen benutzerdefinierten Namen verwenden. In diesem Szenario wird jedoch „eth0“ verwendet.

Wichtig: Die Bereitstellung eines gemeinsamen Daten- und Verwaltungsnetzwerks, enthält, kann zu Unterbrechungen im Datenverkehr führen. Zum Beispiel können je nach Netzwerkkonfiguration (wenn etwa die Priorität des Serverdatenverkehrs hoch und die Priorität des von Management-Controllern ausgehenden Datenverkehrs gering ist) Pakete verloren gehen oder es können Netzkonnektivitätsprobleme auftreten. Das Verwaltungsnetzwerk verwendet neben TCP- auch UDP-Datenverkehr. UDP-Datenverkehr kann bei hohem Netzwerkverkehrsaufkommen eine niedrigere Priorität haben.

In der folgenden Abbildung wird eine Möglichkeit für die Umgebungskonfiguration dargestellt, wenn das Datennetzwerk und das Verwaltungsnetzwerk dasselbe Netzwerk sind. Die Zahlen in der Abbildung entsprechen den Schritten in den nachfolgenden Abschnitten.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Rack-Server, RackSwitches, Flex-Switches und CMMs abgebildet, da diese bei der Einrichtung von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten erforderlich sind.

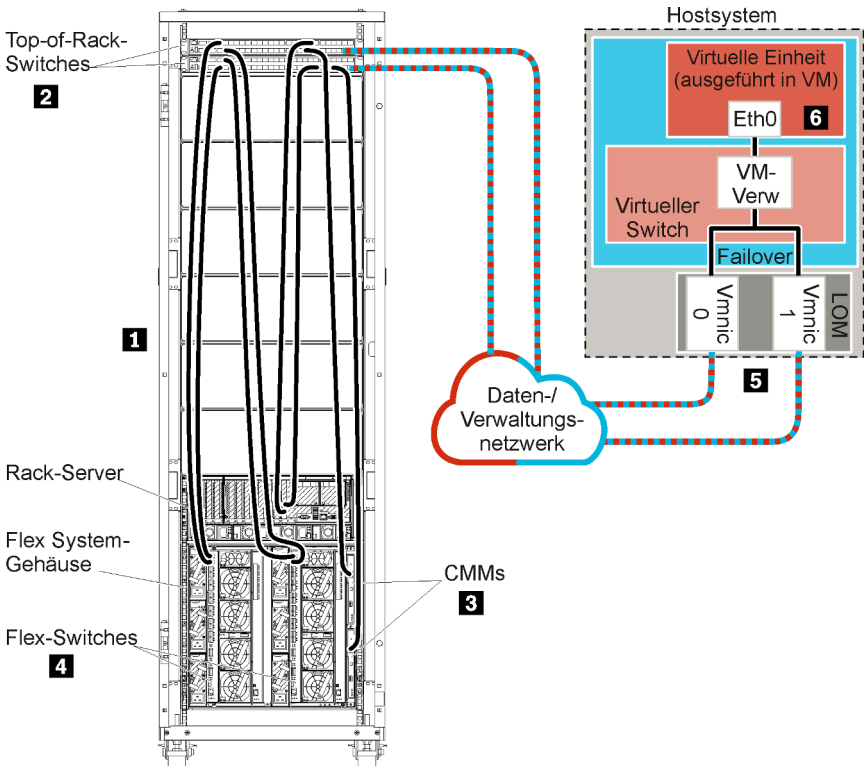


Abbildung 8. Beispiel: Topologie – Gemeinsames Daten- und Verwaltungsnetzwerk für eine virtuelle Einheit

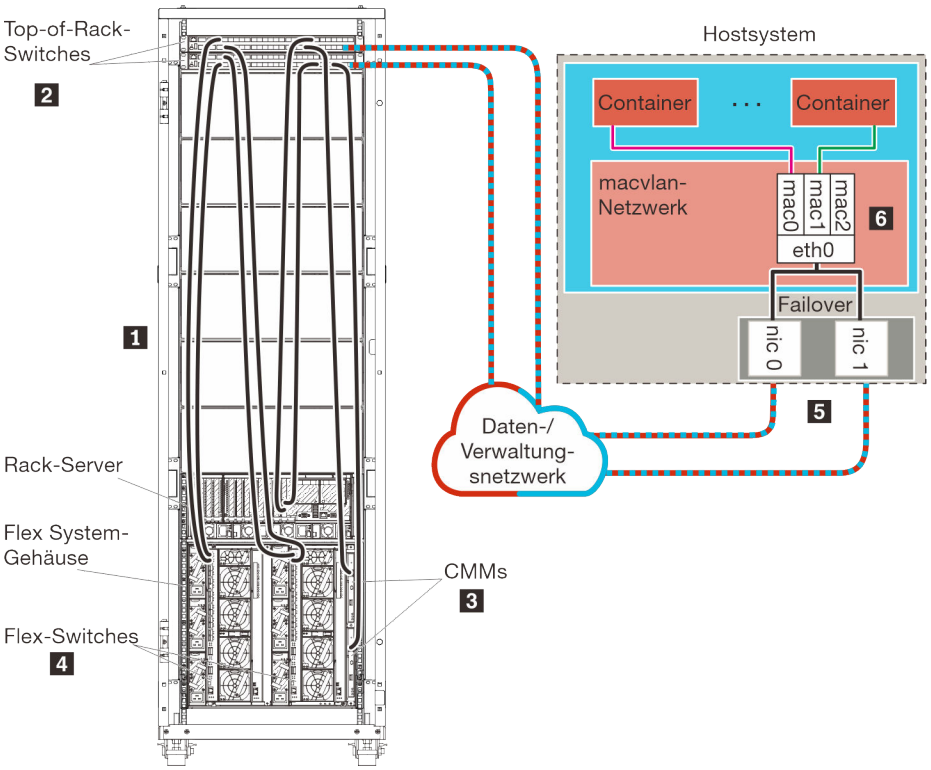


Abbildung 9. Beispiel: Topologie – Gemeinsames Daten- und Verwaltungsnetzwerk für Container

Wichtig: Sie können XClarity Administrator auf jedem System einrichten, das die Anforderungen für XClarity Administrator erfüllt, einschließlich eines verwalteten Servers. Wenn Sie einen verwalteten Server als XClarity Administrator-Host einsetzen:

- Sie müssen entweder eine Topologie von logisch getrennten Daten- und Verwaltungsnetzwerken oder eine Topologie von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten implementieren.
- Sie können mit XClarity Administrator keine Firmwareaktualisierungen für den verwalteten Server ausführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator-Hosts installiert.
- Wenn Sie einen Server in einem Flex System-Gehäuse verwenden, stellen Sie sicher, dass der Server automatisch eingeschaltet wird. Sie können diese Option über die CMM-Webschnittstelle festlegen. Klicken Sie dazu auf **Gehäuseverwaltung → Rechenknoten**, markieren Sie den Server und wählen Sie unter **Automatischer Einschaltmodus** die Option **Automatisches Einschalten** aus.

Wenn Sie XClarity Administrator zur Verwaltung von vorhandenen und bereits konfigurierten Gehäusen und Rack-Servern installieren möchten, fahren Sie mit Schritt 5: Host installieren und konfigurieren fort.

Weitere Informationen über die Planung dieser Topologie - mit Informationen über Netzwerkeinstellungen sowie die Konfiguration von Eth1 und Eth0 - finden Sie unter Einzelne Daten und Verwaltungsnetzwerk.

Schritt 1: Gehäuse, Rack-Server und Lenovo XClarity Administrator-Host mit den Top-of-Rack-Switches verkabeln

Verkabeln Sie die Gehäuse, die Rack-Server und den XClarity Administrator-Host mit den Top-of-Rack-Switches, um die Kommunikation zwischen den Einheiten und dem Netzwerk zu ermöglichen.

Vorgehensweise

Verkabeln Sie jeden Flex-Switch und alle CMMs in den Gehäusen, jeden Rack-Server und den XClarity Administrator-Host mit beiden Top-of-Rack-Switches. Die Ports in den Top-of-Rack-Switches können Sie beliebig auswählen.

In der folgenden Abbildung wird ein Beispiel für die Verkabelung von Gehäusen (Flex-Switches und CMMs), Rack-Servern und XClarity Administrator-Host zu den Top-of-Rack-Switches dargestellt.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Rack-Server, RackSwitches, Flex-Switches und CMMs abgebildet, da diese bei der Einrichtung von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten erforderlich sind.

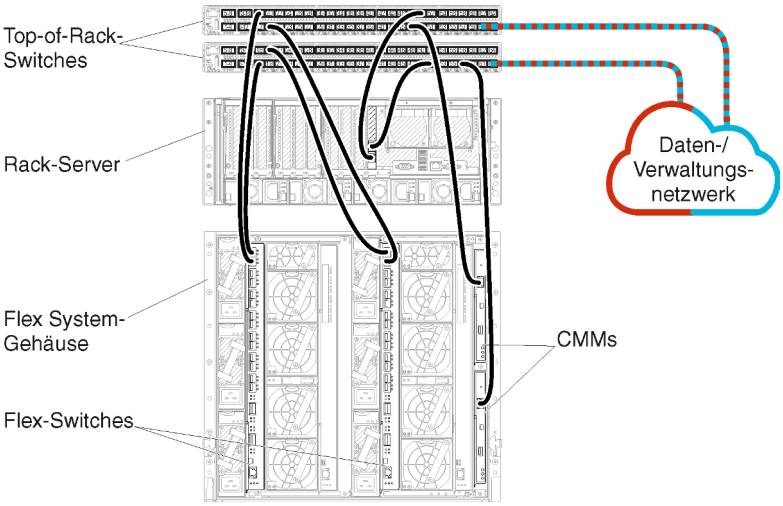


Abbildung 10. Beispiel: Verkabelung für Verwaltungsnetzwerke und Netzwerke mit einzelnen Daten

Schritt 2: Top-of-Rack-Switches konfigurieren

Konfigurieren Sie die Top-of-Rack-Switches.

Vorbereitende Schritte

Stellen Sie zusätzlich zu den üblichen Konfigurationsanforderungen für Top-of-Rack-Switches sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die externen Ports zu Flex-Switches, zu Rack-Servern und zum Netzwerk sowie die internen Ports zum CMM, zu Rack-Servern und zum Netzwerk.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Rack-Switches abweichen.

Weitere Informationen über die Konfiguration der Top-of-Rack-Switches von Lenovo finden Sie unter Online-Dokumentation zu Rack-Switches im System x. Falls ein anderer Top-of-Rack-Switch installiert ist, ziehen Sie die entsprechende Dokumentation zum Switch heran.

Schritt 3: Chassis Management Modules (CMMs) konfigurieren

Konfigurieren Sie das primäre Chassis Management Module (CMM) im Gehäuse zur Verwaltung aller Einheiten im Gehäuse.

Zu dieser Aufgabe

Ausführliche Informationen über die CMM-Konfiguration finden Sie unter Gehäusekomponenten konfigurieren in der Flex System- Onlinedokumentation.

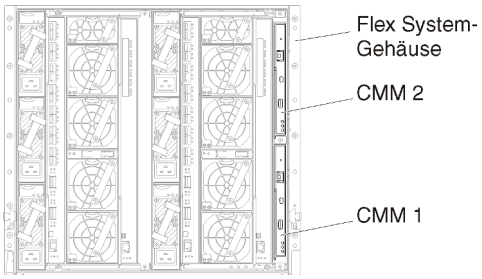
Beachten Sie auch die Schritte 4.1 bis 4.5 der Anleitung zum Gehäuse.

Vorgehensweise

Führen Sie für die CMM-Konfiguration folgende Schritte aus.

Wenn zwei CMMs installiert sind, konfigurieren Sie nur das *primäre* CMM, das automatisch die Konfiguration mit dem Standby-CMM synchronisiert.

Schritt 1. Verbinden Sie das CMM in Position 1 über ein Ethernet-Kabel mit einer Client-Workstation, um eine direkte Verbindung herzustellen.



Um erstmalig eine Verbindung zum CMM herzustellen, müssen Sie möglicherweise die IP-Eigenschaften der Client-Workstation ändern.

Wichtig: Stellen Sie sicher, dass die Client-Workstation und das CMM das gleiche Subnetz nutzen. (Das CMM-Standardsubnetz ist 255.255.255.0). Die für die Client-Workstation gewählte IP-Adresse muss im gleichen Netzwerk sein wie das CMM (z. B. 192.168.70.0 bis 192.168.70.24).

Schritt 2. Zum Starten der CMM-Verwaltungsschnittstelle öffnen Sie einen Webbrowser auf der Client-Workstation und geben die IP-Adresse des CMM ein.

Anmerkungen:

- Stellen Sie sicher, dass Sie eine sichere Verbindung verwenden, und binden Sie **https** in die URL ein (z. B. https://192.168.70.100). Wenn Sie „https“ nicht einbinden, erhalten Sie den Fehler „Seite nicht gefunden“.
- Falls Sie die IP-Standardadresse 192.168.70.100 verwenden, kann es einige Minuten dauern, bevor die CMM-Verwaltungsschnittstelle verfügbar ist. Diese Verzögerung tritt auf, weil das CMM zwei Minuten lang versucht, eine DHCP-Adresse abzurufen, bevor die statische Standardadresse verwendet wird.

Schritt 3. Melden Sie sich mit der Standardbenutzer-ID `USERID` und dem Kennwort `PASSWORD` an der CMM-Verwaltungsschnittstelle an. Sie müssen das Standardkennwort nach der ersten Anmeldung ändern.

Schritt 4. Führen Sie die Schritte im Assistenten für die CMM-Erstkonfiguration aus und geben Sie die Details für Ihre Umgebung an. Im Assistenten für die Erstkonfiguration können Sie folgende Schritte ausführen:

- Zeigen Sie den Bestand und den Status des Gehäuses an.
- Importieren Sie die Konfiguration aus einer vorhandenen Konfigurationsdatei.
- Konfigurieren Sie allgemeine CMM-Einstellungen.

- Stellen Sie das Datum und die Uhrzeit für das CMM ein.

  Tipp: Bei der Installation von XClarity Administrator konfigurieren Sie XClarity Administrator und alle von XClarity Administrator verwalteten Gehäuse zur Verwendung eines NTP-Servers.
- Konfigurieren Sie die IP-Daten für das CMM.
- Konfigurieren Sie die CMM-Sicherheitsrichtlinie.
- Konfigurieren Sie den DNS (Domain Name System).
- Konfigurieren Sie die Ereignisweiterleitungen.

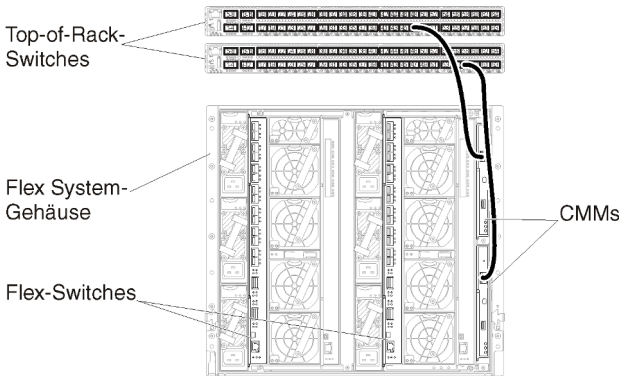
Schritt 5. Nachdem Sie die Einstellungen im Konfigurationsassistenten gespeichert und übernommen haben, konfigurieren Sie die IP-Adressen für alle Komponenten im Gehäuse.

Beachten Sie Schritt 4.6 der Anleitung zum Gehäuse.

Anmerkung: Sie müssen den Systemverwaltungsprozessor für jeden Rechenknoten zurücksetzen und die Flex-Switches neu starten, damit die neuen IP-Adressen angezeigt werden.

Schritt 6. Starten Sie das CMM mithilfe der CMM-Verwaltungsschnittstelle neu.

Schritt 7. Beim CMM-Neustart verbinden Sie ein Kabel vom Ethernet-Port des CMM mit dem Netzwerk.



Schritt 8. Melden Sie sich mit der neuen IP-Adresse an der CMM-Verwaltungsschnittstelle an.

Nach dieser Aufgabe

Sie können das CMM auch zur Unterstützung von Redundanz konfigurieren. Im CMM-Hilfesystem erhalten Sie weitere Informationen über die Felder, die auf den folgenden Seiten verfügbar sind.

- Konfigurieren Sie ein Failover für das CMM, falls im primären CMM ein Hardwareausfall auftritt. Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Eigenschaften → Erweitertes Failover**.
- Konfigurieren Sie das Failover als Folge eines Netzwerkproblems (Uplink). Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Netzwerk** und klicken Sie dann auf die Registerkarte **Ethernet** und dort auf **Erweitertes Ethernet**. Wählen Sie mindestens **Funktionsübernahme bei Verlust der physischen Netzwerkverbindung** aus.

Schritt 4: Flex-Switches konfigurieren

Konfigurieren Sie Flex-Switches (E/A-Module) in jedem Gehäuse.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch externe Ports vom Flex-Switch zum Top-of-Rack-Switch sowie interne Ports zum CMM.

Wenn die Flex-Switches so konfiguriert sind, dass sie dynamische Netzwerkeinstellungen (IP-Adresse, Netzmaske, Gateway und DNS-Adresse) über DHCP abrufen, müssen die Einstellungen der Flex-Switches konsistent sein (z. B. müssen die IP-Adressen im gleichen Subnetz sein wie das CMM).

Wichtig: Stellen Sie bei jedem Flex System-Gehäuse sicher, dass der Fabric-Typ der Erweiterungskarte in den einzelnen Servern im Gehäuse mit dem Fabric-Typ aller Flex-Switches im gleichen Gehäuse kompatibel ist. Wenn beispielsweise Ethernet-Switches in einem Gehäuse installiert sind, müssen alle Server in diesem Gehäuse Ethernet-Konnektivität aufweisen (durch einen LAN-on-Motherboard-Anschluss oder eine Ethernet-Erweiterungskarte). Weitere Informationen über die Konfiguration von Flex-Switches finden Sie unter E/A-Module konfigurieren in der Flex Systems- Onlinedokumentation.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Flex-Switches abweichen. Weitere Informationen über die unterstützten Flex-Switches finden Sie unter Flex System-Netzwerkswitches in der Flex Systems- Onlinedokumentation.

In der Regel werden die Flex-Switches in Flex-Switch-Positionen 1 und 2 konfiguriert.

Tipp: Wenn Sie die Rückseite des Gehäuses betrachten, handelt es sich bei Flex-Switch-Position 2 um die dritte Modulposition.

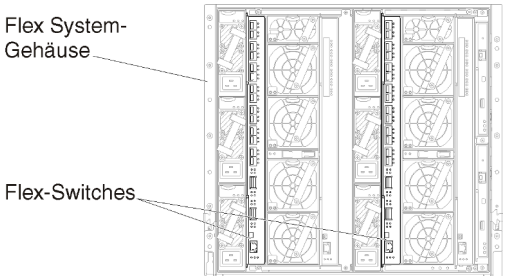


Abbildung 11. Flex-Switch-Positionen in einem Gehäuse

Schritt 5: Host installieren und konfigurieren

Sie können Docker auf jedem Server installieren, der den Anforderungen für Lenovo XClarity Administrator entspricht.

Vorbereitende Schritte

Mit Docker Datacenter können Sie eine Hochverfügbarkeitsumgebung für XClarity Administrator Container einrichten, die in der Docker Engine ausgeführt werden. Weitere Informationen über Hochverfügbarkeit mit Docker Datacenter finden Sie unter Webseite „Hochverfügbarkeitsarchitektur und Apps mit Docker Datacenter“.

Stellen Sie sicher, dass der Host die Voraussetzungen erfüllt, die unter Voraussetzungen bei Hardware und Software.

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Wichtig: Sie können XClarity Administrator auf jedem System einrichten, das die Anforderungen für XClarity Administrator erfüllt, einschließlich eines verwalteten Servers. Wenn Sie einen verwalteten Server als XClarity Administrator-Host einsetzen:

- Sie müssen entweder eine Topologie von logisch getrennten Daten- und Verwaltungsnetzwerken oder eine Topologie von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten implementieren.
- Sie können mit XClarity Administrator keine Firmwareaktualisierungen für den verwalteten Server ausführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator-Hosts installiert.
- Wenn Sie einen Server in einem Flex System-Gehäuse verwenden, stellen Sie sicher, dass der Server automatisch eingeschaltet wird. Sie können diese Option über die CMM-Webschnittstelle festlegen. Klicken Sie dazu auf **Gehäuseverwaltung → Rechenknoten**, markieren Sie den Server und wählen Sie unter **Automatischer Einschaltmodus** die Option **Automatisches Einschalten** aus.

Vorgehensweise

Installieren und konfigurieren Sie Docker auf dem Host mithilfe der Anleitungen, die mit Ihrer Docker-Distribution mitgeliefert wurden.

Schritt 6. XClarity Administrator installieren und konfigurieren

Installieren und konfigurieren Sie den Lenovo XClarity Administrator-Container auf dem gerade installierten Docker Host.

Vorbereitende Schritte

Stellen Sie sicher, dass das Hostsystem die Mindestanforderungen für Hardware und Software erfüllt (siehe Voraussetzungen bei Hardware und Software).

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Stellen Sie sicher, dass das Host-BS und XClarity Administrator denselben NTP-Server verwenden.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für Daten- und Hardwareverwaltung und BS-Implementierung festgelegt werden (siehe Netzwerkkonfigurationen). Im folgenden Beispiel wird „eth0“ verwendet.

Stellen Sie sicher, dass ein macvlan-Netzwerk in den Kernel auf dem Hostsystem geladen ist. Mit dem Befehl **lsmod | grep macvlan** können Sie prüfen, ob es geladen ist. Mit dem Befehl **modprobe macvlan** wird macvlan in den Kernel geladen.

Stellen Sie sicher, dass Sie einen eindeutigen Namen und eine IP-Adresse für jeden Container verwenden, wenn Sie mehrere XClarity Administrator-Container auf demselben Host ausführen.

Wenn Sie ThinkServer und andere Legacy-Einheiten verwalten wollen, stellen Sie sicher, dass Docker aktiviert ist, damit IPv6 unterstützt wird.

1. Bearbeiten Sie die Datei /etc/docker/daemon.json. Legen Sie den Schlüssel **ipv6** auf „wahr“ fest und legen Sie den Schlüssel **fixed-cidr-v6** auf Ihr IPv6-Subnetz fest. Nachfolgend finden Sie ein Beispiel für eine Daemon-Datei.
   ```
   {
      "ipv6": true,
      "fixed-cidr-v6": "2001:db8:1::/64",
   ```

```
    "experimental": true,
    "ip6tables": true
}
```

2. Laden Sie die Docker-Konfigurationsdatei neu, indem Sie den folgenden Befehl ausführen.
   `systemctl reload docker`

Anmerkung: XClarity Administrator wird *nicht* als privilegierter Container ausgeführt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen XClarity Administrator-Container mithilfe von Docker zu installieren.

Schritt 1. Sie können das Image der virtuellen XClarity Administrator-Einheit, die Umgebungs- und YAML-Datei über Website zum Herunterladen von XClarity Administrator auf eine Client-Workstation herunterladen. Melden Sie sich auf der Website an und verwenden Sie dann den erhaltenen Zugriffsschlüssel für den Image-Download.

Schritt 2. Importieren Sie das XClarity Administrator-Container-Image mit dem folgenden Befehl in Ihren Docker-Host.
`docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz`

Schritt 3. Bearbeiten Sie die Datei `docker_compose.env` und aktualisieren Sie die folgenden Umgebungsvariablen.

- **CONTAINER_NAME**. Eindeutiger Containername, der zum Erstellen von Docker-Datenträgern für jede XClarity Administrator-Instanz verwendet wird (z. B. `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Statische IPv4-Adresse für den Container (z. B. `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die zum Speichern der Sicherungen von XClarity Administrator verwendet werden kann. Der Pfad muss `/mnt/backup_share` sein.
- **FIRMWARE_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die als Remote-Repository für Firmwareaktualisierungen verwendet werden kann. Der Pfad muss `/mnt/fw_share` sein.

Nachfolgend finden Sie ein Beispiel für eine Umgebungsdatei.

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

Schritt 4. Bearbeiten Sie die Datei `docker_compose.yml` und aktualisieren Sie die folgenden Eigenschaften.

- Legen Sie die Eigenschaft **image** auf den Namen der in Schritt 2 verwendeten Installations-Image-Datei fest.

  Anmerkung: Sie können den Namen der Image-Datei mit dem Befehl `docker tag` ändern (z. B. zu „aktuell“).
- Wenn Sie die Remote-Freigabe als Remote-Firmware-Repository verwenden und XClarity Administrator-Sicherungen speichern möchten, legen Sie den Host-Mountpunkt für jede Remote-Freigabe in der Eigenschaft **volumes** fest.
- Legen Sie die Eigenschaft **dns** auf die IP-Adresse der DNS-Server fest.
- Der Container nutzt den Pool aus Prozessor- und Hauptspeicherressourcen, die für den Host verfügbar sind. Optional können Sie mit den Eigenschaften **cpus** und **memory** Grenzwerte für die Ressourcennutzung festlegen.
- Legen Sie für die Eigenschaft **parent** den Netzwerkschnittstellennamen auf dem Hostsystem fest, das als übergeordnete Schnittstelle für die macvlan-Schnittstelle im Container verwendet werden soll. Diese Schnittstelle muss direkten Zugriff auf das Subnetz haben, das dem Container zugeordnet ist.

- Legen Sie **subnet** und **gateway** entsprechend Ihrer Netzwerktopologie fest. In der Regel gehören Subnetz und Gateway zum Verwaltungsnetzwerk, zu dem die ${ADDRESS} gehört.
- Wenn IPv6 unterstützt werden soll, legen Sie die Eigenschaft **enable_ipv6** auf „wahr“ fest, legen Sie die Eigenschaft **ipv6_address** auf die IPv6-Adresse fest und fügen Sie je nach Netzwerktopologie einen weiteren Satz der Eigenschaften **subnet** und **gateway** hinzu (typisch für Verwaltungsnetzwerk, zu dem die IPv6-Adresse gehört).

Anmerkung: XClarity Administrator verwendet macvlan zum Konfigurieren des Containernetzwerks. Weitere Informationen finden Sie unter Webseite zur Verwendung von macvlan-Netzwerken.

Nachfolgend finden Sie ein Beispiel für eine YML-Datei mit aktiviertem IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

```
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

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

Schritt 5. Implementieren Sie das Image in Docker, indem Sie den folgenden Befehl ausführen. Dabei ist <*ENV_FILENAME*> der Name der Datei mit Umgebungsvariablen, die Sie in Schritt 2 erstellt haben.

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

Nach dieser Aufgabe

Melden Sie sich bei XClarity Administrator an und nehmen Sie die Konfiguration vor (siehe Erster Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle und Lenovo XClarity Administrator konfigurieren).

Physisch getrennte Daten- und Verwaltungsnetzwerke

In dieser Topologie sind Daten- und Verwaltungsnetzwerke physisch voneinander getrennt. Die Verwaltungskommunikation zwischen Lenovo XClarity Administrator und dem Netzwerk erfolgt über die Eth0-Netzwerkschnittstelle auf dem Host. Die Datenkommunikation findet über die Eth1-Netzwerkschnittstelle statt.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jeder Einheit installiert ist, die Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Wichtig: 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. Wenn Sie DHCP nutzen, stellen Sie sicher, dass die IP-Adressenänderungen minimiert werden.

Zu dieser Aufgabe

In der folgenden Abbildung wird eine Möglichkeit für die Umgebungskonfiguration dargestellt, wenn Daten- und Verwaltungsnetzwerke physisch voneinander getrennt sind. Die Zahlen in der Abbildung entsprechen den Schritten in den nachfolgenden Abschnitten.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Flex-Switches, CMMs und Rack-Server abgebildet, da diese bei der Einrichtung von physisch getrennten Daten- und Verwaltungsnetzwerken erforderlich sind.

Tipp: Anstatt aus Redundanzgründen zwei physische Switches zu konfigurieren, die mit jedem Netzwerk verbunden sind (für insgesamt vier Switches), können Sie einen einzelnen physischen Switch konfigurieren, der mit jedem Netzwerk verbunden ist (für insgesamt zwei Switches). In diesem Fall wäre jeder Switch mit beiden Netzwerken verbunden und Sie würden zur Trennung des Datenverkehrs zwei VLANs implementieren, nämlich eines für das Datennetzwerk und eines für das Verwaltungsnetzwerk.

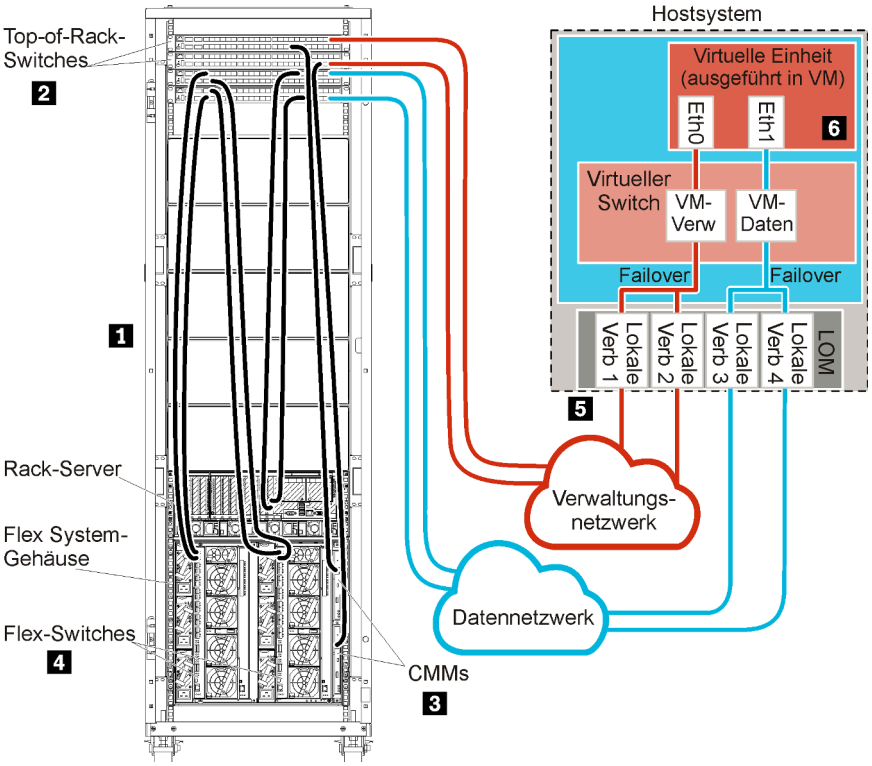


Abbildung 12. Beispiel: Topologie – Physisch getrenntes Daten- und Verwaltungsnetzwerk für eine virtuelle Einheit

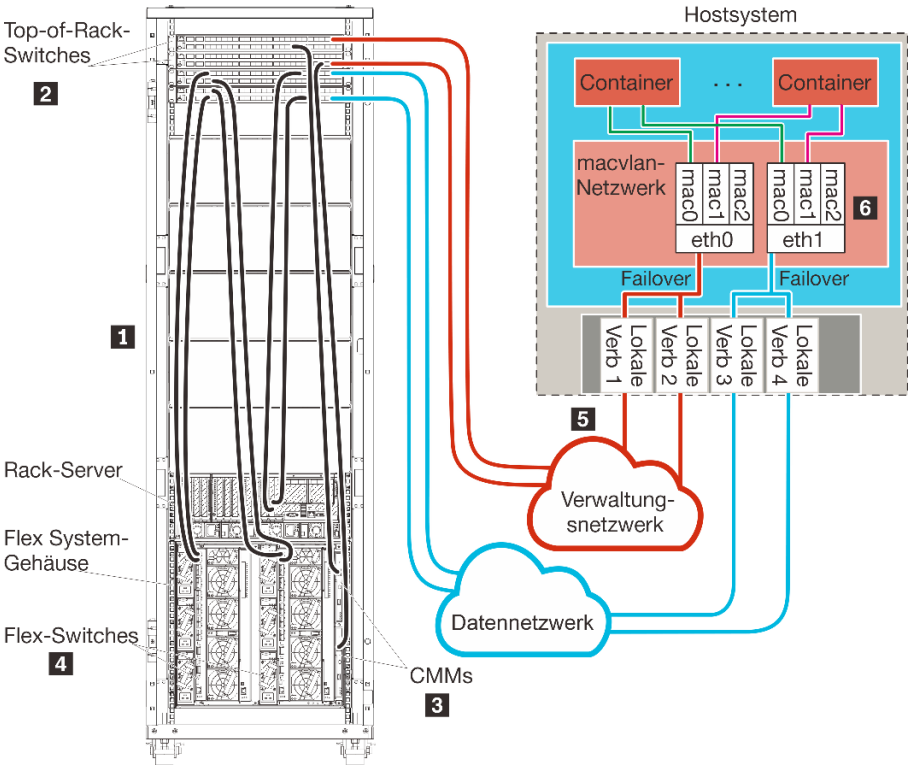


Abbildung 13. Beispiel: Topologie – Physisch getrenntes Daten- und Verwaltungsnetzwerk für Container

Wenn Sie XClarity Administrator zur Verwaltung von vorhandenen und bereits konfigurierten Gehäusen und Rack-Servern installieren möchten, fahren Sie mit Schritt 5: Host installieren und konfigurieren fort.

Weitere Informationen über die Planung dieser Topologie - mit Informationen über Netzwerkeinstellungen sowie die Konfiguration von Eth1 und Eth0 - finden Sie unter Physisch getrennte Daten und Verwaltungsnetzwerk.

Schritt 1: Gehäuse, Rack-Server und Lenovo XClarity Administrator-Host mit den Top-of-Rack-Switches verkabeln

Verkabeln Sie die Gehäuse, die Rack-Server und den XClarity Administrator-Host mit den Top-of-Rack-Switches, um die Kommunikation zwischen den Einheiten und den Netzwerken zu ermöglichen.

Vorgehensweise

Verkabeln Sie jeden Flex-Switch und alle CMMs in den Gehäusen, jeden Rack-Server und den XClarity Administrator-Host mit beiden Top-of-Rack-Switches. Die Ports in den Top-of-Rack-Switches können Sie beliebig auswählen.

In der folgenden Abbildung wird ein Beispiel für die Verkabelung von Gehäusen (Flex-Switches und CMMs), Rack-Servern und XClarity Administrator-Host zu den Top-of-Rack-Switches dargestellt.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Flex-Switches, CMMs und Rack-Server abgebildet, da diese bei der Einrichtung von physisch getrennten Daten- und Verwaltungsnetzwerken erforderlich sind.

Tipp: Anstatt aus Redundanzgründen zwei physische Switches zu konfigurieren, die mit jedem Netzwerk verbunden sind (für insgesamt vier Switches), können Sie einen einzelnen physischen Switch konfigurieren, der mit jedem Netzwerk verbunden ist (für insgesamt zwei Switches). In diesem Fall wäre jeder Switch mit beiden Netzwerken verbunden und Sie würden zur Trennung des Datenverkehrs zwei VLANs implementieren, nämlich eines für das Datennetzwerk und eines für das Verwaltungsnetzwerk.

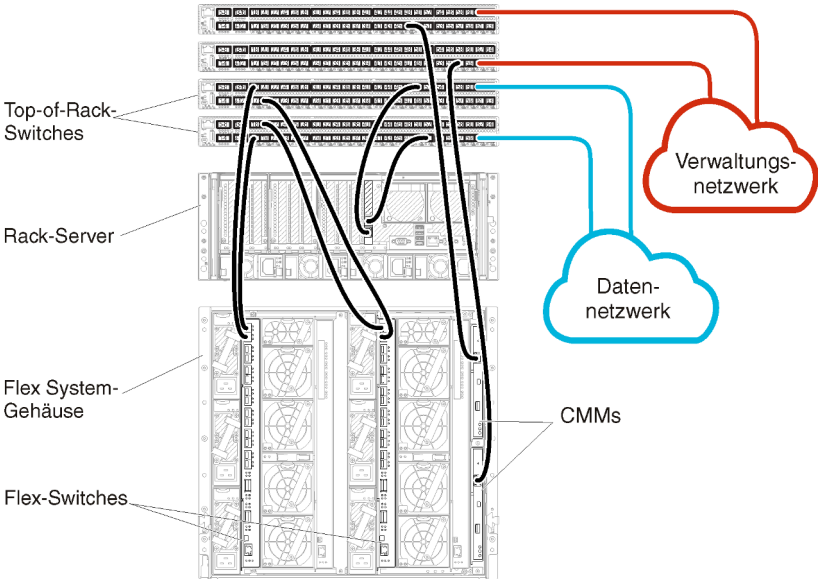


Abbildung 14. Beispiel: Verkabelung für physisch getrennte Daten- und Verwaltungsnetzwerke

Schritt 2: Top-of-Rack-Switches konfigurieren

Konfigurieren Sie die Top-of-Rack-Switches.

Vorbereitende Schritte

Stellen Sie zusätzlich zu den üblichen Konfigurationsanforderungen für Top-of-Rack-Switches sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die externen Ports zu Flex-Switches, zu Rack-Servern und zum Netzwerk sowie die internen Ports zum CMM, zu Rack-Servern und zum Netzwerk.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Rack-Switches abweichen.

Weitere Informationen über die Konfiguration der Top-of-Rack-Switches von Lenovo finden Sie unter Online-Dokumentation zu Rack-Switches im System x. Falls ein anderer Top-of-Rack-Switch installiert ist, ziehen Sie die entsprechende Dokumentation zum Switch heran.

Schritt 3: Chassis Management Modules (CMMs) konfigurieren

Konfigurieren Sie das primäre Chassis Management Module (CMM) im Gehäuse zur Verwaltung aller Einheiten im Gehäuse.

Zu dieser Aufgabe

Ausführliche Informationen über die CMM-Konfiguration finden Sie unter Gehäusekomponenten konfigurieren in der Flex System- Onlinedokumentation.

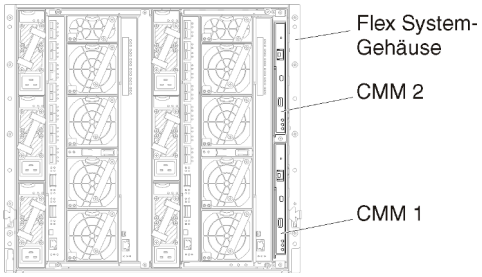
Beachten Sie auch die Schritte 4.1 bis 4.5 der Anleitung zum Gehäuse.

Vorgehensweise

Führen Sie für die CMM-Konfiguration folgende Schritte aus.

Wenn zwei CMMs installiert sind, konfigurieren Sie nur das *primäre* CMM, das automatisch die Konfiguration mit dem Standby-CMM synchronisiert.

Schritt 1. Verbinden Sie das CMM in Position 1 über ein Ethernet-Kabel mit einer Client-Workstation, um eine direkte Verbindung herzustellen.



Um erstmalig eine Verbindung zum CMM herzustellen, müssen Sie möglicherweise die IP-Eigenschaften der Client-Workstation ändern.

Wichtig: Stellen Sie sicher, dass die Client-Workstation und das CMM das gleiche Subnetz nutzen. (Das CMM-Standardsubnetz ist 255.255.255.0). Die für die Client-Workstation gewählte IP-Adresse muss im gleichen Netzwerk sein wie das CMM (z. B. 192.168.70.0 bis 192.168.70.24).

Schritt 2. Zum Starten der CMM-Verwaltungsschnittstelle öffnen Sie einen Webbrowser auf der Client-Workstation und geben die IP-Adresse des CMM ein.

Anmerkungen:

- Stellen Sie sicher, dass Sie eine sichere Verbindung verwenden, und binden Sie **https** in die URL ein (z. B. https://192.168.70.100). Wenn Sie „https“ nicht einbinden, erhalten Sie den Fehler „Seite nicht gefunden“.
- Falls Sie die IP-Standardadresse 192.168.70.100 verwenden, kann es einige Minuten dauern, bevor die CMM-Verwaltungsschnittstelle verfügbar ist. Diese Verzögerung tritt auf, weil das CMM zwei Minuten lang versucht, eine DHCP-Adresse abzurufen, bevor die statische Standardadresse verwendet wird.

Schritt 3. Melden Sie sich mit der Standardbenutzer-ID `USERID` und dem Kennwort `PASSWORD` an der CMM-Verwaltungsschnittstelle an. Sie müssen das Standardkennwort nach der ersten Anmeldung ändern.

Schritt 4. Führen Sie die Schritte im Assistenten für die CMM-Erstkonfiguration aus und geben Sie die Details für Ihre Umgebung an. Im Assistenten für die Erstkonfiguration können Sie folgende Schritte ausführen:

- Zeigen Sie den Bestand und den Status des Gehäuses an.
- Importieren Sie die Konfiguration aus einer vorhandenen Konfigurationsdatei.
- Konfigurieren Sie allgemeine CMM-Einstellungen.
- Stellen Sie das Datum und die Uhrzeit für das CMM ein.

  Tipp: Bei der Installation von XClarity Administrator konfigurieren Sie XClarity Administrator und alle von XClarity Administrator verwalteten Gehäuse zur Verwendung eines NTP-Servers.
- Konfigurieren Sie die IP-Daten für das CMM.

- Konfigurieren Sie die CMM-Sicherheitsrichtlinie.
- Konfigurieren Sie den DNS (Domain Name System).
- Konfigurieren Sie die Ereignisweiterleitungen.

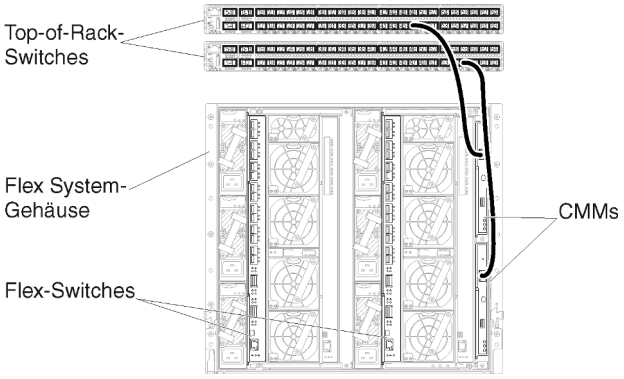
Schritt 5. Nachdem Sie die Einstellungen im Konfigurationsassistenten gespeichert und übernommen haben, konfigurieren Sie die IP-Adressen für alle Komponenten im Gehäuse.

Beachten Sie Schritt 4.6 der Anleitung zum Gehäuse.

Anmerkung: Sie müssen den Systemverwaltungsprozessor für jeden Rechenknoten zurücksetzen und die Flex-Switches neu starten, damit die neuen IP-Adressen angezeigt werden.

Schritt 6. Starten Sie das CMM mithilfe der CMM-Verwaltungsschnittstelle neu.

Schritt 7. Beim CMM-Neustart verbinden Sie ein Kabel vom Ethernet-Port des CMM mit dem Netzwerk.



Schritt 8. Melden Sie sich mit der neuen IP-Adresse an der CMM-Verwaltungsschnittstelle an.

Nach dieser Aufgabe

Sie können das CMM auch zur Unterstützung von Redundanz konfigurieren. Im CMM-Hilfesystem erhalten Sie weitere Informationen über die Felder, die auf den folgenden Seiten verfügbar sind.

- Konfigurieren Sie ein Failover für das CMM, falls im primären CMM ein Hardwareausfall auftritt. Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Eigenschaften → Erweitertes Failover**.
- Konfigurieren Sie das Failover als Folge eines Netzwerkproblems (Uplink). Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Netzwerk** und klicken Sie dann auf die Registerkarte **Ethernet** und dort auf **Erweitertes Ethernet**. Wählen Sie mindestens **Funktionsübernahme bei Verlust der physischen Netzwerkverbindung** aus.

Schritt 4: Flex-Switches konfigurieren

Konfigurieren Sie Flex-Switches in jedem Gehäuse.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch externe Ports vom Flex-Switch zum Top-of-Rack-Switch sowie interne Ports zum CMM.

Wenn die Flex-Switches so konfiguriert sind, dass sie dynamische Netzwerkeinstellungen (IP-Adresse, Netzmaske, Gateway und DNS-Adresse) über DHCP abrufen, müssen die Einstellungen der Flex-Switches konsistent sein (z. B. müssen die IP-Adressen im gleichen Subnetz sein wie das CMM).

Wichtig: Stellen Sie bei jedem Flex System-Gehäuse sicher, dass der Fabric-Typ der Erweiterungskarte in den einzelnen Servern im Gehäuse mit dem Fabric-Typ aller Flex-Switches im gleichen Gehäuse kompatibel ist. Wenn beispielsweise Ethernet-Switches in einem Gehäuse installiert sind, müssen alle Server in diesem Gehäuse Ethernet-Konnektivität aufweisen (durch einen LAN-on-Motherboard-Anschluss oder eine Ethernet-Erweiterungskarte). Weitere Informationen über die Konfiguration von Flex-Switches finden Sie unter E/A-Module konfigurieren in der Flex Systems- Onlinedokumentation.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Flex-Switches abweichen. Weitere Informationen über die unterstützten Flex-Switches finden Sie unter Flex System-Netzwerkswitches in der Flex Systems- Onlinedokumentation.

In der Regel werden die Flex-Switches in Flex-Switch-Positionen 1 und 2 konfiguriert.

Tipp: Wenn Sie die Rückseite des Gehäuses betrachten, handelt es sich bei Flex-Switch-Position 2 um die dritte Modulposition.

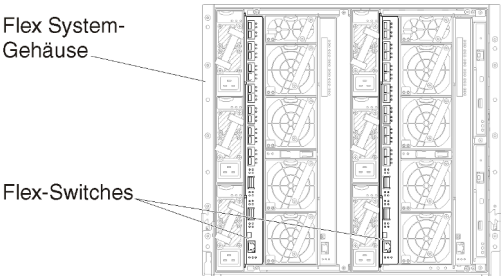


Abbildung 15. Flex-Switch-Positionen in einem Gehäuse

Schritt 5: Host installieren und konfigurieren

Sie können Docker auf jedem Server installieren, der den Anforderungen für Lenovo XClarity Administrator entspricht.

Vorbereitende Schritte

Mit Docker Datacenter können Sie eine Hochverfügbarkeitsumgebung für XClarity Administrator Container einrichten, die in der Docker Engine ausgeführt werden. Weitere Informationen über Hochverfügbarkeit mit Docker Datacenter finden Sie unter Webseite „Hochverfügbarkeitsarchitektur und Apps mit Docker Datacenter“.

Stellen Sie sicher, dass der Host die Voraussetzungen erfüllt, die unter Voraussetzungen bei Hardware und Software.

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Wichtig: Sie können XClarity Administrator auf jedem System einrichten, das die Anforderungen für XClarity Administrator erfüllt, einschließlich eines verwalteten Servers. Wenn Sie einen verwalteten Server als XClarity Administrator-Host einsetzen:

- Sie müssen entweder eine Topologie von logisch getrennten Daten- und Verwaltungsnetzwerken oder eine Topologie von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten implementieren.
- Sie können mit XClarity Administrator keine Firmwareaktualisierungen für den verwalteten Server ausführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet.

Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator-Hosts installiert.

- Wenn Sie einen Server in einem Flex System-Gehäuse verwenden, stellen Sie sicher, dass der Server automatisch eingeschaltet wird. Sie können diese Option über die CMM-Webschnittstelle festlegen. Klicken Sie dazu auf **Gehäuseverwaltung → Rechenknoten**, markieren Sie den Server und wählen Sie unter **Automatischer Einschaltmodus** die Option **Automatisches Einschalten** aus.

Vorgehensweise

Installieren und konfigurieren Sie Docker auf dem Host mithilfe der Anleitungen, die mit Ihrer Docker-Distribution mitgeliefert wurden.

Schritt 6. XClarity Administrator installieren und konfigurieren

Installieren und konfigurieren Sie den Lenovo XClarity Administrator-Container auf dem gerade installierten Docker Host.

Vorbereitende Schritte

Stellen Sie sicher, dass das Hostsystem die Mindestanforderungen für Hardware und Software erfüllt (siehe Voraussetzungen bei Hardware und Software).

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Stellen Sie sicher, dass das Host-BS und XClarity Administrator denselben NTP-Server verwenden.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für Daten- und Hardwareverwaltung und BS-Implementierung festgelegt werden (siehe Netzwerkkonfigurationen). Im folgenden Beispiel wird „eth0“ verwendet.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für Daten- und Hardwareverwaltung und das Netzwerk für die BS-Implementierung festgelegt werden (siehe Netzwerkkonfigurationen). In den folgenden Beispielen wird „eth0“ bzw. „eth1“ verwendet.

Stellen Sie sicher, dass ein macvlan-Netzwerk in den Kernel auf dem Hostsystem geladen ist. Mit dem Befehl **lsmod | grep macvlan** können Sie prüfen, ob es geladen ist. Mit dem Befehl **modprobe macvlan** wird macvlan in den Kernel geladen.

Stellen Sie sicher, dass Sie einen eindeutigen Namen und eine IP-Adresse für jeden Container verwenden, wenn Sie mehrere XClarity Administrator-Container auf demselben Host ausführen.

Wenn Sie ThinkServer und andere Legacy-Einheiten verwalten wollen, stellen Sie sicher, dass Docker aktiviert ist, damit IPv6 unterstützt wird.

1. Bearbeiten Sie die Datei /etc/docker/daemon.json. Legen Sie den Schlüssel **ipv6** auf „wahr“ fest und legen Sie den Schlüssel **fixed-cidr-v6** auf Ihr IPv6-Subnetz fest. Nachfolgend finden Sie ein Beispiel für eine Daemon-Datei.

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

```
}
```

2. Laden Sie die Docker-Konfigurationsdatei neu, indem Sie den folgenden Befehl ausführen.
   ```
   systemctl reload docker
   ```

Anmerkung: XClarity Administrator wird *nicht* als privilegierter Container ausgeführt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen XClarity Administrator-Container mithilfe von Docker zu installieren.

Schritt 1. Sie können das Image der virtuellen XClarity Administrator-Einheit, die Umgebungs- und YAML-Datei über Website zum Herunterladen von XClarity Administrator auf eine Client-Workstation herunterladen. Melden Sie sich auf der Website an und verwenden Sie dann den erhaltenen Zugriffsschlüssel für den Image-Download.

Schritt 2. Importieren Sie das XClarity Administrator-Container-Image mit dem folgenden Befehl in Ihren Docker-Host.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Schritt 3. Bearbeiten Sie die Datei `docker_compose.env` und aktualisieren Sie die folgenden Umgebungsvariablen.

- **CONTAINER_NAME**. Eindeutiger Containername, der zum Erstellen von Docker-Datenträgern für jede XClarity Administrator-Instanz verwendet wird (z. B. `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Statische IPv4-Adresse für den Container (z. B. `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die zum Speichern der Sicherungen von XClarity Administrator verwendet werden kann. Der Pfad muss `/mnt/backup_share` sein.
- **FIRMWARE_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die als Remote-Repository für Firmwareaktualisierungen verwendet werden kann. Der Pfad muss `/mnt/fw_share` sein.

Nachfolgend finden Sie ein Beispiel für eine Umgebungsdatei.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Schritt 4. Bearbeiten Sie die Datei `docker_compose.yml` und aktualisieren Sie die folgenden Eigenschaften.

- Legen Sie die Eigenschaft **image** auf den Namen der in Schritt 2 verwendeten Installations-Image-Datei fest.

  Anmerkung: Sie können den Namen der Image-Datei mit dem Befehl `docker tag` ändern (z. B. zu „aktuell“).
- Wenn Sie die Remote-Freigabe als Remote-Firmware-Repository verwenden und XClarity Administrator-Sicherungen speichern möchten, legen Sie den Host-Mountpunkt für jede Remote-Freigabe in der Eigenschaft **volumes** fest.
- Legen Sie die Eigenschaft **dns** auf die IP-Adresse der DNS-Server fest.
- Der Container nutzt den Pool aus Prozessor- und Hauptspeicherressourcen, die für den Host verfügbar sind. Optional können Sie mit den Eigenschaften **cpus** und **memory** Grenzwerte für die Ressourcennutzung festlegen.
- Legen Sie für die Eigenschaft **parent** den Netzwerkschnittstellennamen auf dem Hostsystem fest, das als übergeordnete Schnittstelle für die macvlan-Schnittstelle im Container verwendet werden soll. Diese Schnittstelle muss direkten Zugriff auf das Subnetz haben, das dem Container zugeordnet ist.

- Legen Sie **subnet** und **gateway** entsprechend Ihrer Netzwerktopologie fest. In der Regel gehören Subnetz und Gateway zum Verwaltungsnetzwerk, zu dem die ${ADDRESS} gehört.
- Wenn IPv6 unterstützt werden soll, legen Sie die Eigenschaft **enable_ipv6** auf „wahr“ fest, legen Sie die Eigenschaft **ipv6_address** auf die IPv6-Adresse fest und fügen Sie je nach Netzwerktopologie einen weiteren Satz der Eigenschaften **subnet** und **gateway** hinzu (typisch für Verwaltungsnetzwerk, zu dem die IPv6-Adresse gehört).

Nachfolgend finden Sie ein Beispiel für eine YML-Datei mit aktiviertem IPv6.

```
version: '3.8'

services:

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

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

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

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

Schritt 5. Implementieren Sie das Image in Docker, indem Sie den folgenden Befehl ausführen. Dabei ist <*ENV_FILENAME*> der Name der Datei mit Umgebungsvariablen, die Sie in Schritt 2 erstellt haben.

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

Nach dieser Aufgabe

Melden Sie sich bei XClarity Administrator an und nehmen Sie die Konfiguration vor (siehe Erster Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle und Lenovo XClarity Administrator konfigurieren).

Topologie von virtuell getrennten Daten- und Verwaltungsnetzwerken

In dieser Topologie sind Daten- und Verwaltungsnetzwerk logisch getrennt. Die Pakete aus dem Datennetzwerk und die Pakete aus dem Verwaltungsnetzwerk werden über dieselbe physische Verbindung übertragen. Mithilfe von VLAN-Tagging bei allen Datenpaketen des Verwaltungsnetzwerks wird der Datenverkehr zwischen den beiden Netzwerken getrennt.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jeder Einheit installiert ist, die Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Stellen Sie sicher, dass VLAN-IDs für Daten- und Verwaltungsnetzwerke konfiguriert werden. Optional können Sie VLAN-Tagging über die Flex-Switches oder über die Top-of-Rack Switches aktivieren (vorausgesetzt, Sie haben die Tagging-Aktivierung über Flex-Switches oder Top-of-Rack-Switches implementiert).

Achten Sie darauf, dass die Ports für die CMM-Verbindung als Teil des Verwaltungs-VLANs definiert werden.

Wichtig: 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. Wenn Sie DHCP nutzen, stellen Sie sicher, dass die IP-Adressenänderungen minimiert werden.

Zu dieser Aufgabe

In der folgenden Abbildung wird eine Möglichkeit für die Umgebungskonfiguration dargestellt, in der Verwaltungsnetzwerk und logisches Netzwerk getrennt sind. Die Zahlen in der Abbildung entsprechen den Schritten in den nachfolgenden Abschnitten.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Flex-Switches, CMMs und Rack-Server abgebildet, da diese bei der Einrichtung von logisch getrennten Daten- und Verwaltungsnetzwerken erforderlich sind.

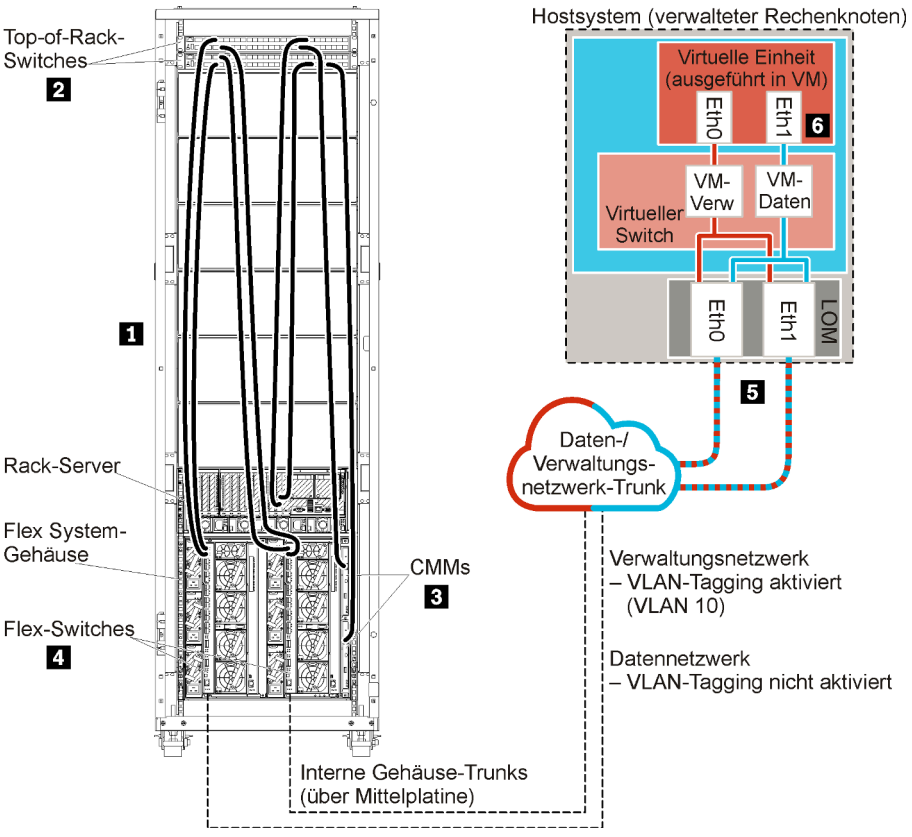


Abbildung 16. Beispiel: Topologie – Virtuell getrenntes Daten- und Verwaltungsnetzwerk für eine virtuelle Einheit

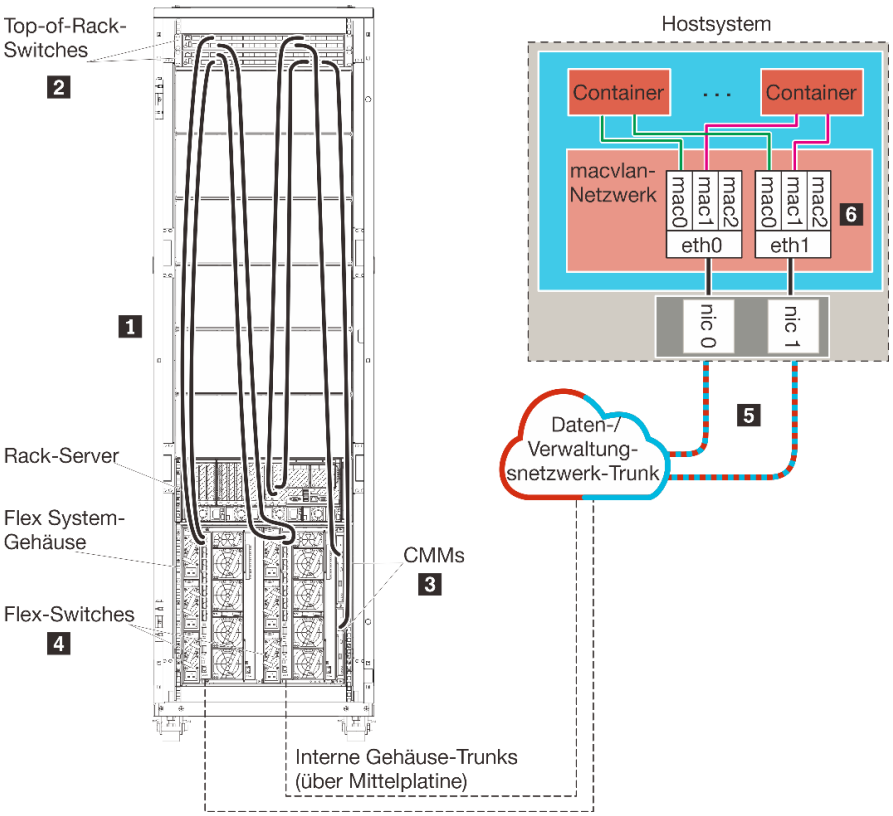


Abbildung 17. Beispiel: Topologie – Virtuell getrenntes Daten- und Verwaltungsnetzwerk für Container

In diesem Szenario wird XClarity Administrator auf einem Server in einem Flex System-Gehäuse installiert, das von XClarity Administrator verwaltet wird.

Wichtig: Sie können XClarity Administrator auf jedem System einrichten, das die Anforderungen für XClarity Administrator erfüllt, einschließlich eines verwalteten Servers. Wenn Sie einen verwalteten Server als XClarity Administrator-Host einsetzen:

- Sie müssen entweder eine Topologie von logisch getrennten Daten- und Verwaltungsnetzwerken oder eine Topologie von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten implementieren.
- Sie können mit XClarity Administrator keine Firmwareaktualisierungen für den verwalteten Server ausführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator-Hosts installiert.
- Wenn Sie einen Server in einem Flex System-Gehäuse verwenden, stellen Sie sicher, dass der Server automatisch eingeschaltet wird. Sie können diese Option über die CMM-Webschnittstelle festlegen. Klicken Sie dazu auf **Gehäuseverwaltung → Rechenknoten**, markieren Sie den Server und wählen Sie unter **Automatischer Einschaltmodus** die Option **Automatisches Einschalten** aus.

Zudem werden in diesem Szenario alle Daten über dieselben physischen Verbindungen gesendet. Die Trennung von Daten- und Verwaltungsnetzwerken wird durch VLAN-Tagging ermöglicht. Dabei werden spezielle Tags (die dem Verwaltungsnetzwerk entsprechen) an eingehende Datenpakete angehängt, um sicherzustellen, dass diese an die entsprechenden Schnittstellen weitergeleitet werden. Diese Tags werden aus ausgehenden Datenpaketen entfernt.

Auf einer der folgenden Einheiten kann VLAN-Tagging aktiviert werden:

- **Top-of-Rack-Switches**. Die VLAN-Tags (die dem Verwaltungsnetzwerk entsprechen) werden an eingehende Pakete für die Top-of-Rack-Switches angehängt und über die Flex-Switches bis zu den Servern im Flex System-Gehäuse weitergegeben. Auf dem Rückweg vom Top-of-Rack-Switch zu den Management-Controllern werden die VLAN-Tags entfernt.
- **Flex-Switches**. Die VLAN-Tags (die dem Verwaltungsnetzwerk entsprechen) werden an eingehende Pakete für die Flex-Switches angehängt und bis zu den Servern in einem Flex System-Gehäuse weitergegeben. Auf dem Rückweg werden VLAN-Tags von den Servern hinzugefügt und an die Flex-Switches übergeben, die dann diese Tags bei der Weiterleitung an die Management-Controller entfernen.

Die Entscheidung, VLAN-Tagging zu implementieren, hängt von den Anforderungen und der Komplexität Ihrer Umgebung ab.

Wenn Sie XClarity Administrator zur Verwaltung von vorhandenen und bereits konfigurierten Gehäusen und Rack-Servern installieren möchten, fahren Sie mit Schritt 5: Host installieren und konfigurieren fort.

Weitere Informationen über die Planung dieser Topologie - mit Informationen über Netzwerkeinstellungen sowie die Konfiguration von Eth1 und Eth0 - finden Sie unter Virtuell getrennte Daten und Verwaltungsnetzwerk.

Schritt 1: Gehäuse und Rack-Server mit den Top-of-Rack-Switches verkabeln

Verkabeln Sie die Gehäuse und die Rack-Server mit dem gleichen Top-of-Rack-Switch, um die Kommunikation zwischen den Einheiten zu ermöglichen.

Vorgehensweise

Verkabeln Sie jeden Flex-Switch und alle CMMs in den Gehäusen sowie jeden Rack-Server mit beiden Top-of-Rack-Switches. Die Ports in diesem Top-of-Rack-Switch können Sie beliebig auswählen.

In der folgenden Abbildung wird ein Beispiel für die Verkabelung von Gehäusen (Flex-Switches und CMMs) und Rack-Servern zu den Top-of-Rack-Switches dargestellt, wenn Lenovo XClarity Administrator auf einem Server in einem Gehäuse installiert ist, der von XClarity Administrator verwaltet wird.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Flex-Switches, CMMs und Rack-Server abgebildet, da diese bei der Einrichtung von logisch getrennten Daten- und Verwaltungsnetzwerken erforderlich sind.

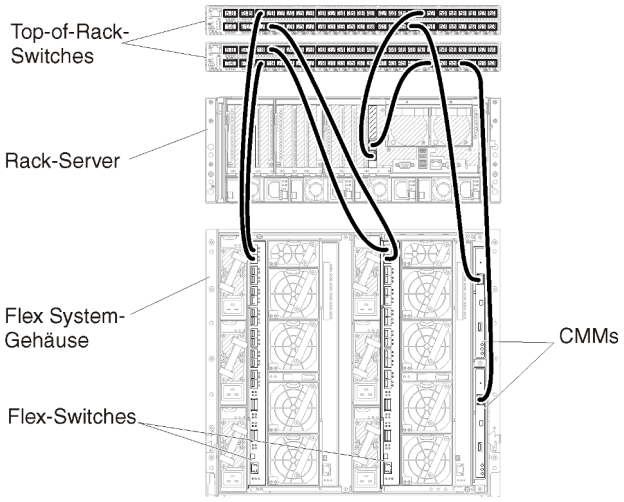


Abbildung 18. Beispiel: Verkabelung für logisch getrennte Daten- und Verwaltungsnetzwerke

Schritt 2: Top-of-Rack-Switches konfigurieren

Konfigurieren Sie die Top-of-Rack-Switches.

Vorbereitende Schritte

Stellen Sie zusätzlich zu den üblichen Konfigurationsanforderungen für Top-of-Rack-Switches sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die externen Ports zu Flex-Switches, zu Rack-Servern und zum Netzwerk sowie die internen Ports zum CMM, zu Rack-Servern und zum Netzwerk.

Je nach den Anforderungen und der Komplexität Ihrer Umgebung können Sie VLAN-Tagging in den Flex-Switches oder den Top-of-Rack-Switches implementieren. Wenn Sie Tagging über Top-of-Rack-Switches implementieren möchten, müssen Sie VLAN-Tagging über die Top-of-Rack-Switches aktivieren.

Stellen Sie sicher, dass VLAN-IDs für Daten- und Verwaltungsnetzwerke konfiguriert werden.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Rack-Switches abweichen.

In der folgenden Abbildung wird beispielhaft das VLAN-Tagging veranschaulicht, das in die Top-of-Rack-Switches implementiert ist und nur im Verwaltungsnetzwerk aktiviert wird. Das Verwaltungs-VLAN wird als VLAN 10 konfiguriert.

In diesem Szenario müssen die Ports für die CMM-Verbindung als Teil des Verwaltungs-VLANs definiert werden.

Anmerkung: Sie können VLAN-Tagging auch im Datennetzwerk aktivieren, um ein Daten-VLAN zu konfigurieren.

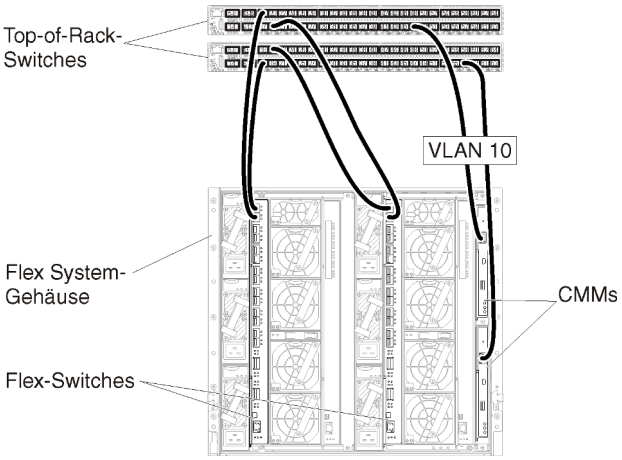


Abbildung 19. Beispiel: Konfiguration für Flex-Switches in logisch getrennten Daten- und Verwaltungsnetzwerken (VMware ESXi) mit aktiviertem VLAN-Tagging im Verwaltungsnetzwerk

Weitere Informationen über die Konfiguration der Top-of-Rack-Switches von Lenovo finden Sie unter Online-Dokumentation zu Rack-Switches im System x. Falls ein anderer Top-of-Rack-Switch installiert ist, ziehen Sie die entsprechende Dokumentation zum Switch heran.

Schritt 3: Chassis Management Modules (CMMs) konfigurieren

Konfigurieren Sie das primäre Chassis Management Module (CMM) im Gehäuse zur Verwaltung aller Einheiten im Gehäuse.

Zu dieser Aufgabe

Ausführliche Informationen über die CMM-Konfiguration finden Sie unter Gehäusekomponenten konfigurieren in der Flex System- Onlinedokumentation.

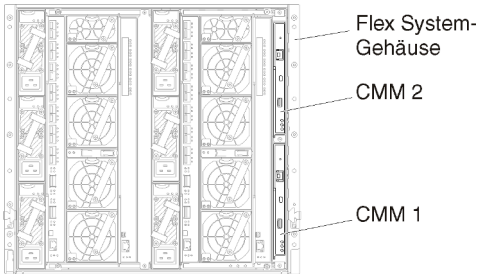
Beachten Sie auch die Schritte 4.1 bis 4.5 der Anleitung zum Gehäuse.

Vorgehensweise

Führen Sie für die CMM-Konfiguration folgende Schritte aus.

Wenn zwei CMMs installiert sind, konfigurieren Sie nur das *primäre* CMM, das automatisch die Konfiguration mit dem Standby-CMM synchronisiert.

Schritt 1. Verbinden Sie das CMM in Position 1 über ein Ethernet-Kabel mit einer Client-Workstation, um eine direkte Verbindung herzustellen.



Um erstmalig eine Verbindung zum CMM herzustellen, müssen Sie möglicherweise die IP-Eigenschaften der Client-Workstation ändern.

Wichtig: Stellen Sie sicher, dass die Client-Workstation und das CMM das gleiche Subnetz nutzen. (Das CMM-Standardsubnetz ist 255.255.255.0). Die für die Client-Workstation gewählte IP-Adresse muss im gleichen Netzwerk sein wie das CMM (z. B. 192.168.70.0 bis 192.168.70.24).

Schritt 2. Zum Starten der CMM-Verwaltungsschnittstelle öffnen Sie einen Webbrowser auf der Client-Workstation und geben die IP-Adresse des CMM ein.

Anmerkungen:

- Stellen Sie sicher, dass Sie eine sichere Verbindung verwenden, und binden Sie **https** in die URL ein (z. B. https://192.168.70.100). Wenn Sie „https“ nicht einbinden, erhalten Sie den Fehler „Seite nicht gefunden“.
- Falls Sie die IP-Standardadresse 192.168.70.100 verwenden, kann es einige Minuten dauern, bevor die CMM-Verwaltungsschnittstelle verfügbar ist. Diese Verzögerung tritt auf, weil das CMM zwei Minuten lang versucht, eine DHCP-Adresse abzurufen, bevor die statische Standardadresse verwendet wird.

Schritt 3. Melden Sie sich mit der Standardbenutzer-ID `USERID` und dem Kennwort `PASSWORD` an der CMM-Verwaltungsschnittstelle an. Sie müssen das Standardkennwort nach der ersten Anmeldung ändern.

Schritt 4. Führen Sie die Schritte im Assistenten für die CMM-Erstkonfiguration aus und geben Sie die Details für Ihre Umgebung an. Im Assistenten für die Erstkonfiguration können Sie folgende Schritte ausführen:

- Zeigen Sie den Bestand und den Status des Gehäuses an.
- Importieren Sie die Konfiguration aus einer vorhandenen Konfigurationsdatei.
- Konfigurieren Sie allgemeine CMM-Einstellungen.
- Stellen Sie das Datum und die Uhrzeit für das CMM ein.

  Tipp: Bei der Installation von XClarity Administrator konfigurieren Sie XClarity Administrator und alle von XClarity Administrator verwalteten Gehäuse zur Verwendung eines NTP-Servers.
- Konfigurieren Sie die IP-Daten für das CMM.
- Konfigurieren Sie die CMM-Sicherheitsrichtlinie.
- Konfigurieren Sie den DNS (Domain Name System).
- Konfigurieren Sie die Ereignisweiterleitungen.

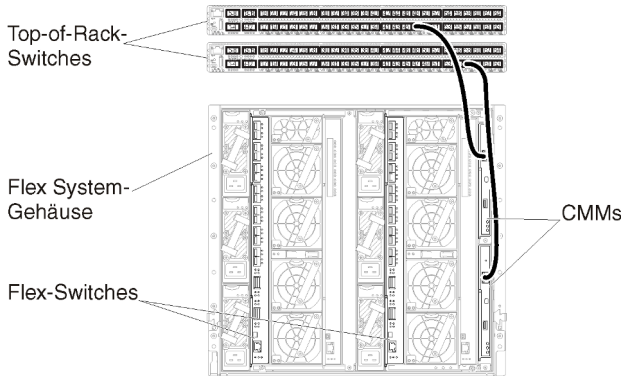
Schritt 5. Nachdem Sie die Einstellungen im Konfigurationsassistenten gespeichert und übernommen haben, konfigurieren Sie die IP-Adressen für alle Komponenten im Gehäuse.

Beachten Sie Schritt 4.6 der Anleitung zum Gehäuse.

Anmerkung: Sie müssen den Systemverwaltungsprozessor für jeden Rechenknoten zurücksetzen und die Flex-Switches neu starten, damit die neuen IP-Adressen angezeigt werden.

Schritt 6. Starten Sie das CMM mithilfe der CMM-Verwaltungsschnittstelle neu.

Schritt 7. Beim CMM-Neustart verbinden Sie ein Kabel vom Ethernet-Port des CMM mit dem Netzwerk.



Schritt 8. Melden Sie sich mit der neuen IP-Adresse an der CMM-Verwaltungsschnittstelle an.

Nach dieser Aufgabe

Sie können das CMM auch zur Unterstützung von Redundanz konfigurieren. Im CMM-Hilfesystem erhalten Sie weitere Informationen über die Felder, die auf den folgenden Seiten verfügbar sind.

- Konfigurieren Sie ein Failover für das CMM, falls im primären CMM ein Hardwareausfall auftritt. Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Eigenschaften → Erweitertes Failover**.
- Konfigurieren Sie das Failover als Folge eines Netzwerkproblems (Uplink). Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Netzwerk** und klicken Sie dann auf die Registerkarte **Ethernet** und dort auf **Erweitertes Ethernet**. Wählen Sie mindestens **Funktionsübernahme bei Verlust der physischen Netzwerkverbindung** aus.

Schritt 4: Flex-Switches

Konfigurieren Sie Flex-Switches in jedem Gehäuse.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch externe Ports vom Flex-Switch zum Top-of-Rack-Switch sowie interne Ports zum CMM.

Je nach den Anforderungen und der Komplexität Ihrer Umgebung können Sie VLAN-Tagging in den Flex-Switches oder den Top-of-Rack-Switches implementieren. Wenn Sie Tagging über Flex-Switches implementieren möchten, müssen Sie VLAN-Tagging über die Flex-Switches aktivieren.

Stellen Sie sicher, dass VLAN-IDs für Daten- und Verwaltungsnetzwerke konfiguriert werden.

Wichtig: Stellen Sie bei jedem Flex System-Gehäuse sicher, dass der Fabric-Typ der Erweiterungskarte in den einzelnen Servern im Gehäuse mit dem Fabric-Typ aller Flex-Switches im gleichen Gehäuse kompatibel ist. Wenn beispielsweise Ethernet-Switches in einem Gehäuse installiert sind, müssen alle Server in diesem Gehäuse Ethernet-Konnektivität aufweisen (durch einen LAN-on-Motherboard-Anschluss oder eine Ethernet-Erweiterungskarte). Weitere Informationen über die Konfiguration von Flex-Switches finden Sie unter E/A-Module konfigurieren in der Flex Systems- Onlinedokumentation.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Flex-Switches abweichen. Weitere Informationen über die unterstützten Flex-Switches finden Sie unter Flex System-Netzwerkswitches in der Flex Systems- Onlinedokumentation.

In der folgenden Abbildung wird beispielhaft das VLAN-Tagging veranschaulicht, das in die Flex-Switches implementiert ist und nur im Verwaltungsnetzwerk aktiviert wird. Das Verwaltungs-VLAN wird als VLAN 10 konfiguriert.

Anmerkung: Sie können ein Daten-VLAN konfigurieren, indem Sie VLAN-Tagging im Datennetzwerk aktivieren.

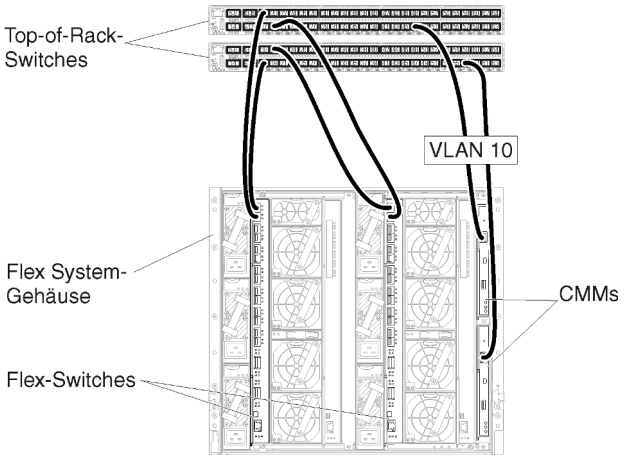


Abbildung 20. Beispiel: Konfiguration für Flex-Switches in logisch getrennten Daten- und Verwaltungsnetzwerken (VMware ESXi) mit aktiviertem VLAN-Tagging im Verwaltungsnetzwerk

Gehen Sie wie folgt vor, um die Flex-Switches für dieses Szenario zu konfigurieren:

Schritt 1. Konfigurieren Sie den Flex-Switch in Flex-Position 1:

a. Legen Sie fest, dass im Verwaltungs-VLAN (in diesem Beispiel VLAN 10) der externe Port für die Verkabelung zum Top-of-Rack-Verwaltungs-Switch (Ext1) enthalten ist.

b. Legen Sie einen internen Port für VLAN 10 (Verwaltungs-VLAN) fest. Stellen Sie sicher, dass VLAN-Trunking für diesen Port aktiviert ist.

Schritt 2. Konfigurieren Sie den Flex-Switch in Flex-Position 2:

Tipp: Wenn Sie die Rückseite des Gehäuses betrachten, handelt es sich bei Flex-Switch-Position 2 um die dritte Modulposition:

a. Legen Sie fest, dass im Verwaltungs-VLAN (in diesem Beispiel VLAN 10) der externe Port für die Verkabelung zum Top-of-Rack-Verwaltungs-Switch enthalten ist.

b. Legen Sie einen internen Port für VLAN 10 (Verwaltungs-VLAN) fest. Stellen Sie sicher, dass VLAN-Trunking für diesen Port aktiviert ist.

Schritt 5: Host installieren und konfigurieren

Sie können Docker in jedem System installieren, das den Anforderungen für Lenovo XClarity Administrator entspricht.

Vorbereitende Schritte

Mit Docker Datacenter können Sie eine Hochverfügbarkeitsumgebung für XClarity Administrator Container einrichten, die in der Docker Engine ausgeführt werden. Weitere Informationen über Hochverfügbarkeit mit Docker Datacenter finden Sie unter Webseite „Hochverfügbarkeitsarchitektur und Apps mit Docker Datacenter“.

Stellen Sie sicher, dass der Host die Voraussetzungen erfüllt, die unter Voraussetzungen bei Hardware und Software.

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Wichtig: Sie können XClarity Administrator auf jedem System einrichten, das die Anforderungen für XClarity Administrator erfüllt, einschließlich eines verwalteten Servers. Wenn Sie einen verwalteten Server als XClarity Administrator-Host einsetzen:

- Sie müssen entweder eine Topologie von logisch getrennten Daten- und Verwaltungsnetzwerken oder eine Topologie von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten implementieren.
- Sie können mit XClarity Administrator keine Firmwareaktualisierungen für den verwalteten Server ausführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator-Hosts installiert.
- Wenn Sie einen Server in einem Flex System-Gehäuse verwenden, stellen Sie sicher, dass der Server automatisch eingeschaltet wird. Sie können diese Option über die CMM-Webschnittstelle festlegen. Klicken Sie dazu auf **Gehäuseverwaltung → Rechenknoten**, markieren Sie den Server und wählen Sie unter **Automatischer Einschaltmodus** die Option **Automatisches Einschalten** aus.

Vorgehensweise

Installieren und konfigurieren Sie Docker auf dem Host mithilfe der Anleitungen, die mit Ihrer Docker-Distribution mitgeliefert wurden.

Schritt 6. XClarity Administrator installieren und konfigurieren

Installieren und konfigurieren Sie den Lenovo XClarity Administrator-Container auf dem gerade installierten Docker Host.

Vorbereitende Schritte

Stellen Sie sicher, dass das Hostsystem die Mindestanforderungen für Hardware und Software erfüllt (siehe Voraussetzungen bei Hardware und Software).

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Stellen Sie sicher, dass das Host-BS und XClarity Administrator denselben NTP-Server verwenden.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für Daten- und Hardwareverwaltung und BS-Implementierung festgelegt werden (siehe Netzwerkkonfigurationen). Im folgenden Beispiel wird „eth0“ verwendet.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für Daten- und Hardwareverwaltung und das Netzwerk für die BS-Implementierung festgelegt werden (siehe Netzwerkkonfigurationen). In den folgenden Beispielen wird „eth0“ bzw. „eth1“ verwendet.

Stellen Sie sicher, dass ein macvlan-Netzwerk in den Kernel auf dem Hostsystem geladen ist. Mit dem Befehl **lsmod | grep macvlan** können Sie prüfen, ob es geladen ist. Mit dem Befehl **modprobe macvlan** wird macvlan in den Kernel geladen.

Stellen Sie sicher, dass Sie einen eindeutigen Namen und eine IP-Adresse für jeden Container verwenden, wenn Sie mehrere XClarity Administrator-Container auf demselben Host ausführen.

Wenn Sie ThinkServer und andere Legacy-Einheiten verwalten wollen, stellen Sie sicher, dass Docker aktiviert ist, damit IPv6 unterstützt wird.

1. Bearbeiten Sie die Datei /etc/docker/daemon.json. Legen Sie den Schlüssel **ipv6** auf „wahr“ fest und legen Sie den Schlüssel **fixed-cidr-v6** auf Ihr IPv6-Subnetz fest. Nachfolgend finden Sie ein Beispiel für eine Daemon-Datei.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Laden Sie die Docker-Konfigurationsdatei neu, indem Sie den folgenden Befehl ausführen.
```
systemctl reload docker
```

Anmerkung: XClarity Administrator wird *nicht* als privilegierter Container ausgeführt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen XClarity Administrator-Container mithilfe von Docker zu installieren.

Schritt 1. Sie können das Image der virtuellen XClarity Administrator-Einheit, die Umgebungs- und YAML-Datei über Website zum Herunterladen von XClarity Administrator auf eine Client-Workstation herunterladen. Melden Sie sich auf der Website an und verwenden Sie dann den erhaltenen Zugriffsschlüssel für den Image-Download.

Schritt 2. Importieren Sie das XClarity Administrator-Container-Image mit dem folgenden Befehl in Ihren Docker-Host.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Schritt 3. Bearbeiten Sie die Datei `docker_compose.env` und aktualisieren Sie die folgenden Umgebungsvariablen.

- **CONTAINER_NAME**. Eindeutiger Containername, der zum Erstellen von Docker-Datenträgern für jede XClarity Administrator-Instanz verwendet wird (z. B. `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Statische IPv4-Adresse für den Container (z. B. `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die zum Speichern der Sicherungen von XClarity Administrator verwendet werden kann. Der Pfad muss `/mnt/backup_share` sein.
- **FIRMWARE_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die als Remote-Repository für Firmwareaktualisierungen verwendet werden kann. Der Pfad muss `/mnt/fw_share` sein.

Nachfolgend finden Sie ein Beispiel für eine Umgebungsdatei.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Schritt 4. Bearbeiten Sie die Datei `docker_compose.yml` und aktualisieren Sie die folgenden Eigenschaften.

- Legen Sie die Eigenschaft **image** auf den Namen der in Schritt 2 verwendeten Installations-Image-Datei fest.

  Anmerkung: Sie können den Namen der Image-Datei mit dem Befehl `docker tag` ändern (z. B. zu „aktuell“).

- Wenn Sie die Remote-Freigabe als Remote-Firmware-Repository verwenden und XClarity Administrator-Sicherungen speichern möchten, legen Sie den Host-Mountpunkt für jede Remote-Freigabe in der Eigenschaft **volumes** fest.
- Legen Sie die Eigenschaft **dns** auf die IP-Adresse der DNS-Server fest.
- Der Container nutzt den Pool aus Prozessor- und Hauptspeicherressourcen, die für den Host verfügbar sind. Optional können Sie mit den Eigenschaften **cpus** und **memory** Grenzwerte für die Ressourcennutzung festlegen.
- Legen Sie für die Eigenschaft **parent** den Netzwerkschnittstellennamen auf dem Hostsystem fest, das als übergeordnete Schnittstelle für die macvlan-Schnittstelle im Container verwendet werden soll. Diese Schnittstelle muss direkten Zugriff auf das Subnetz haben, das dem Container zugeordnet ist.
- Legen Sie **subnet** und **gateway** entsprechend Ihrer Netzwerktopologie fest. In der Regel gehören Subnetz und Gateway zum Verwaltungsnetzwerk, zu dem die ${ADDRESS} gehört.
- Wenn IPv6 unterstützt werden soll, legen Sie die Eigenschaft **enable_ipv6** auf „wahr“ fest, legen Sie die Eigenschaft **ipv6_address** auf die IPv6-Adresse fest und fügen Sie je nach Netzwerktopologie einen weiteren Satz der Eigenschaften **subnet** und **gateway** hinzu (typisch für Verwaltungsnetzwerk, zu dem die IPv6-Adresse gehört).

Nachfolgend finden Sie ein Beispiel für eine YML-Datei mit aktiviertem IPv6.

```
version: '3.8'

services:

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

```
          memory: "8g"

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

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

Schritt 5. Implementieren Sie das Image in Docker, indem Sie den folgenden Befehl ausführen. Dabei ist <*ENV_FILENAME*> der Name der Datei mit Umgebungsvariablen, die Sie in Schritt 2 erstellt haben.

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

Nach dieser Aufgabe

Melden Sie sich bei XClarity Administrator an und nehmen Sie die Konfiguration vor (siehe Erster Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle und Lenovo XClarity Administrator konfigurieren).

Topologie von Nur-Verwaltungsnetzwerken

In dieser Topologie steht Lenovo XClarity Administrator nur ein Verwaltungsnetzwerk, aber kein Datennetzwerk zur Verfügung.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch:
- Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit)
- Externe Ports zum Netzwerk
- Interne Ports zum CMM

Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jeder Einheit installiert ist, die Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Wichtig: 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. Wenn Sie DHCP nutzen, stellen Sie sicher, dass die IP-Adressenänderungen minimiert werden.

Zu dieser Aufgabe

In der folgenden Abbildung wird eine Möglichkeit für die Umgebungskonfiguration dargestellt, wenn Lenovo XClarity Administrator nur ein Verwaltungsnetzwerk (und kein Datennetzwerk) zur Verfügung steht. Die Zahlen in der Abbildung entsprechen den Schritten in den nachfolgenden Abschnitten.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Flex-Switches, CMMs und Rack-Server abgebildet, da diese bei der Einrichtung von Nur-Verwaltungsnetzwerken erforderlich sind.

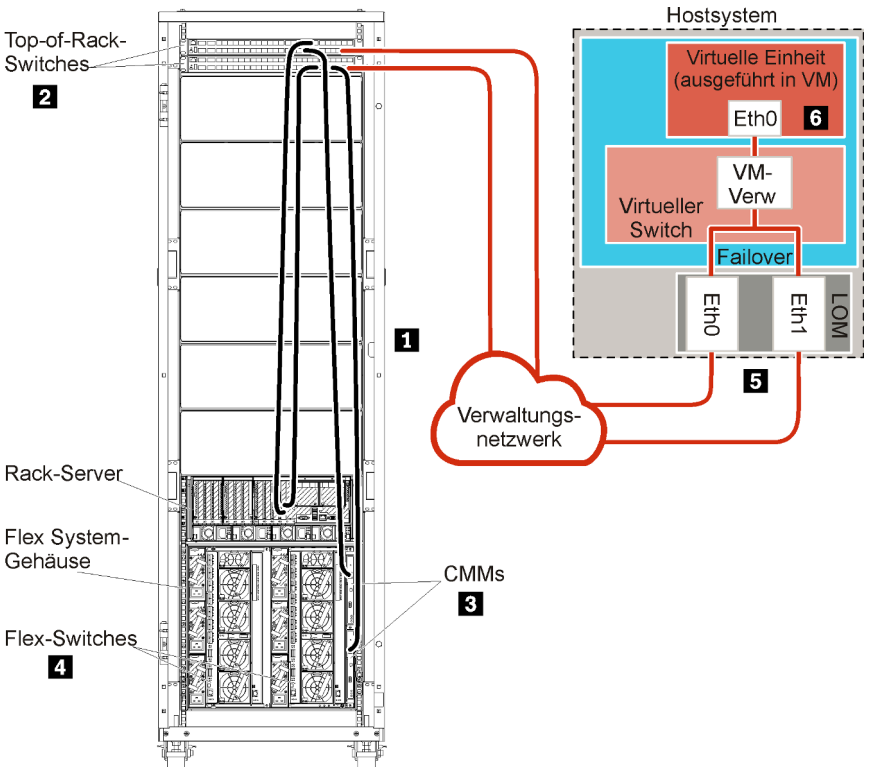


Abbildung 21. Beispiel: Topologie von Nur-Verwaltungsnetzwerken für eine virtuelle Einheit

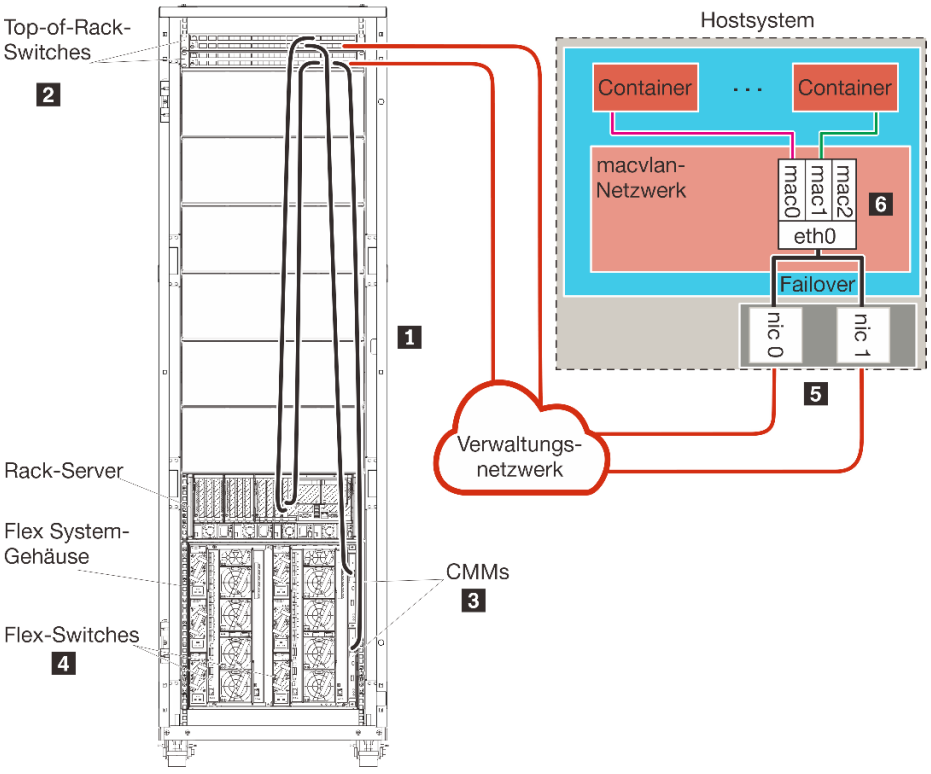


Abbildung 22. Beispiel: Topologie von Nur-Verwaltungsnetzwerken für Container

Wenn Sie XClarity Administrator zur Verwaltung von vorhandenen und bereits konfigurierten Gehäusen und Rack-Servern installieren möchten, fahren Sie mit Schritt 5: Host installieren und konfigurieren fort.

Weitere Informationen über die Planung dieser Topologie - mit Informationen über Netzwerkeinstellungen sowie die Konfiguration von Eth1 und Eth0 - finden Sie unter Nur-Verwaltungsnetzwerk.

Schritt 1: Gehäuse, Rack-Server und Lenovo XClarity Administrator-Host mit den Top-of-Rack-Switches verkabeln

Verkabeln Sie die Gehäuse, die Rack-Server und den XClarity Administrator-Host mit den Top-of-Rack-Switches, um die Kommunikation zwischen den Einheiten und dem Netzwerk zu ermöglichen.

Vorgehensweise

Verkabeln Sie jeden Flex-Switch und alle CMMs in den Gehäusen, jeden Rack-Server und den XClarity Administrator-Host mit beiden Top-of-Rack-Switches. Die Ports in den Top-of-Rack-Switches können Sie beliebig auswählen.

In der folgenden Abbildung wird ein Beispiel für die Verkabelung von Gehäusen (Flex-Switches und CMMs), Rack-Servern und dem XClarity Administrator-Host zu den Top-of-Rack-Switches dargestellt.

Anmerkung: In dieser Abbildung werden nicht alle Verkabelungsoptionen angegeben, die Sie möglicherweise in Ihrer Umgebung benötigen. Stattdessen werden nur die Verkabelungsanforderungen für Flex-Switches, CMMs und Rack-Server abgebildet, da diese bei der Einrichtung von Nur-Verwaltungsnetzwerken erforderlich sind.

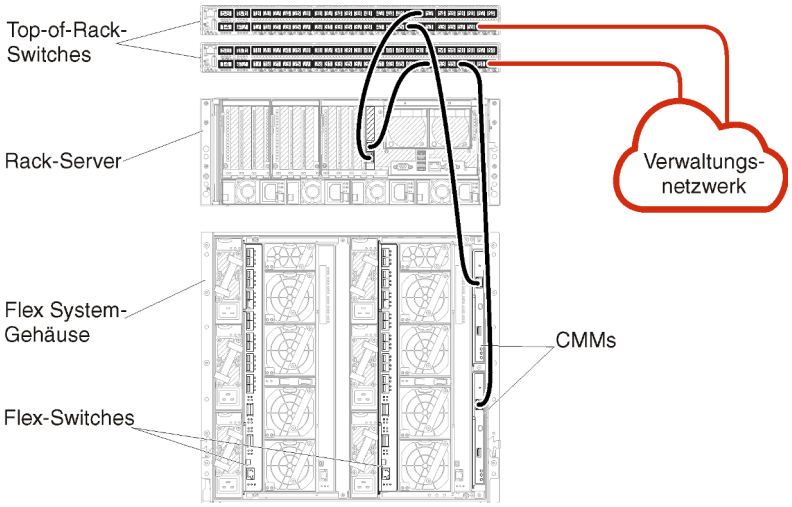


Abbildung 23. Beispiel: Verkabelung für Nur-Verwaltungsnetzwerke

Schritt 2: Top-of-Rack-Switches konfigurieren

Konfigurieren Sie die Top-of-Rack-Switches.

Vorbereitende Schritte

Stellen Sie zusätzlich zu den üblichen Konfigurationsanforderungen für Top-of-Rack-Switches sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die externen Ports zu Flex-Switches, zu Rack-Servern und zum Netzwerk sowie die internen Ports zum CMM, zu Rack-Servern und zum Netzwerk.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Rack-Switches abweichen.

Weitere Informationen über die Konfiguration der Top-of-Rack-Switches von Lenovo finden Sie unter Online-Dokumentation zu Rack-Switches im System x. Falls ein anderer Top-of-Rack-Switch installiert ist, ziehen Sie die entsprechende Dokumentation zum Switch heran.

Schritt 3: Chassis Management Modules (CMMs) konfigurieren

Konfigurieren Sie das primäre Chassis Management Module (CMM) im Gehäuse zur Verwaltung aller Einheiten im Gehäuse.

Zu dieser Aufgabe

Ausführliche Informationen über die CMM-Konfiguration finden Sie unter Gehäusekomponenten konfigurieren in der Flex System- Onlinedokumentation.

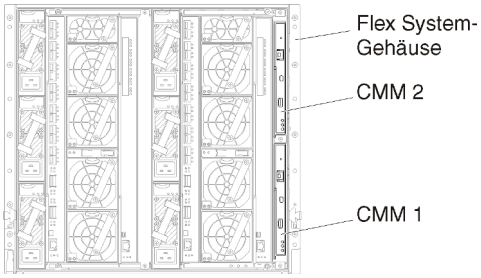
Beachten Sie auch die Schritte 4.1 bis 4.5 der Anleitung zum Gehäuse.

Vorgehensweise

Führen Sie für die CMM-Konfiguration folgende Schritte aus.

Wenn zwei CMMs installiert sind, konfigurieren Sie nur das *primäre* CMM, das automatisch die Konfiguration mit dem Standby-CMM synchronisiert.

Schritt 1. Verbinden Sie das CMM in Position 1 über ein Ethernet-Kabel mit einer Client-Workstation, um eine direkte Verbindung herzustellen.



Um erstmalig eine Verbindung zum CMM herzustellen, müssen Sie möglicherweise die IP-Eigenschaften der Client-Workstation ändern.

Wichtig: Stellen Sie sicher, dass die Client-Workstation und das CMM das gleiche Subnetz nutzen. (Das CMM-Standardsubnetz ist 255.255.255.0). Die für die Client-Workstation gewählte IP-Adresse muss im gleichen Netzwerk sein wie das CMM (z. B. 192.168.70.0 bis 192.168.70.24).

Schritt 2. Zum Starten der CMM-Verwaltungsschnittstelle öffnen Sie einen Webbrowser auf der Client-Workstation und geben die IP-Adresse des CMM ein.

Anmerkungen:

- Stellen Sie sicher, dass Sie eine sichere Verbindung verwenden, und binden Sie **https** in die URL ein (z. B. https://192.168.70.100). Wenn Sie „https“ nicht einbinden, erhalten Sie den Fehler „Seite nicht gefunden“.
- Falls Sie die IP-Standardadresse 192.168.70.100 verwenden, kann es einige Minuten dauern, bevor die CMM-Verwaltungsschnittstelle verfügbar ist. Diese Verzögerung tritt auf, weil das

CMM zwei Minuten lang versucht, eine DHCP-Adresse abzurufen, bevor die statische Standardadresse verwendet wird.

Schritt 3. Melden Sie sich mit der Standardbenutzer-ID `USERID` und dem Kennwort `PASSWORD` an der CMM-Verwaltungsschnittstelle an. Sie müssen das Standardkennwort nach der ersten Anmeldung ändern.

Schritt 4. Führen Sie die Schritte im Assistenten für die CMM-Erstkonfiguration aus und geben Sie die Details für Ihre Umgebung an. Im Assistenten für die Erstkonfiguration können Sie folgende Schritte ausführen:

- Zeigen Sie den Bestand und den Status des Gehäuses an.
- Importieren Sie die Konfiguration aus einer vorhandenen Konfigurationsdatei.
- Konfigurieren Sie allgemeine CMM-Einstellungen.
- Stellen Sie das Datum und die Uhrzeit für das CMM ein.

  Tipp: Bei der Installation von XClarity Administrator konfigurieren Sie XClarity Administrator und alle von XClarity Administrator verwalteten Gehäuse zur Verwendung eines NTP-Servers.
- Konfigurieren Sie die IP-Daten für das CMM.
- Konfigurieren Sie die CMM-Sicherheitsrichtlinie.
- Konfigurieren Sie den DNS (Domain Name System).
- Konfigurieren Sie die Ereignisweiterleitungen.

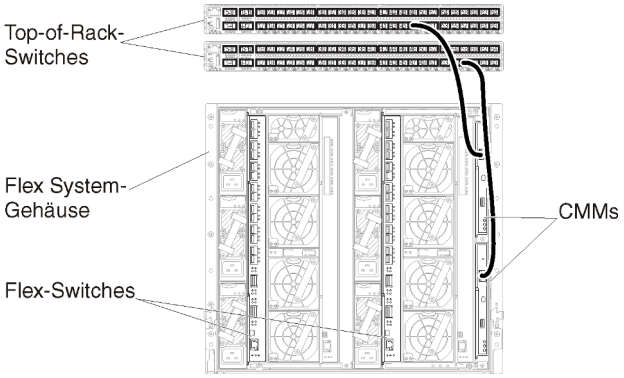
Schritt 5. Nachdem Sie die Einstellungen im Konfigurationsassistenten gespeichert und übernommen haben, konfigurieren Sie die IP-Adressen für alle Komponenten im Gehäuse.

Beachten Sie Schritt 4.6 der Anleitung zum Gehäuse.

Anmerkung: Sie müssen den Systemverwaltungsprozessor für jeden Rechenknoten zurücksetzen und die Flex-Switches neu starten, damit die neuen IP-Adressen angezeigt werden.

Schritt 6. Starten Sie das CMM mithilfe der CMM-Verwaltungsschnittstelle neu.

Schritt 7. Beim CMM-Neustart verbinden Sie ein Kabel vom Ethernet-Port des CMM mit dem Netzwerk.



Schritt 8. Melden Sie sich mit der neuen IP-Adresse an der CMM-Verwaltungsschnittstelle an.

Nach dieser Aufgabe

Sie können das CMM auch zur Unterstützung von Redundanz konfigurieren. Im CMM-Hilfesystem erhalten Sie weitere Informationen über die Felder, die auf den folgenden Seiten verfügbar sind.

- Konfigurieren Sie ein Failover für das CMM, falls im primären CMM ein Hardwareausfall auftritt. Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Eigenschaften → Erweitertes Failover**.

- Konfigurieren Sie das Failover als Folge eines Netzwerkproblems (Uplink). Klicken Sie in der CMM-Verwaltungsschnittstelle auf **Mgt Modulverwaltung → Netzwerk** und klicken Sie dann auf die Registerkarte **Ethernet** und dort auf **Erweitertes Ethernet**. Wählen Sie mindestens **Funktionsübernahme bei Verlust der physischen Netzwerkverbindung** aus.

Schritt 4: Flex-Switches konfigurieren

Konfigurieren Sie Flex-Switches in jedem Gehäuse.

Vorbereitende Schritte

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch externe Ports vom Flex-Switch zum Top-of-Rack-Switch sowie interne Ports zum CMM.

Wenn die Flex-Switches so konfiguriert sind, dass sie dynamische Netzwerkeinstellungen (IP-Adresse, Netzmaske, Gateway und DNS-Adresse) über DHCP abrufen, müssen die Einstellungen der Flex-Switches konsistent sein (z. B. müssen die IP-Adressen im gleichen Subnetz sein wie das CMM).

Wichtig: Stellen Sie bei jedem Flex System-Gehäuse sicher, dass der Fabric-Typ der Erweiterungskarte in den einzelnen Servern im Gehäuse mit dem Fabric-Typ aller Flex-Switches im gleichen Gehäuse kompatibel ist. Wenn beispielsweise Ethernet-Switches in einem Gehäuse installiert sind, müssen alle Server in diesem Gehäuse Ethernet-Konnektivität aufweisen (durch einen LAN-on-Motherboard-Anschluss oder eine Ethernet-Erweiterungskarte). Weitere Informationen über die Konfiguration von Flex-Switches finden Sie unter E/A-Module konfigurieren in der Flex Systems- Onlinedokumentation.

Vorgehensweise

Die Konfigurationsschritte können abhängig vom Typ der installierten Flex-Switches abweichen. Weitere Informationen über die unterstützten Flex-Switches finden Sie unter Flex System-Netzwerkswitches in der Flex Systems- Onlinedokumentation.

In der Regel werden die Flex-Switches in Flex-Switch-Positionen 1 und 2 konfiguriert.

Tipp: Wenn Sie die Rückseite des Gehäuses betrachten, handelt es sich bei Flex-Switch-Position 2 um die dritte Modulposition.

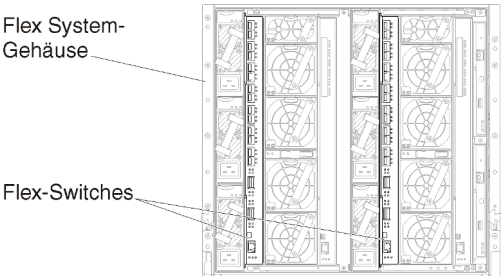


Abbildung 24. Flex-Switch-Positionen in einem Gehäuse

Schritt 5: Host installieren und konfigurieren

Sie können Docker in jedem System installieren, das den Anforderungen für Lenovo XClarity Administrator entspricht.

Vorbereitende Schritte

Mit Docker Datacenter können Sie eine Hochverfügbarkeitsumgebung für XClarity Administrator Container einrichten, die in der Docker Engine ausgeführt werden. Weitere Informationen über Hochverfügbarkeit mit Docker Datacenter finden Sie unter Webseite „Hochverfügbarkeitsarchitektur und Apps mit Docker Datacenter“.

Stellen Sie sicher, dass der Host die Voraussetzungen erfüllt, die unter Voraussetzungen bei Hardware und Software.

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Wichtig: Sie können XClarity Administrator auf jedem System einrichten, das die Anforderungen für XClarity Administrator erfüllt, einschließlich eines verwalteten Servers. Wenn Sie einen verwalteten Server als XClarity Administrator-Host einsetzen:

- Sie müssen entweder eine Topologie von logisch getrennten Daten- und Verwaltungsnetzwerken oder eine Topologie von Verwaltungsnetzwerken und Netzwerken mit einzelnen Daten implementieren.
- Sie können mit XClarity Administrator keine Firmwareaktualisierungen für den verwalteten Server ausführen. Auch wenn nur ein Teil der Firmware mit sofortiger Aktivierung installiert wird, zwingt XClarity Administrator den Zielserver zu einem Neustart, dabei wird XClarity Administrator ebenfalls neu gestartet. Bei einer verzögerten Aktivierung wird nur ein Teil der Firmware bei einem Neustart des XClarity Administrator-Hosts installiert.
- Wenn Sie einen Server in einem Flex System-Gehäuse verwenden, stellen Sie sicher, dass der Server automatisch eingeschaltet wird. Sie können diese Option über die CMM-Webschnittstelle festlegen. Klicken Sie dazu auf **Gehäuseverwaltung → Rechenknoten**, markieren Sie den Server und wählen Sie unter **Automatischer Einschaltmodus** die Option **Automatisches Einschalten** aus.

Vorgehensweise

Installieren und konfigurieren Sie Docker auf dem Host mithilfe der Anleitungen, die mit Ihrer Docker-Distribution mitgeliefert wurden.

Schritt 6. XClarity Administrator installieren und konfigurieren

Installieren und konfigurieren Sie den Lenovo XClarity Administrator-Container auf dem gerade installierten Docker Host.

Vorbereitende Schritte

Stellen Sie sicher, dass das Hostsystem die Mindestanforderungen für Hardware und Software erfüllt (siehe Voraussetzungen bei Hardware und Software).

Stellen Sie sicher, dass alle entsprechenden Ports aktiviert sind, darunter auch die Ports, die von XClarity Administrator benötigt werden (siehe Portverfügbarkeit).

Achten Sie darauf, dass sich das Hostsystem und die zu verwaltenden Einheiten im gleichen Netzwerk befinden.

Stellen Sie sicher, dass das Host-BS und XClarity Administrator denselben NTP-Server verwenden.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für Daten- und Hardwareverwaltung und BS-Implementierung festgelegt werden (siehe Netzwerkkonfigurationen). Im folgenden Beispiel wird „eth0“ verwendet.

Mit XClarity Administrator kann ein benutzerdefinierter Name für das Netzwerk für die Daten- und Hardwareverwaltung festgelegt werden (siehe Netzwerkkonfigurationen). Im folgenden Beispiel wird „eth0“ verwendet.

Stellen Sie sicher, dass ein macvlan-Netzwerk in den Kernel auf dem Hostsystem geladen ist. Mit dem Befehl **lsmod | grep macvlan** können Sie prüfen, ob es geladen ist. Mit dem Befehl **modprobe macvlan** wird macvlan in den Kernel geladen.

Stellen Sie sicher, dass Sie einen eindeutigen Namen und eine IP-Adresse für jeden Container verwenden, wenn Sie mehrere XClarity Administrator-Container auf demselben Host ausführen.

Wenn Sie ThinkServer und andere Legacy-Einheiten verwalten wollen, stellen Sie sicher, dass Docker aktiviert ist, damit IPv6 unterstützt wird.

1. Bearbeiten Sie die Datei /etc/docker/daemon.json. Legen Sie den Schlüssel **ipv6** auf „wahr“ fest und legen Sie den Schlüssel **fixed-cidr-v6** auf Ihr IPv6-Subnetz fest. Nachfolgend finden Sie ein Beispiel für eine Daemon-Datei.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Laden Sie die Docker-Konfigurationsdatei neu, indem Sie den folgenden Befehl ausführen.
```
systemctl reload docker
```

Anmerkung: XClarity Administrator wird *nicht* als privilegierter Container ausgeführt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen XClarity Administrator-Container mithilfe von Docker zu installieren.

Schritt 1. Sie können das Image der virtuellen XClarity Administrator-Einheit, die Umgebungs- und YAML-Datei über Website zum Herunterladen von XClarity Administrator auf eine Client-Workstation herunterladen. Melden Sie sich auf der Website an und verwenden Sie dann den erhaltenen Zugriffsschlüssel für den Image-Download.

Schritt 2. Importieren Sie das XClarity Administrator-Container-Image mit dem folgenden Befehl in Ihren Docker-Host.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Schritt 3. Bearbeiten Sie die Datei `docker_compose.env` und aktualisieren Sie die folgenden Umgebungsvariablen.

- **CONTAINER_NAME**. Eindeutiger Containername, der zum Erstellen von Docker-Datenträgern für jede XClarity Administrator-Instanz verwendet wird (z. B. `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Statische IPv4-Adresse für den Container (z. B. `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die zum Speichern der Sicherungen von XClarity Administrator verwendet werden kann. Der Pfad muss `/mnt/backup_share` sein.
- **FIRMWARE_MOUNT**. (Optional) Pfad für die Remote-Freigabe, die als Remote-Repository für Firmwareaktualisierungen verwendet werden kann. Der Pfad muss `/mnt/fw_share` sein.

Nachfolgend finden Sie ein Beispiel für eine Umgebungsdatei.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Schritt 4. Bearbeiten Sie die Datei `docker_compose.yml` und aktualisieren Sie die folgenden Eigenschaften.

- Legen Sie die Eigenschaft **image** auf den Namen der in Schritt 2 verwendeten Installations-Image-Datei fest.

  Anmerkung: Sie können den Namen der Image-Datei mit dem Befehl `docker tag` ändern (z. B. zu „aktuell“).
- Wenn Sie die Remote-Freigabe als Remote-Firmware-Repository verwenden und XClarity Administrator-Sicherungen speichern möchten, legen Sie den Host-Mountpunkt für jede Remote-Freigabe in der Eigenschaft **volumes** fest.
- Legen Sie die Eigenschaft **dns** auf die IP-Adresse der DNS-Server fest.
- Der Container nutzt den Pool aus Prozessor- und Hauptspeicherressourcen, die für den Host verfügbar sind. Optional können Sie mit den Eigenschaften **cpus** und **memory** Grenzwerte für die Ressourcennutzung festlegen.
- Legen Sie für die Eigenschaft **parent** den Netzwerkschnittstellennamen auf dem Hostsystem fest, das als übergeordnete Schnittstelle für die macvlan-Schnittstelle im Container verwendet werden soll. Diese Schnittstelle muss direkten Zugriff auf das Subnetz haben, das dem Container zugeordnet ist.
- Legen Sie **subnet** und **gateway** entsprechend Ihrer Netzwerktopologie fest. In der Regel gehören Subnetz und Gateway zum Verwaltungsnetzwerk, zu dem die ${ADDRESS} gehört.
- Wenn IPv6 unterstützt werden soll, legen Sie die Eigenschaft **enable_ipv6** auf „wahr“ fest, legen Sie die Eigenschaft **ipv6_address** auf die IPv6-Adresse fest und fügen Sie je nach Netzwerktopologie einen weiteren Satz der Eigenschaften **subnet** und **gateway** hinzu (typisch für Verwaltungsnetzwerk, zu dem die IPv6-Adresse gehört).

Nachfolgend finden Sie ein Beispiel für eine YML-Datei mit aktiviertem IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
```

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

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

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

Schritt 5. Implementieren Sie das Image in Docker, indem Sie den folgenden Befehl ausführen. Dabei ist <*ENV_FILENAME*> der Name der Datei mit Umgebungsvariablen, die Sie in Schritt 2 erstellt haben.

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

Nach dieser Aufgabe

Melden Sie sich bei XClarity Administrator an und nehmen Sie die Konfiguration vor (siehe Erster Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle und Lenovo XClarity Administrator konfigurieren).

Hochverfügbarkeit implementieren

Mit Docker Datacenter können Sie eine Hochverfügbarkeitsumgebung für Lenovo XClarity Administrator Container einrichten, die in der Docker Engine ausgeführt werden.

Weitere Informationen über Hochverfügbarkeit mit Docker Datacenter finden Sie unter Webseite „Hochverfügbarkeitsarchitektur und Apps mit Docker Datacenter“.

Kapitel 4. Lenovo XClarity Administrator konfigurieren

Wenn Sie zum ersten Mal auf Lenovo XClarity Administrator zugreifen, müssen Sie bestimmte Schritte für die Erstkonfiguration von XClarity Administrator ausführen.

Weitere Informationen: XClarity Administrator: Erstkonfiguration ausführen

Vorgehensweise

Gehen Sie wie folgt vor, um die Erstkonfiguration von XClarity Administrator auszuführen.

Schritt 1. Rufen Sie die XClarity Administrator-Webschnittstelle auf.

Schritt 2. Lesen und akzeptieren Sie die Lizenzvereinbarung.

Schritt 3. Erstellen Sie Benutzeraccounts mit Supervisorberechtigungen.

Tipp: Erstellen Sie zur Sicherheit mindestens zwei Benutzeraccounts mit Supervisorberechtigungen, damit Ihnen bei Bedarf ein weiterer Benutzeraccount zur Verfügung steht.

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. Konfigurieren Sie Service- und Unterstützungseinstellungen, einschließlich der Datenschutzrichtlinie, Nutzungs- und Hardwaredaten, Lenovo Support (Call-Home-Funktion), Lenovo Upload-Funktionalität und Produktgarantie.

Schritt 7. Konfigurieren Sie die Sicherheitseinstellungen einschließlich Authentifizierungsserver, Benutzergruppen, Serverzertifikaten und Verschlüsselungsmodus.

Schritt 8. Verwalten Sie Ihr Gehäuse, Server, Switches und Speichereinheiten.

Erster Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle

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

Vorbereitende Schritte

Vergewissern Sie sich, dass Sie einen der folgenden unterstützten Webbrowser verwenden:
- Chrome™ 48.0 oder höher (55.0 oder höher für Ferne Konsole)
- Firefox® ESR 38.6.0 oder höher
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 oder höher (IOS7 oder höher und OS X)

Anmerkung: Das Starten der Management-Controller-Schnittstellen von XClarity Administrator unter Verwendung des Safari-Webbrowsers wird nicht unterstützt.

Stellen Sie sicher, dass Sie sich bei der XClarity Administrator-Webschnittstelle über ein System anmelden, das über eine Netzwerkverbindung zum XClarity Administrator-Verwaltungsknoten verfügt.

Vorgehensweise

Gehen Sie wie folgt vor, wenn Sie zum ersten Mal auf die XClarity Administrator-Webschnittstelle zugreifen.

Schritt 1. Öffnen Sie im Browser die IP-Adresse von XClarity Administrator.

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

- **Für Container**: Verwenden Sie die IPv4-Adresse, die für die Variable ${ADDRESS} angegeben ist, um über die folgende URL auf XClarity Administrator zuzugreifen:
  `https://<IPv4_address>/ui/login.html`

  Beispiel:
  `https://192.0.2.10/ui/login.html`
- **Für virtuelle Einheiten**: Die verwendete IP-Adresse hängt davon ab, wie Ihre Umgebung eingerichtet ist.

  Wenn Sie Eth0- und Eth1-Netzwerke auf separaten Teilnetzen haben und DHCP auf beiden Teilnetzen verwendet wird, verwenden Sie die IP-Adresse *Eth1*, wenn Sie für die Erstkonfiguration auf die Webschnittstelle zugreifen. Beim ersten Starten von XClarity Administrator wird Eth0 und Eth1 eine von DHCP zugeordnete IP-Adresse zugewiesen und das Standard-Gateway XClarity Administrator wird für *Eth1* auf das von DHCP zugeordnete Gateway festgelegt.

  Statische IPv4-Adresse verwenden

  Wenn Sie eine IPv4-Adresse in eth0_config angegeben haben, verwenden Sie diese, um über die folgende URL auf XClarity Administrator zuzugreifen:
  `https://<IPv4_address>/ui/login.html`

  Beispiel:
  `https://192.0.2.10/ui/login.html`

  DHCP-Server in derselben Übertragungsdomäne wie XClarity Administrator verwenden

  Wenn ein DHCP-Server in derselben Übertragungsdomäne wie XClarity Administrator eingerichtet ist, greifen Sie über die IPv4-Adresse, die in der Konsole der virtuellen Maschine von XClarity Administrator angezeigt wird, über die folgende URL auf XClarity Administrator zu:
  `https://<IPv4_address>/ui/login.html`

  Beispiel:
  `https://192.0.2.10/ui/login.html`

  DHCP-Server in einer anderen Übertragungsdomäne als XClarity Administrator verwenden

  Wenn *kein* DHCP-Server in derselben Übertragungsdomäne eingerichtet ist, verwenden Sie die lokale IPv6-Linkadresse (Link-Local Address, LLA), die für eEth0 (Verwaltungsnetzwerk) in der Konsole der virtuellen Maschine von XClarity Administrator angezeigt wird, um auf XClarity Administrator zuzugreifen. Beispiel:

```
------------------------------------------
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
  … …
```

Tipp: Die lokale IPv6-Linkadresse (LLA) wird von der MAC-Adresse der Schnittstelle abgeleitet.

Achtung: Wenn Sie XClarity Administrator 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 Administrator zugreifen, die eine Verbindung zu XClarity Administrator aufweist. Beispielsweise können Sie über eine andere VM auf dem Host, auf der XClarity Administrator installiert ist, auf XClarity Administrator zugreifen.

– **Firefox:**

  Melden Sie sich mit folgender URL an, um über den Firefox-Browser auf XClarity Administrator zuzugreifen. Beachten Sie, dass bei der Eingabe von IPv6-Adressen Klammern erforderlich sind.

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

  Geben Sie beispielsweise auf Grundlage des vorherigen Beispiels für Eth0 die folgende URL in Ihren Webbrowser ein:

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

– **Internet Explorer:**

  Melden Sie sich mit folgender URL an, um über einen Internet Explorer-Browser auf XClarity Administrator zuzugreifen. Beachten Sie, dass bei der Eingabe von IPv6-Adressen Klammern erforderlich sind.

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

  wobei *<zone_index>* die Kennung für den Ethernet-Adapter ist, der vom Computer, auf dem Sie den Webbrowser gestartet haben, mit dem Verwaltungsnetzwerk verbunden ist. Wenn Sie einen Browser unter Windows verwenden, können Sie mit dem Befehl `ipconfig` den Zonenindex suchen, der nach dem Prozentzeichen (%) im Feld **Lokale IPv6-Verbindungsadresse** für den Adapter angezeigt wird. Im folgenden Beispiel ist der Zonenindex „30.“

  ```
  PS C:> ipconfig
  Windows IP-Konfiguration

  Ethernet-Adapter vEthernet (teamVirtualSwitch):

     Verbindungsspezifisches DNS-Suffix:
     Verbindungslokale IPv6-Adresse . . . . . : 2001:db8:56ff:fe80:bea3%30
     Autokonfiguration IPv4-Adresse. . : 192.0.2.30
     Standard-Gateway . . . . . :
  ```

Wenn Sie einen Browser unter Linux verwenden, suchen Sie den Zonenindex mit dem Befehl `ifconfig`. Sie können auch den Namen des Adapters (in der Regel Eth0) als Zonenindex verwenden.

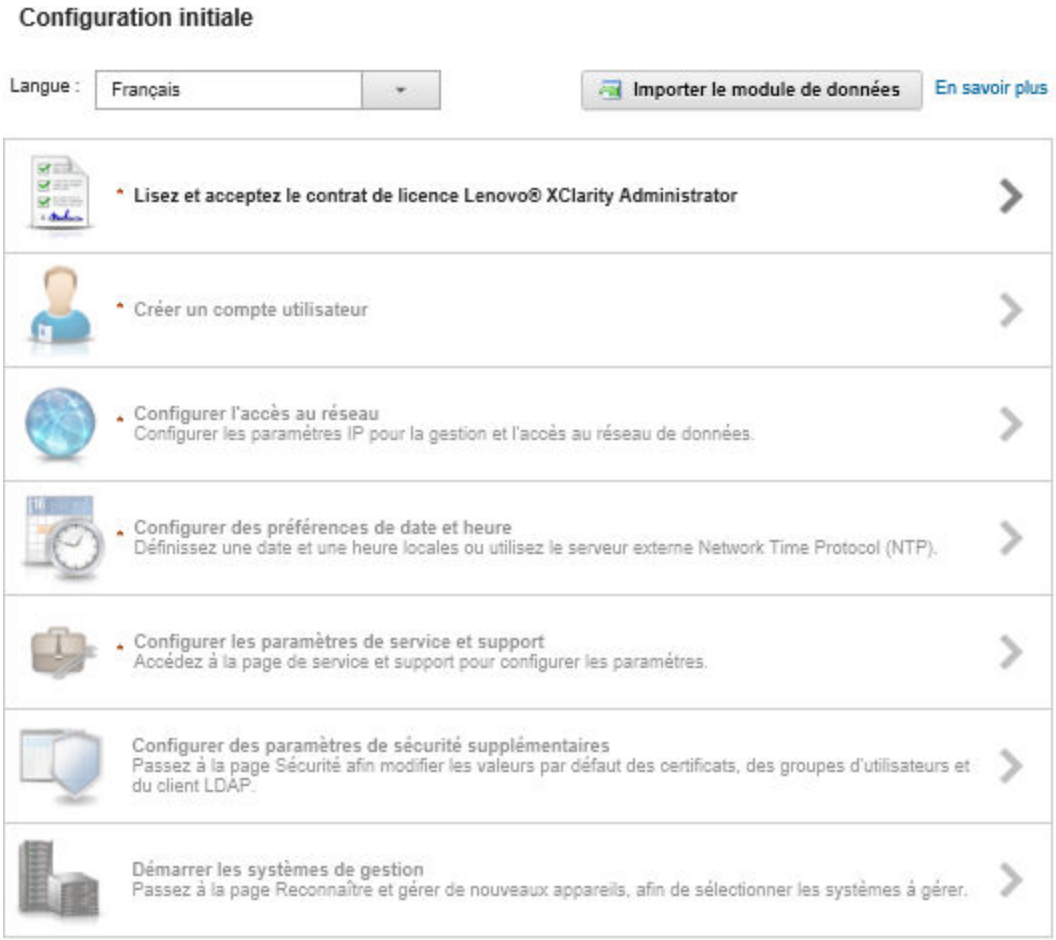
Geben Sie beispielsweise auf Grundlage der Beispiele für Eth0 und den Zonenindex die folgende URL in Ihren Webbrowser ein:

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

Schritt 2. Möglicherweise werden Ihnen beim ersten Zugriff auf Lenovo XClarity Administrator Sicherheits- oder Zertifikatwarnungen angezeigt. Diese Warnungen können Sie ignorieren.

Ergebnisse

Die Seite Erstkonfiguration wird angezeigt.



Nach dieser Aufgabe

Führen Sie die Schritte der Erstkonfiguration aus, um XClarity Administrator zu konfigurieren (siehe Lenovo XClarity Administrator konfigurieren).

Benutzeraccounts erstellen

Benutzeraccounts werden verwendet, um die Autorisierung und den Zugriff auf Lenovo XClarity Administrator sowie auf Einheiten mit einer verwalteten Authentifizierung zu verwalten.

Zu dieser Aufgabe

Der erste Benutzeraccount, den Sie erstellen, muss die Rolle Supervisor haben und aktiviert sein.

Als zusätzliche Sicherheitsmaßnahme sollten Sie mindestens zwei Benutzeraccounts mit der Rolle **Supervisor** erstellen. Halten Sie die Kennwörter für diese Benutzeraccounts fest und hinterlegen Sie sie für den Fall einer Wiederherstellung von Lenovo XClarity Administrator an einem sicheren Ort.

Vorgehensweise

Gehen Sie wie folgt vor, um Benutzeraccounts zu erstellen.

Schritt 1. Tragen Sie die folgenden Informationen im Dialogfeld „Neuen Supervisor-Benutzer erstellen“ ein.

- Geben Sie einen Benutzernamen und eine Beschreibung für den Benutzer ein.
- Geben Sie das neue Kennwort ein und bestätigen Sie es. Die Regeln für Kennwörter basieren auf den aktuellen Accountsicherheitseinstellungen.
- Wählen Sie mindestens eine Rollengruppen aus, um den Benutzer für die Ausführung entsprechender Aufgaben zu autorisieren.

  Informationen zu Rollengruppen und zur Erstellung angepasster Rollengruppen finden Sie unter Rollengruppe verwalten in der XClarity Administrator Onlinedokumentation.
- (Optional) Legen Sie die Option **Kennwort beim ersten Zugriff ändern** auf `Yes` fest, wenn Sie den Benutzer bei der ersten Anmeldung an XClarity Administrator zur Kennwortänderung zwingen möchten.

Schritt 2. Klicken Sie auf **Erstellen**.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ) und wiederholen Sie die vorherigen Schritte, um zusätzliche Benutzer zu erstellen.

Schritt 4. Klicken Sie auf **Zu Erstkonfiguration zurückkehren**.

Netzwerkzugriff konfigurieren

Zur Konfiguration des Netzwerkzugriffs können Sie bis zu zwei Netzwerkschnittstellen, den Hostnamen für Lenovo XClarity Administrator und die verwendeten DNS-Server konfigurieren.

Zu dieser Aufgabe

XClarity Administrator verfügt über zwei separate Netzwerkschnittstellen, die je nach implementierter Netzwerktopologie für Ihre Umgebung definiert werden können. Bei virtuellen Einheiten werden diese Netzwerke als „eth0“ und „eth1“ bezeichnet. Sie können benutzerdefinierte Namen für Container festlegen.

- Wenn nur eine Netzwerkschnittstelle (Eth0) vorhanden ist:
  - Die Schnittstelle muss für die Ermittlung und Verwaltung (z. B. Serverkonfiguration und Firmwareaktualisierungen) konfiguriert werden. Sie muss mit CMMs und Flex-Switches in allen verwalteten Gehäusen, den Baseboard Management Controllern in sämtlichen verwalteten Servern und mit allen RackSwitch-Switches kommunizieren können.
  - Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein,

vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.

  - Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
  - Wenn Sie Betriebssystem-Images implementieren und BS-Einheitentreiber aktualisieren möchten, muss die Schnittstelle eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle haben, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

    Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.

- Wenn zwei Netzwerkschnittstellen (Eth0 und Eth1) vorhanden sind:
  - Die erste Netzwerkschnittstelle (in der Regel die Eth0-Schnittstelle) muss mit dem Verwaltungsnetzwerk verbunden und für die Unterstützung der Einheitenermittlung und -verwaltung (einschließlich Serverkonfiguration und Firmwareaktualisierungen) konfiguriert sein. Sie muss mit CMMs und Flex-Switches in sämtlichen verwalteten Gehäusen, den Management-Controllern in allen verwalteten Servern und mit sämtlichen RackSwitch-Switches kommunizieren können.
  - Die zweite Netzwerkschnittstelle (in der Regel die Eth1-Schnittstelle) kann so konfiguriert werden, dass eine Kommunikationsverbindung mit einem internen Datennetzwerk, einem öffentlichen Datennetzwerk oder mit beiden möglich ist.
  - Wenn Sie beabsichtigen, Firmwareaktualisierungen und BS-Einheitentreiber über XClarity Administrator abzurufen, muss mindestens eine Netzwerkschnittstelle mit dem Internet verbunden sein, vorzugsweise durch eine Firewall. Andernfalls müssen Sie diese Aktualisierungen in das Repository importieren.
  - Wenn Sie beabsichtigen, Servicedaten zu sammeln oder die automatische Problembenachrichtigung (einschließlich der Call-Home-Funktion und Lenovo Upload-Funktionalität) zu verwenden, muss mindestens eine der Netzwerkschnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
  - Wenn Sie beabsichtigen, Betriebssystem-Images zu implementieren und Einheitentreiber zu aktualisieren, können Sie entweder die Eth1- oder die Eth0-Schnittstelle verwenden. Die Schnittstelle, die Sie verwenden, muss jedoch über eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle verfügen, die für den Zugriff auf das Hostbetriebssystem verwendet wird.

    Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.

In der folgenden Tabelle werden Konfigurationsmöglichkeiten für die XClarity Administrator-Netzwerkschnittstellen auf Basis des Typs der in Ihrer Umgebung implementierten Netzwerktopologie beschrieben. Verwenden Sie diese Tabelle, um zu bestimmen, wie Sie jede Netzwerkschnittstelle definieren.

Tabelle 3. Rolle jeder Netzwerkschnittstelle auf Basis der Netzwerktopologie

Netzwerktopologie	**Rolle von Schnittstelle1 (eth0)**	**Rolle von Schnittstelle2 (eth1)**
Konvergentes Netzwerk (Verwaltungs- und Datennetzwerk mit Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen)	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten • BS-Implementierung • BS-Einheitentreiberaktualisierungen	Keine Angabe
Separates Verwaltungsnetzwerk mit Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen sowie Datennetzwerk	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten • BS-Implementierung • BS-Einheitentreiberaktualisierungen	Datennetzwerk • Keine Angabe
Separates Verwaltungsnetzwerk und Datennetzwerk mit Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten	Datennetzwerk • BS-Implementierung • BS-Einheitentreiberaktualisierungen

Tabelle 3. Rolle jeder Netzwerkschnittstelle auf Basis der Netzwerktopologie (Forts.)

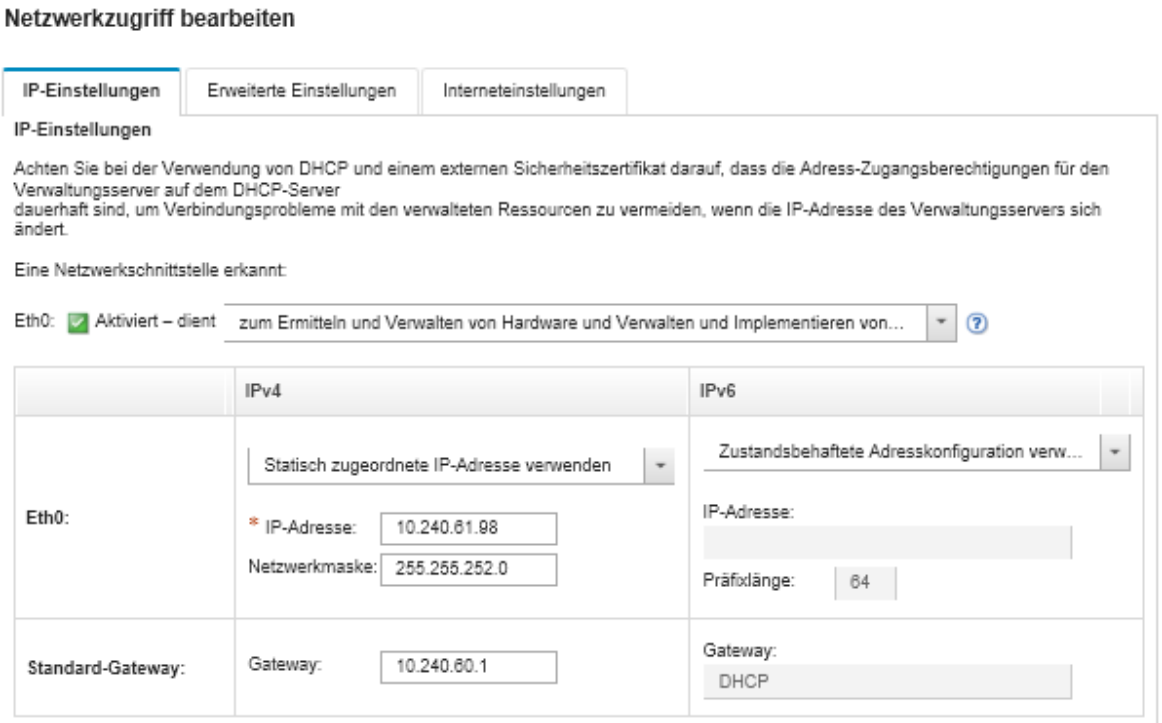
Netzwerktopologie	Rolle von Schnittstelle1 (eth0)	Rolle von Schnittstelle2 (eth1)
Separates Verwaltungsnetzwerk und Datennetzwerk ohne Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten	Datennetzwerk • Keine Angabe
Nur-Verwaltungsnetzwerk (ohne Unterstützung für BS-Implementierung und BS-Einheitentreiber-Aktualisierungen)	Verwaltungsnetzwerk • Ermittlung und Verwaltung • Serverkonfiguration • Firmwareaktualisierungen • Servicedatenerfassung • Automatische Problembenachrichtigung (z. B. Call-Home- und Lenovo Upload-Funktionalität) • Abruf von Garantiedaten	Keine Angabe

Weitere Informationen über XClarity Administrator-Netzwerkschnittstellen finden Sie unter Hinweise zum Netzwerkbetrieb.

Vorgehensweise

Gehen Sie wie folgt vor, um den Netzwerkzugriff zu konfigurieren.

Schritt 1. Klicken Sie auf der Seite Erstkonfiguration auf **Netzwerkzugriff konfigurieren**. Die Seite Netzwerkzugriff bearbeiten wird angezeigt.



Schritt 2. Wenn Sie Betriebssysteme über XClarity Administrator bereitstellen und auch BS-Einheitentreiber aktualisieren möchten, geben Sie die für die Betriebssystemverwaltung zu verwendende Netzwerkschnittstelle an.

- Falls nur eine Schnittstelle für XClarity Administrator definiert ist, legen Sie fest, ob diese Schnittstelle ausschließlich zur Ermittlung und Verwaltung von Hardware oder auch zur Verwaltung von Betriebssystemen verwendet werden soll.
- Sofern zwei Schnittstellen für XClarity Administrator definiert sind (Eth0 und Eth1), legen Sie fest, mit welcher Schnittstelle die Betriebssysteme verwaltet werden sollen. Sollten Sie die Option „Keine“ auswählen, können Sie für verwaltete Server *keine* Betriebssystem-Images mit XClarity Administrator implementieren oder BS-Einheitentreiber aktualisieren.

Schritt 3. Geben Sie die IP-Einstellungen an.

a. Geben Sie für die erste Schnittstelle die IPv4-Adresse, die IPv6-Adresse oder beide an.

- **IPv4**. Sie müssen der Schnittstelle eine IPv4-Adresse zuordnen. Sie können eine statische IP-Adresse zuordnen oder eine IP-Adresse von einem DHCP-Server abrufen.
- **IPv6**. Optional können Sie der Schnittstelle mithilfe einer der folgenden Zuordnungsmethoden eine IPv6-Adresse zuordnen:
  - Statisch zugeordnete IP-Adresse verwenden
  - Zustandsbehaftete Adresskonfiguration verwenden (DHCPv6)
  - Automatische zustandslose Adresskonfiguration verwenden

  Anmerkung: Weitere Informationen über IPv6-Adresseinschränkungen finden Sie unter IP-Konfigurationseinschränkungen.

b. Wenn eine zweite Schnittstelle vorhanden ist, geben Sie die IPv4-Adresse, die IPv6-Adresse oder beide an.

Anmerkung: Die dieser Schnittstelle zugeordnete IP-Adresse und die der ersten Schnittstelle zugeordnete IP-Adresse dürfen nicht im gleichen Subnetz sein. Falls die IP-Adressen für beide Schnittstellen (Eth0 und Eth1) über DHCP zugeordnet werden, darf der DHCP-Server den IP-Adressen der beiden Schnittstellen nicht dasselbe Subnetz zuordnen.

- **IPv4**. Sie können eine statische IP-Adresse zuordnen oder eine IP-Adresse von einem DHCP-Server abrufen.
- **IPv6**. Optional können Sie der Schnittstelle mithilfe einer der folgenden Zuordnungsmethoden eine IPv6-Adresse zuordnen:
  - Statisch zugeordnete IP-Adresse verwenden
  - Zustandsbehaftete Adresskonfiguration verwenden (DHCPv6)
  - Automatische zustandslose Adresskonfiguration verwenden

c. Geben Sie das Standard-Gateway an.

Sofern Sie ein Standard-Gateway angeben, muss es eine gültige IP-Adresse aufweisen und dieselbe Netzwerkmaske (dasselbe Subnetz) wie die IP-Adresse für eine der beiden Netzwerkschnittstellen (Eth0 oder Eth1) verwenden. Wenn Sie nur eine Schnittstelle verwenden, muss das Standard-Gateway im gleichen Subnetz wie das der Netzwerkschnittstelle sein.

Wenn eine der beiden Schnittstellen eine IP-Adresse über DHCP abruft, verwendet das Standard-Gateway ebenfalls DHCP. Um manuell eine Standard-Gateway-Adresse einzugeben, die die vom DHCP-Server empfangene Adresse überschreibt, aktivieren Sie das Kontrollkästchen **Gateway überschreiben**.

Tipps:

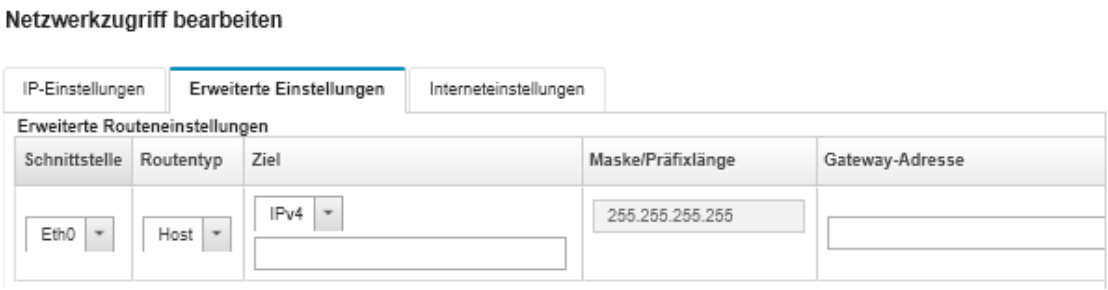
- Stellen Sie sicher, dass das Gateway mit einem Subnetz der Netzwerkschnittstellen übereinstimmt. Das Standard-Gateway wird automatisch über diese Netzwerkschnittstelle festgelegt.
- Wenn Sie zu einem von DHCP bereitgestellten Gateway zurückkehren möchten, deaktivieren Sie das Kontrollkästchen **Gateway überschreiben**.

Vorsicht:
Wenn Sie das Gateway überschreiben wollen, müssen Sie die richtige Gateway-Adresse eingeben. Andernfalls ist dieser Verwaltungsserver nicht erreichbar und es gäbe keine Möglichkeit, sich für eine Korrektur remote anzumelden.

d. Klicken Sie auf **IP-Einstellungen speichern**.

Schritt 4. **Optional:** Konfigurieren Sie erweiterte Einstellungen.

a. Klicken Sie auf die Registerkarte **Erweitertes Routing**.



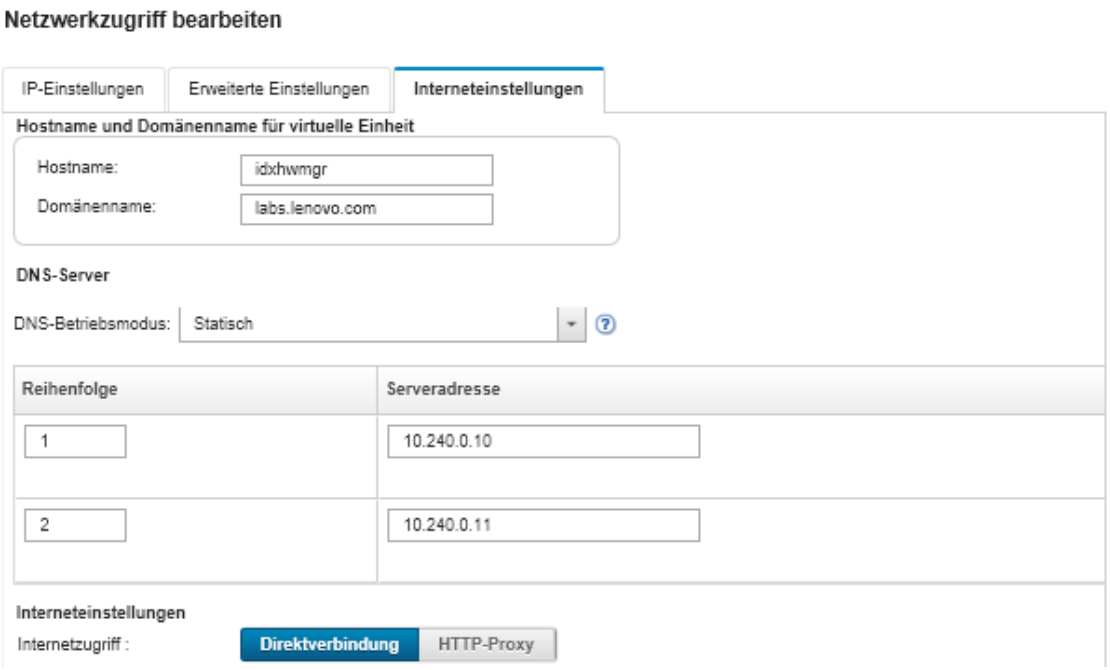
b. Geben Sie in der Tabelle **Erweiterte Routeneinstellungen** mindestens eine Route an, die von dieser Schnittstelle verwendet werden soll.

Gehen Sie wie folgt vor, um eine oder mehrere Routen zu definieren.
1. Wählen Sie die Schnittstelle aus.
2. Geben Sie den Routentyp an (Route zu einem anderen Host oder zu einem Netzwerk).
3. Geben Sie den Zielhost oder die Netzwerkadresse für die Route an.
4. Geben Sie die Subnetzmaske der Zieladresse an.
5. Geben Sie die Gateway-Adresse für die zu sendenden Pakete an.

c. Klicken Sie auf **Erweitertes Routing speichern**.

Schritt 5. Ändern Sie bei Bedarf die DNS- und Proxy-Einstellungen.

a. Klicken Sie auf die Registerkarte **DNS und Proxy**.



b. Geben Sie den Hostnamen und den Domänennamen für XClarity Administrator an.

c. Wählen Sie den DNS-Betriebsmodus aus. Die Einstellung kann **Statisch** oder **DHCP** sein.

   Achtung: Wenn Sie den DNS-Betriebsmodus ändern, müssen Sie den Verwaltungsserver neu starten.

   Anmerkung: Falls die IP-Adresse über DHCP abgerufen werden soll, werden alle Änderungen, die Sie an den Feldern für den **DNS-Server** vorgenommen haben, bei der nächsten Erneuerung der DHCP-Zugangsberechtigung von XClarity Administrator überschrieben.

d. Geben Sie die IP-Adresse eines oder mehrerer zu verwendender DNS-Server (Domain Name System) sowie dessen Prioritätsreihenfolge an.

e. Geben Sie an, ob der Internetzugriff über eine Direktverbindung oder einen HTTP-Proxy erfolgen soll (sofern XClarity Administrator über Internetzugriff verfügt).

   Anmerkungen: Stellen Sie beim HTTP-Proxy sicher, dass die folgenden Anforderungen erfüllt sind.
   - 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).

   Wenn Sie einen HTTP-Proxy verwenden, geben Sie Daten in den folgenden Feldern an:
   1. Geben Sie den Hostnamen und den Port für den Proxy-Server an.
   2. Legen Sie fest, ob eine Authentifizierung verwendet werden soll. Geben Sie ggf. den Benutzernamen und das Kennwort an.
   3. Geben Sie eine Test-URL für den Proxy an.
   4. Klicken Sie auf **Proxy-Test** und prüfen Sie, ob die Proxy-Einstellungen konfiguriert sind und ordnungsgemäß funktionieren.

f. Klicken Sie auf **DNS und Proxy speichern**.

g. Leiten Sie den vollständig qualifizierten Domänennamen (FQDN) und DNS-Informationen des XClarity Administrator-Verwaltungsservers an verwaltete Server mit IMM2, XCC und XCC2 weiter, damit die verwalteten Server den Verwaltungsserver mithilfe dieser Informationen finden können.

   1. Klicken Sie auf **FQDN/DNS an BMC weiterleiten**.
   2. Wählen Sie aus, wie vorhandene DNS-Einträge im Baseboard Management Controller behandelt werden sollen.
      - Vorhandene DNS-Einträge beibehalten und die DNS-Einträge des Verwaltungsservers im nächsten verfügbaren Steckplatz anhängen.
      - Alle vorhandenen DNS-Einträge durch die DNS-Einträge des Verwaltungsservers ersetzen.
   3. Geben Sie im Bearbeitungsfeld **JA** ein.
   4. Klicken Sie auf **Übernehmen**.

   Für diesen Vorgang muss ein Job erstellt werden. Sie können den Fortschritt des Jobs in der Übersicht **Überwachung → Jobs** verfolgen. Wenn der Job nicht erfolgreich abgeschlossen wurde, klicken Sie auf den Job-Link, um Details zum Job anzuzeigen (siehe Mit Jobs arbeiten in der XClarity Administrator Onlinedokumentation).

   Sie können die FQDN- und DNS-Informationen des Verwaltungsservers auch von verwalteten Servern mit IMM2, XCC und XCC2 entfernen, indem Sie auf **FQDN/DNS von BMC entfernen** klicken. Sie können auswählen, ob Sie andere vorhandene DNS-Einträge beibehalten, alle DNS-Einträge entfernen oder nur Einträge entfernen, die mit den Verwaltungsserverinformationen übereinstimmen.

Schritt 6. Klicken Sie auf **Zurück**.

Schritt 7. Klicken Sie auf **Verbindung testen**, um die Netzwerkeinstellungen zu überprüfen.

Datum und Uhrzeit konfigurieren

Sie können das Datum und die Uhrzeit für Lenovo XClarity Administrator manuell einstellen. Besser ist jedoch, die Zeitstempel zwischen XClarity Administrator und allen verwalteten Einheiten über einen NTP-Server (Network Time Protocol) zu synchronisieren.

Vorbereitende Schritte

Sie müssen mindestens einen (und maximal vier) NTP-Server (Network Time Protocol) verwenden, um die Zeitstempel für alle Ereignisse zu synchronisieren, die mit XClarity Administrator von verwalteten Einheiten empfangen werden.

Tipp: Auf den NTP-Server muss über das Verwaltungsnetzwerk (in der Regel über die Eth0-Schnittstelle) zugegriffen werden können. Ziehen Sie in Betracht, den NTP-Server auf dem Host einzurichten, auf dem auch XClarity Administrator ausgeführt wird.

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

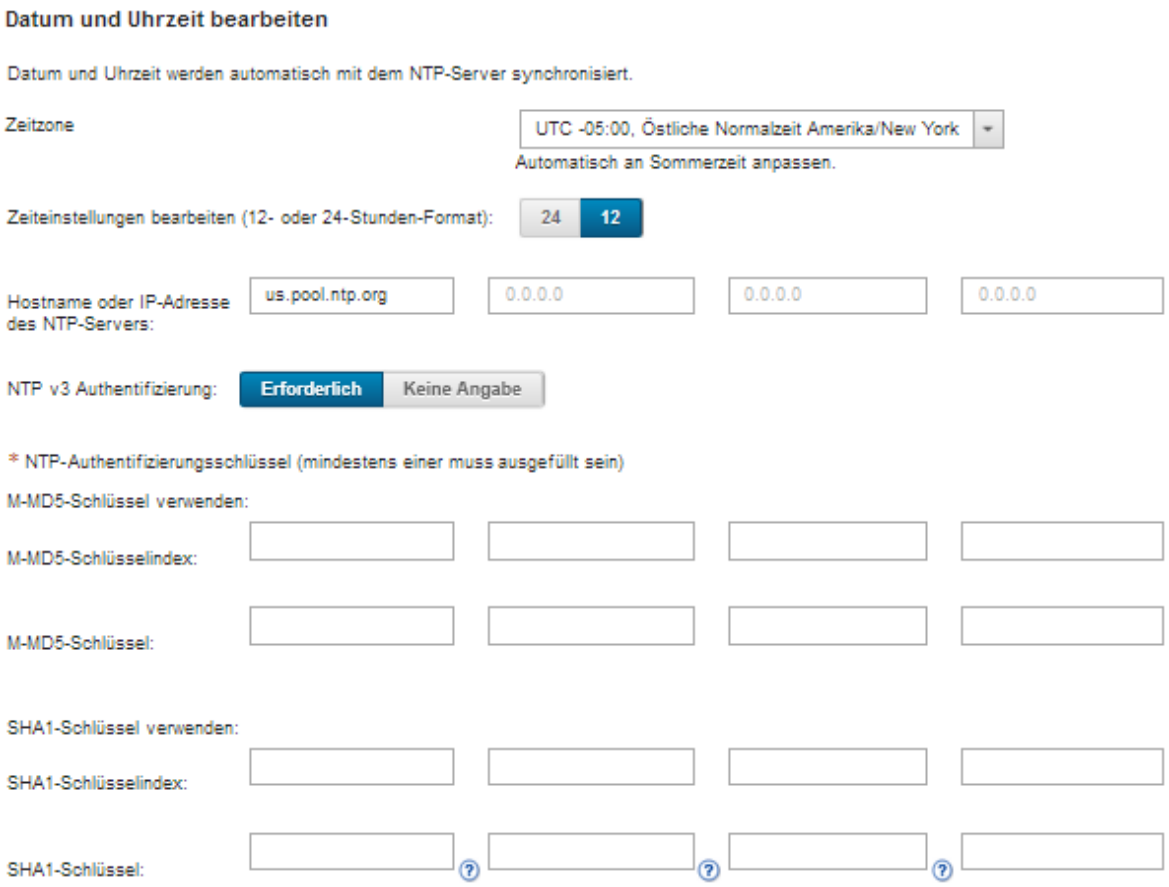
Achtung: Die virtuelle XClarity Administrator-Einheit und ihr Host müssen mit derselben Zeitquelle synchronisiert werden, um eine unbeabsichtigte fehlerhafte Zeitsynchronisation zwischen XClarity Administrator und dem Host zu verhindern. In der Regel ist der Host so konfiguriert, dass eine Zeitsynchronisation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

- Befolgen Sie für ESXi die Anweisungen auf der VMware – Website zur Deaktivierung der Zeitsynchronisation.
- Klicken Sie bei Hyper-V im Hyper-V-Manager mit der rechten Maustaste auf die virtuelle XClarity Administrator-Maschine und klicken Sie anschließend auf **Einstellungen**. Klicken Sie im Dialogfeld im Navigationsbereich auf **Verwaltung > Integration Services** und deaktivieren Sie dann **Zeitsynchronisation**.

Vorgehensweise

Gehen Sie wie folgt vor, um einen NTP-Server für XClarity Administrator einzurichten.

Schritt 1. Klicken Sie auf der Seite „Erstkonfiguration“ auf **Einstellungen für Datum und Uhrzeit konfigurieren**. Die Seite Datum und Uhrzeit bearbeiten wird angezeigt.



Schritt 2. Geben Sie Daten in das Dialogfenster „Datum und Uhrzeit“ ein.

1. Wählen Sie die Zeitzone für den Host von XClarity Administrator aus.

   Sofern in der ausgewählten Zeitzone die Sommerzeit gilt, wird die Uhrzeit automatisch angepasst.
2. Wählen Sie das 12- und 24-Stunden-Format aus.
3. Geben Sie den Hostnamen oder die IP-Adresse für jeden NTP-Server im Netzwerk an. Sie können bis zu vier NTP-Server definieren.
4. Wählen Sie **Erforderlich** aus, um die NTP v3 Authentifizierung zu aktivieren, oder wählen Sie **Keine** aus, um die NTP v1 Authentifizierung zwischen XClarity Administrator und den NTP-Servern im Netzwerk zu verwenden.

   Sie können die v3-Authentifizierung verwenden, wenn verwaltete Flex System-CMMs und -BMCs (Baseboard Management Controller) über Firmware verfügen, die eine v3-

Authentifizierung erfordert, und wenn zwischen XClarity Administrator und einem oder mehreren NTP-Servern eine NTP v3 Authentifizierung erforderlich ist.

5. Wenn Sie die NTP v3 Authentifizierung aktiviert haben, müssen Sie den Authentifizierungsschlüssel und den Index für alle entsprechenden NTP-Server festlegen. Sie können einen M-MD5-Schlüssel, einen SHA1-Schlüssel oder beides angeben. Wenn sowohl M-MD5- als auch SHA1-Schlüssel angegeben wurden, überträgt XClarity Administrator entweder den M-MD5- oder den SHA1-Schlüssel an die verwalteten Flex System-CMMs und -Management Controller, die sie unterstützen. XClarity Administrator verwendet den Schlüssel für die Authentifizierung am NTP-Server.
   - Geben Sie für den M-MD5-Schlüssel eine ASCII-Zeichenfolge an, die nur Buchstaben in Groß- und Kleinschreibung (a–Z, A–Z), Ziffern (0–9) und die Sonderzeichen @# enthält.
   - Für den SHA1-Schlüssel geben Sie eine ASCII-Zeichenfolge mit 40 Zeichen (nur 0–9 und a–f) an.
   - Der angegebene Schlüsselindex und der Authentifizierungsschlüssel müssen mit den Werten für Schlüssel-ID und Kennwort auf dem NTP-Server übereinstimmen. Wenn z. B. der Schlüsselindex des eingegebenen SHA1-Schlüssels auf dem NTP-Server 5 lautet, ist der Schlüsselindex des SHA1-Schlüssels von XClarity Administrator ebenfalls 5. Weitere Informationen zum Festlegen der Schlüssel-ID und des Kennwort finden Sie in der Dokumentation zum NTP-Server.
   - Sie müssen den Schlüssel für jeden NTP-Server, der die v3-Authentifizierung verwendet, angeben, auch wenn zwei oder mehr NTP-Server denselben Schlüssel nutzen.
   - Falls Sie die v3-Authentifizierung aktivieren, aber keinen Authentifizierungsschlüssel und keinen Index für den NTP-Server bereitstellen, wird standardmäßig die v1-Authentifizierung verwendet.
   - Sofern Sie mehrere NTP-Server angeben, müssen die NTP-Server entweder alle die v3-Authentifizierung oder alle die v1-Authentifizierung nutzen. Eine Kombination aus v3- und v1-Authentifizierung für NTP-Server wird nicht unterstützt.
   - Wenn Sie mehrere NTP-Server mit v3-Authentifizierung angeben und die Schlüssel nicht identisch sind, müssen die Schlüsselindizes eindeutig sein. Beispielsweise dürfen NTP-Server 1 und 2 nicht den SHA1-Schlüsselindex 1 haben, wenn die SHA1-Schlüssel der NTP-Server 1 und 2 unterschiedlich sind. Sie müssen einen der beiden NTP-Server so umkonfigurieren, dass ein Schlüssel mit einem anderen Schlüsselindex als der andere NTP-Server akzeptiert wird. Andernfalls wird der letzte definierte und einem Schlüsselindex zugeordnete Schlüssel für alle NTP-Server mit dem gleichen Schlüsselindex konfiguriert.

Schritt 3. Klicken Sie auf **Speichern**.

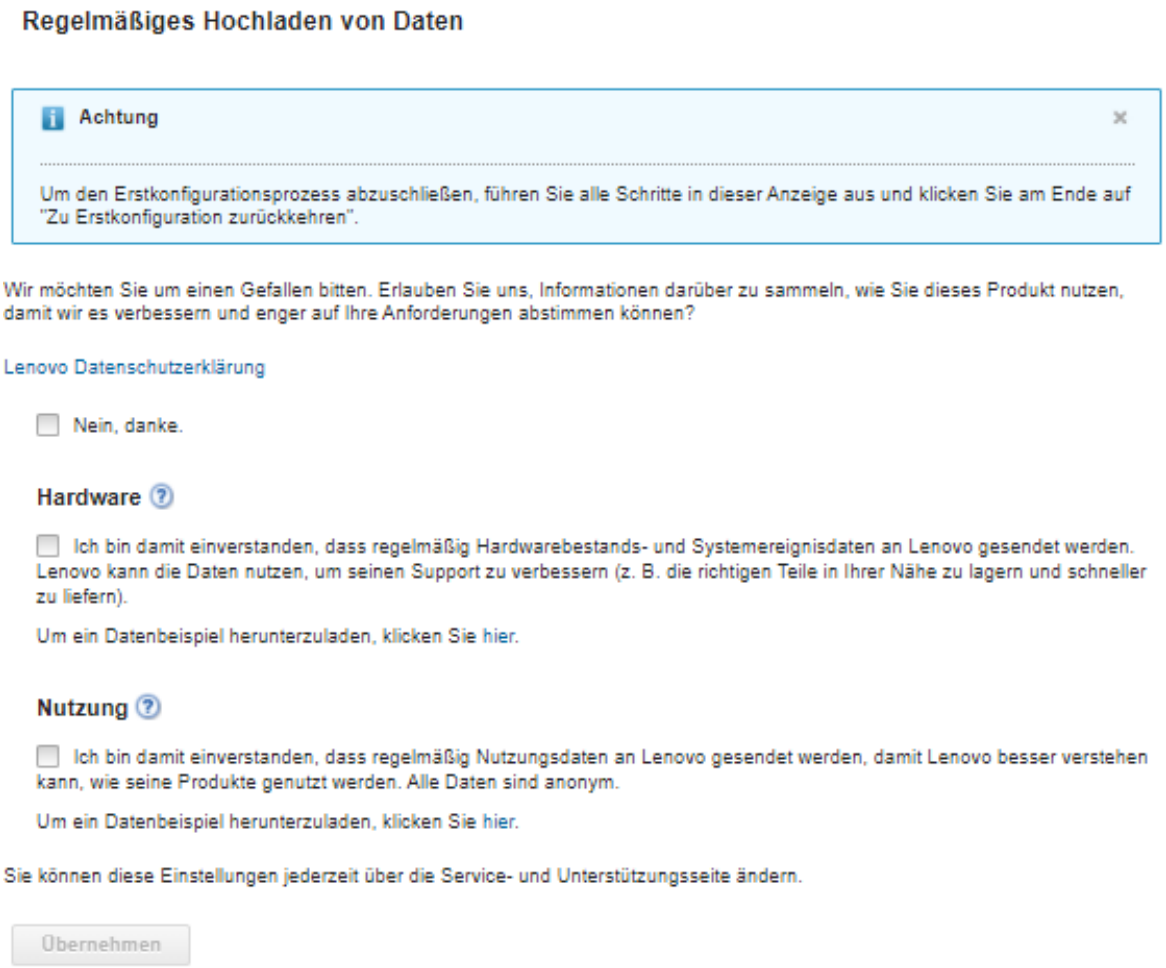
Service und Support konfigurieren

Sie können Service- und Unterstützungseinstellungen konfigurieren, einschließlich Nutzungsdaten, Lenovo Support (Call-Home-Funktion), Lenovo Upload-Funktionalität und Produktgarantie.

Vorgehensweise

Gehen Sie zum Konfigurieren der Sicherheit wie folgt vor.

Schritt 1. Klicken Sie auf der Seite „Erstkonfiguration“ auf **Service- und Supporteinstellungen konfigurieren**. Die Seite Service und Support wird angezeigt.



Schritt 2. Lesen und akzeptieren Sie die Lenovo Datenschutzerklärung.

Anmerkung: Sie können keine Daten an Lenovo sammeln und an Lenovo senden, ohne zuerst die Lenovo Datenschutzerklärung zu akzeptieren. Wenn Sie die Datenschutzrichtlinie ablehnen, können Sie die Datenschutzrichtlinie zu einem späteren Zeitpunkt über die Seite **Service und Support → Call-Home-Konfiguration** überprüfen und akzeptieren.

Schritt 3. Optional können Sie Lenovo XClarity Administrator erlauben, Nutzungs- und Hardwareinformationen zu erfassen. Klicken Sie anschließend auf **Übernehmen**.

Sie können die folgenden Datentypen sammeln und an Lenovo senden.

- **Nutzungsdaten**

  Wenn Sie zustimmen, Nutzungsdaten an Lenovo zu senden, werden die folgenden Daten gesammelt und wöchentlich gesendet. Diese Daten sind *anonym*. Es werden keine privaten Daten (einschließlich Seriennummern, UUIDs, Hostnamen, IP-Adressen und Benutzernamen) gesammelt oder an Lenovo gesendet.
  - Protokoll der ausgeführten Aktionen
  - Liste der ausgelösten Ereignisse und des Zeitstempels, zu dem Sie ausgelöst wurden
  - Liste der ausgelösten Prüfeignisse und des Zeitstempels, zu dem Sie ausgelöst wurden
  - Liste der ausgeführten Jobs sowie Informationen über Erfolg oder Misserfolg für die einzelnen Jobs
  - XClarity Administrator-Metriken, einschließlich Speicherauslastung, Prozessorauslastung und Plattenspeicherplatz
  - Beschränkte Bestandsdaten über alle verwalteten Einheiten

- **Hardwaredaten**

  Wenn Sie zustimmen, Hardwaredaten an Lenovo zu senden, werden die folgenden Daten gesammelt und regelmäßig gesendet. Diese Daten sind *nicht anonym*. Zu den Hardwaredaten gehören Attribute, z. B. UUIDs und Seriennummern. IP-Adressen oder Hostnamen fallen nicht darunter.

  - **Tägliche Hardwaredaten**. Jede Bestandsänderung umfasst die folgenden Daten.
    - Ereignis zur Bestandsänderung (FQXHMDM0001I)
    - Änderungen der Bestandsdaten für die Einheit, die diesem Ereignis zugeordnet ist
  - **Wöchentliche Hardwaredaten**. Bestandsdaten sind für alle verwalteten Einheiten inbegriffen.

Wenn Nutzungs- und Hardwaredaten an Lenovo gesendet werden, wird ein Ereignis im Prüfprotokoll aufgezeichnet.

Sie können diese Einstellung jederzeit ändern und das letzte Archiv, das gesammelt und an Lenovo gesendet wurde, herunterladen, indem Sie auf Links **Verwaltung → Service und Support** sowie **Regelmäßiges Hochladen von Daten** klicken.

Schritt 4. Klicken Sie optional auf **Call-Home-Konfiguration**, um die automatische Problembenachrichtigung für den Lenovo Support (Call- Home-Funktion) einzurichten. Klicken Sie dann auf **Übernehmen & Aktivieren**, um den Service-Weiterleiter für die Standard-Call-Home-Funktion zu erstellen, oder klicken Sie auf **Nur übernehmen**, um die Kontaktinformationen zu speichern.

Weitere Informationen zum Einrichten der automatischen Problembenachrichtigung für den Lenovo Support erhalten Sie unter Call-Home-Funktion einrichten in der XClarity Administrator Onlinedokumentation.

Schritt 5. Klicken Sie optional auf **Lenovo Upload-Funktionalität**, um die automatische Problembenachrichtigung für die Lenovo Upload-Funktionalität einzurichten. Klicken Sie dann auf **Übernehmen & Aktivieren**, um den Service-Weiterleiter für die Lenovo Upload-Funktionalität zu erstellen, oder klicken Sie auf **Nur übernehmen**, um die Einstellungsinformationen zu speichern.

Weitere Informationen zum Einrichten der automatischen Problembenachrichtigung für die Lenovo Upload-Funktionalität erhalten Sie unter Automatische Problembenachrichtigung an die Lenovo Upload-Funktionalität in der XClarity Administrator Onlinedokumentation.

Schritt 6. Klicken Sie optional auf **Garantie**, um externe Verbindungen zu aktivieren, die zum Erfassen von Garantieinformationen für Ihre verwalteten Einheiten benötigt werden.

Weitere Informationen zum Anzeigen des Garantiestatus (einschließlich verlängerter Garantien) der verwalteten Einheiten erhalten Sie unter Informationen zur Garantie anzeigen in der XClarity Administrator Onlinedokumentation.

Schritt 7. Klicken Sie optional auf **Lenovo Service-Bulletin**, damit Lenovo Ihnen Service-Bulletins an XClarity Administrator senden kann. Klicken Sie anschließend auf **Übernehmen**.

Wenn der Job nicht erfolgreich abgeschlossen wurde, klicken Sie auf den Job-Link, um Details zum Job anzuzeigen (siehe Bulletins von Lenovo erhalten in der XClarity Administrator Onlinedokumentation.

Schritt 8. Geben Sie das Kennwort für die Service-Wiederherstellung an, mit dem Sie Servicedaten und Protokolle sammeln und herunterladen können, wenn XClarity Administrator nicht mehr reagiert und nicht wiederhergestellt werden kann.

Weitere Informationen zum Kennwort zur Service-Wiederherstellung erhalten Sie unter Kennwort zur Service-Wiederherstellung ändern in der Onlinedokumentation von XClarity Administrator.

Schritt 9. Klicken Sie auf **Zu Erstkonfiguration zurückkehren**.

Sicherheitsfunktionen konfigurieren

Sie können die Sicherheitseinstellungen einschließlich Rollengruppen, Authentifizierungsserver, Benutzeraccounts, Verschlüsselung und Zertifikaten konfigurieren.

Vorgehensweise

Gehen Sie zum Konfigurieren der Sicherheit wie folgt vor.

Schritt 1. Klicken Sie auf der Seite „Erstkonfiguration“ auf **Weitere Sicherheitseinstellungen konfigurieren**. Die Seite Sicherheit wird angezeigt.

Schritt 2. Erstellen Sie benutzerdefinierte Rollengruppen, um Berechtigungen und den Ressourcenzugriff zu verwalten (siehe Rollengruppe verwalten in der Onlinedokumentation von XClarity Administrator).

Eine *Rollengruppe* ist eine Sammlung mit einer oder mehreren Rollen. Sie wird verwendet, um die Rollen mehreren Benutzern zuzuweisen. Die von Ihnen für eine Rollengruppe konfigurierten Rollen legen die Zugriffsebene für die Benutzer fest, die Mitglied der Rollengruppe sind. Jeder XClarity Administrator-Benutzer muss in mindestens einer Rollengruppe Mitglied sein.

Schritt 3. Konfigurieren Sie den Authentifizierungsserver (siehe Authentifizierungsserver verwalten in der Onlinedokumentation von XClarity Administrator).

Der *Authentifizierungsserver* ist ein LDAP-Server (Microsoft Active Directory), mit dem die Benutzeranmeldeinformationen authentifiziert werden. XClarity Administrator verwendet einen einzigen Authentifizierungsserver für die zentrale Benutzerverwaltung aller verwalteten Einheiten (außer Flex-Switches). Wenn eine Einheit von XClarity Administrator verwaltet wird, konfiguriert XClarity Administrator die verwaltete Einheit und die installierten Komponenten (außer Flex-Switches) zur Verwendung dieses Authentifizierungsservers. Auf dem Authentifizierungsserver definierte Benutzeraccounts werden zur Anmeldung bei XClarity Administrator, CMMs und dem Baseboard Management Controller verwendet.

Sie können festlegen, dass ein externer Authentifizierungsserver anstelle des lokalen Authentifizierungsservers auf dem Verwaltungsknoten verwendet wird.

Schritt 4. Sie konfigurieren Sicherheitseinstellungen für Benutzeraccounts, mit denen die Komplexität von Kennwörtern, Accountsperren und Timeouts für inaktive Websitzungen gesteuert werden (siehe Die Sicherheitseinstellungen eines Benutzeraccounts ändern in der XClarity Administrator Onlinedokumentation).

Schritt 5. Sie konfigurieren die Verschlüsselungseinstellungen, mit denen Kommunikationsmodi und -protokolle für die sichere Kommunikation zwischen XClarity Administrator und verwalteten Einheiten festgelegt werden (siehe Verschlüsselungsmodus und Kommunikationsprotokolle festlegen in der Onlinedokumentation von XClarity Administrator).

Schritt 6. Falls Sie planen, Rack-Server mit einer lokalen Authentifizierung anstatt mit einer verwalteten XClarity Administrator Authentifizierung zu verwalten, erstellen Sie eine oder mehrere gespeicherte Anmeldeinformationen, die den aktiven Benutzeraccounts auf der Einheit oder im Active Directory entsprechen, die zur Anmeldung bei den Einheiten während des Verwaltungsprozesses verwendet werden können. Weitere Informationen zu gespeicherten Anmeldeinformationen finden Sie im Abschnitt Gespeicherte Anmeldeinformationen verwalten in der XClarity Administrator Onlinedokumentation.

Schritt 7. Wenn Sie ein eigenes Serverzertifikat mit eigenen Informationen oder ein extern signiertes Serverzertifikat verwenden möchten, müssen Sie das neue Zertifikat generieren und bereitstellen, bevor Sie mit der Verwaltung der Systeme beginnen. Weitere Informationen zum Generieren eines

eigenen Sicherheitszertifikats finden Sie unter Mit Sicherheitszertifikaten arbeiten in der Onlinedokumentation von XClarity Administrator.

Schritt 8. Klicken Sie im vertikalen Menü auf der Seite „Sicherheit“ auf **Zu Erstkonfiguration zurückkehren**.

Einheiten verwalten

Lenovo XClarity Administrator kann verschiedene Arten von Systemen verwalten, darunter Flex System-Gehäuse, Rack- und Tower-Server, RackSwitch-Switches und Speichereinheiten. Sie können eine Vielzahl von Einheiten, die sich in Ihrer Umgebung befinden, auf einfache Weise ermitteln und verwalten, indem Sie Informationen zu den Einheiten über eine Massenimportdatei importieren.

Vorbereitende Schritte

Wichtig:

- Sie können maximal 300 Einheiten gleichzeitig verwalten. Sie sollten maximal 300 Einheiten zu einer Massenimportdatei hinzufügen.
- Nachdem Sie einen Vorgang zur Einheitenverwaltung gestartet haben, sollten Sie warten, bis der gesamte Verwaltungsjob abgeschlossen ist, bevor Sie einen anderen Vorgang zur Einheitenverwaltung starten.

Gehäusekomponenten (z. B. CMMs, Rechenknoten, Switches und Speichereinheiten) werden automatisch ermittelt und verwaltet, wenn Sie das sie enthaltende Gehäuse verwalten. Sie können Gehäusekomponenten nicht getrennt vom Gehäuse ermitteln und verwalten.

Für die Kommunikation mit den CMMs im Gehäuse und den Baseboard Management Controllern in den Servern werden bestimmte Ports benötigt. Stellen Sie sicher, dass diese Ports verfügbar sind, bevor Sie versuchen, Systeme zu verwalten. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit.

Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jedem System installiert ist, das Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Stellen Sie sicher, dass mindestens drei Sitzungen im TCP-Befehlsmodus vorhanden sind, die für die Out-of-band-Kommunikation mit dem CMM festgelegt wurden. Informationen zum Einstellen der Anzahl von Sitzungen finden Sie unter Befehl „tcpcmdmode“ in der CMM-Onlinedokumentation.

Erwägen Sie die Implementierung von IPv4- *oder* IPv6-Adressen für alle CMMs und Flex-Switches, die von XClarity Administrator verwaltet werden. Wenn Sie IPv4 für einige CMMs und Flex-Switches und IPv6 für andere implementieren, werden einige Ereignisse möglicherweise nicht im Prüfprotokoll (oder als Audit-Traps) erfasst.

Stellen Sie sicher, dass Sie die Multicast-SLP-Weiterleitung für die Top-of-Rack-Switches sowie für die Router in Ihrer Umgebung aktivieren. Lesen Sie die mit dem jeweiligen Switch oder Router bereitgestellte Dokumentation, um herauszufinden, ob die Multicast-SLP-Weiterleitung aktiviert ist und falls nicht, wie Sie sie aktivieren können.

Wichtig:

- Abhängig von der Firmwareversion des RackSwitch-Switches müssen Sie möglicherweise die Multicast-SLP-Weiterleitung und SSH auf allen entsprechenden Switches manuell mithilfe der unten stehenden Befehle aktivieren, bevor die Switches von XClarity Administrator erkannt und verwaltet werden. Weitere Informationen finden Sie unter Online-Dokumentation zu Rack-Switches im System x.
- Auf jeder Speichereinheit muss die Multicast SLP-Weiterleitung aktiviert sein, bevor sie von XClarity Administrator ermittelt werden kann.

- Wenn Sie ein eigenes Serverzertifikat mit eigenen Informationen oder ein extern signiertes Serverzertifikat verwenden möchten, müssen Sie das neue Zertifikat generieren und bereitstellen, bevor Sie mit der Verwaltung der Systeme beginnen. Weitere Informationen zum Generieren eines eigenen Sicherheitszertifikats finden Sie unter Mit Sicherheitszertifikaten arbeiten in der Onlinedokumentation von XClarity Administrator.
- Wenn Sie neben Lenovo XClarity Administrator weitere Verwaltungssoftware verwenden möchten, um Ihr Gehäuse zu überwachen, und wenn diese Verwaltungssoftware SNMPv3-Kommunikation nutzt, müssen Sie zuerst eine lokale CMM-Benutzer-ID erstellen, die mit den geeigneten SNMPv3-Informationen konfiguriert ist, und sich dann am CMM mit dieser Benutzer-ID anmelden und das Kennwort ändern. Weitere Informationen hierzu finden Sie unter Verwaltungshinweise in der XClarity Administrator Onlinedokumentation.
- Mithilfe von Netzwerkprotokollen wie SLP und SSDP kann XClarity Administrator automatisch den Typ der Einheit ermitteln, die verwaltet werden soll, und dann den entsprechenden Mechanismus zur Verwaltung der Einheit verwenden. Einige Einheitentypen unterstützen keine Netzwerkprotokolle und in einigen Umgebungen werden Netzwerkprotokolle gezielt ausgeschaltet. In beiden Fällen müssen Sie den entsprechenden Einheitentyp auswählen, um den Verwaltungsprozess abzuschließen. Die folgenden Einheitentypen müssen explizit identifiziert werden.
  - Switch der Lenovo ThinkSystem DB Serie
  - NVIDIA Mellanox Switch

Zu dieser Aufgabe

XClarity Administrator ermittelt Systeme in Ihrer Umgebung und sucht dazu nach verwaltbaren Einheiten, die im gleichen IP-Subnetz sind wie XClarity Administrator. Dies erfolgt anhand der IP-Adresse oder eines IP-Adressbereichs oder durch den Import der Informationen aus einem Arbeitsblatt.

Standardmäßig werden Einheiten anhand der verwalteten XClarity Administrator Authentifizierung verwaltet, um sich bei den Einheiten anzumelden. Bei der Verwaltung von Rack-Servern und Lenovo Gehäusen können Sie auswählen, ob Sie die lokale Authentifizierung oder die verwaltete Authentifizierung zur Anmeldung bei den Einheiten verwenden möchten.

- Wenn die *lokale Authentifizierung* für Rack-Server, Lenovo Gehäuse und Lenovo Rack-Switches verwendet wird, verwendet XClarity Administrator gespeicherte Anmeldeinformationen zur Authentifizierung der Einheit. Bei den *gespeicherten Anmeldeinformationen* kann es sich um einen aktiven Benutzeraccount auf der Einheit oder um einen Benutzeraccount auf dem Active Directory-Server handeln.

  Sie müssen gespeicherte Anmeldeinformationen in XClarity Administrator erstellen, die mit einem aktiven Benutzeraccount auf der Einheit oder mit einem Benutzeraccount auf einem Active Directory-Server übereinstimmen, bevor Sie die Einheit über die lokale Authentifizierung verwalten können (siehe Gespeicherte Anmeldeinformationen verwalten in der Onlinedokumentation von XClarity Administrator).

  Anmerkungen:

  - RackSwitch-Einheiten unterstützen nur gespeicherte Anmeldeinformationen für die Authentifizierung. Benutzeranmeldeinformationen für XClarity Administrator werden nicht unterstützt.
- Mit der *verwalteten Authentifizierung* können Sie mehrere Einheiten mithilfe von Anmeldeinformationen auf dem XClarity Administrator-Authentifizierungsserver anstatt lokaler Anmeldeinformationen verwalten und überwachen. Wenn die verwaltete Authentifizierung für eine Einheit (außer ThinkServer-Server, System x M4-Servern und Switches) verwendet wird, konfiguriert XClarity Administrator die Einheit und deren installierte Komponenten zur Verwendung eines bestimmten XClarity Administrator-Authentifizierungsservers für eine zentrale Verwaltung.

  - Wenn die verwaltete Authentifizierung aktiviert ist, können Sie Einheiten entweder über manuell eingegebene oder gespeicherte Anmeldeinformationen verwalten (siehe Benutzeraccounts verwalten und in der Onlinedokumentation zu XClarity Administrator).

Die gespeicherten Anmeldeinformationen werden nur verwendet, bis XClarity Administrator die LDAP-Einstellungen auf dem Gerät konfiguriert. Danach haben Änderungen an den gespeicherten Anmeldeinformationen keine Auswirkungen auf die Verwaltung oder Überwachung dieser Einheit.

Anmerkung: Wenn die verwaltete Authentifizierung für ein Gerät aktiviert ist, können Sie mit XClarity Administrator keine gespeicherten Anmeldeinformationen für dieses Gerät bearbeiten.

- Wenn Sie den lokalen oder externen LDAP-Server als XClarity Administrator-Authentifizierungsserver nutzen, werden auf diesem Authentifizierungsserver definierte Benutzeraccounts für die Anmeldung bei XClarity Administrator, CMMs und BMCs (Baseboard Management Controllern) in der XClarity Administrator-Domäne verwendet. Lokale CMM- und Management-Controller-Benutzeraccounts werden deaktiviert.
- Bei Verwendung eines SAML 2.0 Identity Provider als XClarity Administrator-Authentifizierungsserver sind SAML-Accounts für verwaltete Einheiten nicht zugänglich. Wenn Sie jedoch einen SAML Identitiy Provider und einen LDAP-Server zusammen verwenden und der Identity Provider Konten nutzt, die sich auf dem LDAP-Server befinden, können LDAP-Benutzeraccounts zur Anmeldung bei den verwalteten Einheiten und gleichzeitig modernere von SAML 2.0 bereitgestellte Authentifizierungsmethoden (z. B. mehrstufige Authentifizierung und Single Sign-on) zur Anmeldung bei XClarity Administrator verwendet werden.
- Mit Single Sign-On kann sich ein Benutzer, der bereits bei XClarity Administrator angemeldet ist, automatisch beim Baseboard Management Controller anmelden. Single Sign-On ist standardmäßig aktiviert, wenn ein ThinkSystem oder ThinkAgile Server von XClarity Administrator verwaltet wird (es sei denn, der Server wird mit CyberArk-Kennwörtern verwaltet). Sie können global konfigurieren, dass Single Sign-On für alle verwalteten ThinkSystem und ThinkAgile Server aktiviert oder deaktiviert ist. Das Aktivieren von Single Sign-On für einen bestimmten ThinkSystem und ThinkAgile Server überschreibt die globale Einstellung für alle ThinkSystem und ThinkAgile Server (siehe Server verwalten in der XClarity Administrator Onlinedokumentation).

  Anmerkung: Single Sign-On ist automatisch deaktiviert, wenn das CyberArk Identitätsverwaltungssystem zur Authentifizierung verwendet wird.
- Wenn die verwaltete Authentifizierung für ThinkSystem SR635 und SR655 Server aktiviert ist:
  - Die Baseboard Management Controller-Firmware unterstützt bis zu fünf LDAP-Benutzerrollen. XClarity Administrator fügt diese LDAP-Benutzerrollen während der Verwaltung zu den Servern hinzu: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** und **lxc-os-admin**.

    Benutzern muss mindestens eine der angegebenen LDAP-Benutzerrollen zugeordnet werden, damit sie mit den ThinkSystem SR635 und SR655 Servern kommunizieren können.
  - Die Management-Controller-Firmware unterstützt keine LDAP-Benutzer mit demselben Benutzernamen wie der lokale Benutzer des Servers.
- Für ThinkServer- und System x M4-Server wird der XClarity Administrator-Authentifizierungsserver nicht verwendet. Stattdessen wird ein IPMI-Account in der Einheit mit dem Präfix „LXCA_“ erstellt, auf das eine willkürliche Zeichenfolge folgt. (Die vorhandenen lokalen IPMI-Benutzeraccounts werden nicht deaktiviert.) Wenn Sie die Verwaltung eines ThinkServer-Servers beenden, wird der Benutzeraccount „LXCA_“ deaktiviert und das Präfix „LXCA_“ wird durch das Präfix „DISABLED_“ ersetzt. Um festzustellen, ob ein ThinkServer-Server durch eine andere Instanz verwaltet wird, sucht XClarity Administrator nach IPMI-Accounts mit dem Präfix „LXCA_“. Wenn Sie sich dazu entschließen, die Verwaltung eines verwalteten ThinkServer-Servers zu erzwingen, werden alle IPMI-Accounts in der Einheit mit dem Präfix „LXCA_“ deaktiviert und umbenannt. IPMI-Konten, die nicht mehr verwendet werden, sollten Sie manuell löschen.

  Wenn Sie manuell eingegebene Anmeldeinformationen verwenden, werden in XClarity Administrator automatisch gespeicherte Anmeldeinformationen erstellt und zur Verwaltung der Einheit verwendet.

  Anmerkungen: Wenn die verwaltete Authentifizierung für ein Gerät aktiviert ist, können Sie mit XClarity Administrator keine gespeicherten Anmeldeinformationen für dieses Gerät bearbeiten.

- Jedes Mal, wenn Sie ein Gerät mit manuell eingegebenen Anmeldeinformationen verwalten, werden auch dann neue gespeicherte Anmeldeinformationen für dieses Gerät erstellt, wenn bei einem vorherigen Verwaltungsprozess andere gespeicherte Anmeldeinformationen für dieses Gerät erstellt wurden.
- Wenn Sie die Verwaltung eines Geräts aufheben, löscht XClarity Administrator keine gespeicherten Anmeldeinformationen, die während des Verwaltungsprozesses automatisch für dieses Gerät erstellt wurden.

Nachdem die Systeme von XClarity Administrator verwaltet werden, fragt XClarity Administrator alle verwalteten Systeme regelmäßig ab, um Informationen zu sammeln, z. B. Bestand, elementare Produktdaten und Status. Sie können jedes verwaltete System anzeigen und überwachen sowie Verwaltungsaktionen ausführen (z. B. Systemeinstellungen konfigurieren, Betriebssystem-Images bereitstellen, ein- und ausschalten).

Ein System kann jeweils nur von einem XClarity Administrator verwaltet werden. Die Verwaltung durch mehrere Manager wird nicht unterstützt. Wenn ein System von einem XClarity Administrator verwaltet wird und Sie es mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die derzeitige Verwaltung des Systems von XClarity Administrator aufheben. Anschließend können Sie das System mit einem anderen XClarity Administrator verwalten. Weitere Informationen über die Verwaltungsaufhebung für ein System finden Sie unter Beenden der Gehäuseverwaltung, Serververwaltung beenden, RackSwitch-Switchverwaltung aufheben und Verwaltung eines Lenovo Storage Speichersystems aufheben in der Onlinedokumentation von XClarity Administrator.

Anmerkung: XClarity Administrator ändert die Sicherheitseinstellungen oder die Verschlüsselungseinstellungen (Verschlüsselungsmodus und den für sichere Kommunikation verwendeten Modus) im Verwaltungsprozess nicht. Sie können die Verschlüsselungseinstellungen ändern, nachdem das System verwaltet wurde (siehe Verschlüsselungsmodus und Kommunikationsprotokolle festlegen in der Onlinedokumentation von XClarity Administrator).

Anmerkung: In XClarity Administrator kann vorab ein Hardwarebestand (z. B. CMM, Rechenknoten und Switches) für ein Demo-Gehäuse sowie ein Demo-Rack-Server oder -Tower-Server zur Simulation „echter“ Hardware eingerichtet werden. Die Demo-Einheiten werden in den Webschnittstellenseiten belegt und können verwendet werden, um Verwaltungsvorgänge zu veranschaulichen. Die Verwaltungsvorgänge werden jedoch fehlschlagen. Sie können beispielsweise ein Konfigurationsmuster erstellen und das Muster auf einem Demo-Server implementieren, die Implementierung wird aber fehlschlagen. Sie können die Demo-Einheiten entfernen, indem Sie deren Verwaltung aufheben (siehe Beenden der Gehäuseverwaltung und Serververwaltung beenden in der Onlinedokumentation von XClarity Administrator). Nachdem die Demo-Einheiten gelöscht wurden, können nicht sie erneut verwaltet werden.

Vorgehensweise

Um Ihre Systeme in XClarity Administrator mithilfe einer Massenimportdatei zu ermitteln und zu verwalten, führen Sie die folgenden Schritte aus.

Anmerkung: Beim Verwalten von Switches per Massenimport ist HTTPS auf dem Switch aktiviert und NTP-Clients auf dem Switch werden für die Verwendung der NTP-Einstellungen vom Verwaltungsserver konfiguriert. Wenn Sie diese Einstellung ändern möchten, müssen Sie die Switches manuell verwalten.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen **Kapselung für alle zukünftig verwalteten Einheiten aktivieren**, um die Firewallregeln während des Verwaltungsprozesses auf allen Einheiten dahingehend zu ändern, dass eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.

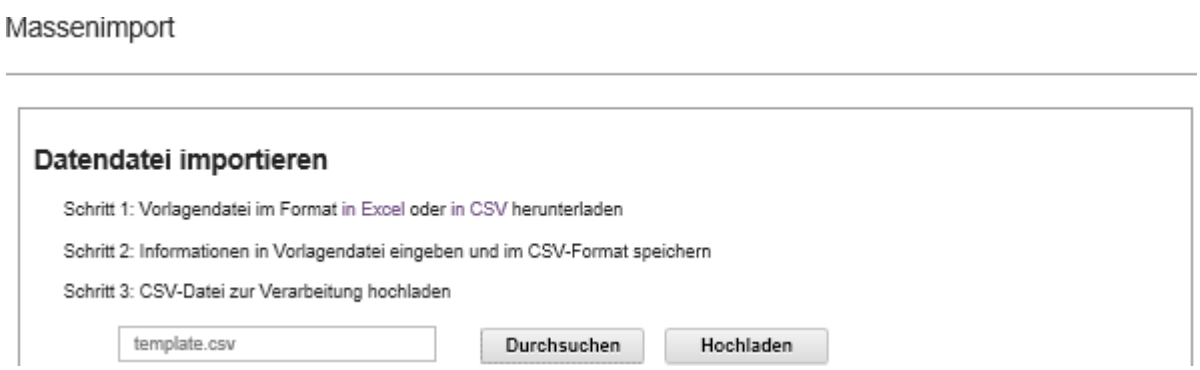
   Anmerkungen:

- Die Kapselung wird für Switches, Speichereinheiten und Gehäuse bzw. Server anderer Hersteller (nicht Lenovo) nicht unterstützt.
- Wenn die Verwaltungsnetzwerkschnittstelle zur Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert ist und die Kapselung aktiviert ist, kann die Verwaltung eines Rack-Servers sehr viel Zeit in Anspruch nehmen.

Die Kapselung kann auf bestimmten Einheiten nach der Verwaltung aktiviert oder deaktiviert werden.

Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Gehäuseverwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen und Rack- oder Tower-Serververwaltung nach einem Verwaltungsserverausfall wiederherstellen in der Onlinedokumentation von XClarity Administrator.

3. Klicken Sie auf **Massenimport**. Der Massenimport-Assistent wird angezeigt.



4. Klicken Sie auf der Seite „Datei importieren“ auf den Link **In Excel** oder **In CSV**, um die Massenimportvorlagendatei im Excel- oder CSV-Format herunterzuladen.

   Wichtig: Die Vorlagendatei kann sich von einem Release zum nächsten ändern. Stellen Sie sicher, dass Sie immer die neueste Vorlage verwenden.

5. Füllen Sie das Datenarbeitsblatt in der Vorlagendatei aus und speichern Sie die Datei im *durch Kommas getrennten* CSV-Format.

   Tipp: Die Excel-Vorlagendatei enthält ein Arbeitsblatt namens **Data** und eines namens **Readme**. Verwenden Sie das Arbeitsblatt **Data**, um die Daten zu Ihrer Einheit einzugeben. Das Arbeitsblatt **Readme** enthält Informationen zum Ausfüllen der Felder im Arbeitsblatt **Data**, z. B. die Pflichtfelder und einige Beispiele.

   Wichtig:

   - Die Einheiten werden in der Reihenfolge verwaltet, die in der Massenimportdatei angegeben ist.
   - XClarity Administrator verwendet Informationen zur Rack-Zuordnung, die bei der Verwaltung der Einheit in deren Konfiguration definiert werden. Wenn Sie in die Rack-Zuordnung in XClarity Administrator ändern, aktualisiert XClarity Administrator die Konfiguration für die Einheit. Wenn Sie die Einheitenkonfiguration aktualisieren, nachdem die Einheit verwaltet wurde, werden die Änderungen in XClarity Administrator angezeigt.
   - Es wird empfohlen (dies ist jedoch nicht erforderlich), ein Rack explizit in der Tabelle zu erstellen, bevor Sie das Rack einer Einheit zuordnen. Wenn ein Rack nicht explizit definiert und noch nicht in XClarity Administrator vorhanden ist, werden die Informationen zur Rack-Zuordnung, die für eine Einheit angegeben sind, verwendet, um das Rack mit einer Standardhöhe von 52 U zu erstellen.

     Wenn Sie eine andere Höhe für das Rack wünschen, müssen Sie das Rack explizit in der Tabelle definieren, bevor Sie es einer Einheit zuordnen.

Um Ihre Einheiten in der Massenimportdatei zu definieren, füllen die folgenden Spalten.

- (Spalten A – C) Für die grundlegende Ermittlung müssen Sie den Einheitentyp und entweder die aktuelle IP-Adresse oder die Seriennummer der Einheit angeben. Folgende Typen werden unterstützt:
  - **Abdeckblende**. Platzhalter für eine nicht verwaltete Einheit. In der Rack-Ansicht wird diese Einheit als generische Abdeckblendengrafik angezeigt. Im Arbeitsblatt **Readme** in der Excel-Vorlage finden Sie weitere Abdeckblendentypen.
  - **Flexchassis**. 10 U Flex System-Gehäuse
  - **Server**. Rack- und Tower-Server, die von XClarity Administrator unterstützt werden
  - **Rack**. Racks mit einer Höhe von 6 U, 12 U, 18 U, 25 U, 37 U, 42 U, 45 U, 46 U, 48 U, 50 U und 52 U. Andere Rack-Höhen werden nicht unterstützt. Standardmäßig wird 52 U verwendet.
  - **Speicher**. Speichereinheiten
  - **Switch**. RackSwitch-Switches

  Anmerkung: Flex System-Rechenknoten, Switches und Speichereinheiten werden als Teil des Gehäuseermittlungs- und -Verwaltungsprozesses angesehen.
- (Spalten D – H) Wenn Sie manuell eingegebene Anmeldeinformationen anstelle von gespeicherten Anmeldeinformationen (Spalte Z) oder Identität (Spalten AF – AJ) verwenden möchten, geben Sie den aktuellen Benutzernamen und das Kennwort an. Manuell eingegebene Anmeldeinformationen sind sinnvoll, wenn die Anmeldeinformationen für einige Einheiten unterschiedlich sind. Wenn Sie keine Anmeldeinformationen für eine oder mehrere Einheiten in der Massenimportdatei angeben, werden stattdessen die globalen Anmeldeinformationen verwendet, die Sie im Dialog Massenimport angegeben haben. Weitere Informationen zu manuell eingegebenen Benutzern und verwalteten Authentifizierung finden Sie unter Benutzeraccounts verwalten in der Onlinedokumentation von XClarity Administrator.

  Anmerkungen:
  - Um manuell eingegebene Anmeldeinformationen zu verwenden, müssen Sie die verwaltete XClarity Administrator-Authentifizierung auswählen.
  - Einige Felder gelten für einige Einheiten nicht.
  - (Für Gehäuse) Wenn Sie die verwaltete Authentifizierung (in Spalte AA oder im Dialogfeld „Massenimport“) auswählen, müssen Sie das `RECOVERY_ID`-Kennwort in Spalte G der Massenimportdatei oder im Dialogfeld „Massenimport“ angeben. Bei Auswahl einer lokalen Authentifizierung ist ein Kennwort zur Wiederherstellung nicht zulässig; geben Sie kein Kennwort zur Wiederherstellung in Spalte G der Massenimportdatei oder im Dialogfeld „Massenimport“ an.
  - (Für Rack-Server) Wenn Sie die verwaltete Authentifizierung (in Spalte AA oder im Dialogfeld „Massenimport“) auswählen, können Sie optional ein Kennwort zur Wiederherstellung in Spalte G der Massenimportdatei oder im Dialogfeld „Massenimport“ angeben. Bei Auswahl einer lokalen Authentifizierung ist ein Kennwort zur Wiederherstellung nicht zulässig; geben Sie kein Kennwort zur Wiederherstellung in Spalte G der Massenimportdatei oder im Dialogfeld „Massenimport“ an.
  - (Nur für Rack-Switches) RackSwitch-Einheiten unterstützen nur gespeicherte Anmeldeinformationen (in Spalte Z) für die Authentifizierung bei den Switches. Manuelle Benutzeranmeldeinformationen werden nicht unterstützt.
- (Spalten I – U) Optional können Sie weitere Informationen bereitstellen, wenn Sie nach erfolgreicher Verwaltung Änderungen an der Einheit vornehmen möchten.

  Anmerkung: Einige Felder gelten für einige Einheiten nicht. Diese Felder gelten nicht für RackSwitch-Switches.
- (Spalten V – Z) Sie können optional Informationen zur Rack-Erstellung und -Zuordnung angeben, z. B. Rack-Name, Standort, Raum, unterste Rack-Einheit und Höhe.

Anmerkungen:

- Wenn Sie ein Rack erstellen, müssen Sie den Rack-Namen und die Rack-Höhe angeben. Die folgenden Rack-Höhen werden unterstützt: 6 U, 12 U, 18 U, 25 U, 37 U, 42 U, 45 U, 46 U, 48 U, 50 U und 52 U. Andere Rack-Höhen werden nicht unterstützt.
- Wenn Sie eine generische Abdeckblende erstellen, müssen Sie den Rack-Namen und die Höhe der Abdeckblende angeben. Die folgenden Höhen für Abdeckblenden werden unterstützt: 1 U, 2 U und 4 U.
- Beim Erstellen einer spezifischen Abdeckblende wird die Höhe ignoriert, da XClarity Administrator die Höhe zu jeder Abdeckblende kennt. Im Arbeitsblatt der Vorlage finden Sie weitere Abdeckblendentypen und -höhen.
- Beim Zuordnen einer Einheit zu einem Rack wird die Höhe der Einheit ignoriert. Die Einheitenhöhe wird vom Einheitenbestand abgerufen.

- (Spalte AA) Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option „Verwaltung erzwingen“.
  - Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

    Anmerkung: Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option „Verwaltung erzwingen“ verwalten.
  - Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
  - Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

  Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie es mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

  Wichtig: Wenn Sie die IP-Adresse eines Server ändern, nachdem dieser von XClarity Administrator verwaltet wird, erkennt XClarity Administrator die neue IP-Adresse und verwaltet den Server weiterhin. Allerdings wird die IP-Adressänderung für einige Server von XClarity Administrator nicht erkannt. Falls XClarity Administrator anzeigt, dass der Server nach der IP-Adressänderung offline ist, können Sie den Server mit der Option „Verwaltung erzwingen“ wieder verwalten.
- (Spalte AB) Wenn Sie gespeicherte Anmeldeinformationen anstelle der manuell eingegebenen Anmeldeinformationen (Spalten D – H) oder Identität (Spalten AF – AJ) verwenden, geben Sie eine gespeicherte Anmelde-ID an. Sie finden die gespeicherte Anmelde-ID auf der Seite „Gespeicherte Anmeldeinformationen“ durch Klicken auf **Verwaltung → Sicherheit** im XClarity Administrator Menü und durch anschließendes Klicken auf **Gespeicherte Anmeldeinformationen** über die linke Navigation. Weitere Informationen zu gespeicherten Anmeldeinformationen und lokaler Authentifizierung finden Sie unter Gespeicherte Anmeldeinformationen verwalten in der Onlinedokumentation von XClarity Administrator.

  Anmerkungen:

  - RackSwitch-Geräte unterstützen nur gespeicherte Anmeldeinformationen für die Authentifizierung. Manuelle Benutzeranmeldeinformationen (in Spalte D) werden nicht unterstützt.
  - Wenn Sie eine Einheit mit gespeicherten Anmeldeinformationen verwalten und die verwaltete Authentifizierung aktivieren, können Sie diese gespeicherten Anmeldeinformationen nicht bearbeiten.

- (Spalte AC) Wenn Sie für Gehäuse und Rack-Server die verwaltete Authentifizierung auswählen, müssen Sie das RECOVERY_ID-Kennwort in Spalte G der Massenimportdatei oder im Dialogfeld „Massenimport“ angeben. Bei Auswahl einer lokalen Authentifizierung ist ein Kennwort zur Wiederherstellung nicht zulässig; geben Sie kein Kennwort zur Wiederherstellung in Spalte G der Massenimportdatei oder im Dialogfeld „Massenimport“ an.
- (Spalte AD) Für Rack-Server können Sie optional auswählen, die lokale Authentifizierung anstelle der verwalteten XClarity Administrator-Authentifizierung zu verwenden, indem Sie in dieser Spalte „FALSE“ angeben. Weitere Informationen zur verwalteten und lokalen Authentifizierung finden Sie unter Authentifizierungsserver verwalten in der XClarity Administrator Onlinedokumentation.
- (Spalte AE) Sie können optional eine Liste der Rollengruppen angeben, die die Einheit anzeigen und verwalten dürfen. Sie können nur Rollengruppen angeben, zu denen der aktuelle Benutzer gehört.

  Anmerkung: Wenn Sie Einheiten zu einem verwalteten Gehäuse hinzufügen, gehören die neuen Einheiten zu den gleichen Rollengruppen wie das Gehäuse.
- (Spalten AF – AJ) Wenn Sie ein Identitätsverwaltungssystem anstelle von manuell eingegebenen Anmeldeinformationen (Spalten D – H) oder gespeicherten Anmeldeinformationen (Spalte AB) verwenden, geben Sie die IP-Adresse oder den Hostnamen des verwalteten Servers, den Benutzernamen und optional die Anwendungs-ID, den Safe und den Ordner an.

  Wenn Sie die Anwendungs-ID angeben, müssen Sie ggf. auch den Safe und den Ordner angeben.

  Wenn Sie die Anwendungs-ID nicht angeben, verwendet XClarity Administrator die Pfade, die bei der Einrichtung von CyberArk definiert wurden, um die integrierten Accounts in CyberArk zu identifizieren.

  Anmerkung: Es werden nur ThinkSystem oder ThinkAgile Server unterstützt. Das Identitätsverwaltungssystem muss in XClarity Administrator konfiguriert sein und der Lenovo XClarity Controller für die verwalteten ThinkSystem oder ThinkAgile Server muss in CyberArk integriert sein.

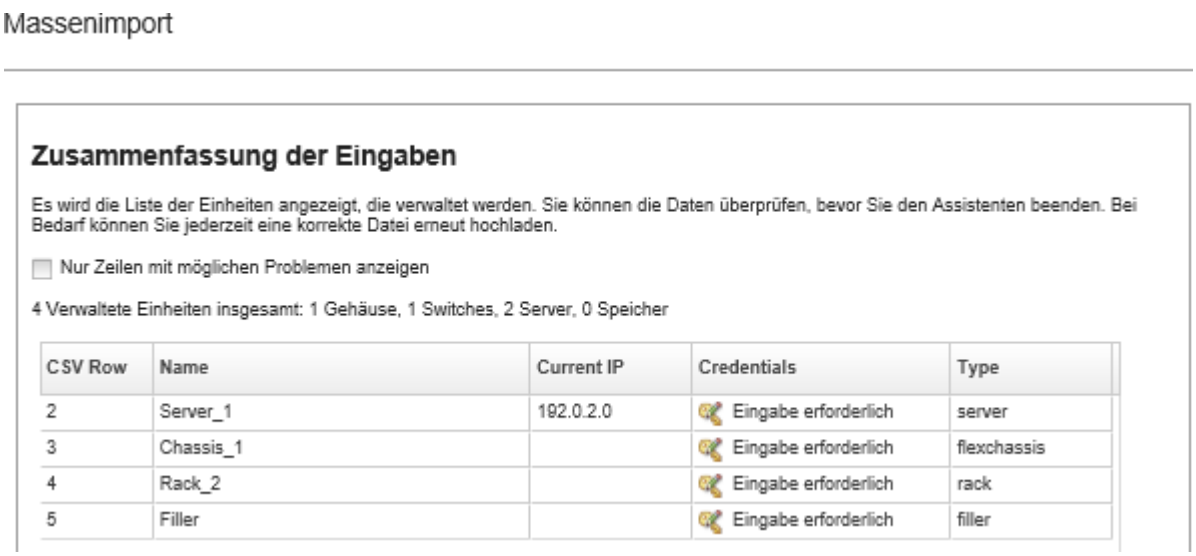
Die folgende Abbildung zeigt ein Beispiel für eine Massenimportdatei:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)			Optional fields															
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X30EL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	35T88XP												2002:939	2002:9	2002:939:	2002:9	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. Geben Sie im Assistenten Massenimport den Namen der CSV-Datei ein, um sie für die Verarbeitung hochzuladen. Sie können auf **Durchsuchen** klicken, um die Datei zu suchen.
7. Klicken Sie auf **Hochladen**, um die Datei hochzuladen und zu überprüfen.

8. Klicken Sie auf **Weiter**, um die Seite mit der Eingabezusammenfassung mit einer Liste der zu verwaltenden Einheiten anzuzeigen.



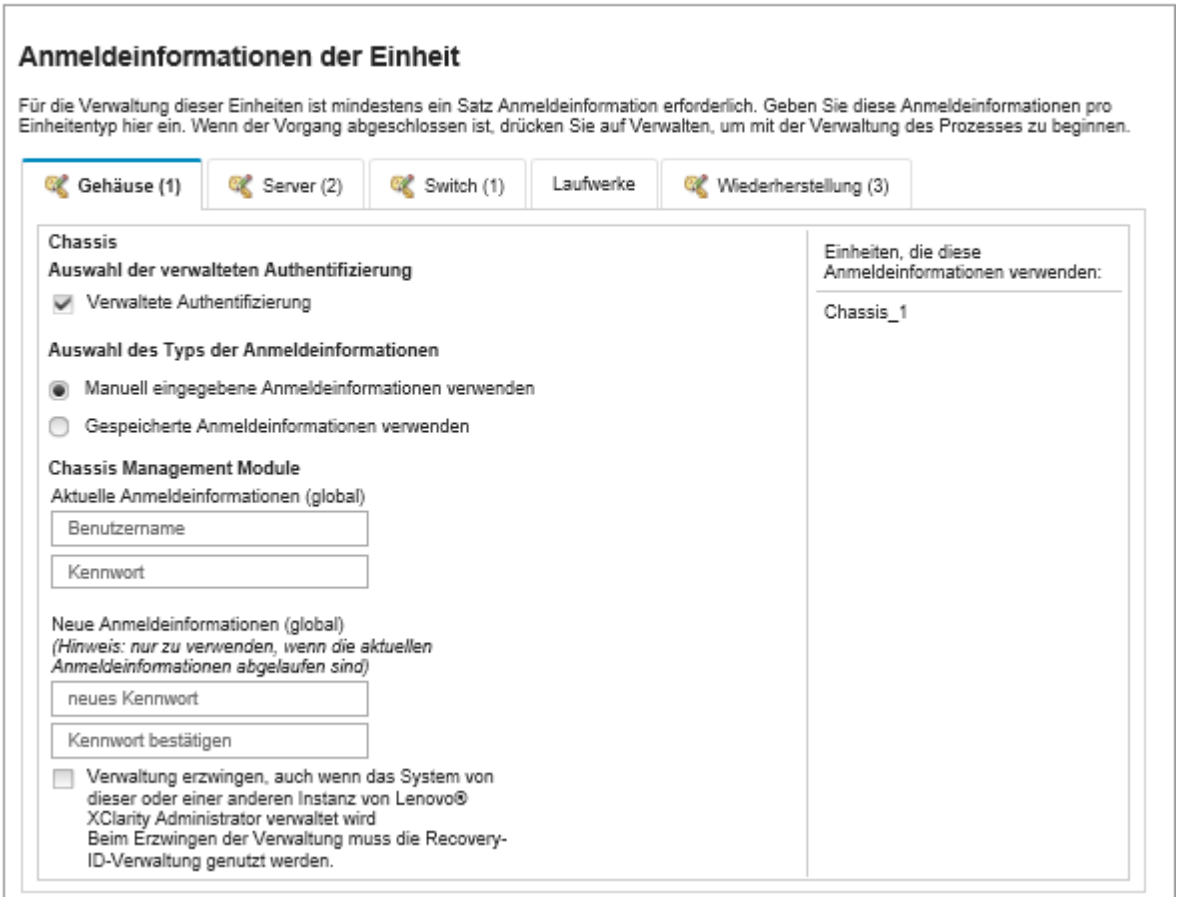
9. Überprüfen Sie die Zusammenfassung der Einheiten, die Sie verwalten möchten.

   Wählen Sie **Nur Zeilen mit möglichen Probleme anzeigen** aus, um die Zeilen mit unvollständigen Daten anzuzeigen. Beheben Sie eventuelle Probleme in der Massenimportdatei und klicken Sie dann auf **Zurück**, um die korrigierte CSV-Datei hochzuladen.

   Anmerkungen:

   - Wenn die erforderlichen Daten in der Massenimportdatei nicht angegeben sind, werden die zugeordneten Einheiten nicht verwaltet.
   - Auf der Seite Eingabezusammenfassung werden die Zeilen markiert, die keine Anmeldeinformationen enthalten. Wenn Sie keine Anmeldeinformationen in der Massenimportdatei angeben, werden stattdessen die globalen Anmeldeinformationen verwendet, die Sie im Assistenten Massenimport angegeben haben.

10. Klicken Sie auf **Weiter**, um die Seite „Anmeldeinformationen für Einheiten“ anzuzeigen.



11. **Optional:** Klicken Sie auf jede Registerkarte und geben Sie optional die globalen Einstellungen und Anmeldeinformationen an, die für alle Einheiten eines bestimmten Typs verwendet werden sollen. Die Einheiten, die die globalen Einstellungen und Anmeldeinformationen verwenden, werden auf der rechten Seite jeder Registerkarte aufgelistet.

    Wenn Sie die globalen Anmeldeinformationen verwenden, müssen die Anmeldeinformationen eines bestimmten Einheitentyps für alle Einheiten desselben Typs gleich sein, für die in der Massenimportdatei keine Anmeldeinformationen eingegeben wurden. Beispiel: CMM-Anmeldeinformationen müssen für alle Gehäuse gleich sein und die Speicherverwaltungsanmeldeinformationen müssen für alle Speichereinheiten gleich sein. Wenn die Anmeldeinformationen nicht identisch sind, müssen Sie Anmeldeinformationen in der Massenimportdatei eingeben.

    - **Gehäuse**. Geben Sie den Authentifizierungsmodus und den Typ der Anmeldeinformationen an. Geben Sie die aktuellen Anmeldeinformationen für die Anmeldung an allen Gehäusen an, die in der Massenimportdatei definiert sind. Geben Sie das neue Kennwort an, das verwendet werden soll, wenn die aktuellen CMM-Anmeldeinformationen abgelaufen sind.

      Wenn Sie die Verwaltung eines Gehäuses erzwingen, geben Sie den Account und das Kennwort RECOVERY_ID für die Anmeldeinformationen der Einheit an.
    - **Server**. Geben Sie den Authentifizierungsmodus und den Typ der Anmeldeinformationen an. Geben Sie die aktuellen Anmeldeinformationen bei der Anmeldung an allen Rack- und Tower-Servern an, die in der Massenimportdatei definiert sind. Geben Sie das neue Kennwort an, das verwendet werden soll, wenn die aktuellen Baseboard Management Controller-Anmeldeinformationen abgelaufen sind.

Wenn Sie die Verwaltung eines Servers erzwingen, geben Sie den Account und das Kennwort RECOVERY_ID für die Anmeldeinformationen der Einheit an.

- **Switches**. Geben Sie die gespeicherten Anmeldeinformationen für die Anmeldung an allen RackSwitch-Switches an, die in der Massenimportdatei definiert sind. Falls festgelegt, geben Sie auch das „Enable“-Kennwort an, das zur Eingabe des EXEC/Privileged Mode auf dem Switch verwendet wird.
- **Storage**. Geben Sie die aktuellen Anmeldeinformationen für die Anmeldung an allen Speichereinheiten an, die in der Massenimportdatei definiert sind.
- **Wiederherstellung**. Geben Sie das Wiederherstellungskennwort für die Anmeldung an allen Servern und Gehäusen an, die in der Massenimportdatei definiert sind.

  Sie können auswählen, ob Sie für die Wiederherstellung ein lokales Benutzeraccount oder gespeicherte Anmeldeinformationen verwenden möchten. In beiden Fällen lautet der Benutzername immer `RECOVERY_ID`.

  Ein Account für die Wiederherstellung (`RECOVERY_ID`) wird bei Angabe eines Kennworts auf der Einheit erstellt und alle lokalen Benutzeraccounts werden deaktiviert.

  – Für das Gehäuse ist ein Kennwort für die Wiederherstellung erforderlich.
  – Für Server ist das Kennwort zur Wiederherstellung optional, wenn Sie sich für die verwaltete Authentifizierung entscheiden und ist nicht zulässig, wenn Sie die lokale Authentifizierung wählen.
  – Stellen Sie sicher, dass das Kennwort den Sicherheits- und Kennwortrichtlinien der Einheit entspricht. Sicherheits- und Kennwortrichtlinien können variieren.
  – Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.
  – Der Wiederherstellungsaccount wird für ThinkServer- und System x M4-Server nicht unterstützt.

Die Informationen, die Sie in der Massenimportdatei angeben, überschreiben alle ähnlichen Informationen, die Sie auf der Seite „Anmeldeinformationen für Einheiten“ angeben.

Optional können Sie die Verwaltung für jeden Einheitentyp in folgenden Fällen erzwingen:

- Die Einheiten werden derzeit von einem anderen Verwaltungssystem verwaltet, z. B. von einer anderen XClarity Administrator-Instanz oder von IBM Flex System Manager.
- XClarity Administrator wurde heruntergefahren, aber die Verwaltung der Einheiten wurde zuvor nicht aufgehoben.
- Die Verwaltung der Einheiten wurde nicht ordnungsgemäß aufgehoben und das CIM-Abonnement nicht gelöscht.

Anmerkung: Wenn die Einheit von einer anderen XClarity Administrator-Instanz verwaltet wird, scheint die Einheit nach der erzwungenen Verwaltung für einen bestimmten Zeitraum von der ursprünglichen Instanz verwaltet zu werden. Sie können die Verwaltung der Einheit aufheben, um sie von der ursprünglichen XClarity Administrator-Instanz zu entfernen.

12. Klicken Sie auf **Verwalten**. Die Seite „Überwachungsergebnisse“ wird mit Informationen zum Verwaltungsstatus der einzelnen Einheiten in der Massenimportdatei angezeigt.

    Für den Verwaltungsprozess wird ein Job erstellt. Wenn Sie den Assistenten für die Massenimportdatei schließen, wird der Verwaltungsprozess im Hintergrund weiterhin ausgeführt. Sie können den Status des Verwaltungsprozesses im Jobprotokoll überwachen. Informationen zum Jobprotokoll finden Sie unter Jobs überwachen in der Onlinedokumentation von XClarity Administrator.

    Wenn sich XClarity Administrator nicht mit den in der Massenimportdatei angegebenen Anmeldeinformationen oder den im Dialog angegebenen globalen Anmeldeinformationen an einer Einheit anmelden kann, schlägt die Verwaltung dieser Einheit fehl und XClarity Administrator geht zur nächsten Einheit in der Massenimportdatei weiter.

Anmerkungen: Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option **Verwaltung erzwingen**.

- Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

  Anmerkung: Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.
- Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

13. Wenn die Massenimportdatei ein neues Gehäuse enthält, überprüfen und ändern Sie die Verwaltungsnetzwerkeinstellungen für das gesamte Gehäuse (einschließlich Rechenknoten und Flex-Switches) und konfigurieren Sie die Rechenknoteninformationen, den lokalen Speicher, die E/A-Adapter, die Bootziele und Firmwareeinstellungen, indem Sie Servermuster erstellen und implementieren. Weitere Informationen finden Sie unter IP-Verwaltungseinstellungen für ein Gehäuse ändern und Server mithilfe von XClarity Administrator konfigurieren in der Onlinedokumentation von XClarity Administrator.

Nach dieser Aufgabe

Nachdem Ihre Systeme verwaltet wurden, können Sie die folgenden Aktionen ausführen:

- Ermitteln und Verwalten weiterer Systeme (siehe Gehäuse verwalten, Racks verwalten, Server verwalten, Speichereinheiten verwalten und Switches verwalten in der Onlinedokumentation von Lenovo XClarity Administrator).
- Konfigurieren Sie Systeminformationen, lokalen Speicher, E/A-Adapter, Boot-Einstellungen und Firmwareeinstellungen, indem Sie Servermuster erstellen und implementieren (siehe Server mithilfe von XClarity Administrator konfigurieren in der Onlinedokumentation von Lenovo XClarity Administrator).
- Implementieren Sie Betriebssystem-Images auf Servern, auf denen noch kein Betriebssystem installiert ist (siehe Betriebssystem-Image implementieren in der Onlinedokumentation von XClarity Administrator).
- Aktualisieren Sie die Firmware auf Einheiten, die nicht den aktuellen Richtlinien entsprechen (siehe Firmware auf verwalteten Einheiten aktualisieren in der Onlinedokumentation von XClarity Administrator).
- Fügen Sie die neu verwalteten Systeme zum entsprechenden Rack hinzu, um die physische Umgebung widerzuspiegeln (siehe Racks verwalten in der Onlinedokumentation von XClarity Administrator).
- Überwachen Sie den Hardwarestatus und die Details (siehe Den Status eines verwalteten Servers anzeigen in der Onlinedokumentation von XClarity Administrator).
- Überwachen Sie Ereignisse und Alerts (siehe Ereignisse handhaben und Mit Alerts arbeiten in der Onlinedokumentation von XClarity Administrator).
- Aktivieren oder deaktivieren Sie Single Sign-On für verwaltete ThinkSystem und ThinkAgile Server.
  - Klicken Sie für alle verwalteten ThinkSystem und ThinkAgile Server (global) in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, wählen Sie dann **Aktive Sitzungen** aus und aktivieren oder deaktivieren Sie **Single Sign-On**.
  - Klicken Sie für einen bestimmten ThinkSystem und ThinkAgile Server in der XClarity Administrator-Menüleiste auf **Hardware → Server** und wählen Sie dann **Alle Aktionen → Sicherheit → Single Sign-On aktivieren** oder **Alle Aktionen → Sicherheit → Single Sign-On deaktivieren** aus.

Anmerkung: Mit Single Sign-On kann sich ein Benutzer, der bereits bei XClarity Administrator angemeldet ist, automatisch beim Baseboard Management Controller anmelden. Single Sign-On ist standardmäßig aktiviert, wenn ein ThinkSystem oder ThinkAgile Server von XClarity Administrator verwaltet wird (es sei denn, der Server wird mit CyberArk-Kennwörtern verwaltet). Sie können global konfigurieren, dass Single Sign-On für alle verwalteten ThinkSystem und ThinkAgile Server aktiviert oder deaktiviert ist. Das Aktivieren von Single Sign-On für einen bestimmten ThinkSystem und ThinkAgile Server überschreibt die globale Einstellung für alle ThinkSystem und ThinkAgile Server.

Kapitel 5. XClarity Administrator registrieren

Wenn Sie Ihre Instanz von Lenovo XClarity Administrator registrieren, können Sie die grundlegenden Funktionen verwenden, ohne die wiederkehrenden Warnungen zum Ablauf der Testversion und nicht konformen Lizenzen zu erhalten. Nach der Registrierung wird keine Warnung mehr zu nicht konformen Lizenzen angezeigt, aber alle Funktionen, für die eine Lizenz erforderlich ist, bleiben deaktiviert, bis Sie Lizenzen basierend auf der Anzahl der verwalteten Einheiten erwerben und installieren.

Zu dieser Aufgabe

Bei der Registrierung Ihrer XClarity Administrator-Instanz müssen Sie keine Kontaktinformationen angeben. Lenovo gibt die angegebenen Informationen nicht an andere externe Entitäten weiter.

Wenn Sie Lizenzen für erweiterte Funktionen installiert haben, müssen Sie Ihre XClarity Administrator-Instanz nicht registrieren. Weitere Informationen zu Lizenzen und erweiterten Funktionen finden Sie unter Lizenz für den vollständigen Funktionsumfang installieren.

Vorgehensweise

Gehen Sie zum Registrieren von XClarity Administrator wie folgt vor.

- Wenn XClarity Administrator mit dem Internet verbunden ist
  1. Navigieren Sie in der Menüleiste von Lenovo XClarity Administrator zu **Verwaltung → Registrierung**, um die Seite „Registrierung“ anzuzeigen.
  2. Klicken Sie auf **Registrieren**, um eine neue Instanz von XClarity Administrator zu registrieren.
  3. Geben Sie den Namen des Unternehmens, die Anzahl der von XClarity Administrator verwalteten Einheiten und das Land an, in dem sich XClarity Administrator befindet.
  4. Klicken Sie auf **Senden**.
- Wenn XClarity Administrator nicht mit dem Internet verbunden ist
  1. Registrieren Sie XClarity Administrator.
     a. Öffnen Sie in einem Webbrowser das Lenovo XClarity-Webportal für Registrierung.
     b. Geben Sie den Namen des Unternehmens, die Anzahl der von XClarity Administrator verwalteten Einheiten und das Land an, in dem sich XClarity Administrator befindet.
     c. Klicken Sie auf **Senden**, um ein Registrierungstoken zu erhalten.
  2. Navigieren Sie in der Menüleiste von Lenovo XClarity Administrator zu **Verwaltung → Registrierung**, um die Seite „Registrierung“ anzuzeigen.
  3. Klicken Sie auf **Importieren**, um das Registrierungstoken zu importieren.
  4. Geben Sie das in Schritt 1 erhaltene Registrierungstoken ein.
  5. Klicken Sie auf **Senden**.

Kapitel 6. Lizenz für den vollständigen Funktionsumfang installieren

Nach Ablauf der kostenlosen 90-Tage-Testversion müssen Sie die Lenovo XClarity Pro Lizenzen für alle verwalteten Einheiten erwerben und installieren, die erweiterte Funktionen unterstützten, damit Sie die Funktionen für Betriebssystemimplementierung und Einheitenkonfiguration in Lenovo XClarity Administrator weiterhin nutzen können. Sie müssen über Lenovo XClarity Pro Lizenzen für *alle* verwalteten Einheiten verfügen, um XClarity Administrator Service und Support zu erhalten.

Weitere Informationen: XClarity Administrator: Lizenz installieren

Vorbereitende Schritte

Lesen Sie die folgenden Lizenzhinweise.

- Eine Lizenz ist *nicht* an eine bestimmte Einheit gebunden.
- Eine Gehäuselizenz enthält Lizenzen für 14 Einheiten.
- Für skalierbare komplexe System x3850 X6 (6241) Server benötigt jeder Server unabhängig von den Partitionen eine separate Lizenz.
- Für skalierbare komplexe System x3950 X6 (6241) Server benötigt jeder Server eine separate Lizenz, wenn es keine Partitionen gibt. Sind Partitionen vorhanden, benötigt jede Partition eine separate Lizenz.
- Die folgenden Einheiten *unterstützen keine* erweiterten Funktionen und *benötigen daher keine* Lizenzen für diese Funktionen. Allerdings muss für jede dieser Einheiten eine Lizenz erworben werden, um Service und Unterstützung für XClarity Administrator zu erhalten.
  - ThinkServer-Server
  - System x M4 Server
  - System x X5 Server
  - System x3850 X6 und x3950 X6 (3837) Server
  - Speichereinheiten
  - Switches

Sie benötigen die Berechtigungen **lxc-supervisor** oder **lxc-security-admin**, um Lizenzen installieren zu können.

Zu dieser Aufgabe

XClarity Administrator unterstützt die folgende Lizenz.

- **Lenovo XClarity Pro**. Jede Lizenz bietet die folgenden Nutzungsrechte für eine einzelne Einheit.
  - Service und Unterstützung für Lenovo XClarity Integrator
  - Service und Unterstützung für XClarity Administrator
  - Erweiterte Funktionen in XClarity Administrator:
    - Server mithilfe von Konfigurationsmustern konfigurieren
    - Betriebssysteme implementieren
    - XClarity Administrator-Probleme mithilfe der Call-Home-Funktion melden (Call-Home-Funktion für Hardware-Alerts ist nicht betroffen)

Der Aktivierungszeitraum für die Lizenz beginnt, wenn sie erworben wurde und der Autorisierungscode erstellt wird.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt, die die verwalteten Funktionen unterstützen. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen gültigen Lizenzschlüsseln nicht überschreiten. Wenn XClarity Administrator nicht den installierten Lizenzen entspricht (z. B. wenn Lizenzen ablaufen oder wenn die Verwaltung zusätzlicher Einheiten die Gesamtanzahl der aktiven Einheiten überschreitet), haben Sie eine Kulanzzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Jedes Mal, wenn XClarity Administrator nicht konform ist, wird die Kulanzzeit auf 90 Tage zurückgesetzt. Wenn die Kulanzzeit (einschließlich der kostenlosen Testversion) endet, bevor die Lizenzen konform sind, werden die erweiterten Funktionen für alle Geräte deaktiviert.

Wenn Sie z. B. weitere 100 ThinkSystem-Server und 20 Rack-Switches in einer vorhandenen XClarity Administrator-Instanz verwalten, haben Sie 90 Tage Zeit, um 100 zusätzliche Lizenzen zu erwerben und zu installieren, bevor die erweiterten Funktionen in der Benutzerschnittstelle deaktiviert werden (für alle Geräte). Für die Verwendung der erweiterten Funktionen sind keine Lizenzen für die 20 Rack-Switches erforderlich. Allerdings sind die Lizenzen jedoch erforderlich, wenn Sie Service und Support wünschen. Wenn die erweiterten Funktionen deaktiviert sind, werden sie erneut aktiviert, sobald Sie genügend Lizenzen für die Konformität installiert haben.

Wenn Sie eine kostenlose Testlizenz verwenden oder zum Erreichen der Konformität über einen Kulanzzeitraum verfügen und auf eine neuere Version von XClarity Administrator aktualisieren, wird die Testlizenz oder die Kulanzzeit auf 90 Tage zurückgesetzt.

Anmerkungen:

- Funktionen für Serverkonfiguration und Betriebssystembereitstellung werden mit Ablauf der Kulanzzeit deaktiviert.
- Die Call-Home-Funktion für Probleme mit XClarity Administrator (Software für die Call-Home-Funktion) ist deaktiviert, wenn die Lizenzen nicht konform sind. Für diese Funktion gibt es keine Kulanzzeit. Die Call-Home-Funktion für Hardware-Alerts ist jedoch nicht betroffen.

Wenn bereits Lizenzen installiert sind, sind *keine* neuen Lizenzen erforderlich, wenn Sie eine Aktualisierung auf eine neue Version von XClarity Administrator ausführen.

Sie können den Lizenzstatus und die Anzahl der verbleibenden Tage der Testlizenz bestimmen, indem Sie auf das Benutzeraktionen-Menü (

) in der XClarity Administrator-Titelleiste und anschließend auf **Info** klicken.

Hilfe anfordern

- Wenn Sie auf Probleme stoßen und das Produkt über einen Business Partner erworben haben, wenden Sie sich an Ihren Business Partner zur Überprüfung der Transaktion und Berechtigung.
- Wenn Sie keinen elektronischen Berechtigungsnachweis, keine Autorisierungscodes oder Aktivierungsschlüssel erhalten haben oder diese der falschen Person zugestellt wurden, wenden Sie sich abhängig von Ihrer Region an einen regionalen Kundendienstmitarbeiter.
  - ESDNA@lenovo.com (Länder in Nordamerika)
  - ESDAP@lenovo.com (Länder im Raum Asien/Pazifik)
  - ESDEMEA@lenovo.com (Länder in Europa, dem nahen Osten und in Asien)
  - ESDLA@lenovo.com (Länder in Lateinamerika)
  - ESDChina@Lenovo.com (China)
- Wenn die Informationen zu Ihrer Berechtigung nicht korrekt sind, kontaktieren Sie die Lenovo Unterstützung über SW_override@lenovo.com. Machen Sie dabei folgende Angaben:
  - Bestellnummer
  - Ihre Kontaktinformationen, einschließlich E-Mail-Adresse
  - Ihre physische Adresse
  - Gewünschte Änderungen

- Wenn Sie Probleme oder Fragen zum Herunterladen der Lizenz haben, kontaktieren Sie die Lenovo Unterstützung über -eSupport_-_Ops@lenovo.com.

Lizenzen für den vollständigen Funktionsumfang mit der XClarity Administrator-Webschnittstelle installieren

Wenn XClarity Administrator Zugriff auf das Internet hat, können Sie die XClarity Administrator-Webschnittstelle verwenden, um Lizenzen für eine vorhandene Autorisierung einzulösen und abzurufen, und die eingelösten Lizenzen anschließend importieren und installieren.

Vorbereitende Schritte

Zum Erwerb von Lenovo XClarity Pro-Lizenzen auf Basis der zu aktivierenden Funktionen und der Anzahl der Einheiten, die Sie verwalten möchten, wenden Sie sich an Ihren Lenovo Ansprechpartner oder autorisierten Business Partner. Nachdem Sie Lizenzen erworben haben, wird Ihnen per E-Mail ein *elektronischer Berechtigungsnachweis* mit einem Autorisierungscode zugesandt. Der Autorisierungscode ist eine 22-stellige alphanumerische Zeichenfolge, die Sie benötigen, um die Lizenzen einzulösen und zu installieren. Wenn Sie die E-Mail nicht erhalten und die Lizenz über einen Business Partner erworben haben, wenden Sie sich an Ihren Business Partner, um den Autorisierungscode anzufordern.

Sie können Ihre Autorisierungscodes auch von Features on Demand-Webportal abrufen, indem Sie auf **Autorisierungscode abrufen** klicken.

Vorgehensweise

Gehen Sie wie folgt vor, um Lenovo XClarity Pro-Lizenzen auf dem Verwaltungsserver zu installieren.

- **Alle oder einen Teil der verbleibenden Lizenzen über einen einzelnen Autorisierungscode einlösen und installieren**

  Sie können alle oder einen Teil der verfügbaren Lizenzen für einen einzelnen Autorisierungscode einlösen, um einen Lizenzaktivierungsschlüssel zu erstellen. Dieser enthält alle Informationen zu einer eingelösten Lizenz. Sie können die eingelösten Lizenzen anschließend mithilfe der Lizenzaktivierungsschlüsseldatei installieren.

  1. Navigieren Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Lizenzen**, um die Seite Lizenzverwaltung aufzurufen.

2. Klicken Sie auf das Symbol **Aktivierungsschlüssel anfordern** ( ), um das Dialogfenster Aktivierungsschlüssel anfordern anzuzeigen.
3. Klicken Sie auf **Einzelner Autorisierungscode**.
4. Geben Sie den 22-stelligen Autorisierungscode ein und klicken Sie auf **Suchen**, um Informationen zu den erworbenen Lizenzen für den angegebenen Autorisierungscode von der FoD-Website abzurufen.

   Wenn der erhaltene Autorisierungscode nicht akzeptiert wird, wenden Sie sich an die Lenovo Unterstützung.
5. Geben Sie Ihre 10-stellige Lenovo Kundennummer im Feld **Lenovo Kundennummer** ein.
6. Geben Sie im Feld **Anzahl einlösen**, die Anzahl der Lizenzen ein, die Sie einlösen möchten und klicken Sie anschließend auf **Fortfahren**.

   Um alle verfügbaren Lizenzen in diesem Autorisierungscode einzulösen, muss die Anzahl mit der im Feld **Verfügbare Lizenzen** angegebenen Anzahl übereinstimmen.

   Wenn Sie nur einen Teil der verfügbaren Lizenzen einlösen, können Sie die verbleibenden Lizenzen später unter Verwendung desselben Autorisierungscodes einlösen.

   Tipp: Jeder XClarity Administrator unterstützt bis zu 1.000 verwaltete Einheiten. Daher kann ein einzelner Lizenzaktivierungsschlüssel, den Sie in einer XClarity Administrator-Instanz installieren, nicht über mehr als 1.000 Lizenzen verfügen.
7. Überprüfen Sie, ob die Kontaktinformationen korrekt sind und nehmen Sie ggf. Änderungen vor.
8. Klicken Sie auf **Anforderung senden**, um die Lizenzen einzulösen und den Lizenzaktivierungsschlüssel zu erstellen.
9. Wählen Sie den Lizenzaktivierungsschlüssel aus, der die zu installierenden Lizenzen enthält.
10. Klicken Sie auf **Installieren**, um die Lizenzen im Verwaltungsserver zu installieren.
11. Klicken Sie auf **Schließen**.

- **Alle verbleibenden Lizenzen über mehrere Autorisierungscodes einlösen und installieren**

  Sie können alle verbleibenden Lizenzen über mehrere Autorisierungscodes einlösen. Für jeden Autorisierungscode wird ein Lizenzaktivierungsschlüssel erstellt. Sie können die eingelösten Lizenzen anschließend mithilfe der Lizenzaktivierungsschlüssel installieren. Die Autorisierungscodes müssen unter Verwendung der bereitgestellten Vorlage als CSV-Datei bereitgestellt werden.

1. Navigieren Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Lizenzen**, um die Seite Lizenzverwaltung aufzurufen.
2. Klicken Sie auf das Symbol **Aktivierungsschlüssel anfordern** (), um das Dialogfenster Aktivierungsschlüssel anfordern anzuzeigen.
3. Klicken Sie auf **Mehrere Autorisierungscodes**.
4. Klicken Sie auf den Link **Vorlage herunterladen**, um eine Excel-Datei zu öffnen. Fügen Sie jeden Autorisierungscode zur Datei hinzu und speichern Sie die Datei im CSV-Format auf Ihrem lokalen System.
5. Klicken Sie auf **Durchsuchen**, um die CSV-Datei mit dem Autorisierungscode auszuwählen und dann auf **Suchen**, um Informationen zum Autorisierungscode von der Lenovo Unterstützungswebsite abrufen.
6. Lesen Sie die Informationen über die erworbene Lizenz und die verfügbaren Lizenzaktivierungsschlüssel, die jedem Autorisierungscode zugeordnet sind.
7. Geben Sie Ihre 10-stellige Lenovo Kundennummer im Feld **Lenovo Kundennummer** ein.
8. Überprüfen Sie, ob die Kontaktinformationen korrekt sind und nehmen Sie ggf. Änderungen vor. Klicken Sie dann auf **Fortfahren**.
9. Wählen Sie **Ja, ich möchte alle gültigen Autorisierungscodes einlösen** aus und klicken Sie anschließend auf **Anforderung senden**, um die Lizenzaktivierungsschlüssel zu generieren.
10. Wählen Sie die Lizenzaktivierungsschlüssel aus, die Sie installieren möchten.
11. Klicken Sie auf **Installieren**, um die Lizenzaktivierungsschlüssel im Verwaltungsserver zu installieren.
12. Klicken Sie auf **Schließen**.

- **Eingelöste Lizenzen abrufen und installieren**

  Sie können Lizenzaktivierungsschlüssel von einer XClarity Administrator-Instanz auf das lokale System herunterladen, die Zugriff auf das Features on Demand-Webportal hat, und diese Lizenzaktivierungsschlüssel in einer anderen XClarity Administrator-Instanz importieren und installieren. Dies ist hilfreich, wenn Sie Lizenzen auf einer XClarity Administrator-Instanz installieren möchten, die keinen Internetzugriff hat, oder wenn Sie XClarity Administrator erneut installiert haben und installierte Lizenzen wiederherstellen müssen.

  1. Navigieren Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Lizenzen**, um die Seite Lizenzverwaltung aufzurufen.
  2. Klicken Sie auf das Symbol **Protokoll abrufen** (), um das Dialogfenster „Protokoll abrufen“ anzuzeigen.
  3. Geben Sie Ihre Lenovo Kundennummer oder den 22-stelligen Autorisierungscode ein.
  4. Klicken Sie auf **Suchen**, um Informationen zu verfügbaren und eingelösten Lizenzen abzurufen.

     Wenn der erhaltene Autorisierungscode nicht akzeptiert wird, wenden Sie sich an die Lenovo Unterstützung.
  5. Wählen Sie die Lizenzschlüsseldateien aus, die Sie installieren möchten.
  6. Klicken Sie auf **Installieren**, um die Lizenzaktivierungsschlüssel in XClarity Administrator zu installieren.
  7. Klicken Sie auf **Schließen**.

- **Eingelöste Lizenzen auf einer anderen XClarity Administrator-Instanz importieren und installieren**

  Wenn Sie Lizenzen über eine XClarity Administrator-Instanz eingelöst haben und diese Lizenzen auf einer anderen XClarity Administrator-Instanz installieren möchten oder wenn eine Fehlerbedingung auftritt, die eine Wiederherstellung der installierten Lizenzen erforderlich macht, können Sie die Lizenzschlüsseldatei aus dem lokalen System zur anderen XClarity Administrator-Instanz importieren.

1. Rufen Sie von einer XClarity Administrator-Instanz, die Zugriff auf Features on Demand-Webportal hat, die Lizenzaktivierungsschlüssel von Features on Demand-Webportal ab und speichern Sie die Lizenzaktivierungsschlüssel anschließend als Datei auf Ihrem lokalen System.
   a. Navigieren Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Lizenzen**, um die Seite Lizenzverwaltung aufzurufen.
   b. Klicken Sie auf das Symbol **Protokoll abrufen** (), um das Dialogfenster „Protokoll abrufen“ anzuzeigen.
   c. Geben Sie den 22-stelligen Autorisierungscode ein.
   d. Klicken Sie auf **Suchen**, um Informationen zu verfügbaren und eingelösten Lizenzen für diesen Autorisierungscode abzurufen.

      Wenn der erhaltene Autorisierungscode nicht akzeptiert wird, wenden Sie sich an die Lenovo Unterstützung.
   e. Wählen Sie die Lizenzaktivierungsschlüsseldateien aus, die Sie installieren möchten.
   f. Klicken Sie auf **Herunterladen**, um die Lizenzschlüsseldateien auf dem lokalen System zu speichern.
2. In der XClarity Administrator-Instanz, auf der Sie Lizenzaktivierungsschlüssel installieren möchten:
   a. Navigieren Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Lizenzen**, um die Seite Lizenzverwaltung aufzurufen.
   b. Klicken Sie auf das Symbol **Importieren und übernehmen** (), um die Lizenzen zu importieren und zu installieren.
   c. Klicken Sie auf **Durchsuchen**, um die Lizenzaktivierungsschlüssel für die Lizenzen auszuwählen, die Sie installieren möchten.

      Um mehrere Lizenzaktivierungsschlüssel zu importieren, komprimieren Sie die KEY-Dateien in eine ZIP-Datei und wählen Sie die ZIP-Datei für den Import aus.
   d. Klicken Sie auf **Lizenz akzeptieren**, um die Lizenzen zu importieren und zu übernehmen.

      Wenn die Installation abgeschlossen ist, werden die Lizenzaktivierungsschlüssel in der Tabelle mit der Anzahl der installierten Lizenzen und dem Aktivierungszeitraum (Start- und Ablaufdatum) aufgeführt.

Nach dieser Aufgabe

Über die Seite Lizenzen können Sie die folgenden Aktionen ausführen.

- Laden Sie einen oder mehrere bestimmte Lizenzaktivierungsschlüssel auf das lokale System herunter, indem Sie auf das Symbol **Exportieren** () klicken.

  Anmerkung: Wenn Sie mehrere Lizenzaktivierungsschlüssel exportieren, werden die Dateien gemeinsam in einer ZIP-Datei heruntergeladen.
- Löschen Sie einen bestimmten Lizenzaktivierungsschlüssel über das Symbol **Löschen** ().
- Konfigurieren Sie die Lizenz-Warndauer, indem Sie auf die Schaltfläche **Bearbeiten** oben auf der Seite klicken. Bei der Lizenz-Warndauer handelt es sich um die Anzahl der Tage vor Ablauf der Lizenzen, wenn XClarity Administrator eine Warnung auslöst.

Hilfe anfordern

- Wenn Sie auf Probleme stoßen und das Produkt über einen Business Partner erworben haben, wenden Sie sich an Ihren Business Partner zur Überprüfung der Transaktion und Berechtigung.

- Wenn Sie keinen elektronischen Berechtigungsnachweis, keine Autorisierungscodes oder Aktivierungsschlüssel erhalten haben oder diese der falschen Person zugestellt wurden, wenden Sie sich abhängig von Ihrer Region an einen regionalen Kundendienstmitarbeiter.
  - ESDNA@lenovo.com (Länder in Nordamerika)
  - ESDAP@lenovo.com (Länder im Raum Asien/Pazifik)
  - ESDEMEA@lenovo.com (Länder in Europa, dem nahen Osten und in Asien)
  - ESDLA@lenovo.com (Länder in Lateinamerika)
  - ESDChina@Lenovo.com (China)
- Wenn die Informationen zu Ihrer Berechtigung nicht korrekt sind, kontaktieren Sie die Lenovo Unterstützung über SW_override@lenovo.com. Machen Sie dabei folgende Angaben:
  - Bestellnummer
  - Ihre Kontaktinformationen, einschließlich E-Mail-Adresse
  - Ihre physische Adresse
  - Gewünschte Änderungen
- Wenn Sie Probleme oder Fragen zum Herunterladen der Lizenz haben, kontaktieren Sie die Lenovo Unterstützung über -eSupport_-_Ops@lenovo.com.

Lizenz für den vollständigen Funktionsumfang über das Features on Demand-Webportal installieren

Wenn XClarity Administrator *keinen* Internetzugriff hat, können Sie Lizenzen für vorhandene Autorisierungscodes mit dem Features on Demand-Webportal von einem anderen System einlösen und abrufen, das Netzwerkzugriff auf XClarity Administrator hat. Sie können die eingelösten Lizenzen dann über die XClarity Administrator-Webschnittstelle importieren und installieren.

Vorgehensweise

Gehen Sie wie folgt vor, um Lenovo XClarity Pro-Lizenzen auf dem Verwaltungsserver zu installieren.

Schritt 1. Erwerben Sie eine Lenovo XClarity Pro-Lizenz für jede verwaltete Einheit.

Zum Erwerb von Lenovo XClarity Pro-Lizenzen auf Basis der zu aktivierenden Funktionen und der Anzahl der Einheiten, die Sie verwalten möchten, wenden Sie sich an Ihren Lenovo Ansprechpartner oder autorisierten Business Partner. Nachdem Sie Lizenzen erworben haben, wird Ihnen per E-Mail ein *elektronischer Berechtigungsnachweis* mit einem Autorisierungscode zugesandt. Der Autorisierungscode ist eine 22-stellige alphanumerische Zeichenfolge, die Sie benötigen, um die Lizenzen einzulösen und zu installieren. Wenn Sie die E-Mail nicht erhalten und die Lizenz über einen Business Partner erworben haben, wenden Sie sich an Ihren Business Partner, um den Autorisierungscode anzufordern.

Sie können Ihre Autorisierungscodes auch von Features on Demand-Webportal abrufen, indem Sie auf **Autorisierungscode abrufen** klicken.

Schritt 2. Lösen Sie alle oder einen Teil der Lizenzen mit dem Autorisierungscode ein. Beim Einlösen von Lizenzen wird eine Lizenzaktivierungsschlüsseldatei generiert.

1. Öffnen Sie Features on Demand-Webportal über einen Webbrowser und melden Sie sich mit Ihrer E-Mail-Adresse als Benutzer-ID beim Portal an.
2. Klicken Sie auf **Aktivierungsschlüssel anfordern**.
3. Wählen Sie **Einzelnen Autorisierungscode eingeben** aus.
4. Geben Sie den 22-stelligen Autorisierungscode ein und klicken Sie auf **Fortfahren**.
5. Geben Sie Ihre Lenovo Kundennummer im Feld **Lenovo Kundennummer** ein.
6. Geben Sie im Feld **Anzahl einlösen**, die Anzahl der Lizenzen ein, die Sie einlösen möchten und klicken Sie anschließend auf **Fortfahren**.

Um alle verfügbaren Lizenzen in diesem Autorisierungscode einzulösen, muss die Anzahl mit der im Feld **Verfügbare Lizenzen** angegebenen Anzahl übereinstimmen.

Wenn Sie nur einen Teil der verfügbaren Lizenzen einlösen, können Sie die verbleibenden Lizenzen unter Verwendung desselben Autorisierungscodes in einem anderen Lizenzaktivierungsschlüssel einlösen.

Tipp: Jeder XClarity Administrator unterstützt bis zu 1.000 verwaltete Einheiten. Daher sollte ein einzelner Lizenzaktivierungsschlüssel, den Sie in einer XClarity Administrator-Instanz installieren, nicht über mehr als 1.000 Lizenzen verfügen.

7. Befolgen Sie die Anweisungen, um Produktdetails und Kontaktinformationen einzugeben, und klicken Sie auf **Fortfahren**, um den Lizenzaktivierungsschlüssel zu generieren.
8. Geben Sie optional zusätzliche Empfänger für den Erhalt der Lizenzaktivierungsschlüssel an.
9. Klicken Sie auf **Senden**, um die Lizenzaktivierungsschlüssel zu senden.

   Die Person, die der Bestellung zugeordnet ist, und die zusätzlichen Empfänger erhalten eine E-Mail mit dem Lizenzaktivierungsschlüssel. Der Schlüssel ist eine Datei im KEY-Format.

   Anmerkung: Sie können Lizenzaktivierungsschlüssel (einzeln oder als Paket) auch über Features on Demand-Webportal herunterladen. Klicken Sie dazu auf **Protokoll abrufen** und verwenden Sie Ihre Lenovo Kundennummer, um Ihre Lizenzaktivierungsschlüssel zu finden, und laden Sie anschließend alle oder einen Teil der Schlüssel herunter. Klicken Sie dann auf **E-Mail**, um die Schlüssel an sich selbst zu senden, oder auf **Herunterladen**, um die Schlüssel auf Ihr lokales System herunterzuladen.

Schritt 3. Importieren und installieren Sie die Lizenzen in XClarity Administrator.

1. Navigieren Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Lizenzen**, um die Seite Lizenzverwaltung aufzurufen.
2. Klicken Sie auf das Symbol **Importieren und übernehmen** (), um die Lizenzen zu installieren.
3. Klicken Sie auf **Durchsuchen**, um die Lizenzaktivierungsschlüsseldatei für die Lizenzen auszuwählen, die Sie installieren möchten.

   Tipp: Um mehrere Lizenzaktivierungsschlüssel zu importieren, komprimieren Sie die KEY-Dateien in eine ZIP-Datei und wählen Sie die ZIP-Datei für den Import aus.
4. Klicken Sie auf **Lizenz akzeptieren**, um die Lizenzen zu importieren und zu übernehmen.

   Wenn die Installation abgeschlossen ist, wird der Lizenzaktivierungsschlüssel in der Tabelle mit der Anzahl der installierten Lizenzen und dem Aktivierungszeitraum (Start- und Ablaufdatum) aufgeführt.

Nach dieser Aufgabe

Über die Seite Lizenzen können Sie die folgenden Aktionen ausführen.

- Laden Sie einen oder mehrere bestimmte Lizenzaktivierungsschlüssel auf das lokale System herunter, indem Sie auf das Symbol **Exportieren** () klicken.

  Anmerkung: Wenn Sie mehrere Lizenzaktivierungsschlüssel exportieren, werden die Dateien gemeinsam in einer ZIP-Datei heruntergeladen.
- Löschen Sie einen bestimmten Lizenzaktivierungsschlüssel über das Symbol **Löschen** ().
- Konfigurieren Sie die Lizenz-Warndauer, indem Sie auf die Schaltfläche **Bearbeiten** oben auf der Seite klicken. Bei der Lizenz-Warndauer handelt es sich um die Anzahl der Tage vor Ablauf der Lizenzen, wenn XClarity Administrator eine Warnung auslöst.

Hilfe anfordern

- Wenn Sie auf Probleme stoßen und das Produkt über einen Business Partner erworben haben, wenden Sie sich an Ihren Business Partner zur Überprüfung der Transaktion und Berechtigung.
- Wenn Sie keinen elektronischen Berechtigungsnachweis, keine Autorisierungscodes oder Aktivierungsschlüssel erhalten haben oder diese der falschen Person zugestellt wurden, wenden Sie sich abhängig von Ihrer Region an einen regionalen Kundendienstmitarbeiter.
  - ESDNA@lenovo.com (Länder in Nordamerika)
  - ESDAP@lenovo.com (Länder im Raum Asien/Pazifik)
  - ESDEMEA@lenovo.com (Länder in Europa, dem nahen Osten und in Asien)
  - ESDLA@lenovo.com (Länder in Lateinamerika)
  - ESDChina@Lenovo.com (China)
- Wenn die Informationen zu Ihrer Berechtigung nicht korrekt sind, kontaktieren Sie die Lenovo Unterstützung über SW_override@lenovo.com. Machen Sie dabei folgende Angaben:
  - Bestellnummer
  - Ihre Kontaktinformationen, einschließlich E-Mail-Adresse
  - Ihre physische Adresse
  - Gewünschte Änderungen
- Wenn Sie Probleme oder Fragen zum Herunterladen der Lizenz haben, kontaktieren Sie die Lenovo Unterstützung über -eSupport_-_Ops@lenovo.com.

Kapitel 7. XClarity Administrator als ein aktualisieren

Wenn Lenovo XClarity Administrator als Container ausgeführt wird, verwenden Sie dieses Aktualisierungsverfahren, um die neueste Software als neuen Container zu installieren und die Datenträger des ursprünglichen Containers an den neuen Container anzubinden.

Vorbereitende Schritte

Sie können XClarity Administrator v4.0 oder höher nur über eine Instanz von XClarity Administrator v3.0 oder höher aktualisieren. Wenn Sie eine Version von XClarity Administrator verwenden, die älter als v3.0 ist, müssen Sie ein Upgrade auf v3.0 oder höher durchführen, bevor Sie eine Aktualisierung auf v4.0 durchführen können.

Zum Verwalten von XClarity Administrator v4.0 oder höheren Instanzen mit Lenovo XClarity Orchestrator ist XClarity Orchestrator v2.0 oder höher erforderlich. Wenn Sie XClarity Administrator auf v4.0 oder höher aktualisieren, stellen Sie sicher, dass XClarity Orchestrator bereits v2.0 oder höher ist.

Zu dieser Aufgabe

Die Datei `docker-compose.yml` verwendet die folgenden Umgebungsvariablen, die Sie während der Installation des *ursprünglichen* Containers festgelegt haben. Diese Umgebungsvariablen werden auch vom neuen Container verwendet.

- **CONTAINER_NAME**. Eindeutiger Containername, der zum Erstellen von Docker-Datenträgern für jede XClarity Administrator-Instanz verwendet wird (z. B. `CONTAINER_NAME=LXCA-203`)

  XClarity Administrator verwendet den Containernamen, um die Datenträger für den Container zu erstellen. Wenn Sie denselben Containernamen für den neuen Container verwenden, verwendet die neue XClarity Administrator-Instanz dieselben Datenträger und hat daher Zugriff auf dieselben Systemdaten und -einstellungen wie die ursprüngliche XClarity Administrator-Instanz (Container).

  Wenn Sie den Containernamen ändern, werden neue Datenträger für den Container erstellt und die neue XClarity Administrator-Instanz hat keinen Zugriff auf dieselben Systemdaten und -einstellungen wie die ursprüngliche XClarity Administrator-Instanz (Container). Wenn Sie den Containernamen oder die IP-Adresse ändern müssen, sichern Sie die Systemdaten und -einstellungen für die ursprüngliche XClarity Administrator-Instanz, bevor Sie den neuen Container installieren. Verwenden Sie anschließend diese Sicherung, um die Systemdaten und -einstellungen im neuen Container wiederherzustellen.
- **ADDRESS**. Statische IPv4- oder IPv6-Adresse für den Container (z. B. `ADDRESS=192.0.2.0`).

  Das Ändern der IP-Adresse von XClarity Administrator nach der Verwaltung von Einheiten kann dazu führen, dass die Einheiten in XClarity Administrator in den Offlinestatus versetzt werden. Stellen Sie sicher, dass die Verwaltung aller Einheiten aufgehoben wurde, bevor Sie die IP-Adresse ändern.
- **BACKUP_MOUNT** und **FIRMWARE_MOUNT**. (Optional) Pfade für die Remote-Freigaben, die zum Speichern von Sicherungen von XClarity Administrator oder als Remote-Repository für Firmwareaktualisierungen verwendet werden können. Die Pfade müssen `/mnt/backup_share` bzw. `/mnt/fw_share` sein.

Anmerkung: XClarity Administrator wird *nicht* als privilegierter Container ausgeführt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen XClarity Administrator Container zu aktualisieren.

Schritt 1. Laden Sie das XClarity Administrator Containerimage über Website zum Herunterladen von XClarity Administrator auf eine Client-Workstation herunter. Melden Sie sich auf der Website an und verwenden Sie dann den erhaltenen Zugriffsschlüssel für den Image-Download.

Schritt 2. Importieren Sie das XClarity Administrator-Container-Image mit dem folgenden Befehl in Ihren Docker-Host.

```
docker load -i lnvgy_sw_lxca_1l0-3.5.0_anyos_noarch
```

Schritt 3. Bearbeiten Sie dieselbe `docker-compose.yml`, die für den ursprünglichen Container verwendet wurde. Aktualisieren Sie die Imageeigenschaft oben in der Datei, um auf das neue Docker-Image von Schritt 2 zu verweisen. Sie können das Image-Tag mit dem Befehl `docker tag` ändern.

Nachfolgend finden Sie ein Beispiel für eine YML-Datei mit aktiviertem IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

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

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

Schritt 4. Fahren Sie den *ursprünglichen* Container herunter, indem Sie den folgenden Befehl ausführen.
`docker-compose -p ${CONTAINER_NAME} down`

Schritt 5. Implementieren Sie das *neue* Image in Docker, indem Sie den folgenden Befehl ausführen. Dabei ist <*ENV_FILENAME*> der Name der Datei mit Umgebungsvariablen.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Kapitel 8. XClarity Administrator deinstallieren

Gehen Sie wie folgt vor, um eine virtuelle Lenovo XClarity Administrator Einheit oder einen Container zu deinstallieren.

Vorgehensweise

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

Schritt 1. Heben Sie die Verwaltung für alle Einheiten auf, die gerade von XClarity Administrator verwaltet werden (siehe Gehäuse verwalten, Server verwalten und Switches verwalten in der Online-Dokumentation von XClarity Administrator).

Schritt 2. Deinstallieren Sie XClarity Administrator, je nach Betriebssystem:

- **Docker-compose**Führen Sie den folgenden Befehl aus, um den Container zu stoppen und die Netzwerke und Datenträger zu entfernen.
  ```
  docker-compose down -v
  ```
- **CentOS, Red Hat, Rocky und Ubuntu**
  1. Stellen Sie über Virtual Machine Manager eine Verbindung zum Host her.
  2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Herunterfahren → Ausschalten erzwingen**.
  3. Klicken Sie erneut mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Löschen**. Das Dialogfenster Löschbestätigung wird angezeigt.
  4. Markieren Sie alle Kontrollkästchen und klicken Sie auf **Löschen**.
- **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**.
- **Hyper-V**
  1. Klicken Sie im Dashboard „Server Manager“ auf **Hyper-V**.
  2. Klicken Sie mit der rechten Maustaste auf den Server und klicken Sie dann auf **Hyper-V-Manager**.
  3. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Herunterfahren**.
  4. Klicken Sie erneut mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Löschen**.