



Lenovo XClarity Orchestrator Planungs- und Installationshandbuch



Version 2.1

Anmerkung

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

Zweite Ausgabe (Juli 2024)

© Copyright Lenovo 2020, 2024.

HINWEIS ZU EINGESCHRÄNKTEN RECHTEN: Werden Daten oder Software gemäß einem GSA-Vertrag (General Services Administration) ausgeliefert, unterliegt die Verwendung, Vervielfältigung oder Offenlegung den in Vertrag Nr. GS-35F-05925 festgelegten Einschränkungen.

Inhaltsverzeichnis

Inhaltsverzeichnis	i	Hochverfügbarkeit implementieren (ESXi).	18
Zusammenfassung der Änderungeniii	Kapitel 4. Erstkonfiguration von XClarity Orchestrator ausführen.	21
Kapitel 1. Planen von XClarity Orchestrator	1	Erster Zugriff auf die XClarity Orchestrator-Webschnittstelle	21
Lizenzierung	1	Einen lokale Benutzer erstellen	23
Unterstützte Hardware und Software	2	Netzwerk konfigurieren	25
Firewalls und Proxy-Server	5	Datum und Uhrzeit konfigurieren	28
Portverfügbarkeit	6	Authentifizierungsserver konfigurieren	29
Hinweise zum Netzwerkbetrieb	7	Zusätzliche Sicherheitseinstellungen konfigurieren	33
Sicherheitsaspekte	8	Automatische Problembenachrichtigung (Call-Home-Funktion) konfigurieren und aktivieren	34
Überlegungen zur sicheren Umgebung	8	Weiterleitung von Ereignisdaten einrichten	37
Hinweise zur Verschlüsselung	9	Ressourcenmanager verbinden	38
Hinweise zu Sicherheitszertifikaten	9	Kapitel 5. Lizenzen von XClarity Orchestrator anwenden	43
Erwägungen zum Authentifizierungsserver	10	Kapitel 6. Aktualisieren von XClarity Orchestrator	49
Hinweise zur Zugriffssteuerung	10	Kapitel 7. XClarity Orchestrator deinstallieren.	55
Hinweise zu hoher Verfügbarkeit	10		
Kapitel 2. XClarity Orchestrator installieren	13		
Kapitel 3. Hochverfügbarkeit implementieren	17		
Hochverfügbarkeit implementieren (Hyper-V)	17		

Zusammenfassung der Änderungen

Nachfolgeversionen der Lenovo XClarity Orchestrator-Verwaltungssoftware bieten Unterstützung für neue Softwareverbesserungen und Fixes.

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

Diese Version unterstützt die folgenden Erweiterungen bei der Planung und Installation. Informationen zu Änderungen in früheren Versionen finden Sie unter [Neuerungen](#) in der Onlinedokumentation zu XClarity Orchestrator.

Funktion	Beschreibung
Planung und Installation	XClarity Orchestrator erfordert mindestens 8 virtuelle Prozessorkerne (siehe Unterstützte Hardware und Software).

Kapitel 1. Planen von XClarity Orchestrator

Lizenzierung

Lenovo XClarity Orchestrator ist eine gebührenpflichtige Anwendung. Mit der kostenlosen Testlizenz können Sie XClarity Orchestrator bis zu 90 Tage lang kostenfrei nutzen. Allerdings müssen Sie nach Ablauf der kostenlosen Testversion entsprechende Lizenzen erwerben und installieren, um XClarity Orchestrator-Funktionen weiterhin verwenden zu können und Service und Support für XClarity Orchestrator zu erhalten.

XClarity Orchestrator unterstützt die folgenden Lizenzen.

- **XClarity Orchestrator.** Aktiviert Orchestrator- und Basisverwaltungsfunktionen für Server, Gehäuse, Switches und Speichereinheiten sowie Anspruch auf XClarity Orchestrator Service und Unterstützung. Für Orchestrator-Funktionen ist eine Lizenz in XClarity Orchestrator für jede Einheit erforderlich, die Serverkonfiguration und BS-Implementierung unterstützt. Für Service und Support für XClarity Orchestrator ist eine Lizenz für *jede verwaltete Einheit* erforderlich.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen gültigen XClarity Orchestrator-Lizenzschlüsseln nicht überschreiten. Wenn die Anzahl der XClarity Orchestrator-Lizenzen nicht konform ist (z. B. wenn Lizenzen ablaufen oder wenn die Verwaltung zusätzlicher Einheiten die Gesamtanzahl der aktiven Lizenzen überschreitet), haben Sie eine Kulanzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Wenn die Kulanfrist (einschließlich der kostenlosen Testversion) für Lizenzen endet, bevor die erforderliche Anzahl an Lizenzen installiert ist, werden *alle* Funktionen von XClarity Orchestrator (einschließlich Überwachung, Basisverwaltung und Analysen) für alle Einheiten deaktiviert. Bei Anmeldung werden Sie auf die Seite „Lizenzinformationen“ umgeleitet, auf der Sie weitere Lizenzen übernehmen können.

Wenn Sie z. B. weitere 100 ThinkSystem Server und 20 Rack-Switches mit einer vorhandenen XClarity Administrator-Instanz verwalten, die Sie über XClarity Orchestrator steuern, haben Sie 90 Tage Zeit, um 100 zusätzliche XClarity Orchestrator-Lizenzen zu erwerben und zu installieren, bevor die alle Funktionen in der Benutzerschnittstelle deaktiviert werden. Für die Verwendung der XClarity Orchestrator-Funktionen sind keine Lizenzen für die 20 Rack-Switches erforderlich. Allerdings sind die Lizenzen erforderlich, wenn Sie Service und Support für XClarity Orchestrator wünschen. Wenn die XClarity Orchestrator-Funktionen deaktiviert sind, werden sie erneut aktiviert, sobald Sie genügend Lizenzen für die Konformität installiert haben.

Wichtig: Beachten Sie, dass die XClarity Orchestrator-Basislizenz eine Voraussetzung für die XClarity Pro- und XClarity Orchestrator Analytics-Lizenzen ist. Wenn die Anzahl der XClarity Pro- oder XClarity Orchestrator-Lizenzen *konform* ist, aber die Anzahl der aktiven Basislizenzen *nicht konform* ist, werden alle XClarity Orchestrator-Funktionen (einschließlich Analysefunktionen) für alle Einheiten deaktiviert.

- **Lenovo XClarity Pro.** Aktiviert erweiterte Verwaltungsfunktionen (Serverkonfiguration und BS-Implementierung). Für jede verwaltete Einheit, die die erweiterten Verwaltungsfunktionen unterstützt, ist eine Lizenz in XClarity Orchestrator erforderlich.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen gültigen XClarity Pro-Lizenzschlüsseln nicht überschreiten. Wenn die Anzahl der XClarity Pro-Lizenzen nicht konform ist, haben Sie eine Kulanzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Wenn die Kulanzeit (einschließlich der kostenlosen Testversion) endet, bevor die erforderliche Anzahl an Lizenzen installiert ist, werden die Serverkonfigurations- und BS-Implementierungsfunktionen für *alle Einheiten* deaktiviert.

Weitere Informationen zum Installieren von XClarity Pro-Lizenzen finden Sie unter [Lizenzen und die kostenlose 90-Tage-Testversion](#) in der Onlinedokumentation zu XClarity Administrator.

- **XClarity Orchestrator Analytics.** Aktiviert Analysefunktionen. Für jede verwaltete Einheit, die die erweiterten Verwaltungsfunktionen unterstützt, ist eine Lizenz in XClarity Orchestrator erforderlich.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen aktiven XClarity Orchestrator Analytics-Lizenzschlüsseln nicht überschreiten. Wenn die Anzahl der XClarity Orchestrator Analytics-Lizenzen nicht konform ist (z. B. wenn Lizenzen ablaufen oder wenn die Verwaltung zusätzlicher Einheiten die Gesamtanzahl der aktiven Lizenzen überschreitet), haben Sie eine Kulanzzzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Wenn die Kulanzzzeit (einschließlich der kostenlosen Testversion) endet, bevor die erforderliche Anzahl an Lizenzen installiert ist, werden die Menüs **Überwachung** → **Analysen** deaktiviert und Sie können auf *allen Einheiten* keine Analysenberichte mehr anzeigen oder angepasste Alertregeln oder Abfragen erstellen.

Wichtig: Nach der Installation von XClarity Orchestrator Analytics-Lizenzen müssen Sie die Benutzerschnittstelle aktualisieren.

Anmerkung: Wenn Sie abgelaufene XClarity Orchestrator Analytics-Lizenzen installieren (die ihr Ablaufdatum über die 90-tägige Kulanzzzeit hinaus überschritten haben) und dann die Benutzerschnittstelle aktualisieren, sind die Analysefunktionen deaktiviert. Dies bedeutet, dass ein aktiver Test- oder Kulanzzzeitraum abgebrochen, die Analyseservices angehalten und die Analysefunktionen ausgegraut werden. (Dies kann einige Minuten dauern.) Durch den Import neuer gültiger Lizenzen können Sie die Analysefunktionen wieder aktivieren.

Eine Lizenz ist *nicht* an bestimmte Einheiten gebunden.

Der Aktivierungszeitraum beginnt, wenn die Lizenzen eingelöst werden.

Die Lizenzen werden mithilfe eines *Aktivierungsschlüssels* für die Lizenz installiert. Nachdem Sie Lizenzen eingelöst haben, können Sie einen Aktivierungsschlüssel für alle oder einen Teil der verfügbaren Lizenzen erstellen und dann den Aktivierungsschlüssel in XClarity Orchestrator herunterladen und installieren.

Jedes Mal, wenn XClarity Orchestrator nicht konform ist, wird die Kulanzzzeit auf 90 Tage zurückgesetzt.

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

Wenn Sie eine kostenlose Testlizenz verwenden oder zum Erreichen der Konformität über einen Kulanzzzeitraum verfügen und auf eine neuere Version von XClarity Orchestrator aktualisieren, wird die Testlizenz oder die Kulanzzzeit auf 90 Tage zurückgesetzt.

Bei der Aktualisierung von XClarity Orchestrator oder wenn ein Fehler auftritt, der erfordert, dass die Aktivierungsschlüssel wiederhergestellt werden müssen, können Sie entweder exportierte Aktivierungsschlüssel verwenden oder alle Aktivierungsschlüssel (für jede Kunden-ID) von [Features on Demand-Webportal](#) herunterladen und die Aktivierungsschlüssel (individuell oder zusammen als ZIP-Datei) anschließend in XClarity Orchestrator importieren.

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

Unterstützte Hardware und Software

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

Hostsysteme

XClarity Orchestrator wird in einer virtuellen Einheit auf einem Hostsystem ausgeführt.

Hypervisor-Anforderungen

Die folgenden Hypervisoren werden für die Installation von XClarity Orchestrator unterstützt.

- Microsoft Windows Server 2019 mit installiertem Hyper-V
- Microsoft Windows Server 2022 mit installiertem Hyper-V
- VMware ESXi 7.0
- VMware ESXi 6.7, U1, U2 und U3
- VMware ESXi 6.5, U1 und U2

Bei Hyper-V ist die virtuelle Einheit ein virtuelles Festplatten-Image (VHD). Bei VMware ESXi ist die virtuelle Einheit eine OVF-Vorlage.

Hardwarevoraussetzungen

Für die virtuelle Einheit gelten die unten stehenden *Mindestanforderungen*. Je nach Größe Ihrer Umgebung und Ihrer Verwendung von Bereitstellungsfunktionen (wie Betriebssystemimplementierung, Firmwareaktualisierungen und Serverkonfigurationen) sind möglicherweise zusätzliche Ressourcen notwendig, um eine optimale Leistung zu erreichen.

- 8 virtuelle Prozessorkerne
- 16 GB-Hauptspeicher
- 551 GB-Speicher über zwei angeschlossene Festplatten.
 - Mindestens 251 GB für die virtuelle Einheit (Datenträger 0)
 - 100 GB für das Aktualisierungs-Repository (Datenträger 1)
 - 200 GB für das BS-Images-Repository (Datenträger 2)

Wichtig: Sie können die Größe des Datenträgers, der für das Aktualisierungs-Repository und das BS-Images-Repository verwendet wird, weder erhöhen noch verringern.

Softwarevoraussetzungen

Die folgende Software wird von XClarity Orchestrator benötigt.

- **Authentifizierungsserver.** XClarity Orchestrator verwendet standardmäßig einen lokalen LDAP-Server (Lightweight Directory Access Protocol) für die Authentifizierung. Wenn Sie einen externen Authentifizierungsserver verwenden, werden die folgenden LDAP-Server unterstützt:
 - Microsoft Active Directory, unter Windows Server 2008 oder höher ausgeführt
- **NTP-Server.** Um sicherzustellen, dass die Zeitstempel für alle Ereignisse und Alerts synchronisiert werden, die mit XClarity Orchestrator von Ressourcenmanagern und verwalteten Einheiten empfangen werden, ist ein NTP-Server (Network Time Protocol) erforderlich. Vergewissern Sie sich, dass der Zugriff über das Verwaltungsnetzwerk (in der Regel über die Eth0-Schnittstelle) auf den NTP-Server funktioniert. Erwägen Sie, das lokale System, auf dem XClarity Orchestrator installiert ist, als NTP-Server zu verwenden. Wenn Sie sich dafür entscheiden, stellen Sie sicher, dass über das Verwaltungsnetzwerk auf das lokale System zugegriffen werden kann.

Verwaltbare Ressourcen

XClarity Orchestrator kann eine unbegrenzte Anzahl von Ressourcenmanagern unterstützen, die zusammen insgesamt maximal 10,000 Einheiten verwalten.

XClarity Orchestrator unterstützt die folgenden Ressourcenmanager.

- **Lenovo XClarity Management Hub 2.0** XClarity Orchestrator verwaltet und überwacht Einheiten, die von XClarity Management Hub 2.0 verwaltet werden. Jede XClarity Management Hub 2.0 Instanz kann bis zu 5,000 Einheiten verwalten.

Wichtig: Erweiterte Funktionen (z. B. Betriebssystembereitstellung und Serverkonfiguration mithilfe von Konfigurationsmustern) werden von diesem Verwaltungshub nicht unterstützt.

Sie finden eine vollständige Liste der unterstützten Einheiten und Zusatzeinrichtungen (z. B. E/A-, DIMM- und Speicheradapter), die mindestens erforderlichen Firmwareversionen und Einschränkungen der [Webseite für XClarity Management Hub 2.0](#).

Allgemeine Informationen zu Hardwarekonfigurationen und Optionen für eine bestimmte Einheit finden Sie unter [Lenovo Server Proven-Website](#).

- **Lenovo XClarity Management Hub**XClarity Orchestrator führt die Verwaltung, Überwachung und Bereitstellung von Einheiten durch, die von XClarity Management Hub verwaltet werden. Jede XClarity Management Hub Instanz kann bis zu **10.000** ThinkEdge Client-Einheiten verwalten.

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

Allgemeine Informationen zu Hardwarekonfigurationen und Optionen für eine bestimmte Einheit finden Sie unter [Lenovo Server Proven-Website](#).

- **Lenovo XClarity Administrator** v2.6 oder höherXClarity Orchestrator führt die Verwaltung, Überwachung und Bereitstellung von physischen Einheiten durch, die von XClarity Administrator verwaltet werden. Jede XClarity Administrator Instanz kann bis zu **1.000** Einheiten (Server, Gehäuse, Switches und Speicher) verwalten.

XClarity Orchestrator unterstützt alle Einheiten, die von unterstützt XClarity Administrator und XClarity Management Hub werden (wenn nicht anders vermerkt). Eine vollständige Liste der unterstützten Einheiten und Zusatzeinrichtungen (z. B. E/A-, DIMM- und Speicheradapter), die mindestens erforderlichen Firmwareversionen und Einschränkungen finden Sie auf den folgenden Lenovo XClarity Support-Webseiten.

- [ThinkAgile, ThinkEdge, ThinkSystem, System x, Converged HX und NeXtScale Server](#)
- [Flex System und ThinkSystem Einheiten im Gehäuse](#)
- [ThinkServer-Server](#)
- [Switches](#)
- [Speichereinheiten](#)

Allgemeine Informationen zu Hardwarekonfigurationen und Optionen für eine bestimmte Einheit finden Sie unter [Lenovo Server Proven-Website](#).

Anmerkung: Die BS-Implementierungsfunktion erfordert XClarity Administrator v4.0 oder höher.

- **Schneider Electric EcoStruxure IT Expert**XClarity Orchestrator verwaltet und überwacht Infrastrukturressourcen wie z. B. PDUs und USUs, die von EcoStruxure IT Expert verwaltet werden.
- **VMware vRealize Operations Manager**XClarity Orchestrator überwacht die Metriken für virtuelle Workloads von vRealize Operations Manager.

Anmerkung: vRealize Operations Manager ist nicht in der Liste der Ressourcenmanager enthalten, da es keine Einheiten in XClarity Orchestrator verwaltet.

Webbrowser

Die XClarity Orchestrator-Webschnittstelle funktioniert mit den folgenden Webbrowsern.

- Chrome 80.0 oder höher
- Firefox ESR 68.6.0 oder höher
- Microsoft Edge 40.0 oder höher
- Safari 13.0.4 oder höher (ausgeführt auf macOS 10.13 oder höher)

Software anderer Anbieter

XClarity Orchestrator kann in die folgende Software integriert werden.

- Splunk v7.0.3 und höher (siehe [XClarity Orchestrator-App für Splunk – Benutzerhandbuch](#))

Firewalls und Proxy-Server

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

Firewalls

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

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

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

Proxy-Server

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

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

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

Portverfügbarkeit

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

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

XClarity Orchestrator

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

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

Service	Ausgehend (Ports auf externen Systemen geöffnet)	Eingehend (Ports auf der XClarity Orchestrator-Einheit geöffnet)
XClarity Orchestrator-Anwendung	<ul style="list-style-type: none"> DNS – TCP/UDP an Port 53 	<ul style="list-style-type: none"> HTTPS – TCP an Port 443
Externe Authentifizierungsserver	<ul style="list-style-type: none"> LDAP– TCP an Port 389¹ 	Nicht zutreffend
Ereignisweiterleitungsservices	<ul style="list-style-type: none"> E-Mail-Server (SMTP) – UDP an Port 25¹ REST-Web-Service (HTTP) – UPD an Port 80¹ Splunk – UDP an Port 8088¹¹, 8089¹ Syslog – UDP an Port 514¹ 	Nicht zutreffend
Lenovo Service (einschließlich Call-Home-Funktion)	<ul style="list-style-type: none"> HTTPS (Call-Home-Funktion) – TCP an Port 443 	Nicht zutreffend

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

XClarity Management Hub 2.0

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

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

Service oder Komponente	Ausgehend (Ports zu externen Systemen geöffnet)	Eingehend (Ports auf Zieleinheiten geöffnet)
XClarity Management Hub 2.0	<ul style="list-style-type: none"> • DNS – UDP an Port 53 • NTP – UDP an Port 123 • HTTPS – TCP an Port 443 • SSDP – UDP an Port 1900 • DHCP – UDP an Port 67 	<ul style="list-style-type: none"> • HTTPS – TCP an Port 443 • SSDP Replay – UDP an Ports 32768-65535
ThinkSystem und ThinkAgile Server	<ul style="list-style-type: none"> • HTTPS – TCP an Port 443 • SSDP-Erkennung – UDP an Port 1900 	<ul style="list-style-type: none"> • HTTPS – TCP an Port 443

XClarity Management Hub

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

Service oder Komponente	Ausgehend (Ports auf externen Systemen geöffnet)	Eingehend (Ports auf der XClarity Management Hub Einheit geöffnet)
XClarity Management Hub-Einheit ¹	<ul style="list-style-type: none"> • DNS – TCP/UDP an Port 53² 	<ul style="list-style-type: none"> • HTTPS – TCP an Port 443 • MQTT – TCP an Port 8883
ThinkEdge Client-Einheiten ³	Nicht zutreffend	<ul style="list-style-type: none"> • MQTT – TCP an Port 8883

1. Bei der Verwendung von XClarity Management Hub zur Verwaltung von Einheiten über XClarity Orchestrator müssen bestimmte Ports geöffnet sein, um die Kommunikation zu erleichtern. Wenn die erforderlichen Ports von einem anderen Prozess blockiert oder verwendet werden, können einige XClarity Orchestrator-Funktionen möglicherweise nicht ordnungsgemäß ausgeführt werden.
2. XClarity Management Hub kann optional für ausgehende Verbindungen zu externen Services konfiguriert werden. Diese Verbindungen erfordern zudem möglicherweise Zugriff auf einen DNS-Server (Domain Name Service) über TCP oder UDP-Port 53, um externe Servernamen aufzulösen.
3. Wenn sich verwaltbare Einheiten hinter einer Firewall befinden und Sie beabsichtigen, diese Einheiten über einen XClarity Management Hub außerhalb der Firewall zu verwalten, müssen alle an der Kommunikation zwischen XClarity Management Hub und den Edge-Einheiten beteiligten Ports geöffnet sein.

XClarity Administrator

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

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

Hinweise zum Netzwerkbetrieb

XClarity Orchestrator verwendet ein einzelnes Subnetz (eth0) für die Verwaltung und Datenkommunikation. Lesen Sie vor der Netzwerkkonfiguration die folgenden Hinweise.

- Die Netzwerkschnittstelle wird für Ermittlung und Verwaltung verwendet. Sie muss mit allen Einheiten kommunizieren können, die Sie verwalten möchten.

- Wenn Sie beabsichtigen, gesammelte Servicedaten manuell an den Lenovo Support zu senden oder die automatische Problembenachrichtigung (Call-Home-Funktion) zu verwenden, müssen die Schnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.
- Wenn Sie die IP-Adresse der virtuellen Einheit von XClarity Orchestrator nach der Verbindung der Ressourcenmanager ändern, verliert XClarity Orchestrator die Verbindung mit den Managern und diese erscheinen offline. Wenn Sie die IP-Adresse der virtuellen Einheit ändern müssen, sobald XClarity Orchestrator betriebsbereit ist, stellen Sie sicher, dass die Verbindung aller Ressourcenmanager getrennt (gelöscht) wird, bevor Sie die IP-Adresse ändern.
- Konfigurieren Sie die Einheiten und die Gehäusekomponenten so, dass möglichst wenige IP-Adressen geändert werden. Ziehen Sie in Betracht, statische IP-Adressen anstelle des Dynamic Host Configuration Protocol (DHCP) zu verwenden. Stellen Sie bei Verwendung von DHCP sicher, dass die IP-Adressänderungen minimiert werden, z. B. durch Basieren der DHCP-Adresse auf einer MAC-Adresse oder dem Konfigurieren von DHCP ohne Ablauf der Zugangsberechtigung. Wenn sich die IP-Adresse ändert, müssen Sie die Verbindung der verwalteten Einheiten zunächst aufheben (löschen) und sie anschließend erneut verbinden.
- Network Address Translation (NAT), die einen IP-Adressraum in einen anderen neu zuordnet, wird nicht unterstützt.

Sicherheitsaspekte

Lesen Sie die folgenden Hinweise, die Ihnen bei der Planung für die Sicherheit von Lenovo XClarity Orchestrator und allen verwalteten Ressourcen helfen können.

Überlegungen zur sicheren Umgebung

Es ist unerlässlich, dass Sie die Sicherheitsanforderungen in Ihrer Umgebung prüfen, alle Sicherheitsrisiken kennen und die entsprechenden Risiken minimieren. Lenovo XClarity Orchestrator umfasst mehrere Funktionen, die Sie bei der Absicherung Ihrer Umgebung unterstützen. Die folgenden Informationen unterstützen Sie bei der Implementierung eines Sicherheitsplans für Ihre Umgebung.

Wichtig: Sie sind für die Auswertung, Auswahl und Implementierung der Sicherheitseinrichtungen, Konfigurationsprozeduren und entsprechenden Kontrollmöglichkeiten für Ihre Umgebung verantwortlich. Bedenken Sie, dass Ihre Umgebung mit den in diesem Abschnitt beschriebenen Sicherheitseinrichtungen nicht vollständig geschützt werden kann.

Beim Abwägen der Sicherheitsanforderungen für Ihre Umgebung sollten Sie Folgendes berücksichtigen:

- Die physische Sicherheit Ihrer Umgebung ist von Bedeutung. Beschränken Sie den Zugriff auf Räume und Racks, in denen Systemmanagement-Hardware aufbewahrt wird.
- Schützen Sie Ihre Netzwerkhardware und -daten mithilfe einer softwarebasierten Firewall vor bekannten und neuen Sicherheitsbedrohungen wie Viren und unbefugten Zugriffen.
- Ändern Sie nicht die Standardsicherheitseinstellungen für Netzwerkschalter und Pass-through-Module. Mit den werkseitigen Standardeinstellungen für diese Komponenten wird die Verwendung nicht sicherer Protokolle deaktiviert und die Verwendung signierter Firmwareaktualisierungen erzwungen.
- Sorgen Sie dafür, dass zumindest kritische Firmwareaktualisierungen installiert werden. Nach jeder Änderung sollte eine Sicherungskopie der Konfiguration erstellt werden.
- Stellen Sie sicher, dass alle sicherheitsspezifischen Updates für DNS-Server unverzüglich installiert werden und der Schutz dieser Server immer aktuell ist.
- Weisen Sie Ihre Benutzer an, keine Zertifikate zu akzeptieren, die nicht vertrauenswürdig sind. Siehe [Mit Sicherheitszertifikaten arbeiten](#) in der Onlinedokumentation zu XClarity Orchestrator für weitere Informationen.

- Bringen Sie die Hardware für die Systemverwaltung nach Möglichkeit in einem eigenen Teilnetz unter. In der Regel sollten keine Benutzer, sondern nur Supervisoren Zugang zu dieser Hardware haben.
- Verwenden Sie keine Kennwörter, die leicht zu erraten sind, wie beispielsweise „Kennwort“ oder den Namen Ihres Unternehmens. Bewahren Sie die Kennwörter an einem sicheren Ort auf und schränken Sie den Zugriff auf die Kennwörter ein. Führen Sie eine Kennwortrichtlinie für Ihr Unternehmen ein.

Wichtig: Für alle Benutzer sollten strikte Kennwortrichtlinien gelten.

- Richten Sie für Benutzer Startkennwörter ein. Auf diese Weise können Sie den Zugriff auf die Daten und Konfigurationsprogramme der Server steuern. Weitere Informationen zu Startkennwörtern finden Sie in der Dokumentation Ihrer Hardware.

Hinweise zur Verschlüsselung

Lenovo XClarity Orchestrator unterstützt TLS 1.2 und stärkere Verschlüsselungsalgorithmen für sichere Netzwerkverbindungen.

Für eine höhere Sicherheit werden nur hohe Verschlüsselungsgrade unterstützt. Ihr Clientbetriebssystem und Ihre Webbrowser müssen eines der folgenden Verschlüsselungssysteme unterstützen.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

Hinweise zu Sicherheitszertifikaten

Lenovo XClarity Orchestrator verwendet Zertifikate für die Einrichtung von sicheren und vertrauenswürdigen Kommunikationsverbindungen zwischen XClarity Orchestrator und den Ressourcenmanagern (z. B. Lenovo XClarity Administrator oder Schneider Electric EcoStruxure IT Expert) sowie für die Herstellung von Kommunikationsverbindungen mit XClarity Orchestrator durch Benutzer oder verschiedenen Services. Standardmäßig verwenden XClarity Orchestrator und Lenovo XClarity Administrator selbst signierte, von XClarity Orchestrator generierte Zertifikate, die von einer internen Zertifizierungsstelle ausgestellt wurden.

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

Erwägungen zum Authentifizierungsserver

Sie können auswählen, ob der lokale LDAP-Server (Lightweight Directory Access Protocol) oder ein anderer externer LDAP-Server als Authentifizierungsserver verwendet werden soll.

Der *Authentifizierungsserver* ist eine Benutzerregistrierung, die zum Authentifizieren von Benutzeranmeldeinformationen verwendet wird. Lenovo XClarity Orchestrator unterstützt zwei Typen von Authentifizierungsservern:

- **Lokaler Authentifizierungsserver.** Standardmäßig ist XClarity Orchestrator für die Verwendung des lokalen (eingebetteten) LDAP-Servers konfiguriert, der sich auf dem Orchestrator-Server befindet.
- **Externer LDAP-Server.** Microsoft Active Directory wird als externer LDAP-Server unterstützt. Dieser Server muss sich auf einem externen Microsoft Windows-Server befinden, der mit dem Verwaltungsnetzwerk verbunden ist.

Weitere Informationen zum Konfigurieren eines externen LDAP-Servers finden Sie unter .

Hinweise zur Zugriffssteuerung

Lenovo XClarity Orchestrator verwendet *Zugriffssteuerungslisten* (ACLs, Access Control Lists) um festzulegen, auf welche Ressourcen (Einheiten, Ressourcenmanager und XClarity Orchestrator) Benutzer zugreifen können. Wenn ein Benutzer Zugriff auf eine bestimmte Ressourcengruppe hat, kann dieser Benutzer Daten (z. B. Bestand, Ereignisse, Alerts und Analysen) anzeigen, die sich nur auf diese Ressourcen beziehen.

Zu dieser Aufgabe

Eine ACL ist eine Gruppe von Benutzergruppen und Ressourcengruppen.

- *Benutzergruppen* identifizieren die Benutzer, die von dieser ACL betroffen sind. Die ACL muss eine einzelne Benutzergruppe enthalten. Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, haben immer Zugriff auf alle Ressourcen. Sie können den Ressourcenzugriff für Supervisor-Benutzer nicht einschränken.

Wenn der ressourcenbasierte Zugriff aktiviert ist, haben Benutzer, die *nicht* Mitglied einer Gruppe sind, der die vordefinierte Rolle **Supervisor** zugewiesen ist, standardmäßig keinen Zugriff auf Ressourcen (Einheiten und Ressourcenmanager). Sie müssen Benutzer ohne Supervisor-Berechtigungen zu einer Benutzergruppe hinzufügen, die Teil einer Zugriffssteuerungsliste ist, damit diese Benutzer auf bestimmte Ressourcengruppen zugreifen können.

Wenn der ressourcenbasierte Zugriff deaktiviert ist, haben alle Benutzer standardmäßig Zugriff auf alle Ressourcen (Einheiten und Ressourcenmanager).

- *Ressourcengruppen* identifizieren die Ressourcen (Einheiten, Ressourcenmanager und XClarity Orchestrator), auf die zugegriffen werden kann. Die ACL muss mindestens eine Ressourcengruppe enthalten.

Anmerkung: Ein Benutzer, der auf eine Managergruppe zugreifen kann, erhält nicht automatisch Zugriff auf alle Einheiten, die von diesem Ressourcenmanager verwaltet werden. Sie müssen den Zugriff auf Einheiten explizit mithilfe von Einheitengruppen erteilen.

Weitere Informationen zu Zugriffssteuerungslisten finden Sie unter [Zugriff auf Ressourcen steuern](#) in der Onlinedokumentation zu XClarity Orchestrator.

Hinweise zu hoher Verfügbarkeit

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

Microsoft Hyper-V

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

VMware ESXi

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

VMware High Availability erfordert die folgenden Komponenten.

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

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

VMware vCenter kann auf einem der Hosts installiert werden, die im Cluster verwendet werden. Wenn dieser Host allerdings ausgeschaltet oder nicht einsetzbar ist, geht auch der Zugriff auf die VMware vCenter-Schnittstelle verloren.

- Gemeinsam genutzter Speicher (Datenspeicher), auf den von allen Hosts im Cluster zugegriffen werden kann. Sie können jeden Typ gemeinsam genutzten Speicher verwenden, der von VMware unterstützt wird. Der Datenspeicher wird von VMware verwendet, um zu bestimmen, ob eine VM einen Failover zu einem anderen Host ausführen soll (Taktsignale).

Kapitel 2. XClarity Orchestrator installieren

Installieren und konfigurieren Sie die virtuelle Einheit von Lenovo XClarity Orchestrator auf einem System in Ihrer lokalen Umgebung.

Vorbereitende Schritte

Stellen Sie sicher, dass die Voraussetzungen für XClarity Orchestrator erfüllt werden, einschließlich der Anforderungen und Empfehlungen für die Hardware (siehe [Unterstützte Hardware und Software](#)).

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

Vergewissern Sie sich, dass die Ressourcenmanager, die verwaltet werden sollen, unterstützt werden und die entsprechenden Versionen aufweisen (siehe [Unterstützte Hardware und Software](#)).

Informationen zur Aktualisierung einer bereits installierten virtuellen XClarity Orchestrator-Einheit finden Sie unter [Aktualisieren von XClarity Orchestrator](#).

Informationen zum Einrichten einer Hochverfügbarkeitsumgebung finden Sie unter [Hochverfügbarkeit implementieren](#).

Lenovo XClarity Orchestrator ist eine gebührenpflichtige Anwendung. Mit der kostenlosen Testlizenz können Sie XClarity Orchestrator bis zu 90 Tage lang kostenfrei nutzen. Allerdings müssen Sie nach Ablauf der kostenlosen Testversion entsprechende Lizenzen erwerben und installieren, um XClarity Orchestrator-Funktionen weiterhin verwenden zu können und Service und Support für XClarity Orchestrator zu erhalten. Informationen zum Kauf von Lizenzen erhalten Sie von Ihrem Lenovo Ansprechpartner oder autorisierten Business Partner. Weitere Informationen zum Installieren der Lizenz finden Sie unter [Lizenzen von XClarity Orchestrator anwenden](#).

Zu dieser Aufgabe

Sie können die IP-Adresse der virtuellen Einheit mithilfe einer statischen IP-Adresse auf dem eth0-Port während der Konfiguration zuordnen.

Wenn Sie keine IP-Adresse während der Konfiguration zuweisen, werden IP-Einstellungen standardmäßig mithilfe des Dynamic Host Configuration Protocol (DHCP) zugewiesen, wenn Sie die virtuelle Einheit zum ersten Mal starten. Sie können die IP-Einstellungen von XClarity Orchestrator beim erstmaligen Starten der virtuellen Einheit konfigurieren. Stellen Sie sicher, dass Sie über die erforderlichen IP-Informationen verfügen, bevor Sie starten. Sie haben maximal 60 Sekunden, um die Einstellungen bei jeder Eingabeaufforderung einzugeben.

- Für statische IPv4-Einstellungen können Sie die IP-Adresse, die Subnetzmaske, die IP-Adresse des Gateways und die IP-Adresse des DNS-Servers 1 (optional) und DNS-Servers 2 (optional) ändern.
- Für statische IPv6-Einstellungen können Sie die IP-Adresse, die Präfixlänge und die IP-Adresse des DNS-Servers 1 (optional) und DNS-Servers 2 (optional) ändern.
- Bei DHCP-Einstellungen können Sie die Einstellungen für die primäre und die Loopback-Schnittstelle ändern („auto lo“, „iface lo inet loopback“, „auto eth0“ und „iface eth0 inet dhcp“).

Achtung: Wenn Sie die IP-Adresse der virtuellen Einheit von XClarity Orchestrator nach der Verbindung der Ressourcenmanager ändern, verliert XClarity Orchestrator die Kommunikation mit den Managern und diese erscheinen offline. Wenn Sie die IP-Adresse der virtuellen Einheit ändern müssen, sobald XClarity

Orchestrator betriebsbereit ist, stellen Sie sicher, dass die Verbindung aller Ressourcenmanager aufgehoben (gelöscht) wird, bevor Sie die IP-Adresse ändern. Weitere Informationen zum Festlegen von IP-Adressen finden Sie unter [Netzwerk konfigurieren](#).

Vorgehensweise

Gehen Sie wie folgt vor, um die virtuelle XClarity Orchestrator-Einheit zu installieren.

Schritt 1. Laden Sie das XClarity Orchestrator-Image von [XClarity Orchestrator Downloads-Website](#) auf das lokale System herunter. Melden Sie sich auf der Website an und verwenden Sie dann den erhaltenen Zugriffsschlüssel für den Image-Download.

Bei Hyper-V ist die virtuelle Einheit ein virtuelles Festplatten-Image (VHD). Bei VMware ESXi ist die virtuelle Einheit eine OVF-Vorlage.

Schritt 2. Installieren und konfigurieren Sie die virtuelle Einheit auf dem lokalen System.

- **Für ESXi mit VMware vSphere**

1. Stellen Sie über VMware vSphere Client eine Verbindung zum Host her.
2. Klicken Sie mit der rechten Maustaste auf **Virtuelle Maschinen → VM erstellen/registrieren → Eine virtuelle Maschine aus einer OVF- oder OVA-Datei implementieren**.
3. Führen Sie die einzelnen Schritte im Implementierungsassistenten für die virtuelle Einheit aus. Beachten Sie im Assistenten die folgenden Aspekte:
 - **Einheitenname**. Wählen Sie einen Namen aus, der auf diesem Host eindeutig ist.
 - **Storage**. Wählen Sie einen Datenspeicher aus, auf dem mindestens 551 GB an Speicher verfügbar sind.
 - **Datenträgerformat**. Wählen Sie das Datenträgerformat aus, das die Anforderungen Ihrer Organisation erfüllt. Wenn Sie in Bezug auf das Format nicht sicher sind, wählen Sie **Thin Provision** aus.
 - **Weitere Einstellungen**. Aktualisieren Sie optional die Netzwerkkonfiguration für die virtuelle Einheit, um die statische IP-Adresse für die eth0-Schnittstelle festzulegen.

- **Für ESXi mit VMware vCenter**

1. Stellen Sie über VMware vCenter eine Verbindung zum Host her.
2. Klicken Sie unter „Hosts und Cluster“ oder „VMs und Vorlagen“ mit der rechten Maustaste auf den Host und dann auf **Datei → OVF-Vorlage implementieren**.
3. Führen Sie die einzelnen Schritte im Implementierungsassistenten für die virtuelle Einheit aus. Beachten Sie im Assistenten die folgenden Aspekte:
 - **Einheitenname**. Wählen Sie einen Namen aus, der auf diesem Host eindeutig ist.
 - **Storage**. Wählen Sie einen Datenspeicher aus, auf dem mindestens 551 GB an Speicher verfügbar sind.
 - **Datenträgerformat**. Wählen Sie das Datenträgerformat aus, das die Anforderungen Ihrer Organisation erfüllt. Wenn Sie in Bezug auf das Format nicht sicher sind, wählen Sie **Thin Provision** aus.
 - **Vorlage anpassen**. Aktualisieren Sie optional die Netzwerkkonfiguration für die virtuelle Einheit, um die statische IP-Adresse für die eth0-Schnittstelle festzulegen.
4. Gehen Sie wie folgt vor, wenn Sie die statische IP-Adresse für die virtuelle Einheit festgelegt haben.
 - a. Wählen Sie die VM im Bestand aus.
 - b. Klicken Sie auf **Konfigurieren → vApp** und wählen Sie dann **vApp-Optionen aktivieren** aus.

- c. Wählen Sie nach dem Aktivieren **OVF-Umgebung** für das IP-Zuordnungsschema aus.
- d. Wählen Sie auf der Registerkarte **OVF-Details** die Option „VMware-Tools“ für den **OVF-Umgebungstransport** aus.

- **Für Microsoft Hyper-V**

1. Klicken Sie im Server-Manager-Dashboard auf **Hyper-V**.
2. Klicken Sie mit der rechten Maustaste auf den Server und klicken Sie dann auf **Hyper-V-Manager**.
3. Klicken Sie unter **Aktionen** auf **Neu → Virtuelle Maschine**, damit der Assistent für neue virtuelle Maschine gestartet wird. Klicken Sie dann auf **Weiter**.
4. Geben Sie auf der Seite Name und Speicherort angeben einen Namen für die neue virtuelle Maschine ein, z. B. LXC0-*{version}*.
5. Wählen Sie auf der Seite Generation angeben die Option **Generation 1** aus.
6. Wählen Sie auf der Seite Speicher zuweisen mindestens 16 GB Speicher aus, die für diese virtuelle Maschine verwendet werden sollen (siehe [Unterstützte Hardware und Software](#)).
7. Wählen Sie auf der Seite Netzwerk konfigurieren den virtuellen Switch aus, den Sie bei der Hostinstallation und -konfiguration erstellt haben.
8. Klicken Sie auf der Seite Virtuelle Festplatte verbinden auf **Vorhandene virtuelle Festplatte verwenden**, navigieren Sie zu dem Speicherort, zu dem Sie das XClarity Orchestrator VHD-Image kopiert haben, und wählen Sie das Image ***disk001*.vhd** aus.
9. Klicken Sie auf **Fertig stellen**.
10. Klicken Sie mit der rechten Maustaste auf die gerade erstellte virtuelle Maschine und klicken Sie dann auf **Einstellungen**.
11. Konfigurieren Sie die Anzahl der Prozessoren, die der virtuellen Maschine zugeordnet werden sollen.
 - a. Wählen Sie **Prozessor** aus und geben Sie mindestens 8 virtuelle Prozessoren an, die für diese virtuelle Maschine verwendet werden sollen (siehe [Unterstützte Hardware und Software](#)).
 - b. Klicken Sie auf **Übernehmen** und auf **OK**.
12. Fügen Sie das zweite Festplattenlaufwerk zur virtuellen Einheit hinzu.
 - a. Erweitern Sie **IDE Controller 0** und wählen Sie **Festplattenlaufwerk** aus.
 - b. Navigieren Sie im Feld **Virtuelle Festplatte** zu dem Speicherort, an den Sie die XClarity Orchestrator VHD-Images kopiert haben, und wählen Sie das Image ***disk002*.vhd** aus.
 - c. Klicken Sie auf **Übernehmen** und auf **OK**.
13. Fügen Sie das dritte Festplattenlaufwerk zur virtuellen Einheit hinzu.
 - a. Erweitern Sie **IDE Controller 1** und wählen Sie **Festplattenlaufwerk** aus.
 - b. Navigieren Sie im Feld **Virtuelle Festplatte** zu dem Speicherort, an den Sie die XClarity Orchestrator VHD-Images kopiert haben, und wählen Sie das Image ***disk003*.vhd** aus.
 - c. Klicken Sie auf **Übernehmen** und auf **OK**.
14. (Optional) Sie können eine statische MAC-Adresse für jeden Netzwerkadapter festlegen, indem Sie **Netzwerkadapter** für den virtuellen Switch erweitern, auf **Erweiterte Funktionen** und anschließend unter der **MAC-Adresse** auf **Statisch** klicken und zuletzt die MAC-Adresse angeben.

Schritt 3. Schalten Sie die virtuelle Einheit ein.

Beim Start der virtuellen Einheit werden die IPv4- und IPv6-Adressen, die von DHCP zugewiesen wurden, für die einzelnen Schnittstellen aufgeführt, wie im folgenden Beispiel dargestellt.

Lenovo XClarity Orchestrator Version x.x.x

```
-----  
eth0    Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56  
        inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0  
        inet6 addr: 2001:db8:56ff:fe80:bea3/64  Scope:Link  
  
=====
```

```
=====
```

You have 118 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
3. To select subnet for Lenovo XClarity virtual appliance internal network
- x. To continue without changing IP settings

... ..

Schritt 4. Optional können Sie die IP-Einstellungen für die virtuelle Einheit über die Konsole konfigurieren. Wenn Sie nicht innerhalb der festgelegten Zeit eine Auswahl treffen oder wenn Sie x eingeben, wird der erste Start mit den standardmäßig zugewiesenen IP-Einstellungen fortgesetzt.

- **Weisen Sie statische IP-Adressen für den eth0-Port zu.** Geben Sie 1 ein und befolgen Sie die Anweisungen, um die Einstellungen zu ändern.
- **Weisen Sie mithilfe von DHCP neue statische IP-Adressen für den eth0-Port zu.** Geben Sie 2 ein und befolgen Sie die Anweisungen, um die Einstellungen zu ändern.
- **Wählen Sie das Subnetz für das interne Netzwerk der virtuellen Einheit aus.** Geben Sie 3 ein und befolgen Sie die Anweisungen, um die Einstellungen zu ändern. Standardmäßig verwendet XClarity Orchestrator das Subnetz **192.168.252.0/24** für sein internes Netzwerk. Wenn sich dieses Subnetz mit dem Hostnetzwerk überschneidet, ändern Sie das Subnetz in eine der anderen verfügbaren Optionen, um Netzwerkprobleme zu vermeiden.
 - 192.168.252.0/24
 - 172.31.252.0/24
 - 10.255.252.0/24

Wichtig: Wenn Sie ungültige Werte angeben, wird ein Fehler zurückgegeben. Sie haben bis zu vier Versuche, gültige Werte einzugeben.

Nach dieser Aufgabe

Melden Sie sich bei XClarity Orchestrator an und nehmen Sie die Konfiguration vor.

Kapitel 3. Hochverfügbarkeit implementieren

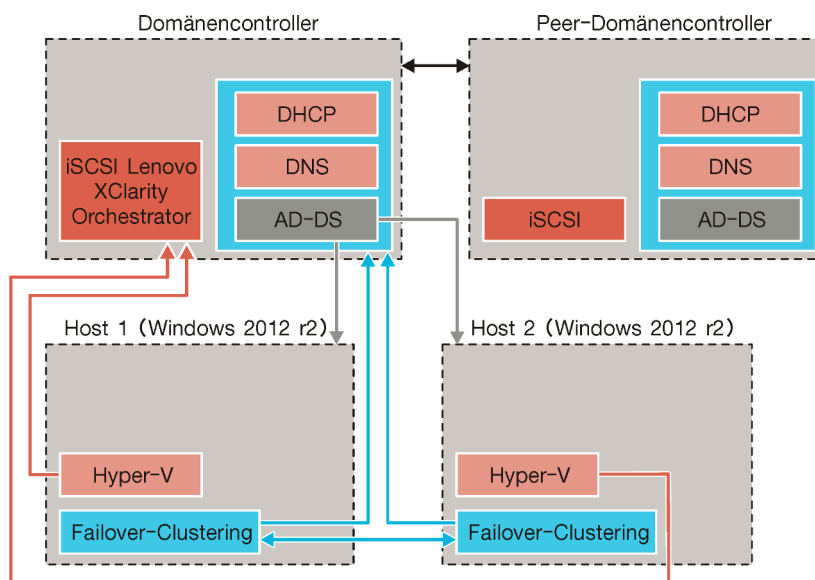
Um Hochverfügbarkeit für Lenovo XClarity Orchestrator zu implementieren, verwenden Sie die Hochverfügbarkeitsfunktion der Hostumgebung.

Hochverfügbarkeit implementieren (Hyper-V)

Um Hochverfügbarkeit für Lenovo XClarity Orchestrator in einer Microsoft Hyper-V-Umgebung zu implementieren, verwenden Sie die Hochverfügbarkeitsfunktion, die von Hyper-V bereitgestellt wird.

Zu dieser Aufgabe

Die folgende Abbildung bietet eine allgemeine Übersicht über eine Möglichkeit, Hochverfügbarkeit für XClarity Orchestrator in einer Hyper-V-Umgebung zu implementieren. In diesem Beispiel wird das XClarity Orchestrator-Image im gemeinsam genutzten Speicher mit Cluster-Zugriff installiert.



Vorgehensweise

Gehen Sie wie folgt vor, um eine Hochverfügbarkeitsumgebung einzurichten.

Schritt 1. Installieren Sie den Domänencontroller.

- Führen Sie die DHCP-Erstkonfiguration aus.
- Konfigurieren Sie DNS.
- Richten Sie AD DS (Active Directory-Domänendienste) ein.
- Schließen Sie die DHCP-Konfiguration ab.

Schritt 2. Richten Sie den ersten Host ein.

- Installieren Sie Microsoft Windows 2012 R2.
- Fügen Sie ihn zur AD DS-Domäne hinzu.
- Fügen Sie folgende Funktionen hinzu.
 - Hyper-V
 - Failover-Clustering

Schritt 3. Richten Sie den zweiten Host ein.

- a. Installieren Sie Microsoft Windows 2012 R2.
- b. Fügen Sie ihn zur AD DS-Domäne hinzu.
- c. Fügen Sie folgende Funktionen hinzu.
 - Hyper-V
 - Failover-Clustering

Schritt 4. Konfigurieren Sie den gemeinsam genutzten Speicher (wie iSCSI) auf dem Domänencontroller und beiden Hosts.

Schritt 5. Konfigurieren Sie das Failover-Clustering.

Schritt 6. Fügen Sie das XClarity Orchestrator-Image hinzu.

Hochverfügbarkeit implementieren (ESXi)

Um Hochverfügbarkeit für Lenovo XClarity Orchestrator in einer VMware ESXi-Umgebung zu implementieren, verwenden Sie die Hochverfügbarkeitsfunktion, die von ESXi bereitgestellt wird.

Zu dieser Aufgabe

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

VMware High Availability erfordert die folgenden Komponenten.

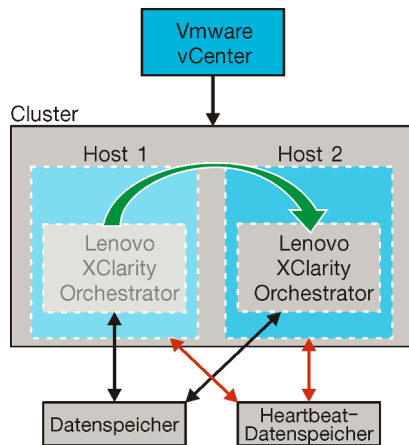
- Mindestens zwei Hosts, auf denen ESXi installiert ist. Diese Hosts werden Teil des VMware-Clusters.
- Einen dritten Host, auf dem VMware vCenter installiert ist.

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

VMware vCenter kann auf einem der Hosts installiert werden, die im Cluster verwendet werden. Wenn dieser Host allerdings ausgeschaltet oder nicht einsetzbar ist, geht auch der Zugriff auf die VMware vCenter-Schnittstelle verloren.

- Gemeinsam genutzter Speicher (Datenspeicher), auf den von allen Hosts im Cluster zugegriffen werden kann. Sie können jeden Typ gemeinsam genutzten Speicher verwenden, der von VMware unterstützt wird. Der Datenspeicher wird von VMware verwendet, um zu bestimmen, ob eine VM einen Failover zu einem anderen Host ausführen soll (Taktsignale).

In der folgenden Abbildung wird eine Möglichkeit dargestellt, um Hochverfügbarkeit für XClarity Orchestrator in einer ESXi-Umgebung zu implementieren. In diesem Szenario wird die virtuelle XClarity Orchestrator-Einheit im gemeinsam genutzten Speicher mit Cluster-Zugriff installiert.



Details zum Einrichten eines VMware High Availability-Clusters (VMware 5.0) finden Sie unter [Website zum Einrichten von Hochverfügbarkeit für VMware](#).

Vorgehensweise

Gehen Sie wie folgt vor, um eine Hochverfügbarkeitsumgebung einzurichten.

- Schritt 1. Konfigurieren Sie den gemeinsam genutzten Speicher, auf den alle Hosts im Cluster zugreifen sollen.
- Schritt 2. Installieren Sie ESXi auf zwei Servern, jeweils mit statischen IP-Adressen. Stellen Sie sicher, dass VMware vCenter auf einem separaten Server konfiguriert ist.
- Schritt 3. Starten Sie VMware vCenter.
- Schritt 4. Konfigurieren Sie die anderen beiden Hosts für die Nutzung von VMware vCenter.
 - a. Erstellen Sie den Cluster.
 - b. Fügen Sie dem Cluster die Hosts hinzu.
 - c. Fügen Sie beide Datenspeicher zu den Hosts im Cluster hinzu.

Anmerkung: Sie benötigen den zweiten Datenspeicher als Heartbeat (Takt).

- Schritt 5. Stellen Sie XClarity Orchestrator im Cluster bereit.

Kapitel 4. Erstkonfiguration von XClarity Orchestrator ausführen

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

Vorgehensweise

Gehen Sie wie folgt vor, um die Erstkonfiguration von XClarity Orchestrator vorzunehmen.

- Schritt 1. Rufen Sie die XClarity Orchestrator-Webschnittstelle auf.
- Schritt 2. Ändern Sie das anfängliche Kennwort.
- Schritt 3. Lesen und akzeptieren Sie die Lizenzvereinbarung.
- Schritt 4. Erstellen Sie zusätzliche Benutzeraccounts.
- Schritt 5. Stellen Sie das Datum und die Uhrzeit ein.
- Schritt 6. Konfigurieren Sie den Netzwerkzugriff einschließlich der IP-Adressen für Daten- und Verwaltungsnetzwerke.
- Schritt 7. Wählen Sie aus, ob Sie den Standard-Authentifizierungsserver verwenden oder einen externen LDAP-Client konfigurieren möchten.
- Schritt 8. Konfigurieren Sie zusätzliche Sicherheitseinstellungen, einschließlich des Imports vertrauenswürdiger Zertifikate für interne und externe Services.
- Schritt 9. Konfigurieren und aktivieren Sie die automatische Problembenachrichtigung (falls zutreffend).
- Schritt 10. Konfigurieren Sie XClarity Orchestrator so, dass Ereignisse an bestimmte Services und Anwendungen weitergeleitet werden (falls zutreffend).
- Schritt 11. Verbinden Sie Ihre Ressourcenmanager.

Erster Zugriff auf die XClarity Orchestrator-Webschnittstelle

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

Vorbereitende Schritte

Vergewissern Sie sich, dass Sie einen der folgenden unterstützten Webbrowser verwenden: Siehe [Unterstützte Hardware und Software](#) für weitere Informationen.

- Chrome 80.0 oder höher
- Firefox ESR 68.6.0 oder höher
- Microsoft Edge 40.0 oder höher
- Safari 13.0.4 oder höher (ausgeführt auf macOS 10.13 oder höher)

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

XClarity Orchestrator verwendet ein einzelnes Subnetz, in der Regel eth0.

Wenn Sie XClarity Orchestrator 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 Orchestrator zugreifen, die eine Verbindung zu XClarity Orchestrator aufweist. Beispielsweise können Sie

über eine andere VM auf dem Host, auf der XClarity Orchestrator installiert ist, auf XClarity Orchestrator zugreifen.

Vorgehensweise

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

1. Öffnen Sie im Browser die IP-Adresse der virtuellen Einheit von XClarity Orchestrator.

- **Statische IPv4-Adresse verwenden** Wenn Sie bei der Installation eine IPv4-Adresse festgelegt haben, verwenden Sie diese IPv4-Adresse, um mithilfe der folgenden URL auf die Webschnittstelle zuzugreifen.

`https://{IPv4_address}/#/login.html`

Beispiel:

`https://192.0.2.10/#/login.html`

- **Einen DHCP-Server in derselben Übertragungsdomäne wie XClarity Orchestrator verwenden** Wenn ein DHCP-Server in derselben Übertragungsdomäne wie XClarity Orchestrator eingerichtet ist, greifen Sie über die IPv4-Adresse, die in der Konsole der virtuellen Einheit von XClarity Orchestrator angezeigt wird, über die folgende URL auf die Webschnittstelle zu.

`https://{IPv4_address}/#/login.html`

Beispiel:

`https://192.0.2.10/#/login.html`

Die Seite für die erste Anmeldung wird angezeigt.



Über die Anmeldeseite können Sie die folgenden Aktionen ausführen:

- Reichen Sie Ideen für XClarity Orchestrator im [Website für Lenovo XClarity Ideation](#) ein oder klicken Sie auf **Idee einreichen**.
 - Sie können im [Community-Forumswebsite für Lenovo XClarity](#) Fragen stellen und Antworten finden, indem Sie auf **Benutzerforum** klicken.
 - Informationen zur Verwendung von XClarity Orchestrator finden Sie mit einem Klick auf **Benutzerhandbuch**.
 - Suchen und verwalten Sie alle Ihre Lenovo Lizenzen des [Features on Demand-Webportal](#) durch Klicken auf **Lizenznutzungsrecht**.
 - Informationen zu den verfügbaren APIs finden Sie mit einem Klick auf **Toolkits**.
2. Wählen Sie die gewünschte Sprache aus der Dropdown-Liste „Sprache“ aus.

Anmerkung: Einige Konfigurationseinstellungen und -daten, die von den Ressourcenmanagern und verwalteten Einheiten bereitgestellt werden, sind möglicherweise nur in Englisch verfügbar.

3. Geben Sie die Standardanmeldeinformationen USERID und PASSWORD (wobei 0 = NULL ist) ein und klicken Sie auf **Anmelden**. Wenn sich ein bestimmter Benutzeraccount zum ersten Mal bei XClarity Orchestrator anmeldet, muss das Kennwort geändert werden. Standardmäßig müssen Kennwörter **8 – 256** Zeichen enthalten und die folgenden Kriterien erfüllen.

Wichtig: Es wird empfohlen, sichere Kennwörter mit mindestens 16 Zeichen zu verwenden.

- Es muss mindestens ein alphabetisches Zeichen und es dürfen nicht mehr als zwei aufeinanderfolgende Zeichen enthalten sein, einschließlich Abfolgen alphabetischer Zeichen, Ziffern und QWERTZ-Tasten (z. B. sind „abc“, „123“ und „asd“ nicht zulässig).
- Sie müssen mindestens eine Zahl enthalten.
- Sie müssen mindestens zwei der folgenden Zeichen enthalten:
 - Großbuchstaben (A – Z)
 - Kleinbuchstaben (a – z)
 - Sonderzeichen ; @ _ ! ' \$ & +
 Leerzeichen sind nicht zulässig.
- Sie dürfen keine Wiederholung oder Umkehrung des Benutzernamens sein.
- Sie dürfen nicht mehr als zwei gleiche Zeichen hintereinander enthalten (z. B. sind „aaa“, „111“ und „...“ nicht zulässig).

Nach dieser Aufgabe

Wichtig: Möglicherweise werden Ihnen beim ersten Zugriff auf XClarity Orchestrator Sicherheits- oder Zertifikatwarnungen angezeigt. Diese Warnungen können Sie ignorieren.

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Einen lokale Benutzer erstellen](#) gehen.

Einen lokale Benutzer erstellen

Sie können Benutzeraccounts manuell im lokalen (integrierten) Authentifizierungsserver erstellen. *Lokale Benutzeraccounts* werden verwendet, um sich bei Lenovo XClarity Orchestrator anzumelden und den Zugriff auf Ressourcen zu genehmigen.

Zu dieser Aufgabe

Als zusätzliche Sicherheitsmaßnahme sollten Sie mindestens zwei Benutzeraccounts erstellen.

Vorgehensweise

So erstellen Sie einen lokalen Benutzer:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⚙️) → **Sicherheit** und dann im linken Navigationsbereich auf **Lokale Benutzer**, um die Übersicht Lokale Benutzer anzuzeigen.



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

Schritt 3. Tragen Sie die folgenden Informationen ein.

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

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

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

Wichtig: Es wird empfohlen, sichere Kennwörter mit mindestens 16 Zeichen zu verwenden.

- Es muss mindestens ein alphabetisches Zeichen und es dürfen nicht mehr als zwei aufeinanderfolgende Zeichen enthalten sein, einschließlich Abfolgen alphabetischer Zeichen, Ziffern und QWERTZ-Tasten (z. B. sind „abc“, „123“ und „asd“ nicht zulässig).
 - Sie müssen mindestens eine Zahl enthalten.
 - Sie müssen mindestens zwei der folgenden Zeichen enthalten:
 - Großbuchstaben (A – Z)
 - Kleinbuchstaben (a – z)
 - Sonderzeichen ; @ _ ! ' \$ & +Leerzeichen sind nicht zulässig.
 - Sie dürfen keine Wiederholung oder Umkehrung des Benutzernamens sein.
 - Sie dürfen nicht mehr als zwei gleiche Zeichen hintereinander enthalten (z. B. sind „aaa“, „111“ und „...“ nicht zulässig).
- (Optional) Geben Sie Kontaktinformationen für den Benutzeraccount an, einschließlich des vollständigen Namens, der E-Mail-Adresse und der Telefonnummer.

Tipp: Für den vollständigen Namen können Sie bis zu 128 Zeichen, darunter Buchstaben, Ziffern, Leerzeichen, Punkte, Bindestriche, Apostrophe und Kommas verwenden.

Schritt 4. Klicken Sie auf die Registerkarte **Benutzergruppen** und wählen Sie die Benutzergruppen aus, denen dieser Benutzer zugewiesen werden soll.

Tipp: Wenn keine Benutzergruppe ausgewählt wird, wird standardmäßig die Gruppe **OperatorGroup** zugewiesen.

Schritt 5. Klicken Sie auf **Erstellen**.

Der Benutzeraccount wird zur Tabelle hinzugefügt.

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Netzwerk konfigurieren](#) gehen.

Netzwerk konfigurieren

Bei der Erstkonfiguration von Lenovo XClarity Orchestrator müssen Sie eine einzelne Netzwerkschnittstelle (mithilfe von IPv4- und IPv6-Einstellungen) konfigurieren. Sie können auch Internet-Routingeinstellungen konfigurieren.

Vorbereitende Schritte


Prüfen Sie die folgenden Hinweise, wenn Sie die Schnittstelle auswählen.

- Die Schnittstelle muss so konfiguriert werden, dass sie die Ermittlung und Verwaltung unterstützt. Sie muss in der Lage sein, mit den Ressourcenmanagern und den Einheiten, die diese verwalten, zu kommunizieren.
- Wenn Sie beabsichtigen, gesammelte Servicedaten manuell an den Lenovo Support zu senden oder die automatische Problembenachrichtigung (Call-Home-Funktion) zu verwenden, müssen die Schnittstellen mit dem Internet verbunden sein, vorzugsweise durch eine Firewall.

Achtung:

- Wenn Sie die IP-Adresse der virtuellen Einheit von XClarity Orchestrator nach der Verbindung der Ressourcenmanager ändern, verliert XClarity Orchestrator die Kommunikation mit den Managern und diese erscheinen offline. Wenn Sie die IP-Adresse der virtuellen Einheit ändern müssen, sobald XClarity Orchestrator betriebsbereit ist, stellen Sie sicher, dass die Verbindung aller Ressourcenmanager aufgehoben (gelöscht) wird, bevor Sie die IP-Adresse ändern.
- Wenn die Netzwerkschnittstelle für die Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert ist, ändert sich möglicherweise die IP-Adresse, wenn die DHCP-Zugangsberechtigung abläuft. Wenn sich die IP-Adresse ändert, müssen Sie die Verbindung der Ressourcenmanager zunächst aufheben (löschen) und sie anschließend erneut verbinden. Sie können dieses Problem vermeiden, indem Sie entweder für die Netzwerkschnittstelle 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.
- Network Address Translation (NAT), die einen IP-Adressraum in einen anderen neu zuordnet, wird nicht unterstützt.

Vorgehensweise

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

- **IP-Einstellungen konfigurieren** Sie können die IPv4- und IPv6-Netzwerkeinstellungen über die Übersichten IPv4-Konfiguration und IPv6-Konfiguration nutzen. Aktivieren und ändern Sie die entsprechenden IP-Konfigurationseinstellungen und klicken Sie dann auf **Übernehmen**.
 - **IPv4-Einstellungen**. Sie können die IP-Zuordnungsmethode, die IPv4-Adresse, die Netzwerkmaske und das Standard-Gateway konfigurieren. Für die IP-Zuordnungsmethode können Sie eine statisch zugewiesene IP-Adresse verwenden oder eine IP-Adresse von einem DHCP-Server abrufen. Wenn Sie eine statische IP-Adresse verwenden, müssen Sie eine IP-Adresse, eine Netzwerkmaske und ein Standard-Gateway angeben. Das Standard-Gateway muss eine gültige IP-Adresse sein und sich im gleichen Subnetz wie die Netzwerkschnittstelle befinden.

Wenn DHCP zum Abrufen einer IP-Adresse verwendet wird, verwendet das Standard-Gateway ebenfalls DHCP.

- **IPv6-Einstellungen.** Sie können die IP-Zuordnungsmethode, die IPv6-Adresse, die Präfixlänge und das Standard-Gateway konfigurieren. Für die IP-Zuordnungsmethode können Sie eine statisch zugewiesene IP-Adresse, eine statusabhängige Adresskonfiguration (DHCPv6) oder eine automatische statusunabhängige IP-Adresskonfiguration verwenden. Wenn Sie eine statische IP-Adresse verwenden, müssen Sie eine IPv6-Adresse, eine Präfixlänge und ein Gateway angeben. Das Gateway muss eine gültige IP-Adresse sein und sich im gleichen Subnetz wie die Netzwerkschnittstelle befinden.

The image shows two configuration panels. The top panel is titled 'IPv4-Konfiguration' and has an 'Enabled' toggle switch. It contains four input fields: 'Methode' (dropdown menu with 'Obtain IP from DHCP'), 'IPv4-Netzwerkmaske' (text input with '255.255.224.0'), 'IPv4-Adresse' (text input with '10.243.14.36'), and 'IPv4-Standard-Gateway' (text input with '10.243.0.1'). Below these are 'Übernehmen' and 'Zurücksetzen' buttons. The bottom panel is titled 'IPv6-Konfiguration' and also has an 'Enabled' toggle switch. It contains four input fields: 'Methode' (dropdown menu with 'Use stateless address...'), 'IPv6-Präfixlänge' (text input with '64'), 'IPv6-Adresse' (text input with 'fd55:faaf:e1ab:2021:20c:2'), and 'IPv6-Standard-Gateway' (text input with 'fe80::5:73ff:fea0:2c'). Below these are 'Übernehmen' and 'Zurücksetzen' buttons.

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

Momentan werden nur Adressen im Format IPv4 unterstützt.

Wählen Sie aus, ob DHCP verwendet werden soll, um die IP-Adressen abzurufen, oder um statische IP-Adressen durch Aktivieren oder Deaktivieren von **DHCP-DNS** anzugeben. Wenn Sie statische IP-Adressen verwenden möchten, geben Sie die IP-Adresse für mindestens einen und bis zu zwei DNS-Servern an.

Geben Sie den DNS-Hostnamen und den Domännennamen an. Sie können auswählen, ob der Domänenname von einem DHCP-Server abgerufen werden soll, oder Sie geben einen benutzerdefinierten Domännennamen an.

Anmerkungen:

- 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 Orchestrator überschrieben.
- Wenn Sie DNS-Einstellungen ändern, müssen Sie die virtuelle Maschine manuell neu starten, damit die Änderungen wirksam werden.

- Wenn Sie die DNS-Einstellung von der DHCP-Verwendung zu einer statischen IP-Adresse ändern, müssen Sie auch die IP-Adresse des DNS-Servers selbst ändern.

DNS-Konfiguration

Wenn Sie die DNS-Einstellungen ändern, müssen Sie den XClarity Orchestrator-Server neu starten, um die Änderungen zu übernehmen.

Bevorzugter DNS-Adresstyp IPv4 IPv6 Enabled

1. DNS-Adresse 10.240.0.10	Methode Use domain name o...
2. DNS-Adresse 10.240.0.11	Domänenname
Hostname lxco	

- **HTTP-Proxy-Einstellungen konfigurieren** Optional können Sie den Hostnamen des Proxyservers, den Port und die optionalen Anmeldeinformationen in der Übersicht Proxy-Konfiguration aktivieren und angeben. Klicken Sie dann auf **Übernehmen**.

Anmerkungen:

- 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).

Proxy-Konfiguration

Disabled

Proxy-Server Hostname	Benutzername
Proxy-Server Port	Kennwort

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Datum und Uhrzeit konfigurieren](#) gehen.

Datum und Uhrzeit konfigurieren

Sie müssen mindestens einen (und maximal vier) NTP-Server (Network Time Protocol) einrichten, um die Zeitstempel für Lenovo XClarity Orchestrator mit Ereignissen zu synchronisieren, die von Ressourcenmanagern empfangen werden.

Vorbereitende Schritte

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

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

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

- **ESXi**Führen Sie die Anweisungen auf der [VMware – Website zur Deaktivierung der Zeitsynchronisation](#) aus.
- **Hyper-V**Klicken Sie im Hyper-V-Manager mit der rechten Maustaste auf die virtuelle XClarity Orchestrator-Maschine und anschließend auf **Einstellungen**. Klicken Sie im Dialogfeld im Navigationsbereich auf **Verwaltung** → **Integrationservices** und deaktivieren Sie dann **Zeitsynchronisation**.

Vorgehensweise

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

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

Datum und Uhrzeit

Datum und Uhrzeit werden automatisch mit dem NTP-Server synchronisiert

Datum 04.10.22

Uhrzeit 18:48:48

Zeitzone UTC -00:00, Coordinated Universal Time Universal

ⓘ Nachdem die Änderungen übernommen wurden, wird diese Seite automatisch aktualisiert, um die neueste Konfiguration abzurufen. ✕

Zeitzone*

UTC -00:00, Coordinated Universal Time Universal
▼

NTP-Server*

NTP-Server 1 FQDN oder IP-Adresse

⊕ Neuen NTP-Server hinzufügen

Übernehmen

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

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

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

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

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Authentifizierungsserver konfigurieren](#) gehen.

Authentifizierungsserver konfigurieren

Lenovo XClarity Orchestrator umfasst einen lokalen (integrierten) Authentifizierungsserver. Sie können auch einen eigenen externen Active Directory LDAP-Server verwenden.

Vorbereitende Schritte

Bevor sich ein externer LDAP-Benutzer bei XClarity Orchestrator anmelden kann, muss der Benutzer ein direktes Mitglied einer LDAP-Benutzergruppe sein, die in XClarity Orchestrator. XClarity Orchestrator erkennt keine Benutzer, die Mitglieder von Benutzergruppen sind, die in der geklonten LDAP-Benutzergruppe verschachtelt sind, die auf dem externen LDAP-Server definiert ist.

Stellen Sie sicher, dass alle für den externen Authentifizierungsserver erforderlichen Ports im Netzwerk und in den Firewalls geöffnet sind. Weitere Informationen zu den Portanforderungen finden Sie unter [Portverfügbarkeit](#).

Zu dieser Aufgabe

Wenn kein externer LDAP-Server konfiguriert ist, authentifiziert XClarity Orchestrator einen Benutzer immer über den lokalen Authentifizierungsserver.

Wenn ein externer LDAP-Server konfiguriert ist, versucht XClarity Orchestrator zunächst, einen Benutzer über den lokalen Authentifizierungsserver zu authentifizieren. Wenn die Authentifizierung fehlschlägt, verwendet XClarity Orchestrator die IP-Adresse des ersten LDAP-Servers für die Authentifizierung. Wenn die Authentifizierung fehlschlägt, verwendet der LDAP-Client die IP-Adresse des nächsten LDAP-Servers für die Authentifizierung.

Wenn ein externer LDAP-Benutzer sich zum ersten Mal bei XClarity Orchestrator anmeldet, wird automatisch ein Benutzeraccount mit dem Namen <Benutzername>@<Domäne> in XClarity Orchestrator geklont. Sie können geklonte externe LDAP-Benutzer zu Benutzergruppen hinzufügen oder LDAP-Gruppen für die Zugriffssteuerung verwenden. Sie können einem externen LDAP-Benutzer auch Supervisor-Berechtigungen zuordnen.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Orchestrator für die Verwendung eines externen LDAP-Authentifizierungsservers zu konfigurieren.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⚙️) → **Sicherheit** und dann im linken Navigationsbereich auf **LDAP-Client**, um die Übersicht LDAP-Client anzuzeigen.

LDAP-Client ↻

Sie können XClarity Orchestrator so konfigurieren, dass externe LDAP-Server zum Authentifizieren von Benutzern verwendet werden. Der lokale Authentifizierungsserver führt immer zuerst die Authentifizierung aus. Wenn die Authentifizierung fehlschlägt, verwendet der LDAP-Client die IP-Adresse des ersten externen LDAP-Servers für die Authentifizierung. Wenn die Authentifizierung fehlschlägt, verwendet der LDAP-Client die nächste Server-IP-Adresse für die Authentifizierung.

Serverinformationen

Domain*

Serveradresse*

Port*
636

+
↑
↓

Active Directory
 Benutzerdefiniertes LDAP

LDAP over SSL

Konfiguration

Base Distinguished Name für Benutzer*

Base Distinguished Name für Gruppen*

Bindungsanmeldeinformationen ⓘ

Bindungsmethode
 Konfigurierter Berechtigungsnachweis ▼

Bindungsbenutzername*

Bindungskennwort* 🔒

Zertifikat abrufen oder im PEM-Format einfügen
(achten Sie darauf, dass die BEGIN- und END-Zeilen enthalten sind): ⓘ

-----BEGIN CERTIFICATE-----
 Zertifikatsinhalte
 -----END CERTIFICATE-----

Abrufen

Zurücksetzen
Änderungen übernehmen

Schritt 2. Konfigurieren Sie jeden externen LDAP-Server mithilfe der folgenden Schritte.

1. Klicken Sie auf das Symbol **Hinzufügen** (+), um einen LDAP-Server hinzuzufügen.
2. Geben Sie den Domännennamen, die IP-Adresse und den Port für den externen LDAP-Server an.

Wenn die Portnummer für einen Eintrag *nicht* explizit auf 3268 oder 3269 festgelegt wurde, geht das System davon aus, dass dieser Eintrag einen Domänencontroller identifiziert.

Wenn die Portnummer auf 3268 oder 3269 festgelegt wurde, wird davon ausgegangen, dass der Eintrag einen globalen Katalog identifiziert. Der LDAP-Client versucht, die Authentifizierung mithilfe des Domänencontrollers für die erste konfigurierte Server-IP-Adresse durchzuführen. Schlägt dieser Versuch fehl, versucht der LDAP-Client, den Domänencontroller der nächsten konfigurierten Server-IP-Adresse für die Authentifizierung zu verwenden.

3. Optional können Sie die Anpassung erweiterter Konfigurationseinstellungen aktivieren. Wenn Sie eine angepasste Konfiguration verwenden, können Sie den Filter für die Benutzersuche angeben. Wenn Sie keinen Filter für die Benutzersuche angeben, wird standardmäßig (&&(objectClass=user)(|(userPrincipalName={0})(sAMAccountName={0}))) verwendet.

Wenn die erweiterte Konfiguration deaktiviert ist, wird die Active Directory-Standardkonfiguration verwendet.

4. Geben Sie den vollständig qualifizierten LDAP-basierten definierten Namen an, von dem der LDAP-Client die Suche für die Benutzerauthentifizierung initiiert.
5. Geben Sie den vollständig qualifizierten LDAP-basierten definierten Namen an, von dem der LDAP-Client die Suche nach Benutzergruppen initiiert (z. B. `dc=company,dc=com`).
6. Sie können optional auch Anmeldeinformationen angeben, um XClarity Orchestrator an den externen Authentifizierungsserver anzubinden. Zwei Bindungsmethoden stehen zur Verfügung.
 - **Konfigurierte Anmeldeinformationen.** Verwenden Sie diese Bindungsmethode, um einen bestimmten Clientnamen und das Kennwort für die Bindung von XClarity Orchestrator an den externen Authentifizierungsserver zu verwenden. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Geben Sie den vollständig qualifizierten LDAP Distinguished Name (z. B. `cn=somebody,dc=company,dc=com`) oder die E-Mail-Adresse (z. B. `somebody@company.com`) des Benutzeraccounts und das Kennwort an, das für die LDAP-Authentifizierung zur Bindung von XClarity Orchestrator an den LDAP-Server verwendet werden soll. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden.

Der definierte Name muss ein Benutzeraccount innerhalb der Domäne sein, der mindestens über Leserechte verfügt.

Wenn der LDAP-Server nicht über Subdomänen verfügt, können Sie den Benutzernamen ohne die Domäne angeben (z. B. `user1`). Wenn der LDAP-Server jedoch über Subdomänen verfügt (z. B. Subdomäne `new.company.com` in Domäne `company.com`), müssen Sie den Benutzernamen und die Domäne angeben (z. B. `user1@company.com`).

Achtung: Wenn Sie das Clientkennwort auf dem externen LDAP-Server ändern, müssen Sie das neue Kennwort auch in XClarity Orchestrator ändern (siehe [Anmelden bei XClarity Orchestrator nicht möglich](#) in der Onlinedokumentation zu XClarity Orchestrator).

- **Anmeldeinformationen.** Verwenden Sie diese Bindungsmethode, um Ihren LDAP XClarity Orchestrator Benutzernamen und das Kennwort für die Bindung von XClarity Orchestrator an den externen Authentifizierungsserver zu verwenden. Geben Sie den vollständig qualifizierten LDAP Distinguished Name eines *Test*-Benutzeraccounts und das Kennwort an, das für die LDAP-Authentifizierung verwendet werden soll, um die Verbindung mit dem Authentifizierungsserver zu überprüfen.

Diese Benutzeranmeldeinformationen werden nicht gespeichert. Bei Erfolg verwenden alle zukünftigen Verbindungen den Benutzernamen und das Kennwort, die Sie für die Anmeldung bei XClarity Orchestrator verwendet haben. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden.

Anmerkung: Sie müssen bei XClarity Orchestrator mit einer vollständig qualifizierten Benutzer-ID angemeldet sein (z. B. `administrator@domain.com`).

7. Wählen Sie optional eine sichere LDAP-Verbindung aus, indem Sie die Umschalt-Schaltfläche **LDAP over SSL** aktivieren und dann auf **Abrufen** klicken, um das vertrauenswürdige SSL-Zertifikat abzurufen und zu importieren. Wenn das Dialogfenster Serverzertifikat abrufen angezeigt wird, klicken Sie auf **Akzeptieren**, um das Zertifikat zu verwenden. Wenn Sie „LDAP über SSL“ verwenden, verwendet XClarity Orchestrator das LDAPS-Protokoll, um eine sichere Verbindung mit dem externen Authentifizierungsserver herzustellen. Wenn diese Option ausgewählt ist, werden vertrauenswürdige Zertifikate verwendet, um die sichere LDAP-Unterstützung zu aktivieren.

Achtung: Wenn Sie „LDAP über SSL“ deaktivieren, verwendet XClarity Orchestrator ein unsicheres Protokoll, um eine sichere Verbindung mit dem externen Authentifizierungsserver herzustellen. Diese Einstellung macht Ihre Hardware eventuell anfälliger für potenzielle Sicherheitsrisiken.

- Optional können Sie die LDAP-Server mithilfe des Symbols **Nach oben verschieben** (↑) und **Nach unten verschieben** (↓) neu anordnen. Der LDAP-Client versucht, die Authentifizierung mithilfe der ersten Server-IP-Adresse durchzuführen. Wenn die Authentifizierung fehlschlägt, verwendet der LDAP-Client die nächste Server-IP-Adresse für die Authentifizierung.

Wichtig: Verwenden Sie für die sichere LDAP-Authentifizierung das Zertifikat für die Stammzertifizierungsstelle des LDAP-Servers oder eines der Zwischenzertifikate des Servers. Sie können das Stamm- oder Zwischen-Zertifizierungsstellenzertifikat über eine Eingabeaufforderung abrufen, indem Sie den folgenden Befehl ausführen, wobei *{FullyQualifiedHostNameOrIpAddress}* der vollständig qualifizierte Name des externen LDAP-Servers ist. Das Stamm- oder Zwischen-Zertifizierungsstellenzertifikat ist in der Regel das letzte Zertifikat in der Ausgabe (der letzte BEGIN- -END-Abschnitt).

```
openssl s_client -showcerts -connect {FullyQualifiedHostNameOrIpAddress}:636
```

- Klicken Sie auf **Änderungen übernehmen**. XClarity Orchestrator versucht, die IP-Adresse, den Port, die SSL-Zertifikate und die Anmeldeinformationen für die Bindung zu testen und überprüft die Verbindung zum LDAP-Server, um allgemeine Fehler zu erkennen. Wenn die Überprüfung erfolgreich war, wird bei der Anmeldung eines Benutzers bei XClarity Orchestrator eine Benutzerauthentifizierung auf dem externen Authentifizierungsserver durchgeführt. Wenn die Validierung fehlschlägt, werden Fehlermeldungen mit der Fehlerquelle angezeigt.

Anmerkung: Wenn die Überprüfung erfolgreich war und Verbindungen zum LDAP-Server hergestellt wurden, können trotzdem Fehler bei der Benutzerauthentifizierung auftreten, wenn der Root-DN falsch ist.

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Zusätzliche Sicherheitseinstellungen konfigurieren](#) gehen.

Zusätzliche Sicherheitseinstellungen konfigurieren

Sie können zusätzliche Sicherheitseinstellungen einschließlich Zertifikaten und Benutzeraccount-Sicherheitseinstellungen konfigurieren.

Vorgehensweise

Gehen Sie wie folgt vor, um zusätzliche Sicherheitseinstellungen zu konfigurieren:

- Lenovo XClarity Orchestrator verwendet Zertifikate für die Einrichtung von sicheren und vertrauenswürdigen Kommunikationsverbindungen zwischen XClarity Orchestrator und den Ressourcenmanagern (z. B. Lenovo XClarity Administrator) sowie für die Herstellung von Kommunikationsverbindungen mit XClarity Orchestrator durch Benutzer. Standardmäßig verwenden XClarity Orchestrator und die Ressourcenmanager XClarity Orchestrator-generierte Zertifikate, die von einer internen Zertifizierungsstelle (Certificate Authority, CA) ausgestellt wurden. Sie können eine Zertifikatssignieranforderung (CSR) zum Signieren durch eine externe Zertifizierungsstelle, z. B. die Zertifizierungsstelle Ihrer Organisation, oder eine unabhängige Zertifizierungsstelle generieren (siehe [Ein vertrauenswürdiges, extern signiertes XClarity Orchestrator-Serverzertifikat installieren](#) in der Onlinedokumentation zu XClarity Orchestrator).
- Sie können vertrauenswürdige Zertifikate für externe Dienste in den XClarity Orchestrator-Truststore importieren, um eine sichere Verbindung zu Ressourcenmanagern und Ereignisweiterleitern herzustellen,

z. B. Splunk (siehe [Vertrauenswürdige Zertifikate für externe Dienste hinzufügen](#) in der Onlinedokumentation zu XClarity Orchestrator).

- Sie können vertrauenswürdige Zertifikate für interne Dienste in den XClarity Orchestrator-Truststore importieren, um eine sichere Verbindung zu Ressourcenmanagern und vertrauenswürdigen LDAP-Servern herzustellen (siehe [Vertrauenswürdige Zertifikate für interne Dienste hinzufügen](#) in der Onlinedokumentation zu XClarity Orchestrator).
- Konfigurieren Sie die Sicherheitseinstellungen für die Komplexität von Kennwörtern, die Sperrung von Accounts und die Einstellungen für das Web-Sitzungszeitlimit bei Inaktivität. Weitere Informationen zu diesen Einstellungen finden Sie unter [Benutzersicherheitseinstellungen konfigurieren](#) in der Onlinedokumentation zu XClarity Orchestrator.

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Automatische Problembenachrichtigung \(Call-Home-Funktion\) konfigurieren und aktivieren](#) gehen.

Automatische Problembenachrichtigung (Call-Home-Funktion) konfigurieren und aktivieren

Sie können Lenovo XClarity Orchestrator so einrichten, dass ein Service-Ticket automatisch geöffnet und erfasste Servicedaten über die Call-Home-Funktion an den Lenovo Support gesendet werden, wenn bestimmte wartungsfähige Ereignisse (z. B. ein nicht wiederherstellbarer Speicher) von einer Einheit erzeugt werden, damit das Problem behoben werden kann.

Vorbereitende Schritte

Stellen Sie sicher, dass alle von XClarity Orchestrator benötigten Ports sowie die Ports, die für die Call-Home-Funktion erforderlich sind, zur Verfügung stehen, bevor Sie die Call-Home-Funktion aktivieren. Weitere Informationen zu Ports finden Sie unter [Portverfügbarkeit](#) in der Onlinedokumentation zu XClarity Orchestrator.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen hergestellt werden kann, die von der Call-Home-Funktion benötigt werden. Informationen zu Firewalls finden Sie unter [Firewalls und Proxy-Server](#) in der Onlinedokumentation zu XClarity Orchestrator.

Wenn XClarity Orchestrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss der Proxy-Server die Standardauthentifizierung verwenden und ein Non-Termination-Proxy sein. Weitere Informationen zum Einrichten des Proxys finden Sie unter [Netzwerkeinstellungen konfigurieren](#) in der Onlinedokumentation zu XClarity Orchestrator.

Wichtig: Wenn die Call-Home-Funktion für XClarity Orchestrator und Lenovo XClarity Administrator aktiviert ist, stellen Sie sicher, dass Lenovo XClarity Administrator v2.7 oder höher verwendet wird, um doppelte Service Tickets zu vermeiden. Wenn die Call-Home-Funktion bei XClarity Orchestrator aktiviert und bei Lenovo XClarity Administrator deaktiviert ist, wird Lenovo XClarity Administrator v2.6 oder höher unterstützt.

Zu dieser Aufgabe

Falls die Call-Home-Funktion konfiguriert und aktiviert wurde und ein Service-Ereignis auf einer bestimmten Einheit eintritt, öffnet XClarity Orchestrator *automatisch* ein Service-Ticket und überträgt die Servicedaten für diese Einheit an das Lenovo Support-Center.

Wichtig: Lenovo setzt sich für Ihre Sicherheit ein. Servicedaten, die Sie normalerweise manuell auf die Lenovo Support-Website hochladen, werden mit TLS 1.2 oder höher automatisch über HTTPS an das

Lenovo Support-Center gesendet. Ihre Geschäftsdaten werden niemals übertragen. Der Zugriff auf Servicedaten im Lenovo Support-Center ist auf autorisiertes Servicepersonal beschränkt.

Ist die Call-Home-Funktion nicht aktiviert, können Sie manuell ein Service-Ticket öffnen und Servicedateien an das Lenovo Support-Center übertragen. Folgen Sie dazu den Anweisungen unter [Öffnen einer Website für das Support-Ticket](#). Weitere Informationen zum Erfassen von Servicedaten finden Sie unter [Service-Ticket im Lenovo Unterstützungszentrum manuell öffnen](#) in der Onlinedokumentation von XClarity Orchestrator.

Weitere Informationen zum Anzeigen von Service-Tickets, die von der Call-Home-Funktion automatisch geöffnet wurden, finden Sie unter [Service-Tickets und Status anzeigen](#) in der Onlinedokumentation von XClarity Orchestrator.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Call-Home-Funktion für die automatische Problembenachrichtigung zu konfigurieren.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⚙️) → **Service und Support** und klicken Sie dann im linken Navigationsbereich auf **Call-Home-Konfiguration**, um die Übersicht Call-Home-Konfiguration anzuzeigen.

Call-Home-Konfiguration

Auf dieser Seite können Sie eine Call-Home-Funktion konfigurieren, die Servicedaten für verwaltete Endpunkte automatisch an den Lenovo Support weiterleitet, wenn auf einem verwalteten Endpunkt bestimmte wartungsfähige Ereignisse auftreten.

[Lenovo Datenschutzerklärung](#)

Ich stimme der Lenovo Datenschutzerklärung zu

Kundendaten

Kundennummer

Primärer Kontakt zur Verwendung aus mehreren Gruppenzuordnungen ?

Erste Gruppenzuordnung
 Letzte Gruppenzuordnung

Standardkontakt

Call-Home-Status: Aktiviert deaktiviert

<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Systemposition ?

Schritt 2. Lesen Sie die [Lenovo Datenschutzerklärung](#) und klicken Sie dann auf **Ich stimme der Lenovo Datenschutzerklärung zu**.

Schritt 3. Geben Sie die standardmäßige Lenovo Kundennummer an, die beim Melden von Problemen verwendet werden soll.

Ihre Kundennummer finden Sie in der E-Mail mit dem Berechtigungsnachweis, die Sie beim Kauf Ihrer XClarity Orchestrator-Lizenz erhalten haben.

Schritt 4. Ändern Sie den Call-Home-Status in **Aktivieren**.

Schritt 5. Wählen Sie den primären Kontakt aus, der aus mehreren Gruppenzuordnungen verwendet werden soll.

Sie können einen primären Support-Kontakt auch einer Gruppe von Einheiten zuordnen. Wenn eine Einheit mehreren Gruppen angehört, ist es möglich, jeder Gruppe einen anderen primären Kontakt zuzuweisen. Sie können angeben, dass die Zuordnung des primären Kontakts für die erste oder letzte Gruppe verwendet werden soll, der die Einheit zugewiesen wurde.

Schritt 6. Geben Sie die Kontaktinformationen und die bevorzugte Kontaktmethode für den Lenovo Support an.

Wenn eine Einheit keiner Gruppe mit einem zugewiesenen primären Kontakt angehört, wird der Standardkontakt für die Call-Home-Funktion verwendet.

Schritt 7. Geben Sie die Standortinformationen für das System an.

Schritt 8. Klicken Sie auf **Call-Home-Verbindungstest**, um zu überprüfen, ob XClarity Orchestrator mit dem Lenovo Support-Center kommunizieren kann.

Schritt 9. Klicken Sie auf **Übernehmen**.

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Weiterleitung von Ereignisdaten einrichten](#) gehen.

Weiterleitung von Ereignisdaten einrichten

Sie können Ereignis-, Bestands- und Metrikdaten von Lenovo XClarity Orchestrator an externe Anwendungen zur Überwachung und Analyse von Daten weiterleiten.

Zu dieser Aufgabe

Ereignisdaten

XClarity Orchestrator kann Ereignisse, die in Ihrer Umgebung auftreten, an externe Tools weiterleiten, die auf den von Ihnen angegebenen Kriterien (Filtern) basieren. Jedes generierte Ereignis wird überwacht, um festzustellen, ob es den Kriterien entspricht. Wenn es übereinstimmt, wird das Ereignis unter Verwendung des angegebenen Protokolls an die angegebene Position weitergeleitet.

XClarity Orchestrator unterstützt das Weiterleiten von Ereignisdaten an die folgenden externen Tools.

- **E-Mail.** Ereignisdaten werden per SMTP an eine oder mehrere E-Mail-Adressen weitergeleitet.
- **Intelligent Insights.** Ereignisdaten werden in einem vordefinierten Format an SAP Data Intelligence weitergeleitet. Sie können SAP Data Intelligence anschließend zum Verwalten und Überwachen der Ereignisdaten verwenden.
- **REST.** Ereignisdaten werden über das Netzwerk an einen REST-Webservice weitergeleitet.
- **Syslog.** Ereignisdaten werden über das Netzwerk an einen zentralen Protokollserver weitergeleitet, wobei systemeigene Tools für die syslog-Überwachung verwendet werden können.

XClarity Orchestrator verwendet *globale Filter*, um den Umfang der zu weitergeleiteten Ereignisdaten zu definieren. Sie können Ereignisfilter erstellen, um nur Ereignisse mit bestimmten Eigenschaften weiterzuleiten, darunter Ereigniscodes, Ereignisklassen, Ereignisschweregrade und Servicetypen. Sie

können auch Einheitenfilter erstellen, die nur Ereignisse weiterleiten, die von bestimmten Einheiten generiert werden.

Bestands- und Ereignisdaten

XClarity Orchestrator kann alle Bestands- und Ereignisdaten für alle Einheiten an externe Anwendungen weiterleiten, die Sie zur Überwachung und Analyse der Daten verwenden können.

- **Splunk.** Ereignisdaten werden in einem vordefinierten Format an eine Splunk-Anwendung weitergeleitet. Sie können Splunk verwenden, um Diagramme und Tabellen zu erstellen, die auf Ereignisdaten basieren. Sie können mehrere Splunk-Konfigurationen definieren. XClarity Orchestrator kann Ereignisse allerdings nur an eine Splunk-Konfiguration weiterleiten. Daher kann jeweils nur eine Splunk-Konfiguration aktiviert sein.

Metrikdaten

XClarity Orchestrator kann Metrikdaten, die es über verwaltete Einheiten erfasst, an das folgende externe Tool weiterleiten.

- **TruScale Infrastructure Services.** Metrikdaten werden in einem vordefinierten Format an den Lenovo TruScale Infrastructure Services weitergeleitet. Sie können TruScale Infrastructure Services anschließend zum Verwalten und Überwachen der Metrikdaten verwenden.

Achtung: Informationen zum TruScale Infrastructure Services-Weiterleiter sind nur für Lenovo Service-Mitarbeiter vorgesehen.

Sie können mehrere TruScale Infrastructure Services-Weiterleiter definieren. XClarity Orchestrator kann Metrikdaten allerdings nur an einen TruScale Infrastructure Services-Weiterleiter weiterleiten. Daher kann jeweils nur ein TruScale Infrastructure Services-Weiterleiter aktiviert sein.

Weitere Informationen:  [Einführung in Lenovo TruScale Infrastructure Services](#)

Weitere Informationen zur Weiterleitung von Ereignisdaten finden Sie unter [Ereignis-, Bestands- und Metrikdaten weiterleiten](#) in der Onlinedokumentation zu XClarity Orchestrator.

Nach dieser Aufgabe

Setzen Sie die Erstkonfiguration fort, indem Sie auf [Ressourcenmanager verbinden](#) gehen.

Ressourcenmanager verbinden

Lenovo XClarity Orchestrator überwacht und verwaltet Einheiten über Ressourcen- und Anwendungsmanager.

Vorbereitende Schritte

XClarity Orchestrator kann eine unbegrenzte Anzahl von Ressourcenmanagern unterstützen, die zusammen insgesamt maximal 10,000 Einheiten verwalten.

Stellen Sie sicher, dass die Ressourcenmanager unterstützt werden (siehe [Unterstützte Hardware und Software](#) in der Onlinedokumentation zu XClarity Orchestrator).

Stellen Sie sicher, dass die Ressourcenmanager online sind und XClarity Orchestrator über das Netzwerk darauf zugreifen kann.

Stellen Sie sicher, dass der Benutzeraccount, den Sie für die Authentifizierung mit dem Ressourcenmanager verwenden, über die richtigen Berechtigungen verfügt. Für XClarity Administrator müssen Benutzeraccounts die Rollen **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-hw-admin** oder **lxc-recovery** zugewiesen werden.

Stellen Sie sicher, dass beim Ressourcenmanager noch nicht maximale Anzahl unterstützter Ereignisweiterleiter erreicht ist. XClarity Orchestrator erstellt einen Ereignisweiterleiter im Ressourcenmanager, wenn eine Verbindung zu diesem Ressourcenmanager hergestellt wird.

Beim Verbinden eines Ressourcenmanagers mit extern signiertem Zertifikat:

- Stellen Sie sicher, dass es ein X.509 v3-Zertifikat ist. XClarity Orchestrator kann keine Verbindung mit einem Ressourcenmanager mit extern signiertem v1-Zertifikat herstellen.
- Stellen Sie sicher, dass die Zertifikatsdetails die folgenden Anforderungen erfüllen.
 - Schlüsselverwendung muss enthalten:
 - Schlüsselvereinbarung
 - Digitale Signatur
 - Schlüsselverschlüsselung
 - Erweiterte Schlüsselverwendung muss enthalten:
 - Serverauthentifizierung (1.3.6.1.5.5.7.3.1)
 - Clientauthentifizierung (1.3.6.1.5.5.7.3.2)

Zu dieser Aufgabe

XClarity Orchestrator unterstützt die folgenden Ressourcen- und Anwendungsmanager.

- **Lenovo XClarity Management Hub 2.0.** Führt Verwaltung, Überwachung und Bereitstellung von ThinkSystem und ThinkAgile Einheiten durch. Auf jeder ThinkEdge Client-Einheit muss ein UDC-Agent installiert sein, damit die Kommunikation zwischen der Einheit und XClarity Orchestrator möglich ist.

Wichtig: Der Registrierungsprozess bei XClarity Management Hub 2.0 unterscheidet sich von dem anderer Ressourcenmanager. Detaillierte Anweisungen siehe .

- **Lenovo XClarity Management Hub.** Verwaltet, überwacht und sorgt für die Bereitstellung von ThinkEdge Client-Einheiten. Auf jeder ThinkEdge Client-Einheit muss ein UDC-Agent installiert sein, damit die Kommunikation zwischen der Einheit und XClarity Orchestrator möglich ist.

Wichtig: Der Registrierungsprozess bei XClarity Management Hub unterscheidet sich von dem anderer Ressourcenmanager. Detaillierte Anweisungen siehe .

- **Lenovo XClarity Administrator.** Verwaltet, überwacht und sorgt für die Bereitstellung von Lenovo Einheiten mit Baseboard Management Controllern.
- **Schneider Electric EcoStruxure IT Expert.** Verwaltet und überwacht Infrastrukturre Ressourcen.
- **VMware vRealize Operations Manager.**

Wenn Sie eine Verbindung mit einem XClarity Management Hub oder XClarity Administrator Ressourcenmanager herstellen, wird XClarity Orchestrator:

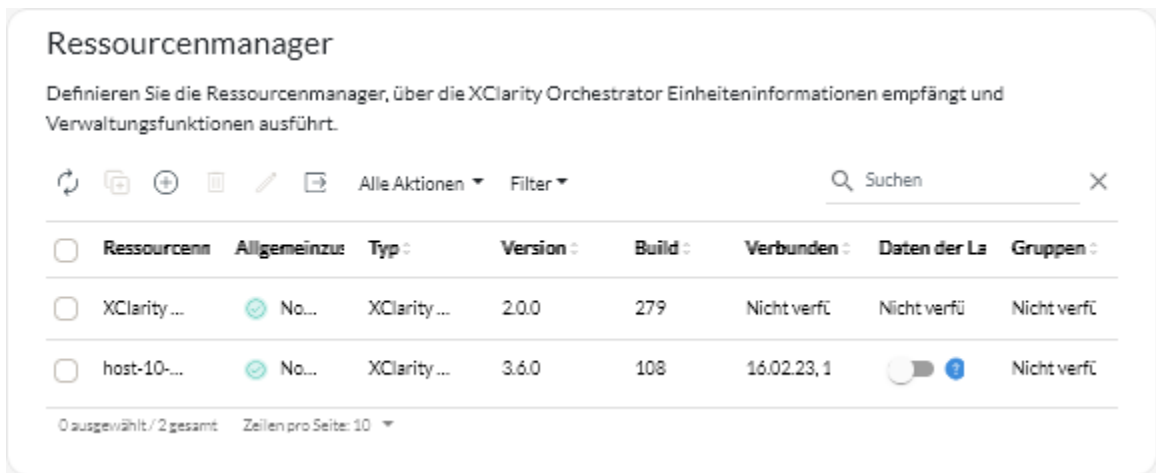
- Informationen zu allen Einheiten abrufen, die vom Ressourcenmanager verwaltet werden.
- Im Verwaltungsserver einen Ereignisweiterleiter (für einen REST-Webservice) erstellen und aktivieren, um Ereignisse zu überwachen und an XClarity Orchestrator weiterzuleiten.

Die Netzwerkadresse (IP-Adresse oder Hostname), die Sie angeben, wird als Name des Managers verwendet.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Ressourcen- oder Anwendungsmanager zu verbinden.

- Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) → **Ressourcenmanager**, um die Übersicht Ressourcenmanager anzuzeigen.



Schritt 2. Klicken Sie auf das Symbol **Verbinden** (+), um den Ressourcenmanager anzuzeigen. Dialogfenster Ressourcenmanager verbinden.

Schritt 3. Wählen Sie den Ressourcenmanagertyp aus und geben Sie die erforderlichen Informationen ein.

- **XClarity Management Hub 2.0 oder XClarity Management Hub**
 1. Geben Sie den Registrierungsschlüssel ein, der von der Verwaltungshub-Instanz generiert wurde, und klicken Sie auf **Verbinden**. Um das Registrierungsanforderungstoken abzurufen, melden Sie sich beim Verwaltungshub-Portal an, klicken Sie auf **Registrierung** und anschließend auf **Registrierungsschlüssel erstellen**.
 2. Kopieren Sie den generierten XClarity Orchestrator-Registrierungsschlüssel.

3. Klicken Sie im Verwaltungshub-Portal auf **Registrierung** und dann auf **Registrierungsschlüssel installieren**. Fügen Sie das XClarity Orchestrator-Registrierungstoken ein und klicken Sie auf **Verbinden**.

• **XClarity Administrator**

- Geben Sie den vollständig qualifizierten Domännennamen oder die IP-Adresse (IPv4 oder IPv6) an. Die Verwendung des Hostnamens ohne den Domännennamen wird nicht unterstützt.
- Optional können Sie auch den Port des Ressourcenmanagers ändern. Der Standardwert ist 443.
- Geben Sie den Benutzeraccount und das Kennwort an, die für die Anmeldung bei Ressourcenmanager verwendet werden sollen.
- Optional können Sie die **Datenerfassung für die Laufwerkanalyse** aktivieren. Wenn diese Option aktiviert ist, werden die Daten der Laufwerkanalyse von ThinkSystem und ThinkAgile Einheiten täglich erfasst und für vorausschauende Analysen verwendet. Die Datenerfassung für die Laufwerkanalyse wird nur für XClarity Administrator v3.3.0 und spätere Ressourcenmanager unterstützt.

Achtung: Die Systemleistung kann bei der Datenerfassung beeinträchtigt werden.

- **EcoStruxure IT Expert.** Geben Sie den Namen, den Token-Schlüssel und die URL an, die für die Verbindung verwendet werden sollen.

• **vRealize Operations Manager**

- Geben Sie den vollständig qualifizierten Domännennamen oder die IP-Adresse (IPv4 oder IPv6) an. Die Verwendung des Hostnamens ohne den Domännennamen wird nicht unterstützt.
- Optional können Sie auch den Port des Ressourcenmanagers ändern. Der Standardwert ist 443.
- Wählen Sie optional die Autorisierungsquelle für die Benutzer und Gruppen aus.
- Geben Sie den Benutzeraccount und das Kennwort an, die für die Anmeldung bei vRealize Operations Manager verwendet werden sollen.

Schritt 4. Klicken Sie auf **Verbinden**.

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).

Bei Herstellen einer Verbindung mit dem Ressourcenmanager wird dieser zur Tabelle hinzugefügt.

Schritt 5. Wenn Sie eine Verbindung mit einem XClarity Management Hub herstellen möchten, wird ein Dialogfenster mit einem Registrierungsschlüssel angezeigt.

Klicken Sie zum Abschließen der Verbindungsherstellung auf **In Zwischenablage kopieren**, um den Registrierungsschlüssel zu kopieren. Melden Sie sich anschließend bei XClarity Management Hub an, klicken Sie auf **Verwaltung** → **Hub-Konfiguration** an und anschließend Sie auf **Registrierungsschlüssel installieren**. Fügen Sie anschließend den Registrierungsschlüssel ein und klicken Sie auf **Senden**.

Nach dieser Aufgabe

Die Erstkonfiguration ist abgeschlossen.

Kapitel 5. Lizenzen von XClarity Orchestratoranwenden

Lenovo XClarity Orchestrator ist eine gebührenpflichtige Anwendung. Mit der kostenlosen Testlizenz können Sie XClarity Orchestrator bis zu 90 Tage lang kostenfrei nutzen. Allerdings müssen Sie nach Ablauf der kostenlosen Testversion entsprechende Lizenzen erwerben und installieren, um XClarity Orchestrator-Funktionen weiterhin verwenden zu können und Service und Support für XClarity Orchestrator zu erhalten.

Vorbereitende Schritte

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

Für jede verwaltete Einheit, die die erweiterten Funktionen (Serverkonfiguration und BS-Implementierung) unterstützt, ist eine Lizenz erforderlich.

- 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 Orchestrator zu erhalten.
 - ThinkServer-Server
 - System x M4 Server
 - System x X5 Server
 - System x3850 X6 und x3950 X6 (3837) Server
 - Speichereinheiten
 - Switches

Sie müssen ein Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** zugewiesen ist.

Zu dieser Aufgabe

XClarity Orchestrator unterstützt die folgenden Lizenzen.

- **XClarity Orchestrator.** Aktiviert Orchestrator- und Basisverwaltungsfunktionen für Server, Gehäuse, Switches und Speichereinheiten sowie Anspruch auf XClarity Orchestrator Service und Unterstützung. Für Orchestrator-Funktionen ist eine Lizenz in XClarity Orchestrator für jede Einheit erforderlich, die Serverkonfiguration und BS-Implementierung unterstützt. Für Service und Support für XClarity Orchestrator ist eine Lizenz für *jede verwaltete Einheit* erforderlich.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen gültigen XClarity Orchestrator-Lizenzschlüsseln nicht überschreiten. Wenn die Anzahl der XClarity Orchestrator-Lizenzen nicht konform ist (z. B. wenn Lizenzen ablaufen oder wenn die Verwaltung zusätzlicher Einheiten die Gesamtanzahl der aktiven Lizenzen überschreitet), haben Sie eine Kulanzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Wenn die Kulanfrist (einschließlich der kostenlosen Testversion) für Lizenzen endet, bevor die erforderliche Anzahl an Lizenzen installiert ist, werden *alle* Funktionen von XClarity Orchestrator (einschließlich Überwachung, Basisverwaltung und Analysen) für alle Einheiten deaktiviert. Bei Anmeldung werden Sie auf die Seite „Lizenzinformationen“ umgeleitet, auf der Sie weitere Lizenzen übernehmen können.

Wenn Sie z. B. weitere 100 ThinkSystem Server und 20 Rack-Switches mit einer vorhandenen XClarity Administrator-Instanz verwalten, die Sie über XClarity Orchestrator steuern, haben Sie 90 Tage Zeit, um 100 zusätzliche XClarity Orchestrator-Lizenzen zu erwerben und zu installieren, bevor die alle Funktionen in der Benutzerschnittstelle deaktiviert werden. Für die Verwendung der XClarity Orchestrator-Funktionen sind keine Lizenzen für die 20 Rack-Switches erforderlich. Allerdings sind die Lizenzen erforderlich, wenn Sie Service und Support für XClarity Orchestrator wünschen. Wenn die XClarity Orchestrator-Funktionen deaktiviert sind, werden sie erneut aktiviert, sobald Sie genügend Lizenzen für die Konformität installiert haben.

Wichtig: Beachten Sie, dass die XClarity Orchestrator-Basislizenz eine Voraussetzung für die XClarity Pro- und XClarity Orchestrator Analytics-Lizenzen ist. Wenn die Anzahl der XClarity Pro- oder XClarity Orchestrator-Lizenzen *konform* ist, aber die Anzahl der aktiven Basislizenzen *nicht konform* ist, werden alle XClarity Orchestrator-Funktionen (einschließlich Analysefunktionen) für alle Einheiten deaktiviert.

- **Lenovo XClarity Pro.** Aktiviert erweiterte Verwaltungsfunktionen (Serverkonfiguration und BS-Implementierung). Für jede verwaltete Einheit, die die erweiterten Verwaltungsfunktionen unterstützt, ist eine Lizenz in XClarity Orchestrator erforderlich.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen gültigen XClarity Pro-Lizenzschlüsseln nicht überschreiten. Wenn die Anzahl der XClarity Pro-Lizenzen nicht konform ist, haben Sie eine Kulanzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Wenn die Kulanzeit (einschließlich der kostenlosen Testversion) endet, bevor die erforderliche Anzahl an Lizenzen installiert ist, werden die Serverkonfigurations- und BS-Implementierungsfunktionen für *alle Einheiten* deaktiviert.

Weitere Informationen zum Installieren von XClarity Pro-Lizenzen finden Sie unter [Lizenzen und die kostenlose 90-Tage-Testversion](#) in der Onlinedokumentation zu XClarity Administrator.

- **XClarity Orchestrator Analytics.** Aktiviert Analysefunktionen. Für jede verwaltete Einheit, die die erweiterten Verwaltungsfunktionen unterstützt, ist eine Lizenz in XClarity Orchestrator erforderlich.

Die Lizenzkonformität wird anhand der Anzahl der verwalteten Einheiten bestimmt. Die Anzahl der verwalteten Einheiten darf die Gesamtanzahl der Lizenzen in allen aktiven XClarity Orchestrator Analytics-Lizenzschlüsseln nicht überschreiten. Wenn die Anzahl der XClarity Orchestrator Analytics-Lizenzen nicht konform ist (z. B. wenn Lizenzen ablaufen oder wenn die Verwaltung zusätzlicher Einheiten die Gesamtanzahl der aktiven Lizenzen überschreitet), haben Sie eine Kulanzeit von 90 Tagen, um die entsprechenden Lizenzen zu installieren. Wenn die Kulanzeit (einschließlich der kostenlosen Testversion) endet, bevor die erforderliche Anzahl an Lizenzen installiert ist, werden die Menüs **Überwachung → Analysen** deaktiviert und Sie können auf *allen Einheiten* keine Analysenberichte mehr anzeigen oder angepasste Alertregeln oder Abfragen erstellen.

Wichtig: Nach der Installation von XClarity Orchestrator Analytics-Lizenzen müssen Sie die Benutzerschnittstelle aktualisieren.

Anmerkung: Wenn Sie abgelaufene XClarity Orchestrator Analytics-Lizenzen installieren (die ihr Ablaufdatum über die 90-tägige Kulanzeit hinaus überschritten haben) und dann die Benutzerschnittstelle aktualisieren, sind die Analysefunktionen deaktiviert. Dies bedeutet, dass ein aktiver Test- oder Kulanzeitraum abgebrochen, die Analyseservices angehalten und die Analysefunktionen ausgegraut werden. (Dies kann einige Minuten dauern.) Durch den Import neuer gültiger Lizenzen können Sie die Analysefunktionen wieder aktivieren.

Eine Lizenz ist *nicht* an bestimmte Einheiten gebunden.

Der Aktivierungszeitraum beginnt, wenn die Lizenzen eingelöst werden.

Die Lizenzen werden mithilfe eines *Aktivierungsschlüssels* für die Lizenz installiert. Nachdem Sie Lizenzen eingelöst haben, können Sie einen Aktivierungsschlüssel für alle oder einen Teil der verfügbaren Lizenzen erstellen und dann den Aktivierungsschlüssel in XClarity Orchestrator herunterladen und installieren.

Jedes Mal, wenn XClarity Orchestrator nicht konform ist, wird die Kulanzeit auf 90 Tage zurückgesetzt.

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

Wenn Sie eine kostenlose Testlizenz verwenden oder zum Erreichen der Konformität über einen Kulanzeitraum verfügen und auf eine neuere Version von XClarity Orchestrator aktualisieren, wird die Testlizenz oder die Kulanzeit auf 90 Tage zurückgesetzt.

Bei der Aktualisierung von XClarity Orchestrator oder wenn ein Fehler auftritt, der erfordert, dass die Aktivierungsschlüssel wiederhergestellt werden müssen, können Sie entweder exportierte Aktivierungsschlüssel verwenden oder alle Aktivierungsschlüssel (für jede Kunden-ID) von [Features on Demand-Webportal](#) herunterladen und die Aktivierungsschlüssel (individuell oder zusammen als ZIP-Datei) anschließend in XClarity Orchestrator importieren.

Sie können eine Liste der aktuellen Softwarelizenzen vom [Features on Demand-Webportal](#) anzeigen.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Orchestrator-Lizenzen zu installieren.

Schritt 1. Wenden Sie sich an Ihren Lenovo Ansprechpartner oder einen autorisierten Business Partner, um Lizenzen entsprechend der gewünschten Anzahl verwalteter Einheiten zu erwerben.

Nachdem Sie Lizenzen erworben haben, wird Ihnen per E-Mail ein *elektronischer Berechtigungsnachweis* mit einem Autorisierungscode zugesandt. Sie können den Autorisierungscode auch von [Features on Demand-Webportal](#) abrufen, indem Sie auf **Berechtigungscodes abrufen** klicken. 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.

Der Autorisierungscode ist eine 22-stellige alphanumerische Zeichenfolge. Sie benötigen den Autorisierungscode, um den nächsten Schritt auszuführen.

Schritt 2. Rufen Sie die Aktivierungsschlüssel für die Lizenzen ab.

- **Aktivierungsschlüssel mithilfe eines Autorisierungscode erstellen**

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 Schlüssel 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 Autorisierungscode in einem anderen Aktivierungsschlüssel einlösen.

7. Befolgen Sie die Anweisungen, um Produktdetails und Kontaktinformationen einzugeben, und klicken Sie auf **Fortfahren**, um den Aktivierungsschlüssel zu generieren.
8. Geben Sie optional zusätzliche Empfänger für den Erhalt der Aktivierungsschlüssel an.

9. Klicken Sie auf **Senden**, um die Aktivierungsschlüssel zu senden. Die Person, die der Bestellung zugeordnet ist, und die zusätzlichen Empfänger erhalten eine E-Mail mit dem Aktivierungsschlüssel. Der Aktivierungsschlüssel ist eine Datei im KEY-Format.

Anmerkung: Sie können Aktivierungsschlüssel (einzeln oder als Paket) auch über [Features on Demand-Webportal](#) herunterladen. Klicken Sie dazu auf den Link **Herunterladen**.

- **Vorhandene Aktivierungsschlüssel herunterladen**

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 **Protokoll abrufen**.
3. Wählen Sie als **Suchtyp** „Protokoll über Lenovo Kundennummer durchsuchen“ aus.
4. Geben Sie Ihre Lenovo Kundennummer im Feld **Suchwert** ein. Das Format für die Kundennummer ist 121XXXXXXX.
5. Klicken Sie auf **Alle auswählen**, um alle Aktivierungsschlüssel herunterzuladen, oder wählen Sie einzelne Aktivierungsschlüssel aus der Liste aus.
6. Klicken Sie auf **E-Mail**, um die Schlüssel an sich selbst zu senden, oder klicken Sie auf **Herunterladen**, um die Schlüssel auf Ihr lokales System herunterzuladen.

Schritt 3. Wenden Sie die Lizenzen in XClarity Orchestrator an.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Wartung** (🔧) und dann auf die Registerkarte **Lizenzen**, um die Übersicht Lizenzinformationen aufzurufen.

Produkt	Lizenzschlüssel-Besch	Anzahl an Lizenzen	Ablaufdatum	Status
XClarity Orchestr...	Lenovo SYSTEM...	Unbegrenzt	01.03.22	Abgelaufen
XClarity Orchestr...	Lenovo SYSTEM...	100000	01.03.20	Abgelaufen

2. Klicken Sie auf das Symbol **Importieren und übernehmen** (📁), um die Lizenzen zu übernehmen.
3. Ziehen Sie den Aktivierungsschlüsseldatei für die Lizenzen, die Sie übernehmen möchten, in das Dialogfeld „Importieren“ oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen.

Um mehrere Aktivierungsschlüssel 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 **Importieren**, um die Lizenzen zu importieren und zu übernehmen. Wenn die Installation abgeschlossen ist, wird der Aktivierungsschlüssel für die Lizenz in der Tabelle mit der Anzahl der installierten Lizenzen und dem Aktivierungszeitraum (Start- und Ablaufdatum) aufgeführt.

Schritt 4. Wenn Sie die gültigen Lizenzen nach Deaktivierung der Funktionen übernommen haben, melden Sie sich ab und wieder an, um die entsprechenden Funktionen zu aktivieren.

Nach dieser Aufgabe

In der Übersicht Lizenzinformationen können Sie die folgenden Aktionen ausführen.

- Speichern Sie einen oder mehrere ausgewählte Aktivierungsschlüssel auf dem lokalen System, indem Sie auf das Symbol **Speichern** (↓) klicken.

Wenn Sie mehrere Aktivierungsschlüssel exportieren, werden die Dateien gemeinsam in einer ZIP-Datei heruntergeladen.

- Löschen Sie einen bestimmten Aktivierungsschlüssel über das Symbol **Löschen** (☒).

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 Autorisierungscode 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 den Lenovo Support 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 den Lenovo Support über -eSupport_-_Ops@lenovo.com.

Kapitel 6. Aktualisieren von XClarity Orchestrator

Sie können Lenovo XClarity Orchestrator aktualisieren, um die neueste Orchestrator-Software zu verwenden.

Vorbereitende Schritte

Weitere Informationen:  [XClarity Orchestrator aktualisieren](#)

Sie müssen ein Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** zugewiesen ist.

Ein XClarity Orchestrator Fix-Paket (z. B. v1.4.2) kann nur auf eine Version desselben Release (z. B. v1.4.0 oder v1.4.1) angewendet werden. Ein Fix-Paket enthält alle vorherigen Fixes (z. B. enthält v1.4.2 dieselben Fixes wie v1.4.1 plus zusätzliche Fixes), wobei ein Fix-Paket allerdings nicht die gesamte Codebasis enthält.

Achtung: Lesen Sie die folgenden Hinweise, bevor Sie die Aktualisierung von XClarity Orchestrator durchführen.

- **Auf XClarity Orchestrator v2.0.** Der für die virtuelle Einheit erforderliche Mindestspeicher ist die **insgesamt** 551 GB über drei angeschlossene Datenträger hinweg. Außerdem müssen Sie einen dritten Datenträger (Datenträger 2) mit mindestens 200 GB anhängen.

Die virtuelle XClarity Orchestrator-Einheit muss ausgeschaltet werden, bevor Sie eine neue Festplatte anhängen.

Gehen Sie wie folgt vor, um eine neue Festplatte zur virtuellen Einheit hinzuzufügen:

– Für ESXi mit VMware vSphere

1. Stellen Sie über VMware vSphere Client eine Verbindung zum Host her.
2. Schalten Sie die virtuelle Maschine von XClarity Orchestrator aus.
3. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Einstellungen bearbeiten**.
4. Wählen Sie **Neue Einheitenfestplatte → Festplatte hinzufügen** aus.
5. Ändern Sie die Größe zu 200 GB.
6. Klicken Sie auf **OK**.
7. Schalten Sie die virtuelle Maschine von XClarity Orchestrator ein.

– Für ESXi mit VMware vCenter

1. Stellen Sie über VMware vCenter eine Verbindung zum Host her.
2. Schalten Sie die virtuelle Maschine aus.
3. Klicken Sie mit der rechten Maustaste auf die Einstellungen der virtuellen Maschine und dann auf **Hinzufügen**.
4. Klicken Sie auf **Festplattenlaufwerk → Neuen virtuellen Datenträger erstellen**.
5. Wählen Sie für das Datenträgerformat **SCSI** aus.
6. Konfigurieren Sie die HDD-Kapazität auf 200 GB.
7. Klicken Sie auf **OK**.
8. Schalten Sie die virtuelle Maschine ein.

– Für Microsoft 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. Wählen Sie die virtuelle Maschine von XClarity Orchestrator aus und klicken Sie im Aktionsfenster auf **Herunterfahren**.
4. Klicken Sie auf **Einstellungen**, um das Dialogfenster Einstellungen zu öffnen.

5. Wählen Sie **IDE Controller 1** aus.
 6. Wählen Sie im rechten Bereich **Festplattenlaufwerk** aus und klicken Sie auf **Hinzufügen**, um eine neue Festplatte hinzuzufügen.
 7. Wählen Sie im rechten Bereich die **Datei der virtuellen Festplatte (.vhd)** aus und klicken Sie dann auf **Neu**, um den Assistenten für neue virtuelle Festplattenlaufwerke aufzurufen.
 8. Folgen Sie den Aufforderungen des Assistenten. Achten Sie darauf, dass Sie den Namen des Festplattenlaufwerks im VHD-Format angeben (z. B. LXC0-disk3.vhd) und legen Sie die Größe auf 200 GB fest.
 9. Wählen Sie die virtuelle Maschine von XClarity Orchestrator aus und klicken Sie im Fenster **Aktionen** auf **Starten**.
- **Auf XClarity Orchestrator v1.6.** Für eine Aktualisierung auf XClarity Orchestrator v1.6 ist XClarity Orchestrator v1.5 erforderlich. Wenn Sie nicht XClarity Orchestrator v1.5 ausführen, müssen Sie auf XClarity Orchestrator v1.5 aktualisieren, bevor Sie eine Aktualisierung auf XClarity Orchestrator v1.6 durchführen.
 - **Auf XClarity Orchestrator v1.5.** Für eine Aktualisierung auf XClarity Orchestrator v1.5 ist XClarity Orchestrator v1.4 erforderlich. Wenn Sie nicht XClarity Orchestrator v1.4 ausführen, müssen Sie auf XClarity Orchestrator v1.4 aktualisieren, bevor Sie eine Aktualisierung auf XClarity Orchestrator v1.5 durchführen.
 - **Auf XClarity Orchestrator v1.4.** Für eine Aktualisierung auf XClarity Orchestrator v1.4 ist XClarity Orchestrator v1.3 erforderlich. Wenn Sie nicht XClarity Orchestrator v1.3 ausführen, müssen Sie auf XClarity Orchestrator v1.3 aktualisieren, bevor Sie eine Aktualisierung auf XClarity Orchestrator v1.4 durchführen.
 - **Auf XClarity Orchestrator v1.3**
 - Die Aktualisierung auf XClarity Orchestrator v1.3 kann zwei Stunden oder länger dauern. Um festzustellen, ob die Aktualisierung abgeschlossen ist, klicken Sie auf **Wartung → Orchestrator-Serveraktualisierungen** und prüfen Sie, ob die neue Version aufgelistet ist und der angewendete Status nicht mehr „Anwenden“ lautet.
 - **Achtung:** Stellen Sie vor der Aktualisierung von XClarity Orchestrator auf v1.3 sicher, dass der Hostname der virtuellen XClarity Orchestrator-Einheit **lxco** lautet und auf der Karte DNS-Konfiguration auf der Seite **Verwaltung (⚙️) → Netzwerk** kein Domänenname festgelegt ist.
 - Benutzer, denen die Rolle **Supervisor** zugewiesen ist, werden während der Aktualisierung zur Benutzergruppe **SupervisorGroup** hinzugefügt.
 - Benutzer, denen die Rolle **Bediener** zugewiesen ist, werden während der Aktualisierung zur Benutzergruppe **OperatorLegacyGroup** hinzugefügt. Die Benutzergruppe **OperatorLegacyGroup** ist der Rolle **Bediener (veraltet)** zugeordnet, die Benutzern die gleichen Berechtigungen wie die Rolle **Operator** in vorherigen Versionen gewährt. Die Rolle **Bediener (veraltet)** und die Benutzergruppe **OperatorLegacyGroup** werden ab einer künftigen Version nicht mehr unterstützt. Vorhandene Benutzergruppen werden während der Aktualisierung der Rolle **Bediener** zugewiesen.
 - Die Erstellung von Regeln zum Auslösen angepasster Analyse-Alerts wurde in XClarity Orchestrator v1.3 vereinfacht. Vorhandene Regeln für angepasste Alerts werden nicht in das neue Format übernommen und gehen nach Abschluss der Aktualisierung verloren.
 - **Von XClarity Orchestrator v1.1**
 - Benutzer, denen die Rolle **Supervisor** zugewiesen ist, werden während der Aktualisierung zur Benutzergruppe **SupervisorGroup** hinzugefügt.
 - Benutzer, denen die Rolle **Bediener** zugewiesen ist, werden während der Aktualisierung zur Benutzergruppe **OperatorLegacyGroup** hinzugefügt. Die Benutzergruppe **OperatorLegacyGroup** ist der Rolle **Bediener (veraltet)** zugeordnet, die Benutzern die gleichen Berechtigungen wie die Rolle **Operator** in vorherigen Versionen gewährt. Die Rolle **Bediener (veraltet)** und die Benutzergruppe **OperatorLegacyGroup** werden ab einer künftigen Version nicht mehr unterstützt. Vorhandene Benutzergruppen werden während der Aktualisierung der Rolle **Bediener** zugewiesen.

- Die Erstellung von Regeln zum Auslösen angepasster Analyse-Alerts wurde in XClarity Orchestrator v1.3 vereinfacht. Vorhandene Regeln für angepasste Alerts werden nicht in das neue Format übernommen und gehen nach Abschluss der Aktualisierung verloren.
- Der für die virtuelle Einheit erforderliche Mindestspeicher ist **insgesamt 301 GB** über zwei angeschlossene Datenträger hinweg. Sie müssen den Speicher des Datenträgers 0 auf ein Minimum von 251 GB erhöhen. Außerdem müssen Sie einen zweiten Datenträger (Datenträger 1) mit einem Minimum von 100 GB anhängen. Die virtuelle XClarity Orchestrator-Einheit muss ausgeschaltet werden, bevor Sie eine neue Festplatte anhängen.

Gehen Sie wie folgt vor, um eine neue Festplatte zur virtuellen Einheit hinzuzufügen:

- **Für ESXi mit VMware vSphere**

1. Stellen Sie über VMware vSphere Client eine Verbindung zum Host her.
2. Schalten Sie die virtuelle Maschine von XClarity Orchestrator aus.
3. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Einstellungen bearbeiten**.
4. Wählen Sie **Neue Einheitenfestplatte → Festplatte hinzufügen** aus.
5. Ändern Sie die Größe zu 100 GB.
6. Klicken Sie auf **OK**.
7. Schalten Sie die virtuelle Maschine von XClarity Orchestrator ein.

- **Für ESXi mit VMware vCenter**

1. Stellen Sie über VMware vCenter eine Verbindung zum Host her.
2. Schalten Sie die virtuelle Maschine aus.
3. Klicken Sie mit der rechten Maustaste auf die Einstellungen der virtuellen Maschine und dann auf **Hinzufügen**.
4. Klicken Sie auf **Festplattenlaufwerk → Neuen virtuellen Datenträger erstellen**.
5. Wählen Sie für das Datenträgerformat **SCSI** aus.
6. Konfigurieren Sie die HDD-Kapazität auf 100 GB.
7. Klicken Sie auf **OK**.
8. Schalten Sie die virtuelle Maschine ein.

- **Für Microsoft 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. Wählen Sie die virtuelle Maschine von XClarity Orchestrator aus und klicken Sie im Aktionsfenster auf **Herunterfahren**.
4. Klicken Sie auf **Einstellungen**, um das Dialogfenster Einstellungen zu öffnen.
5. Wählen Sie **IDE Controller 0** aus.
6. Wählen Sie im rechten Bereich **Festplattenlaufwerk** aus und klicken Sie auf **Hinzufügen**, um eine neue Festplatte hinzuzufügen.
7. Wählen Sie im rechten Bereich die **Datei der virtuellen Festplatte (.vhd)** aus und klicken Sie dann auf **Neu**, um den Assistenten für neue virtuelle Festplattenlaufwerke aufzurufen.
8. Folgen Sie den Aufforderungen des Assistenten. Achten Sie darauf, dass Sie den Namen des Festplattenlaufwerks im VHD-Format angeben (z. B. LXC0-disk2.vhd) und legen Sie die Größe auf 100 GB fest.
9. Wählen Sie die virtuelle Maschine von XClarity Orchestrator aus und klicken Sie im Fenster **Aktionen** auf **Starten**.

- **Auf XClarity Orchestrator v1.1**

- Alle Benutzer werden automatisch zur Benutzergruppe **SupervisorGroup** hinzugefügt. Standardmäßig haben alle Benutzer nach Abschluss der Aktualisierung Supervisor-Berechtigungen.

Ein Supervisor-Benutzer kann die Supervisor-Berechtigungen für andere Benutzer entfernen, die nicht über diese Berechtigungen verfügen sollten.

- Vorhandene externe LDAP-Konfigurationen werden entfernt. Sie müssen externe LDAP-Authentifizierungsserver neu konfigurieren, nachdem die Aktualisierung abgeschlossen ist.

Während des Aktualisierungsvorgangs werden alle Benutzer abgemeldet, wenn der Orchestrator-Server neu gestartet wird. Sie müssen einige Minuten warten, bis der Neustart abgeschlossen ist. Nachdem die Aktualisierung abgeschlossen und ein Neustart durchgeführt wurde, löschen Sie den Cache des Webbrowsers und aktualisieren Sie den Webbrowser, bevor Sie sich wieder anmelden.

Stellen Sie sicher, dass die virtuelle XClarity Orchestrator-Einheit vor der Installation einer Aktualisierung gesichert wird (siehe [Verwaltungsserverdaten sichern und wiederherstellen](#) in der Onlinedokumentation zu XClarity Orchestrator).

Stellen Sie vor dem Aktualisieren von XClarity Orchestrator sicher, dass alle benötigten Ports und Internetadressen verfügbar sind. Weitere Informationen finden Sie in den Abschnitten [Portverfügbarkeit](#) und [Firewalls und Proxy-Server](#).

Vorgehensweise

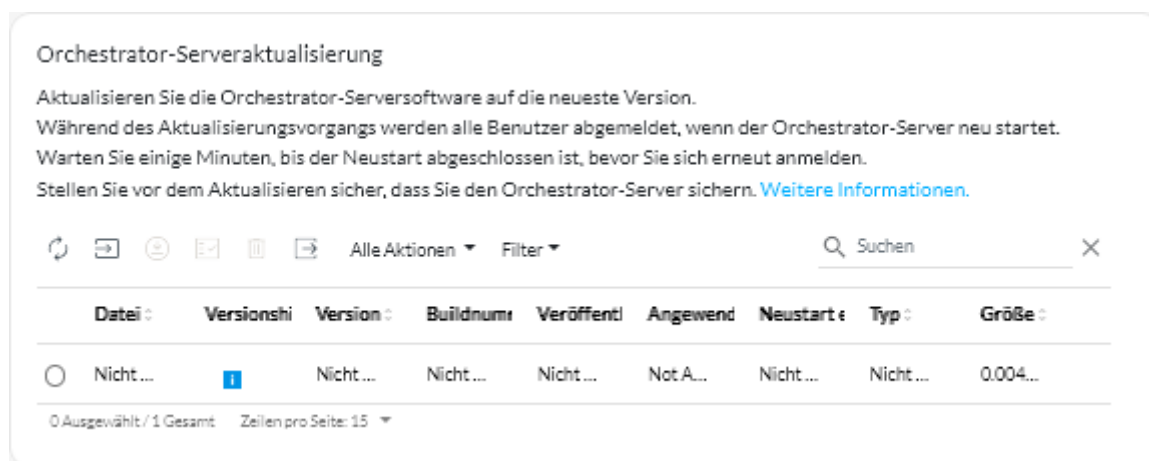
So aktualisieren Sie XClarity Orchestrator.

Schritt 1. Laden Sie die Aktualisierungspaketdatei (.tgz) für Orchestrator-Server von [XClarity Orchestrator Downloads-Website](#) auf eine Arbeitsstation herunter, die über eine Netzwerkverbindung zum XClarity Orchestrator-Host verfügt.

Die Aktualisierungspaketdatei enthält alle erforderlichen Dateien: Nutzlastdatei (.tar.gz), Metadaten (.xml), Änderungsprotokoll (.chg) und Readme (.txt).

Schritt 2. Klicken Sie im XClarity Orchestrator-Hauptmenü auf **Wartung**  und dann auf **Orchestrator-Serveraktualisierungen**, um die Übersicht Orchestrator-Serveraktualisierungen anzuzeigen.

Orchestrator-Serveraktualisierungen, die älter als die derzeit installierte Version sind, werden in der Tabelle mit dem angewendeten Status „Nicht zutreffend“ aufgeführt und können nicht auf den Orchestrator-Server angewendet werden.



Orchestrator-Serveraktualisierung

Aktualisieren Sie die Orchestrator-Serversoftware auf die neueste Version.
Während des Aktualisierungsvorgangs werden alle Benutzer abgemeldet, wenn der Orchestrator-Server neu startet.
Warten Sie einige Minuten, bis der Neustart abgeschlossen ist, bevor Sie sich erneut anmelden.
Stellen Sie vor dem Aktualisieren sicher, dass Sie den Orchestrator-Server sichern. [Weitere Informationen](#).

Alle Aktionen Filter Suchen

Datei	Versionshi	Version	Buildnumr	Veröffentli	Angewend	Neustart	Typ	Größe
Nicht...	1	Nicht...	Nicht...	Nicht...	Not A...	Nicht...	Nicht...	0.004...

0 Ausgewählt / 1 Gesamt Zellen pro Seite: 15

Schritt 3. Klicken Sie auf das Symbol **Importieren** , um das Dialogfeld „Importieren“ anzuzeigen.

Schritt 4. Ziehen Sie die gesamte Aktualisierungspaketdatei (.tgz) in das Dialogfenster Importieren oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen.

Schritt 5. Klicken Sie auf **Importieren**.

Achtung: Das Importieren der Aktualisierungsdateien kann eine Weile dauern. Sie müssen in der Übersicht Orchestrator-Serveraktualisierungen bleiben, bis der Importvorgang abgeschlossen ist. Wenn Sie die Übersicht Orchestrator-Serveraktualisierungen verlassen, wird der Importvorgang abgebrochen.

Wenn der Import abgeschlossen ist, wird die Orchestrator-Serveraktualisierung in der Tabelle in der Übersicht Orchestrator-Serverdateien aufgeführt.

Sie können den Importfortschritt überwachen, indem Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Jobs** klicken.

Schritt 6. Wählen Sie in der Übersicht Orchestrator-Serverdateien das zu installierende Aktualisierungspaket aus.

Schritt 7. Klicken Sie auf das Symbol **Aktualisierung übernehmen** (📄).

Sie können den Aktualisierungsfortschritt überwachen, indem Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Jobs** klicken.

Schritt 8. Warten Sie, bis die Aktualisierung abgeschlossen und XClarity Orchestrator neu gestartet ist. Der Aktualisierungsprozess kann eine Weile dauern.

Wenn Sie Zugriff auf den Host der virtuellen Einheit haben, können Sie den Status der Konsole der virtuellen Einheit überwachen, z. B.

```
Lenovo XClarity Orchestrator Version x.x.x
```

```
-----  
eth0      Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56  
          inet addr: 192.0.2.10  Bcast 192.0.2.255  Mask 255.255.255.0  
          inet6 addr: 2001:db8:56ff:fe80:bea3/64  Scope:Link
```

```
=====  
=====  
You have 118 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  
  3. To select subnet for Lenovo XClarity virtual appliance internal network  
  x. To continue without changing IP settings  
... ..
```

Schritt 9. Löschen Sie den Cache des Webbrowsers und aktualisieren Sie den Webbrowser.

Wenn die Aktualisierung abgeschlossen ist, ändert sich die Spalte **Angewendeter Status** in „Angewendet“.

Nach dieser Aufgabe

In der Übersicht Orchestrator-Serverdateien können Sie die folgenden Aktionen ausführen.

- Sie können die aktuelle Version und Buildnummer für die XClarity Orchestrator-Instanz aufrufen, indem Sie auf das Menü **Benutzerkonto** (👤) in der XClarity Orchestrator-Titelleiste und dann auf **Info** klicken.
- Zeigen Sie den Aktualisierungsverlauf für eine bestimmte Aktualisierung an, die auf XClarity Orchestrator angewendet wurde, indem Sie auf den Link „Update-Status“ in der Spalte **Angewendeter Status** klicken.
- Speichern Sie eine ausgewählte Orchestrator-Serveraktualisierung auf dem lokalen System. Klicken Sie dazu auf das Symbol **Speichern unter** (💾).
- Löschen Sie eine ausgewählte Orchestrator-Serveraktualisierung, indem Sie auf das Symbol **Löschen** klicken (🗑️).

Kapitel 7. XClarity Orchestrator deinstallieren

Sie können die virtuelle Lenovo XClarity Orchestrator-Einheit mithilfe der Verwaltungstools für virtuelle Maschinen deinstallieren.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Orchestrator zu deinstallieren.

Schritt 1. Trennen Sie alle Ressourcenmanager-Verbindungen und entfernen Sie sie.

- a. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) → **Ressourcenmanager**, um die Übersicht Ressourcenmanager aufzurufen.
- b. Wählen Sie alle Ressourcenmanager aus.
- c. Klicken Sie auf das Symbol für **Löschen** (🗑️).

Schritt 2. Deinstallieren Sie XClarity Orchestrator mithilfe der Verwaltungstools für virtuellen Maschinen.

- **ESXi mit VMware vCenter**

1. Stellen Sie über VMware vCenter eine Verbindung zum Host her.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine XClarity Orchestrator im Bestand des **VMware Host**-Clients und wählen Sie **Gastbetriebssystem** aus dem Popup-Menü aus.
3. Klicken Sie auf **Herunterfahren**.
4. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine im Bestand des **VMware-Host**-Clients und wählen Sie **Gastbetriebssystem** aus dem Popup-Menü aus.
5. Klicken Sie auf **Löschen**.

- **ESXi mit VMware vSphere**

1. Stellen Sie über VMware vSphere Client eine Verbindung zum Host her.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine XClarity Orchestrator 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 XClarity Orchestrator und dann auf **Herunterfahren**.
4. Klicken Sie erneut mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Löschen**.

Lenovo