



Lenovo XClarity Orchestrator Benutzerhandbuch



Version 2.1

Anmerkung

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

Zweite Ausgabe (Juli 2024)

© 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
Zusammenfassung der Änderungeniii
Kapitel 1. Lenovo XClarity Orchestrator – Übersicht	1
Bei XClarity Orchestrator anmelden	3
Tipps und Verfahren für die Benutzerschnittstelle.	7
Kapitel 2. XClarity Orchestrator verwalten.	11
Ressourcenmanager verbinden	11
Einheiten ermitteln und verwalten	15
Hinweise zur Verwaltung von Einheiten	16
Globale Ermittlungseinstellungen konfigurieren	21
Server verwalten.	22
ThinkEdge Client-Einheiten verwalten	27
Speichereinheiten verwalten	31
Gehäuse verwalten.	34
Verwaltung von Einheiten aufheben	37
VMware Tools verwenden	38
Netzwerkeinstellungen konfigurieren	38
Datum und Uhrzeit konfigurieren	41
Mit Sicherheitszertifikaten arbeiten	42
Vertrauenswürdige Zertifikate für externe Dienste hinzufügen.	44
Vertrauenswürdige Zertifikate für interne Dienste hinzufügen.	45
Ein vertrauenswürdige, extern signiertes XClarity Orchestrator-Serverzertifikat installieren	46
Intern signiertes XClarity Orchestrator-Serverzertifikat neu generieren	48
Das Serverzertifikat in einen Webbrowser importieren	50
Authentifizierung verwalten	51
Externen LDAP-Authentifizierungsserver konfigurieren	51
Benutzer und Benutzersitzungen verwalten	55
Benutzer erstellen	55
Benutzergruppen erstellen	57
Details für Ihren Benutzeraccount ändern	60
Details für einen anderen Benutzer ändern	61
Benutzersicherheitseinstellungen konfigurieren	62
Aktive Benutzersitzungen überwachen	67
Zugriff auf Funktionen steuern	67

Rollen Benutzern zuweisen	69
Zugriff auf Ressourcen steuern	69
Ressourcenbasierten Zugriff aktivieren	70
Zugriffssteuerungslisten erstellen	71
Plattenspeicher verwalten	73
Neustart von XClarity Orchestrator	74
Orchestrator-Serverdaten sichern und wiederherstellen	75
Orchestrator-Serverdaten auf einem VMware ESXi-Host sichern und wiederherstellen	76
Orchestrator-Serverdaten auf einem Microsoft Hyper-V-Host sichern und wiederherstellen	77

Kapitel 3. Ressourcen und Aktivitäten überwachen	79
Übersicht über Ihre Umgebung anzeigen	79
Status und Details von Ressourcenmanagern anzeigen	83
Status von Einheiten anzeigen	84
Einheitendetails anzeigen	87
Status und Details zu Infrastrukturrressourcen anzeigen	89
Jobs überwachen	91
Aktive Alerts überwachen	93
Überwachen von Ereignissen	95
Ereignisse und Alerts ausschließen	96
Ereignis-, Bestands- und Metrikdaten weiterleiten	98
Filter für die Datenweiterleitung erstellen	99
Ereignisse an SAP Data Intelligence weiterleiten.	103
Ereignisse an einen REST-Webservice weiterleiten.	105
Ereignisse an einen E-Mail-Service über SMTP weiterleiten	107
Bestand und Ereignisse an Splunk weiterleiten.	113
Ereignisse an ein Syslog weiterleiten	114
Metrikdaten an ein Lenovo TruScale Infrastructure Services weiterleiten	117
Berichte weiterleiten	119
Zielonfigurationen für Weiterleiter erstellen	120
Berichte per E-Mail weiterleiten	121

Kapitel 4. Ressourcen verwalten	125
Ressourcengruppen erstellen	125
Einheiten offline verwalten.	128
Stromversorgungsaktionen auf verwalteten Servern ausführen	128

Fernsteuerungssitzung für verwaltete Server öffnen	130
Fernsteuerungssitzung für ThinkSystem oder ThinkAgile Server öffnen	130
Fernsteuerungssitzung für ThinkServer Server öffnen	131
Fernsteuerungssitzung für System x-Server öffnen	132

Kapitel 5. Ressourcen bereitstellen139

Serverkonfigurationen bereitstellen	139
Hinweise zur Serverkonfiguration	141
Serverkonfigurationsmuster von einem vorhandenen Server übernehmen	142
Serverkonfigurationsmuster zuordnen und implementieren	145
Serverkonfigurationskonformität pflegen	149
Betriebssysteme bereitstellen	150
Hinweise zur Betriebssystembereitstellung	152
Unterstützte Betriebssysteme	155
Betriebssystem-Image-Profile	156
Portverfügbarkeit für implementierte Betriebssysteme	159
Betriebssystem-Images importieren	160
Betriebssystemprofile konfigurieren	162
Ein Betriebssystem-Image implementieren	164
Aktualisierungen für verwaltete Ressourcen bereitstellen	167
Bereitstellungshinweise aktualisieren	169
Aktualisierungen herunterladen und importieren	171
Aktualisierungskonformitätsrichtlinien erstellen und zuordnen	175
Aktualisierungen für Ressourcenmanager anwenden und aktivieren	179
Aktualisierungen für verwaltete Server anwenden und aktivieren	182

Kapitel 6. Trends analysieren und Probleme vorhersagen.187

Angepasste Analyseberichte erstellen	187
Regeln für angepasste Analyse-Alerts erstellen	187
Angepasste Berichte erstellen (Abfragen)	190
Bootzeiten der Einheit analysieren	193
Verbindungsprobleme analysieren	194
Sicherheitskorrekturen analysieren	194
Integrität des Laufwerks analysieren	195
Firmware analysieren	195
Verlorene Ereignisse analysieren	196
Kapazität des Ressourcenmanagers analysieren und vorhersagen	196
Auslastungstrends analysieren und vorhersagen	197
Leistungs- und Nutzungsmetriken analysieren	198
Wiederholte Ereignisse analysieren	199
Nicht autorisierte Anmeldeversuche analysieren	200
Integrität der Einheit analysieren	200
Infrastrukturressourcenzustand analysieren	202
Aktive Alerts analysieren	203

Kapitel 7. Mit Service und Unterstützung arbeiten205

Regelmäßig Daten an Lenovo senden	205
Service-daten für XClarity Orchestrator erfassen	206
Service-daten für Einheiten erfassen	208
Service-daten für Einheiten importieren	210
Kontakte für Service und Support erstellen und zuordnen	211
Service-Tickets mit Call-Home-Funktion automatisch öffnen	212
Service-Ticket im Lenovo Support-Center manuell öffnen	216
Service-Tickets und Status anzeigen	218
Informationen zur Garantie anzeigen	221

Zusammenfassung der Änderungen

Nachfolgeversionen der Lenovo XClarity Orchestrator-Verwaltungssoftware unterstützen neue Softwareverbesserungen und Fixes.

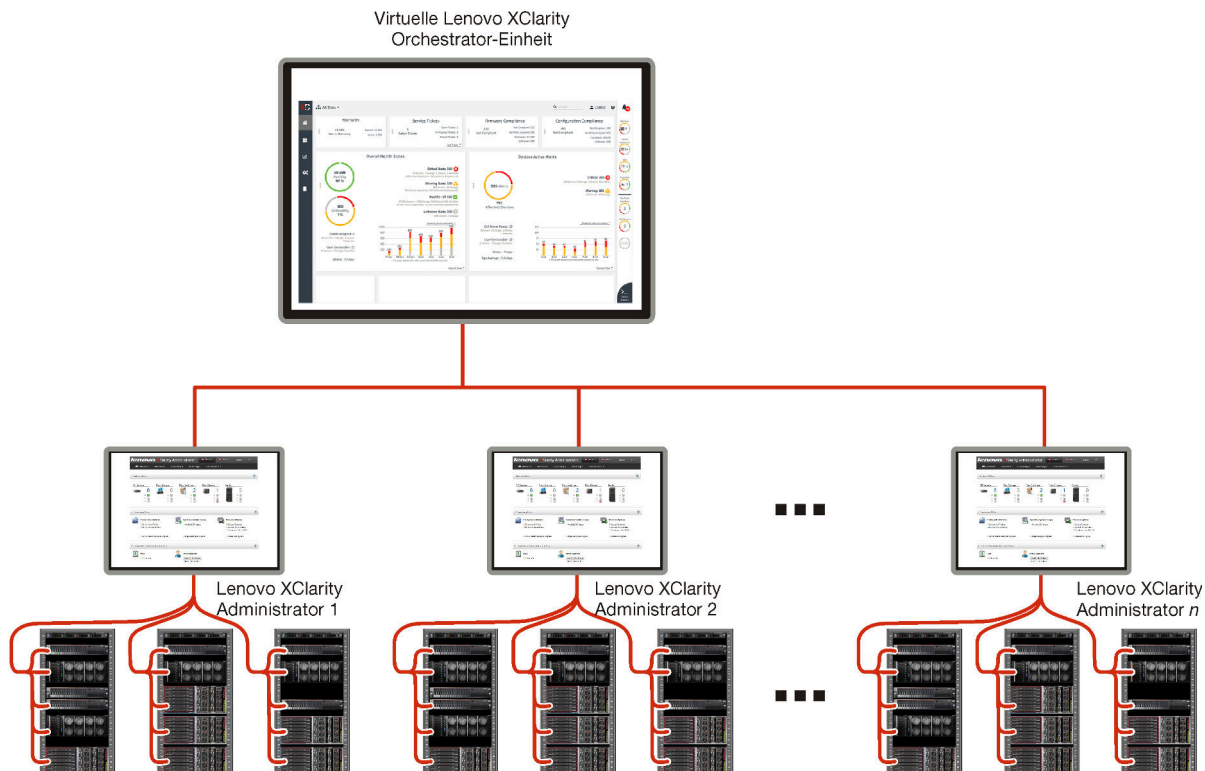
Informationen zu Fixes finden Sie in der Änderungsprotokolldatei (*.chg), die im Aktualisierungspaket enthalten ist.

Diese Version unterstützt die folgenden Optimierungen an der Verwaltungssoftware. Informationen zu Änderungen in früheren Versionen finden Sie unter [Neuerungen](#) in der Onlinedokumentation zu XClarity Orchestrator.

Funktion	Beschreibung
Verwaltung	Sie können den Orchestrator-Server über die Benutzerschnittstelle neu starten (siehe Neustart von XClarity Orchestrator).
Ressourcen verwalten	Lenovo XClarity Management Hub 2.0 ist ein neuer schlanker Einheitenmanager, mit dem Sie Lenovo ThinkSystem und ThinkEdge Server verwalten können (siehe Ressourcenmanager verbinden). Mit der Massenverwaltungsoption können Sie eine große Anzahl von Servern verwalten (siehe Server verwalten). Sie können Server mithilfe von vollständig qualifizierten Domännennamen verwalten (siehe Server verwalten).
Ressourcen und Aktivitäten überwachen	Speicherbestandsdaten werden jetzt in einem Tabellenformat angezeigt (siehe Einheitendetails anzeigen). Sie können eine Liste aller geplanten Jobs anzeigen (siehe Jobs überwachen).
Ressourcen bereitstellen	Sie können planen, dass eine Firmwareaktualisierung zu einem bestimmten Datum und einer bestimmten Uhrzeit ausgeführt wird (siehe Aktualisierungen für verwaltete Server anwenden und aktivieren).

Kapitel 1. Lenovo XClarity Orchestrator – Übersicht

Lenovo XClarity Orchestrator bietet eine zentrale Überwachung, Verwaltung, Bereitstellung sowie Analysen für Umgebungen mit einer großen Anzahl von Einheiten. Vorhandene Ressourcenmanager (z. B. Lenovo XClarity Administrator und Schneider Electric EcoStruxure IT Expert) an mehreren Standorten werden genutzt, um den Gesamtzustand anzuzeigen, Zusammenfassungen zu Einheitenbestand und -zustand zu sammeln, Details zu den Einheiten zu überprüfen, Ereignis- und Prüfprotokolle anzuzeigen und Updates auf verwaltete Ressourcen anzuwenden.



Weitere Informationen:

- [XClarity Orchestrator Übersicht](#)
- [Verwaltungsfunktionen](#)

Zentrale Überwachung und Verwaltung von Ressourcen

XClarity Orchestrator bietet eine zentrale Schnittstelle zum Überwachen und Verwalten von Ressourcenmanagern und den über diese Ressourcenmanager verwalteten Einheiten.

- Zusammenfassungsansichten zum Zustand Ihrer verwalteten Ressourcen, einschließlich Ressourcenmanagern, Einheiten und Infrastrukturrressourcen (z. B. PDUs und USVs)
- Zusammenfassungs- und ausführliche Ansichten von Komponentenzustand, Ressourcenbestand, Garantiestatus und der Hinweise für Einheiten für mehrere Standorte
- Aggregation kritischer Alerts und Ereignisse, Erstellung angepasster Alerts und Weiterleitung von Ereignissen an externe Anwendungen
- Lebenszyklussteuerung für verwaltete Einheiten (einschließlich Stromversorgungsvorgänge)
- Launch-in-Context zur Benutzerschnittstelle für Ressourcenmanager und verwaltete Einheiten aus den Einheitenübersichten

Bereitstellen von Aktualisierungen

Sie können XClarity Orchestrator verwenden, um aktuelle Softwareversionen auf verwalteten Ressourcen zu verwalten. Mithilfe des Aktualisierungskatalogs können Sie herausfinden, welche Softwareversionen verfügbar sind. Verwenden Sie Aktualisierungskonformitätsrichtlinien, um zu ermitteln, welche Ressourcen basierend auf benutzerdefinierten Kriterien aktualisiert werden müssen, und implementieren Sie dann die gewünschten Aktualisierungen für diese Ressourcen. XClarity Orchestrator stellt sicher, dass die Software auf den Zielressourcen in der richtigen Reihenfolge bereitgestellt wird.

XClarity Orchestrator unterstützt die folgenden Bereitstellungsvorgänge.

- Aktualisierungen auf Lenovo XClarity Administrator Ressourcenmanager implementieren
- Firmwareaktualisierungen auf Einheiten bereitstellen, die von XClarity Administrator verwaltet werden

Weitere Informationen zum Bereitstellen von Aktualisierungen finden Sie unter [Aktualisierungen für verwaltete Ressourcen bereitstellen](#).

Serverkonfiguration bereitstellen

Mithilfe einer konsistenten Konfiguration können Sie verwaltete Server bereitstellen. Konfigurationseinstellungen (z. B. Baseboard Management Controller- und UEFI-Einstellungen) werden als Muster gespeichert, das auf mehrere Server angewendet werden kann.

XClarity Orchestrator stellt Konfigurationsmuster nicht direkt auf verwalteten Servern bereit. Stattdessen wird eine Anfrage an den zuständigen Ressourcenmanager gesendet, um einen Auftrag zur Durchführung der Bereitstellung zu starten, und dann den Fortschritt des Auftrags zu verfolgen.

Weitere Informationen zum Bereitstellen von Serverkonfigurationen finden Sie unter [Serverkonfigurationen bereitstellen](#).

Betriebssysteme bereitstellen

Sie können XClarity Orchestrator verwenden, um Betriebssystem-Images auf mehreren Servern zu implementieren.

XClarity Orchestrator stellt Betriebssysteme nicht direkt auf verwalteten Servern bereit. Stattdessen wird eine Anfrage an den zuständigen XClarity Administrator Ressourcenmanager gesendet, um einen Auftrag zur Durchführung der Aktualisierung zu starten, und dann den Fortschritt des Auftrags zu verfolgen.

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

Weitere Informationen zum Bereitstellen von Serverkonfigurationen finden Sie unter [Betriebssysteme bereitstellen](#).

Maschinelles Lernen von geschäftlichen Informationen und prädiktive Analysen

XClarity Orchestrator kann aus folgenden Gründen Verbindungen zu Services von Drittanbietern (z. B. Splunk) für das maschinelle Lernen von geschäftlichen Informationen und prädiktive Analysen herstellen:

- Erfassen und Anzeigen von Trenddaten (z. B. Prozessor- und Hauptspeicherauslastung, Stromverbrauch, Temperatur, unbefugter Zugriff, wiederholte und verlorene Ereignisse und durchschnittliche Zeit zwischen Prozessen wie Firmwareaktualisierungen und Systemneustarts)
- Verwendet metrische Daten, um Fehler vorherzusagen (z. B. wiederholte Ereignisse und Zustandsberichte)
- Erstellen benutzerdefinierter Analyseberichte basierend auf vorhandenen Daten, einschließlich Alerts, Ereignissen, Einheitenbestand und -metriken

- Definieren von Regeln für angepasste Alerts, die – sofern aktiviert – Alerts auslösen, wenn bestimmte Bedingungen in Ihrer Umgebung zutreffen

Weitere Informationen:  [Analyse- und Vorhersagefunktionen](#)

Weitere Informationen zur vorausschauenden Analyse finden Sie unter [Trends analysieren und Probleme vorhersagen](#).

Service und Support

XClarity Orchestrator kann so installiert werden, dass Diagnosedateien automatisch gesammelt und mithilfe der Call-Home-Funktion an den Lenovo Support gesendet werden, wenn bestimmte wartungsfähige Ereignisse in verwalteten Ressourcen auftreten. Sie können Diagnosedateien auch manuell sammeln, einen Problemdatensatz öffnen und Diagnosedateien an das Lenovo Support-Center senden.

Weitere Informationen zu Service und Support finden Sie unter [Mit Service und Unterstützung arbeiten](#).

Dokumentation

Die englischsprachige Onlinedokumentation wird regelmäßig aktualisiert. Die aktuellen Informationen und Verfahren finden Sie unter [XClarity Orchestrator Onlinedokumentation](#).

Die Onlinedokumentation ist in den folgenden Sprachen verfügbar:

- Englisch (en)
- Vereinfachtes Chinesisch (zh-CN)
- Traditionelles Chinesisch (zh-TW)
- Französisch (fr)
- Deutsch (de)
- Italienisch (it)
- Japanisch (ja)
- Koreanisch (ko)
- Portugiesisch, Brasilien (pt-BR)
- Russisch (ru)
- Spanisch (es)
- Thailändisch (th)

Sie können die Sprache der Onlinedokumentation folgendermaßen ändern.

- Fügen Sie nach `https://pubs.lenovo.com/lxco/` z. B. `<language_code>` hinzu, um die Onlinedokumentation in vereinfachtem Chinesisch anzuzeigen.
`https://pubs.lenovo.com/lxco/zh-CN/`

Bei XClarity Orchestrator anmelden

Melden Sie sich bei der Lenovo XClarity Orchestrator-Webschnittstelle über ein System an, das über eine Netzwerkverbindung zur virtuellen Einheit von XClarity Orchestrator verfügt.

Vorbereitende Schritte

Vergewissern Sie sich, dass Sie einen der folgenden unterstützten Webbrowser verwenden: Siehe [Unterstützte Hardware und Software](#) in der Onlinedokumentation zu XClarity Orchestrator 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.

Wenn Sie ein LDAP-Benutzeraccount verwenden, können Sie sich mit dem Benutzernamen oder mit `benutzername@domain` (z. B. `user1@company.com`) anmelden.

XClarity Orchestrator meldet Benutzersitzungen automatisch ab, die für eine bestimmte Zeit inaktiv waren, oder die für einen bestimmten Zeitraum geöffnet waren, und zwar unabhängig von der Aktivität. Die folgenden Standardwerte werden von XClarity Orchestrator festgelegt.

- Wenn Sie die Benutzerschnittstelle **30 Minuten** lang nicht angeklickt oder keine Eingabe gemacht haben, wird Ihre Benutzersitzung auf schreibgeschützte Vorgänge beschränkt. Wenn Sie versuchen, Daten zu ändern, wird die Benutzersitzung automatisch beendet.
- Wenn Sie Daten seit **1440 Minuten** (24 Stunden) nicht aktiv aufgerufen haben, wird die Benutzersitzung automatisch beendet.
- Nach **24 Stunden** werden Benutzersitzungen unabhängig von der Benutzeraktivität automatisch beendet.

Vorgehensweise

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

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`

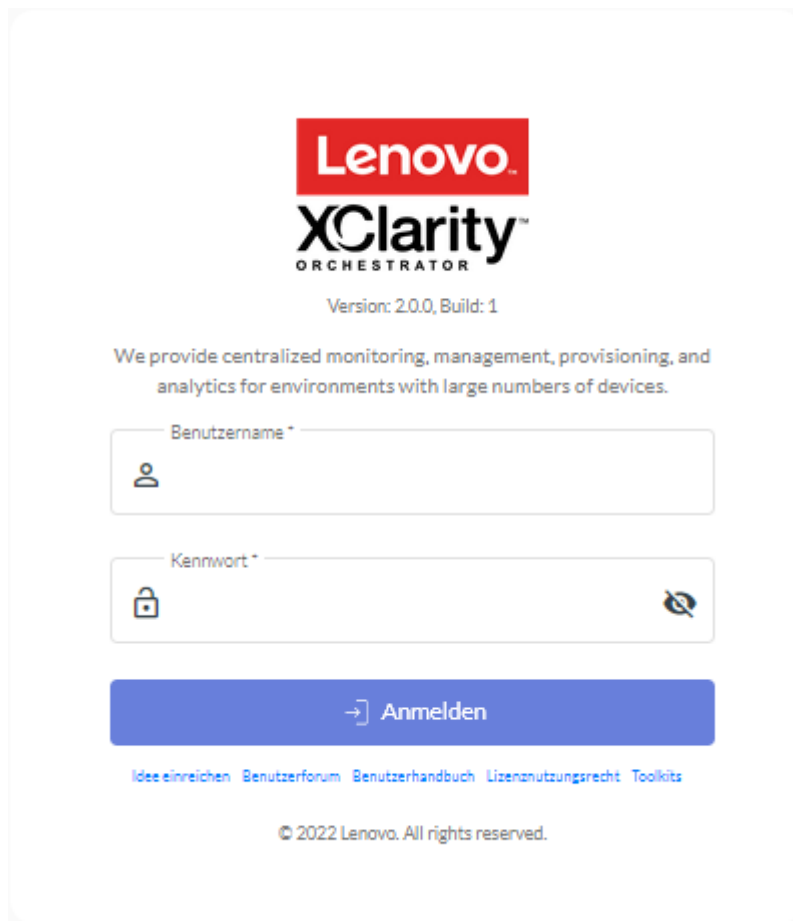
- **Einen DHCP-Server in derselben Übertragungsdomäne wie XClarity Orchestrator verwenden** Wenn ein DHCP-Server in derselben Übertragungsdomäne wie XClarity Orchestrator eingerichtet ist, greifen Sie über die IPv4-Adresse, die in der Konsole der virtuellen Einheit von XClarity Orchestrator angezeigt 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 eine gültige Benutzer-ID und ein gültiges Kennwort 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

Im XClarity Orchestrator-Dashboard wird eine Zusammenfassung des Zustands und der Aktivitäten von Ressourcen in Ihrer Umgebung angezeigt.

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

- Ändern Sie das Kennwort des aktuellen Benutzers, indem Sie auf **Kennwort ändern** klicken.
- Sie können sich durch Klicken auf **Abmelden** von der aktuellen Sitzung abmelden. Die XClarity Orchestrator-Anmeldeseite wird angezeigt.

Auf der Anmeldeseite können Sie auf den Link **Lizenznutzungsrecht** klicken, um das [Features on Demand-Webportal](#) zu öffnen, wo Sie alle Lenovo Produktlizenzen finden und verwalten können.

- 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.
- Laden Sie das XClarity Orchestrator PowerShell-Toolkit (LXCOPSTool) herunter, indem Sie auf **Toolkits** klicken. LXCOPSTool enthält eine Bibliothek mit Cmdlets, um die Bereitstellung und Ressourcenverwaltung von einer Microsoft-PowerShell-Sitzung zu automatisieren.
- Informationen zur Verwendung von XClarity Orchestrator mithilfe des eingebetteten Hilfesystems finden Sie durch Klicken auf **Hilfe**.

Die englischsprachige Onlinedokumentation wird regelmäßig aktualisiert. Die aktuellen Informationen und Verfahren finden Sie unter [XClarity Orchestrator Onlinedokumentation](#).

- Sie können Informationen zur XClarity Orchestrator-Version durch Klicken auf **Info** anzeigen.

Im Dialogfenster Info finden Sie Links zum Aufrufen der **Lizenzvereinbarung für Endbenutzer**, der **Open-Source-Lizenzen** und der **Lenovo Datenschutzerklärung**.

- Sie können die Sprache der Benutzerschnittstelle durch Klicken auf **Sprache ändern** ändern. Die folgenden Sprachen werden unterstützt.
 - Englisch (en)
 - Vereinfachtes Chinesisch (zh-CN)
 - Traditionelles Chinesisch (zh-TW)
 - Französisch (fr)
 - Deutsch (de)
 - Italienisch (it)
 - Japanisch (ja)
 - Koreanisch (ko)
 - Portugiesisch, Brasilien (pt-BR)
 - Russisch (ru)

- Spanisch (es)
- Thailändisch (th)

Tipps und Verfahren für die Benutzerschnittstelle

Beachten Sie diese Tipps und Verfahren, wenn Sie die Lenovo XClarity Orchestrator- und Lenovo XClarity Management Hub-Benutzerschnittstellen verwenden.

Dateien importieren

Sie können Dateien importieren, indem Sie diese in ein Dialogfeld „Importieren“ ziehen und ablegen.

Wenn Sie eine Datei importieren, wird in der unteren rechten Ecke der Benutzerschnittstelle ein erweiterbares Popup mit Informationen über den Fortschritt und Status jedes Importvorgangs angezeigt. Über die Symbole in dem Popup können Sie den Bearbeitungsstatus für jeden Import schnell identifizieren. Nachdem ein Import erfolgreich abgeschlossen wurde, wird ein Auftrag gestartet, um die Datei zu validieren. Wenn während des Importvorgangs ein Fehler auftritt, wird im Popup eine Fehlermeldung angezeigt, die Ihnen dabei hilft, das Problem schnell zu beheben.

Wenn das Popup ausgeblendet ist, können Sie auf das Symbol zum **Ziehen** (☷) klicken und die Maustaste gedrückt halten, um das Popup an eine andere Position zu verschieben.

Klicken Sie auf **Alle löschen**, um die Liste der abgeschlossenen Importvorgänge zu löschen. Wenn alle Importvorgänge abgeschlossen sind, wird das Popup ausgeblendet.

Text in Textfeldern eingeben

Welche Zeichen eingegeben werden können, ist bei einigen Textfeldern eingeschränkt. Die folgende Liste enthält die zulässigen Zeichen.

- **Namen.** Enthält alle Buchstaben und Ziffern in unterstützten Sprachen und die Sonderzeichen @ - _ + / [] . , : und Leerzeichen.
- **Beschreibungen.** Enthält alle Buchstaben und Ziffern in unterstützten Sprachen und die Sonderzeichen @ - _ % & * + = / () { } [] . , : und Leerzeichen.
- **Kennwörter.** Für lokale Benutzeraccounts können Kennwörter standardmäßig **8 – 256** Zeichen lang sein, wobei mindestens 16 Zeichen empfohlen werden. Für Kennwörter gibt es keine Zeicheneinschränkungen. Kennwörter müssen jedoch bestimmte Zeichentypen enthalten, und einige Zeichenfolgen sind aus Sicherheitsgründen eingeschränkt.
 - 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).

Navigationfenster erweitern und ausblenden

Der Navigationsbereich ist standardmäßig ausgeblendet und zeigt nur Symbole an, die bestimmte Menüelemente darstellen. Sie können auf ein Symbol klicken, um den Navigationsbereich und das Menü für dieses Symbol vorübergehend zu erweitern. Wenn Sie den Cursor aus dem Navigationsfenster bewegen, wird der Bereich ausgeblendet, sodass nur die Symbole angezeigt werden.

Um den Navigationsbereich dauerhaft zu erweitern, klicken Sie auf das Symbol für **Erweitern** (☰). Sie können den Navigationsbereich dann ausblenden, indem Sie auf das Symbol für **Ausblenden** (✕) klicken.

Bereich der Benutzerschnittstelle einschränken

XClarity Orchestrator zeigt standardmäßig Daten zu *allen Ressourcen* an. Sie können die angezeigten Daten in der aktuellen Benutzersitzung auf die Ressourcen beschränken, die sich in bestimmten Ressourcenmanagern und -gruppen befinden, indem Sie das Dropdown-Menü **Aktueller Bereich** oben auf der Seite verwenden. Im Dropdown-Menü können Sie die Liste der Ressourcenmanager und -gruppen im aktuellen Bereich anzeigen, indem Sie **Meine Bereichsliste** auswählen. Wenn Sie auf **Bereich ändern** klicken, wird ein Dialogfenster angezeigt, in dem Sie einen angepassten Bereich mit mehreren Ressourcenmanagern und -gruppen erstellen können. Sie können auch **Alle Ressourcen** auswählen, um den Bereich zur Anzeige von allen Ressourcen zu ändern.

Der ausgewählte Bereich wird nur während der aktuellen Benutzersitzung beibehalten. Sie können mehrere Benutzersitzungen mit jeweils verschiedenen Ansichten von Dashboard, Ressourcen, Ereignissen und Alertdaten öffnen.

Anmerkung: VMware vRealize Operations Manager Ressourcenmanager sind nicht in der Liste der Ressourcenmanager enthalten, da sie keine Einheiten in XClarity Orchestrator verwalten.

Mehr oder weniger Daten pro Seite anzeigen

Ändern Sie die Anzahl der Zeilen, die in einer Tabelle pro Seite angezeigt werden. Verwenden Sie dazu die Dropdown-Liste **Zeilen pro Seite** unten in der Tabelle. Sie können 10, 15, 25 oder 50 Zeilen anzeigen.

Daten in großen Listen suchen

Es gibt mehrere Möglichkeiten, um eine Teilmenge einer großen Liste auf der Grundlage bestimmter Kriterien anzuzeigen.

- Sie können die Tabellenzeilen mit einem Klick auf die Spaltenüberschrift sortieren.
- Sie können die angezeigten Daten in der aktuellen Benutzersitzung auf die Ressourcen beschränken, die sich in einem bestimmten Ressourcenmanager oder in einer bestimmten Ressourcenbgruppe befinden, indem Sie oben auf der Seite das Dropdown-Menü **Aktueller Bereich** verwenden (siehe „Bereich der Benutzerschnittstelle einschränken“ oben).
- Über die Eingabefelder **Filter** können Sie dynamisch eine Teilmenge von Listen basierend auf Daten erstellen, die in bestimmten Spalten gefunden werden. Sie können nach angezeigten und ausgeblendeten Spalten filtern. Sie können auch Filterabfragen speichern, die regelmäßig verwendet werden sollen.
- Sie können die Teilmenge weiter verfeinern, indem Sie im Feld **Suchen** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um nach Daten zu suchen, die in jeder verfügbaren Spalte gefunden werden.

Tipp: Trennen Sie mehrere Suchbegriffe durch ein Komma. „180,190“ zeigt z. B. alle Zeilen an, die 180 oder 190 in einer der verfügbaren Spalten enthalten.

- Aktivieren Sie das Kontrollkästchen im Tabellenkopf, um alle in der Tabelle aufgeführten Elemente auszuwählen oder zu entfernen.

Tabellendaten anzeigen

Aktualisieren Sie Datentabellen, indem Sie auf das Symbol **Aktualisieren** (↻) klicken.

Sie können die einzelnen Zeilen erweitern oder reduzieren, um Details in Tabellen mit erweiterbaren Zeilen anzuzeigen oder auszublenden (z. B. für Jobs oder die Übersichten „Repository-Verwaltung“). Sie können auch auf das Symbol **Alle ausblenden** (☰) klicken, um die Details für sämtliche Zeilen auszublenden.

Wenn die Spaltengröße verhindert, dass alle Informationen in der Tabellenzelle angezeigt werden (durch Auslassungspunkte gekennzeichnet), können Sie die vollständigen Informationen in einem Dialogfenster anzeigen, indem Sie den Mauszeiger über die Zelle bewegen.

Tabellendaten exportieren

Exportieren Sie die Daten in der aktuellen Tabelle in Ihr lokales System, indem Sie auf das Symbol **Daten exportieren** (📄) klicken. Sie können alle Seiten, die aktuelle Seite oder die ausgewählten Zeilen exportieren, das Dateiformat (XLSX, CSV oder JSON) auswählen und angeben, ob alle Spalten oder nur sichtbaren Spalten berücksichtigt werden sollen. Für das CSV-Format können Sie auch angeben, wie die Daten getrennt werden sollen (mit einem Semikolon, einer Registerkarte oder einem Pipe-Zeichen).

Tipp: Beim JSON-Format geben die Zeitstempel in den exportierten Daten die Zeitzone an, die für XClarity Orchestrator und nicht für das lokale System festgelegt ist. Beim CSV- und XLSX-Format werden Zeitstempel in die Zeitzone des Benutzers umgewandelt, die in der Webschnittstelle angezeigt wird.

Wenn Sie Daten exportieren, wird in der unteren rechten Ecke der Benutzerschnittstelle ein erweiterbares Popup mit Informationen über Fortschritt und Status angezeigt. Über die Symbole in dem Popup können Sie den Verarbeitungsstatus für jeden Export schnell identifizieren. Wenn während des Exportvorgangs ein Fehler auftritt, wird im Popup eine Fehlermeldung angezeigt, die Ihnen dabei hilft, das Problem schnell zu beheben.

Wenn das Popup ausgeblendet ist, können Sie auf das Symbol zum **Ziehen** (☰) klicken und die Maustaste gedrückt halten, um das Popup an eine andere Position zu verschieben.

Klicken Sie auf **Alle löschen**, um die Liste der abgeschlossenen Exportvorgänge zu löschen. Wenn alle Exportvorgänge abgeschlossen sind, wird das Popup ausgeblendet.

Tabellenspalten konfigurieren

Sie können Tabellen so konfigurieren, dass die Informationen angezeigt werden, die für Sie am wichtigsten sind.

- Sie können auswählen, welche Spalten ein- oder ausgeblendet werden sollen, indem Sie auf **Alle Aktionen → Spalten ein-/ausschalten** klicken.
- Sie können Spalten neu anordnen, indem Sie die Spaltenüberschriften an die bevorzugte Position ziehen.

Die Sprache der Benutzerschnittstelle ändern

Sie können die Sprache der Benutzerschnittstelle ändern, wenn Sie sich zum ersten Mal anmelden.



Nachdem Sie sich angemeldet haben, können Sie die Sprache ändern, indem Sie auf das Menü

Benutzerkonto (👤) und dann auf **Spracher ändern** klicken.

Anmerkung: Das Hilfesystem wird in derselben Sprache angezeigt, die für die Benutzerschnittstelle festgelegt wurde.

Hilfe anfordern

Es gibt verschiedene Möglichkeiten, um Hilfe zur Benutzerschnittstelle zu erhalten.

- Auf einigen Seiten können Sie den Cursor über ein **Hilfe**-Symbol () bewegen, um ein Popup-Fenster mit zusätzlichen Details zu einem bestimmten Feld anzuzeigen.
- Auf einigen Seiten können Sie auf den Link **Weitere Informationen** klicken, um das Hilfesystem zu öffnen und weitere Informationen für den Kontext zu erhalten.
- Sie erhalten Hilfe zur Ausführung von bestimmten Aktionen über die Benutzerschnittstelle, wenn Sie auf das Menü **Benutzerkonto** () und dann auf **Hilfe** klicken. Die englischsprachige Onlinedokumentation wird regelmäßig aktualisiert. Die aktuellen Informationen und Verfahren finden Sie unter [XClarity Orchestrator Onlinedokumentation](#).

Kapitel 2. XClarity Orchestrator verwalten

Es stehen mehrere Verwaltungsaktivitäten zur Verfügung, z. B. die Konfiguration von Systemeinstellungen wie Datum/Uhrzeit und Netzwerkzugriff, die Verbindung von Ressourcenmanagern, die Verwaltung von Authentifizierungsservern und des Benutzerzugriffs sowie die Verwaltung von Sicherheitszertifikaten.

Ressourcenmanager verbinden

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

Vorbereitende Schritte

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

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 [XClarity Management Hub 2.0 mit XClarity Orchestrator verbinden](#) in der Onlinedokumentation zu XClarity Orchestrator.

- **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 [XClarity Management Hub mit XClarity Orchestrator verbinden](#) in der Onlinedokumentation zu XClarity Orchestrator.

- **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 Infrastrukturreourcen.
- **VMware vRealize Operations Manager.**

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

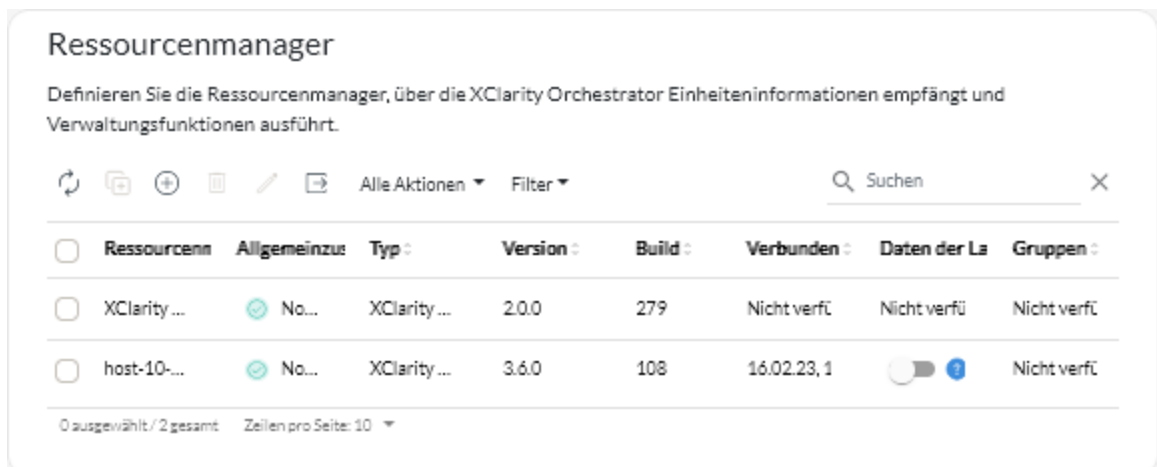
- Informationen zu allen Einheiten abrufen, die vom Ressourcenmanager verwaltet werden.
- Im Verwaltungsserver einen Ereignisweiterleiter (für einen REST-Webservice) erstellen und aktivieren, um Ereignisse zu überwachen und an XClarity Orchestrator weiterzuleiten.

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

In der Übersicht Ressourcenmanager können Sie die folgenden Aktionen ausführen.

- Sie können den Verbindungsstatus für den Ressourcenmanager in der Spalte **Allgemeinzustand** anzeigen.
- Sie können die Anmeldeinformationen und Eigenschaften eines bestimmten Ressourcenmanagers bearbeiten, indem Sie auf das Symbol **Bearbeiten** (✎) klicken. 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).
- Aktivieren oder Deaktivieren der Datenerfassung für die Laufwerkanalyse für einen ausgewählten XClarity Administrator Ressourcenmanager über das Symbol **Bearbeiten** (✎).

Anmerkung: Die Umschalt-Schaltfläche **Datenerfassung für die Laufwerkanalyse** ist deaktiviert, wenn XClarity Administrator Probleme mit der Verbindung oder Anmeldeinformationen hat (siehe [Plötzlicher Verbindungsabbruch zu einem Ressourcenmanager](#) in der Onlinedokumentation zu XClarity Orchestrator).

- Sie können einen bestimmten Ressourcenmanager trennen und löschen, indem Sie auf das Symbol **Löschen** klicken (🗑️).

Anmerkung: Wenn XClarity Orchestrator keine Verbindung zum Ressourcenmanager herstellen kann, weil z. B. wenn die Anmeldeinformationen abgelaufen sind oder es Netzwerkprobleme gibt, wählen Sie **Trennen erzwingen** aus.

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).

Wenn der Ressourcenmanager entfernt wird, werden alle von diesem Ressourcenmanager verwalteten Geräte ebenfalls entfernt. Dazu gehören Einheitenbestand, Protokolle, Metrikdaten und analytische Berichte.

- Probleme beim Verbinden eines Ressourcenmanagers beheben (siehe [Ressourcenmanager kann nicht verbunden werden](#) in der Onlinedokumentation zu XClarity Orchestrator).

Einheiten ermitteln und verwalten

Sie können Einheiten mit Lenovo XClarity Orchestrator ermitteln und verwalten und die Verwaltung dieser Einheiten einem bestimmten Ressourcenmanager zuordnen.

Vorbereitende Schritte

Zur Durchführung dieser Aufgabe müssen Sie Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** oder **Sicherheitsadministrator** zugewiesen ist.

Zu dieser Aufgabe

XClarity Orchestrator überwacht und verwaltet Einheiten über Ressourcenmanager. Wenn Sie einen Ressourcenmanager verbinden, verwaltet XClarity Orchestrator alle Einheiten, die von diesem Ressourcenmanager verwaltet werden.

Sie können Einheiten auch mit XClarity Orchestrator verwalten. XClarity Orchestrator listet Einheiten auf, die von den Ressourcenmanagern bereits ermittelt (aber nicht verwaltet) wurden. Wenn Sie ermittelte Einheiten mit XClarity Orchestrator verwalten, werden die Einheiten vom Ressourcenmanager verwaltet, der sie ermittelt hat. Wenn Sie Einheiten manuell mithilfe von IP-Adressen, Hostnamen oder Subnetzen ermitteln und verwalten, wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten. XClarity Management Hub kann zur Verwaltung von ThinkEdge Client-Einheiten verwendet werden. XClarity Management Hub 2.0 kann zur Verwaltung von ThinkServer Einheiten verwendet werden. Lenovo XClarity Administrator kann zur Verwaltung von Servern, Speicher, Switches und Gehäusen verwendet werden.

Anmerkungen:

- Wenn Sie versuchen, eine Einheit über XClarity Management Hub 2.0 zu verwalten, die bereits über einen anderen XClarity Management Hub 2.0 verwaltet wird, entfernt XClarity Orchestrator den Benutzeraccount zur Verwaltung und die Abonnements der Einheit ohne die Bestätigung des alten Verwaltungshubs und verwaltet die Einheit dann erneut über den neuen Verwaltungshub. Nach diesem Prozess gilt die Einheit weiterhin als durch den alten Verwaltungshub verwaltet, ist aber offline und sendet keine Daten mehr an ihn. Beachten Sie, dass Sie die Verwaltung der Einheiten vom ersten Verwaltungshub manuell über das verbundene Portal aufheben müssen.
- Wenn Sie versuchen, eine Einheit über XClarity Management Hub 2.0 zu verwalten, die bereits über einen anderen XClarity Administrator verwaltet wird, entfernt XClarity Orchestrator den Benutzeraccount zur Verwaltung, die Abonnements, LDAP- und SSO-Informationen der Einheit, die von XClarity Administrator beim XCC registriert sind, ohne die Bestätigung durch XClarity Administrator von der Einheit und verwaltet die Einheit dann erneut über den neuen XClarity Management Hub 2.0. Nach diesem Prozess gilt die Einheit weiterhin als durch den XClarity Administrator-Hub verwaltet, ist aber offline und sendet keine Daten mehr an ihn. Beachten Sie, dass Sie die Verwaltung der Einheiten vom XClarity Administrator manuell über das verbundene Portal aufheben müssen.

Die folgenden Einheiten können automatisch von Ressourcenmanagern mithilfe eines Service-Ermittlungsprotokolls ermittelt werden.

- ThinkSystem und ThinkAgile Server und Einheiten
- ThinkEdge SE Server
- Flex System Gehäuse, und ThinkSystem und Flex System Einheiten in einem Flex System Gehäuse
- ThinkServer Rack- und Tower-Server
- System x, Converged HX und NeXtScale Server und Einheiten
- Speichereinheiten

Die folgenden Einheiten können *nicht* automatisch von Ressourcenmanagern mithilfe eines Service-Ermittlungsprotokolls ermittelt werden. Sie müssen den UDC-Agent auf diesen Einheiten installieren, bevor dieser sicher ermittelt und verwaltet werden können.

- ThinkCentre Client
- ThinkEdge Clients

Derzeit können Sie keine Switches mit XClarity Orchestrator verwalten. Sie können zudem nicht die Verwaltung von Flex System-Switches mit XClarity Orchestrator aufheben.

Hinweise zur Verwaltung von Einheiten

Lesen Sie die folgenden Hinweise, bevor Sie versuchen, Einheiten mit XClarity Orchestrator zu ermitteln und zu verwalten.

- [Allgemeine Hinweise](#)
- [Hinweise zum Server](#)
- [Hinweise zum Speicher](#)
- [Hinweise zum Switch](#)
- [Hinweise zum Gehäuse](#)
- [Hinweise zur Verwendung mehrerer Verwaltungstools](#)

Allgemeine Hinweise

Stellen Sie sicher, dass XClarity Orchestrator die zu verwaltenden Einheiten unterstützt.

Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jedem System installiert ist, das Sie verwalten möchten.

Für die Kommunikation mit den Einheiten müssen bestimmte Ports verfügbar sein. Stellen Sie sicher, dass alle erforderlichen Ports verfügbar sind, bevor Sie versuchen, Server zu verwalten.

XClarity Orchestrator kann Einheiten in der Umgebung automatisch ermitteln. Dabei wird nach verwaltbaren Einheiten gesucht, die im gleichen IP-Subnetz wie XClarity Orchestrator sind und ein Service-Ermittlungsprotokoll verwenden. Zur Ermittlung von Einheiten in anderen Subnetzen können Sie manuell IP-Adressen, Hostnamen, IP-Adressbereiche oder Subnetze angeben.

Nachdem die Einheiten von XClarity Orchestrator verwaltet werden, fragt XClarity Orchestrator alle verwalteten Speichereinheiten regelmäßig ab, um Informationen zu sammeln, z. B. Bestand, elementare Produktdaten und Status.

Falls XClarity Orchestrator beim Erfassen von Bestandsdaten während des Verwaltungsprozesses die Kommunikation mit einer Einheit verliert (z. B. wegen eines Stromausfalls oder Netzwerkfehlers oder wenn die Einheit offline ist), wird die Verwaltung erfolgreich abgeschlossen, allerdings sind einige Bestandsinformationen möglicherweise unvollständig. Warten Sie, bis die Einheit wieder online ist und XClarity Orchestrator den Bestand von der Einheit abfragt oder erfassen Sie den Bestand der Einheit manuell mit der Webschnittstelle des Ressourcenmanagers. Wählen Sie dazu die Einheit aus und klicken Sie auf **Alle Aktionen** → **Bestand** → **Bestand aktualisieren**.

Einheiten können immer nur von jeweils einem Ressourcenmanager (XClarity Orchestrator, XClarity Management Hub 2.0, XClarity Management Hub oder XClarity Administrator) verwaltet werden. Wenn eine Einheit von einem Ressourcenmanager verwaltet wird und Sie sie mit einem anderen Ressourcenmanager verwalten möchten, müssen Sie zuerst die Verwaltung der Einheit mit dem ursprünglichen Ressourcenmanager aufheben.

Wenn Sie die IP-Adresse einer Einheit ändern, nachdem diese von XClarity Orchestrator verwaltet wird, erkennt dieser die neue IP-Adresse und verwaltet den Server weiterhin. Allerdings wird die IP-Adressänderung für einige Server von XClarity Orchestrator nicht erkannt. Falls XClarity Orchestrator anzeigt,

dass der Server nach der IP-Adressänderung offline ist, können Sie den Server mit der Option **Verwaltung erzwingen** wieder verwalten.

Wenn Sie Adapter in einer Einheit entfernen, austauschen oder konfigurieren, starten Sie die Einheit mindestens einmal neu, um die Bestandsinformationen zu aktualisieren.

Um eine Einheit zu ermitteln, die sich in einem *anderen* Subnetz als der Ressourcenmanager befindet, muss eine der folgenden Bedingungen erfüllt sein:

- Stellen Sie sicher, dass die Multicast-SLP-Weiterleitung für die Rack-Switches sowie Router in Ihrer Umgebung aktiviert ist. Lesen Sie die mit dem jeweiligen Switch oder Router bereitgestellte Dokumentation, um herauszufinden, ob die Multicast-SLP-Weiterleitung aktiviert ist und falls nicht, wie Sie sie aktivieren können.
- Wenn SLP auf der Einheit oder im Netzwerk deaktiviert ist, können Sie stattdessen die DNS-Ermittlungsmethode nutzen, indem Sie manuell einen Servicedatensatz (SRV) auf Ihrem Domain-Name-Server (DNS) hinzufügen. Beispiel:
`lxco.company.com service = 0 0 443 server1.company.com`
Aktivieren Sie anschließend die DNS-Ermittlung bei der BMC über die Verwaltungsweboberfläche, indem Sie auf **BMC-Konfiguration** → **Netzwerk** und anschließend auf die Registerkarte **DNS** klicken.

Hinweise zur Kapselung

Sie können die Kapselung bei Gehäuse und Servern während des Einheitenverwaltungsprozesses aktivieren. Wenn die globale Kapselungseinstellung aktiviert ist und die Einheit Kapselung unterstützt, kommuniziert der Ressourcenmanager mit der Einheit während des Verwaltungsprozesses, um den Kapselungsmodus der Einheit in **encapsulationLite** zu ändern. Außerdem werden die Firewallregeln auf der Einheit so eingestellt, dass eingehende Anforderungen nur vom Ressourcenmanager akzeptiert werden.

Anmerkung: Wenn die Verwaltungsnetzwerkschnittstelle zur Verwendung des Dynamic Host Configuration Protocol (DHCP), kann die Verwaltung von Einheiten mit aktivierter Kapselung sehr viel Zeit in Anspruch nehmen.

Die globale Kapselungseinstellung ist standardmäßig deaktiviert. Wenn die Einstellung deaktiviert ist, wird der Kapselungsmodus für die Einheiten auf **Normal** gesetzt und die Firewallregeln werden nicht während des Einheitenverwaltungsprozesses geändert.

Achtung: Wenn der Kapselungsmodus auf verwalteten Einheiten **encapsulationLite** ist, können die folgenden Situationen Kommunikations- und Authentifizierungsprobleme zwischen dem Ressourcenmanager und den verwalteten Einheiten verursachen, wodurch die verwalteten Einheiten nicht mehr erreichbar sind. Da die Einheiten so konfiguriert sind, dass sie TCP-Anforderungen von anderen Quellen ignorieren, ist der Zugriff auf diese Einheiten über eine Netzwerkschnittstelle nicht möglich. In den meisten Fällen reagieren diese Einheiten nicht auf Ping-, SSH- oder TELNET-Anforderungen.

- Netzwerkänderungen beim Hypervisor, auf dem der Ressourcenmanager ausgeführt wird
- Änderungen bei VLANs (Virtual Local Area Networks) oder VLAN-Tags
- Permanente Änderungen bei IP-Adressen der Einheiten bei aktivierter Kapselung
- Erzwungene Verwaltungsaufhebung bei einer Einheit bei aktivierter Kapselung
- Verlust der virtuellen Ressourcenmanager-Maschine
- Verlust der TCP-Kommunikation zwischen der virtuellen Maschine und den verwalteten Einheiten
- Andere Netzwerkprobleme, die verhindern, dass der Ressourcenmanager direkt mit verwalteten Einheiten kommuniziert, während der Kapselungsmodus aktiviert ist

Wenn ein permanentes Problem auftritt, führen Sie eine der folgenden Aktionen aus, um wieder Zugriff auf die zuvor verwalteten Einheiten zu erhalten. Weitere Informationen finden Sie in den Abschnitten [Kapselungsverwaltung](#), [Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen](#) und [Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen](#) in der Onlinedokumentation zu XClarity Administrator.

- Um bei aktivierter Kapselung wieder Zugriff auf ein verwaltetes IMM zu erhalten, müssen die Standardeinstellungen über die grafische UEFI-Benutzerschnittstelle von der lokalen Konsole geladen werden.
- Verwenden Sie die USB-to-Ethernet-Bridge, um In-Band-Zugriff auf den Management-Controller zu erhalten, und führen Sie den folgenden Befehl aus:
encaps lite -off
- Um bei aktivierter Kapselung wieder Zugriff auf ein verwaltetes CMM zu erhalten, müssen die Standardeinstellungen über die Taste zum Zurücksetzen an der Rückseite oder Ausführen des folgenden Befehls geladen werden, wenn die Konsole noch erreichbar ist:
accesscontrol -off -T mm[p]

Hinweise zum Server

Stellen Sie sicher, dass CIM over HTTPS auf der Einheit aktiviert ist. Melden Sie sich bei der Verwaltungswebsiteschnittstelle für den Server mit dem Benutzeraccount RECOVERY_ID an. Klicken Sie auf **BMC-Konfiguration → Sicherheit** und anschließend auf die Registerkarte **CIM over HTTPS**. Stellen Sie sicher, dass **CIM over HTTPS aktivieren** ausgewählt ist.

Wenn Sie Verwaltungsaktionen auf einem Server ausführen, muss der Server entweder ausgeschaltet sein oder über die BIOS/UEFI-Konfiguration oder ein laufendes Betriebssystem ausgeführt werden (siehe [Stromversorgungsaktionen auf verwalteten Servern ausführen](#)). Sollte der Server ohne Betriebssystem gestartet werden, wird er vom Management-Controller bei dem Versuch, ein Betriebssystem zu finden, wiederholt zurückgesetzt.

Stellen Sie sicher, dass in den UEFI-Einstellungen des Servers sämtliche Einstellungen für UEFI_Ethernet_* und UEFI_Slot_* aktiviert sind. Zur Überprüfung der Einstellungen starten Sie den Server neu. Wenn die Eingabeaufforderung „Press <F1> Setup“ angezeigt wird, drücken Sie **F1**, um Setup Utility zu starten. Navigieren Sie zu **Systemeinstellungen → Einheiten und E/A-Anschlüsse → Unterstützung für Adapteroptions-ROM aktivieren/deaktivieren** und suchen Sie den Bereich **UEFI-Options-ROMs aktivieren/deaktivieren**. Stellen Sie dort sicher, dass die Einstellungen aktiviert sind. Diese Einstellungen können Sie auch mithilfe der Remote-Konsole (sofern diese Funktion unterstützt wird) in der Baseboard Management Controller-Schnittstelle remote prüfen und ändern.

Wenn das Serverzertifikat der Einheit von einer externen Zertifizierungsstelle signiert ist, müssen Sie sicherstellen, dass das Zertifizierungsstellen und alle Zwischenzertifikate in den [Ein vertrauenswürdiges, extern signiertes XClarity Orchestrator-Serverzertifikat installieren](#)-Truststore importiert werden (siehe XClarity Orchestrator).

ThinkEdge Client-Einheiten

ThinkEdge Client-Einheiten verfügen nicht über Baseboard Management Controller und können daher nicht mithilfe der Service-Ermittlungsprotokolle ermittelt werden. Sie müssen einen UDC-Agent auf ThinkEdge Client-Einheiten installieren, bevor die Einheiten vom zugeordneten Lenovo XClarity Management Hub Ressourcenmanager sicher ermittelt und verwaltet werden können. Siehe [ThinkEdge Client-Einheiten verwalten](#) für weitere Informationen.

ThinkSystem SR635 und SR655 Server

Stellen Sie sicher, dass ein Betriebssystem installiert ist und dass der Server mit dem Betriebssystem gestartet wurde, bootfähige Datenträger angehängt sind oder mindestens einmal EFI-Shell ausgeführt wurde, sodass XClarity Orchestrator Bestandsdaten für diese Server erfassen kann.

Vergewissern Sie sich, dass IPMI-über-LAN aktiviert ist. IPMI-over-LAN ist auf diesen Servern standardmäßig deaktiviert und muss manuell aktiviert werden, bevor die Server verwaltet werden können. Um IPMI over LAN über die ThinkSystem System Manager-Websiteschnittstelle zu aktivieren, klicken Sie auf **Einstellungen → IPMI-Konfiguration**. Möglicherweise müssen Sie den Server neu starten, damit die Änderung übernommen wird.

ThinkServer-Server

Der Hostname des Servers muss mit einem gültigen Hostnamen oder einer gültigen IP-Adresse konfiguriert sein, damit diese Server automatisch ermittelt werden können.

Die Netzwerkkonfiguration muss den SLP-Datenverkehr zwischen XClarity Orchestrator und dem Server zulassen.

Unicast-SLP ist erforderlich.

Zur automatischen Ermittlung von ThinkServer Servern ist Multicast-SLP erforderlich. Zudem muss SLP in ThinkServer System Manager (TSM) aktiviert sein.

Wenn die ThinkServer-Server in einem anderen Netzwerk sind als XClarity Orchestrator, muss das Netzwerk so konfiguriert sein, dass eingehender UDP-Datenverkehr über Port 162 zulässig ist, damit XClarity Orchestrator Ereignisse zu diesen Einheiten erhalten kann.

System x3950 X6 Server

Diese Server müssen als zwei 4U-Gehäuse mit jeweils einem eigenen Baseboard Management Controller verwaltet werden.

Weitere Informationen zur Verwaltung von Servern finden Sie unter [Server verwalten](#) und [ThinkEdge Client-Einheiten verwalten](#).

Hinweise zum Speicher

Stellen Sie vor der Ermittlung und Verwaltung von Rack-Speichereinheiten (außer ThinkSystem DE Serie) sicher, dass die folgenden Anforderungen erfüllt sind.

- Die Netzwerkkonfiguration muss den SLP-Datenverkehr zwischen dem Ressourcenmanager und der Rack-Speichereinheit zulassen.
- Unicast-SLP ist erforderlich.
- Sollen die Lenovo Storage-Einheiten automatisch von XClarity Orchestrator ermittelt werden, ist Multicast-SLP erforderlich. Zudem muss SLP in der Rack-Speichereinheit aktiviert sein.

Weitere Informationen zur Verwaltung von Speichereinheiten finden Sie unter [Speichereinheiten verwalten](#).

Hinweise zum Switch

Die Verwaltung von Rack-Switches mit XClarity Orchestrator wird derzeit nicht unterstützt.

Hinweise zum Gehäuse

Wenn Sie ein Gehäuse verwalten, werden auch alle Einheiten im Gehäuse verwaltet. Komponenten im Gehäuse können nicht unabhängig vom Gehäuse ermittelt und verwaltet werden.

Stellen Sie sicher, dass die Einstellung „Anzahl gleichzeitig aktiver Sitzungen für LDAP-Benutzer“ im CMM für das Gehäuse auf 0 (null) gesetzt ist. Sie können diese Einstellung über die CMM-Webschnittstelle überprüfen, indem Sie auf **BMC-Konfiguration** → **Benutzeraccounts** klicken, dann **Globale Anmeldeeinstellungen** und anschließend die Registerkarte **Allgemein** wählen.

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

Erwägen Sie die Implementierung von IPv4- oder IPv6-Adressen für alle CMMs und Flex System-Switches, die von XClarity Orchestrator verwaltet werden. Wenn Sie IPv4 für einige CMMs und Flex-Switches und IPv6

für andere implementieren, werden einige Ereignisse möglicherweise nicht im Prüfprotokoll (oder als Audit-Traps) erfasst.

Um ein Gehäuse zu ermitteln, das sich in einem *anderen* Subnetz als der Ressourcenmanager befindet, muss eine der folgenden Bedingungen erfüllt sein:

- Stellen Sie sicher, dass die Multicast-SLP-Weiterleitung für die Rack-Switches sowie Router in Ihrer Umgebung aktiviert ist. Lesen Sie die mit dem jeweiligen Switch oder Router bereitgestellte Dokumentation, um herauszufinden, ob die Multicast-SLP-Weiterleitung aktiviert ist und falls nicht, wie Sie sie aktivieren können.
- Wenn SLP auf der Einheit oder im Netzwerk deaktiviert ist, können Sie stattdessen die DNS-Ermittlungsmethode nutzen, indem Sie manuell einen Servicedatensatz (SRV) auf Ihrem Domain-Name-Server (DNS) hinzufügen. Beispiel:
`lxco.company.com service = 0 0 443 cmm1.company.com`
Aktivieren Sie anschließend die DNS-Ermittlung bei der BMC über die Verwaltungswebsiteschnittstelle, indem Sie auf **BMC-Konfiguration** → **Netzwerk** und anschließend auf die Registerkarte **DNS** klicken.

Weitere Informationen zum Verwalten von Gehäusen finden Sie unter [Gehäuse verwalten](#).

Hinweise zur Verwendung mehrerer Verwaltungstools

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

ThinkSystem-, ThinkServer- und System x-Einheiten

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

Flex System-Einheiten

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

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

Globale Ermittlungseinstellungen konfigurieren

Wählen Sie die bevorzugten Einstellungen zur Ermittlung von Einheiten aus.

Vorgehensweise

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.

Schritt 2. Klicken Sie auf ⚙️ **Konfiguration**, um das Dialogfenster Ermittlungseinstellungen anzuzeigen.

Schritt 3. Wählen Sie die bevorzugten Ermittlungseinstellungen aus.

- **SLP-Ermittlung** Gibt an, ob Einheiten automatisch mithilfe von SLP (Service Location Protocol) ermittelt werden.

Wenn diese Option aktiviert ist, versucht XClarity Orchestrator alle 15 Minuten und bei jeder Benutzeranmeldung, neue Einheiten zu ermitteln.

Anmerkung: Die SLP-Ermittlungseinstellung, die Sie in XClarity Orchestrator auswählen, überschreibt alle ausgewählten SLP-Ermittlungseinstellungen für Lenovo XClarity Administrator-Instanzen, die von XClarity Orchestrator verwaltet werden. Wenn die SLP-Ermittlungseinstellung in Lenovo XClarity Administrator geändert wird, wird sie mit XClarity Orchestrator synchronisiert.

- **Kapselung von allen zukünftig verwalteten Einheiten** Gibt an, ob die Kapselung während der Einheitenverwaltung aktiviert ist.

Kapselung ist standardmäßig deaktiviert. Wenn die Einstellung deaktiviert ist, wird der Kapselungsmodus für die Einheiten auf **Normal** gesetzt und die Firewallregeln werden als Teil des Verwaltungsprozesses nicht geändert.

Wenn Kapselung aktiviert ist und eine Einheit Kapselung unterstützt, kommuniziert XClarity Orchestrator während des Verwaltungsprozesses (über den Ressourcenmanager) mit der Einheit, um den Kapselungsmodus der Einheit in **encapsulationLite** zu ändern. Außerdem werden die Firewallregeln auf der Einheit so eingestellt, dass eingehende Anforderungen nur von dem Ressourcenmanager akzeptiert werden, der zur Verwaltung der Einheit ausgewählt wurde.

Achtung: Wenn Kapselung aktiviert ist und der zur Verwaltung der Einheit ausgewählte Ressourcenmanager nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen.

- **Registrierungsanforderung aktiviert** Gibt an, ob Ressourcenmanager (Lenovo XClarity Administrator und Lenovo XClarity Management Hub) Ermittlungsanforderungen von einem Baseboard Management Controller akzeptieren, wenn der Management-Controller DNS verwendet, um Ressourcenmanagerinstanzen zu finden. Wenn diese Option aktiviert ist, kann sich der Management-Controller beim Ressourcenmanager als ermittelte Einheit registrieren.
- **Bereinigung von Offline-Einheiten.** Gibt an, ob die Verwaltung von Einheiten automatisch aufgehoben werden soll, die mindestens die in **Zeitlimitüberschreitung bei Offline-Einheiten** angegebene Dauer offline waren. Wenn diese Option aktiviert ist, sucht XClarity Orchestrator einmal pro Stunde und bei jeder Benutzeranmeldung im Portal nach Offline-Einheiten.
- **Zeitlimitüberschreitung bei Offline-Einheiten** Zeitraum in Stunden, für den Einheiten offline sein müssen, bevor ihre Verwaltung automatisch aufgehoben wird. Dies kann ein Wert zwischen **1 und 24** Stunden sein. Der Standardwert lautet **24** Stunden.

Schritt 4. Klicken Sie auf **Speichern**.

Server verwalten

Sie können Lenovo XClarity Orchestrator verwenden, um verschiedene Servertypen zu verwalten.

Vorbereitende Schritte

Zur Durchführung dieser Aufgabe müssen Sie Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** oder **Sicherheitsadministrator** zugewiesen ist.

Gehen Sie die Verwaltungsaspekte nochmal durch, bevor Sie eine Einheit verwalten (siehe [Hinweise zur Verwaltung von Einheiten](#)).

Überprüfen Sie die globalen Ermittlungseinstellungen, bevor Sie eine Einheit verwalten (siehe [Globale Ermittlungseinstellungen konfigurieren](#)).

Informationen zum Ermitteln und Verwalten von Edge-Einheiten, die nicht auf das Service-Ermittlungsprotokoll reagieren, finden Sie unter [ThinkEdge Client-Einheiten verwalten](#).

Die Massenverwaltungsoption ist nur für Server verfügbar. Andere Einheitentypen werden nicht unterstützt.

Zu dieser Aufgabe

XClarity Orchestrator überwacht und verwaltet Einheiten über Ressourcenmanager. Wenn Sie einen Ressourcenmanager verbinden, verwaltet XClarity Orchestrator alle Einheiten, die von diesem Ressourcenmanager verwaltet werden.

Sie können Einheiten auch mit XClarity Orchestrator verwalten. XClarity Orchestrator listet Einheiten auf, die von den Ressourcenmanagern bereits ermittelt (aber nicht verwaltet) wurden. Wenn Sie ermittelte Einheiten mit XClarity Orchestrator verwalten, werden die Einheiten vom Ressourcenmanager verwaltet, der sie ermittelt hat. Wenn Sie Einheiten manuell mithilfe von IP-Adressen, Hostnamen oder Subnetzen ermitteln und verwalten, wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten. XClarity Management Hub kann zur Verwaltung von ThinkEdge Client-Einheiten verwendet werden. XClarity Management Hub 2.0 kann zur Verwaltung von ThinkServer Einheiten verwendet werden. Lenovo XClarity Administrator kann zur Verwaltung von Servern, Speicher, Switches und Gehäusen verwendet werden.

Anmerkungen:

- Wenn Sie versuchen, eine Einheit über XClarity Management Hub 2.0 zu verwalten, die bereits über einen anderen XClarity Management Hub 2.0 verwaltet wird, entfernt XClarity Orchestrator den Benutzeraccount zur Verwaltung und die Abonnements der Einheit ohne die Bestätigung des alten Verwaltungshubs und verwaltet die Einheit dann erneut über den neuen Verwaltungshub. Nach diesem Prozess gilt die Einheit weiterhin als durch den alten Verwaltungshub verwaltet, ist aber offline und sendet keine Daten mehr an ihn. Beachten Sie, dass Sie die Verwaltung der Einheiten vom ersten Verwaltungshub manuell über das verbundene Portal aufheben müssen.
- Wenn Sie versuchen, eine Einheit über XClarity Management Hub 2.0 zu verwalten, die bereits über einen anderen XClarity Administrator verwaltet wird, entfernt XClarity Orchestrator den Benutzeraccount zur Verwaltung, die Abonnements, LDAP- und SSO-Informationen der Einheit, die von XClarity Administrator beim XCC registriert sind, ohne die Bestätigung durch XClarity Administrator von der Einheit und verwaltet die Einheit dann erneut über den neuen XClarity Management Hub 2.0. Nach diesem Prozess gilt die Einheit weiterhin als durch den XClarity Administrator-Hub verwaltet, ist aber offline und sendet keine Daten mehr an ihn. Beachten Sie, dass Sie die Verwaltung der Einheiten vom XClarity Administrator manuell über das verbundene Portal aufheben müssen.

Die folgenden Einheiten können automatisch von Ressourcenmanagern mithilfe eines Service-Ermittlungsprotokolls ermittelt werden.

- ThinkSystem und ThinkAgile Server und Einheiten
- ThinkEdge SE Server
- Flex System Gehäuse, und ThinkSystem und Flex System Einheiten in einem Flex System Gehäuse
- ThinkServer Rack- und Tower-Server
- System x, Converged HX und NeXtScale Server und Einheiten
- Speichereinheiten

Vorgehensweise

Verwenden Sie eine der folgenden Vorgehensweisen, um Ihre Server zu verwalten.

- [Server manuell ermitteln](#)
- [Ermittelte Server verwalten](#)
- [Große Anzahl von Servern verwalten](#)

Server manuell ermitteln

Gehen Sie wie folgt vor, um bestimmte Server manuell zu ermitteln, die sich nicht im selben Subnetz wie der Orchestrator-Server befinden.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.
2. Klicken Sie auf **Manuelle Eingabe**, um das Dialogfenster Neue Einheiten ermitteln anzuzeigen.
3. Wählen Sie **Einheiten, die auf das Service-Ermittlungsprotokoll reagieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie **Manuell** aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie aus, wie Sie die Einheiten ermitteln möchten, und geben Sie die entsprechenden Werte an.
 - **IP-Adressen/Hostnamen** Geben Sie die IPv4- oder IPv6-IP-Adresse oder den vollständig qualifizierten Domännennamen für jede zu verwaltende Einheit ein (z. B. 192.0.2.0 oder d1.acme.com).
 - **IP-Bereiche**. Geben Sie die Start- und End-IP-Adressen für die zu verwaltenden Einheiten ein.
 - **Subnetze**. Geben Sie die IP-Adresse und die Maske für das Subnetz ein. XClarity Orchestrator scannt das Subnetz nach verwaltbaren Einheiten.
6. Wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten.
7. Klicken Sie auf **Einheiten ermitteln**. Wenn der Ermittlungsprozess abgeschlossen ist, werden die ermittelten Einheiten in der Tabelle „Neue Einheiten“ aufgeführt.

Ermittelte Server verwalten

Gehen Sie wie folgt vor, um bereits ermittelte Einheiten zu verwalten.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.

Neue Einheiten ermitteln und verwalten

Klicken Sie **Konfiguration**, um globale Ermittlungseinstellungen zu definieren.

Klicken Sie auf **Anmeldeinformationen für UDS-Portal**, um die Anmeldeinformationen für das UDS-Portal festzulegen, die zum Herunterladen von UDC-Bereitstellungspaketen für Einheiten erforderlich sind, die nicht auf ein Service-Ermittlungsprotokoll reagieren.

Wenn die folgende Liste nicht die erwarteten Einheiten enthält, nutzen Sie die Option **Manuelle Eingabe**, um die Einheit zu finden. Weitere Informationen dazu, warum eine Einheit möglicherweise nicht automatisch gefunden wird, finden Sie im folgenden Hilfethema: [Einheit kann nicht erkannt werden](#).

Manuelle Eingabe
 Konfiguration
 Anmeldeinformationen für UDS-Portal

Neue Einheiten

Alle Aktionen ▾
 Filter ▾

<input type="checkbox"/>	Ermittelte Einheit	IP-Adressen	Seriennummer	Typ/Modell	Typ	Ermittelt von
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.:	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 ausgewählt / 3 gesamt Zeilen pro Seite: 10 ▾

- Klicken Sie auf das **Alle Aktionen → Aktualisieren**, um alle verwaltbaren Einheiten in der XClarity Orchestrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
- Wählen Sie einen oder mehrere zu verwaltende Server aus.
- Klicken Sie auf das Symbol **Ausgewählte Einheiten verwalten** (**⊕**), um das Dialogfenster Ermittelte Einheiten verwalten anzuzeigen.
- Überprüfen Sie die Liste der ausgewählten Einheiten, die verwaltet werden sollen, und klicken Sie auf **Weiter**.
- Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung am Server an.

Tipp: Erwägen Sie, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigung verwendet wird, kann die Verwaltung fehlschlagen, oder sie ist möglicherweise erfolgreich, aber einige Funktionen sind nicht funktional.

- Optional:** Wählen Sie **Wiederherstellungsaccount erstellen und alle lokalen Benutzer deaktivieren** und geben Sie das Wiederherstellungskennwort an. Wenn diese Option deaktiviert ist, werden lokale Benutzeraccounts für die Authentifizierung verwendet.

Wenn diese Option aktiviert ist, erstellt der zugeordnete Ressourcenmanager einen Benutzeraccount für verwaltete Authentifizierung und einen Wiederherstellungsaccount (RECOVERY_ID) auf dem Server, und alle anderen lokalen Benutzeraccounts werden deaktiviert. Der Benutzeraccount für verwaltete Authentifizierung wird vom XClarity Orchestrator Ressourcenmanager für die Authentifizierung verwendet. Wenn ein Problem mit XClarity Orchestrator oder dem Ressourcenmanager auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich auch am Baseboard Management Controller *nicht* mehr mit den normalen Benutzeraccounts anmelden. Sie können sich allerdings über den RECOVERY_ID-Account anmelden.

Wichtig: Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.

Anmerkung: Der Wiederherstellungsaccount wird für ThinkServer- und System x M4-Server nicht unterstützt.

8. **Optional:** Aktivieren Sie **Neues Kennwort festlegen, wenn Anmeldeinformationen abgelaufen sind** und geben Sie dann das neue Serverkennwort an. Wenn das aktuelle Serverkennwort abgelaufen ist, schlägt die Ermittlung bis zur Änderung des Kennworts fehl. Wenn Sie ein neues Kennwort angeben, werden die Anmeldeinformationen geändert und der Verwaltungsprozess kann fortgesetzt werden. Das Kennwort wird nur geändert, wenn das aktuelle Kennwort abgelaufen ist.
9. Wählen Sie **Verwalten** aus. Es wird ein Job erstellt, um den Verwaltungsprozess im Hintergrund abzuschließen. Sie können den Status des Verwaltungsprozesses im Dialog oder im Jobprotokoll überwachen, indem Sie auf **Überwachung** (📧) → **Jobs** klicken (siehe [Jobs überwachen](#)).

Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option Verwaltung erzwingen.

- Der Ressourcenmanager ist fehlgeschlagen und kann nicht wiederhergestellt werden.

Anmerkung: Wenn der Austausch-Ressourcenmanager dieselbe IP-Adresse wie der ausgefallene Ressourcenmanager verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.

- Der Ressourcenmanager wurde heruntergefahren, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Die Verwaltung der Einheiten wurde nicht erfolgreich aufgehoben.
- XClarity Orchestrator zeigt eine verwaltete Einheit als offline an, nachdem die IP-Adresse der Einheit geändert wurde.

Große Anzahl von Servern verwalten

Gehen Sie wie folgt vor, um eine große Anzahl von Servern zu verwalten.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.
2. Klicken Sie auf die Schaltfläche **Massenverwaltung**, um das Dialogfenster Massenverwaltung anzuzeigen.
3. Wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten.
4. Geben Sie die IP-Adresse oder den vollständig qualifizierten Domänennamen für jeden zu verwaltenden Server ein, getrennt durch Komma (z. B. 192.0.2.0, d1.acme.com).

Wichtig:

- Alle angegebenen Server müssen dieselben Anmeldeinformationen verwenden.
 - FQDNs können nur alphanumerische Zeichen, Punkte und Bindestriche enthalten.
5. Klicken Sie auf **Weiter**.
 6. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung am Server an.

Tipp: Erwägen Sie, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigung verwendet wird, kann die Verwaltung fehlschlagen, oder sie ist möglicherweise erfolgreich, aber einige Funktionen sind nicht funktional.

7. **Optional:** Wählen Sie **Wiederherstellungsaccount erstellen und alle lokalen Benutzer deaktivieren** und geben Sie das Wiederherstellungskennwort an. Wenn diese Option deaktiviert ist, werden lokale Benutzeraccounts für die Authentifizierung verwendet.

Wenn diese Option aktiviert ist, erstellt der zugeordnete Ressourcenmanager einen Benutzeraccount für verwaltete Authentifizierung und einen Wiederherstellungsaccount (RECOVERY_ID) auf dem Server, und

alle anderen lokalen Benutzeraccounts werden deaktiviert. Der Benutzeraccount für verwaltete Authentifizierung wird vom XClarity Orchestrator Ressourcenmanager für die Authentifizierung verwendet. Wenn ein Problem mit XClarity Orchestrator oder dem Ressourcenmanager auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich auch am Baseboard Management Controller *nicht* mehr mit den normalen Benutzeraccounts anmelden. Sie können sich allerdings über den RECOVERY_ID-Account anmelden.

Wichtig: Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.

Anmerkung: Der Wiederherstellungsaccount wird für ThinkServer- und System x M4-Server nicht unterstützt.

8. **Optional:** Aktivieren Sie **Neues Kennwort festlegen, wenn Anmeldeinformationen abgelaufen sind** und geben Sie dann das neue Serverkennwort an. Wenn das aktuelle Serverkennwort abgelaufen ist, schlägt die Ermittlung bis zur Änderung des Kennworts fehl. Wenn Sie ein neues Kennwort angeben, werden die Anmeldeinformationen geändert und der Verwaltungsprozess kann fortgesetzt werden. Das Kennwort wird nur geändert, wenn das aktuelle Kennwort abgelaufen ist.
9. Wählen Sie **Verwalten** aus. Es wird ein Job erstellt, um den Verwaltungsprozess im Hintergrund abzuschließen. Sie können den Status des Verwaltungsprozesses im Dialog oder im Jobprotokoll überwachen, indem Sie auf **Überwachung** (📧) → **Jobs** klicken (siehe [Jobs überwachen](#)).

Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option Verwaltung erzwingen.

- Der Ressourcenmanager ist fehlgeschlagen und kann nicht wiederhergestellt werden.

Anmerkung: Wenn der Austausch-Ressourcenmanager dieselbe IP-Adresse wie der ausgefallene Ressourcenmanager verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.

- Der Ressourcenmanager wurde heruntergefahren, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Die Verwaltung der Einheiten wurde nicht erfolgreich aufgehoben.
- XClarity Orchestrator zeigt eine verwaltete Einheit als offline an, nachdem die IP-Adresse der Einheit geändert wurde.

Nach dieser Aufgabe

Sie können für die verwaltete Einheit die folgenden Aktionen ausführen.

- Hardwarestatus und die Details überwachen (siehe [Status von Einheiten anzeigen](#) und [Einheitendetails anzeigen](#)).
- Verwaltung einer ausgewählten Einheit aufheben und sie entfernen. Klicken Sie dazu auf **Ressourcen** (⚙️) und dann auf den Einheitentyp in der linken Navigation, um eine Übersicht mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs anzuzeigen. Wählen Sie die Einheiten aus, deren Verwaltung aufgehoben werden soll, und klicken Sie auf das Symbol **Verwaltung aufheben** (🗑️).

Anmerkungen:

- Sie können die Verwaltung von maximal **50** Einheiten gleichzeitig aufheben.
- Stellen Sie sicher, dass keine aktiven Jobs auf der Einheit ausgeführt werden.
- Wenn XClarity Orchestrator keine Verbindung zum Ressourcenmanager herstellen kann, weil z. B. wenn die Anmeldeinformationen abgelaufen sind oder es Netzwerkprobleme gibt, wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aus.

- Standardmäßig wird die Verwaltung von Einheiten, die von XClarity Administrator verwaltet werden und 24 Stunden oder länger offline sind, automatisch aufgehoben (siehe [Globale Ermittlungseinstellungen konfigurieren](#)).
- Für die meisten Einheiten werden bestimmte Informationen zur Einheit beibehalten, selbst nachdem ihre Verwaltung aufgehoben wurde. Wenn die Verwaltung der Einheiten aufgehoben wurde:
 - Der Verwaltungsbenutzeraccount sowie die Ereignis- und Metrikabonnements werden von der Einheit entfernt.
 - Bei von XClarity Administrator verwalteten Einheiten: Wenn die Call-Home-Funktion zurzeit auf XClarity Administrator aktiviert ist, ist die Call-Home-Funktion auf der Einheit deaktiviert.
 - Bei von XClarity Administrator verwalteten Einheiten: Wenn die Kapselung auf der Einheit aktiviert ist, werden die Firewallregeln der Einheit zu den Einstellungen vor dem Zeitpunkt der Einheitenverwaltung geändert.
 - Sensible Informationen, Bestand sowie Ereignisse und Alerts, die von der Einheit ausgelöst wurden, werden vom Verwaltungshub gelöscht.
 - Ereignisse und Alerts, die vom Verwaltungshub für die Einheit ausgelöst wurden, bleiben auf dem Verwaltungshub erhalten.

ThinkEdge Client-Einheiten verwalten

ThinkEdge Client-Einheiten verfügen nicht über Baseboard Management Controller und können daher nicht mithilfe der Service-Ermittlungsprotokolle ermittelt werden. Sie müssen einen UDC-Agent (Universal Device Client) auf ThinkEdge Client-Einheiten installieren, bevor die Einheiten vom zugeordneten Lenovo XClarity Management Hub Ressourcenmanager sicher ermittelt und verwaltet werden können. Nur Lenovo XClarity Management Hub Ressourcenmanager können diese Einheiten ermitteln und verwalten.

Vorbereitende Schritte

Gehen Sie die Verwaltungsaspekte nochmal durch, bevor Sie eine Einheit verwalten (siehe [Hinweise zur Verwaltung von Einheiten](#)).

Stellen Sie sicher, dass mindestens ein Lenovo XClarity Management Hub Ressourcenmanager mit XClarity Orchestrator verbunden ist (siehe [Ressourcenmanager verbinden](#)).

Zur Durchführung dieser Aufgabe müssen Sie Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** oder **Sicherheitsadministrator** zugewiesen ist.

Stellen Sie sicher, dass die Anmeldeinformationen für das UDS-Portal mit der Client-ID und dem geheimen Schlüssel konfiguriert sind. Die Anmeldeinformationen werden verwendet, um die Richtlinie zu signieren, die im Client-Bereitstellungspaket verwendet wird. Das UDS-Portal ist die vertrauenswürdige Quelle zum Signieren dieser Richtlinie, damit der UDC-Agent ordnungsgemäß funktioniert. Konfigurieren Sie die Anmeldeinformationen. Navigieren Sie dazu in der Menüleiste zu **Ressourcen** (🔗) → **Neue Einheiten** und klicken Sie dann auf **Anmeldeinformationen für UDS-Portal** und geben Sie die Client-ID und den geheimen Schlüssel ein. Sie müssen die Client-ID und den geheimen Schlüssel von Lenovo anfordern. Senden Sie dazu eine E-Mail an uedmcredreq@lenovo.com mit „Anmeldeinformationen für UDS-Portal“ im Betreff und geben Sie den Namen Ihres Unternehmens, Ihre Kontaktinformationen (E-Mail oder Telefonnummer) und die 10-stellige Lenovo Kundennummer an.

Stellen Sie sicher, dass aktuell *kein* UDC-Agent auf der ThinkEdge Client-Einheit installiert ist. Wenn ein UDC-Agent installiert ist, müssen Sie ihn deinstallieren, indem Sie die folgenden Befehle ausführen. Zum Installieren des UDC-Agent müssen Sie über erweiterte Berechtigungen verfügen.

- **Linux**

```
sudo apt purge udc-release
```
- **Windows**

```
PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\.\UDCInfInstaller.exe -uninstall
```

Stellen Sie sicher, dass Ihr DNS-Server so konfiguriert ist, dass er die folgenden Domänen enthält. Dabei ist *{hub-domain}* der vollständig qualifizierte Domänennamen des XClarity Management Hub Ressourcenmanagers, den Sie zur Verwaltung der ThinkEdge Client-Einheiten verwenden möchten.

- *api.{hub-domain}*
- *api-mtls.{hub-domain}*
- *auth.{hub-domain}*
- *mqtt.{hub-domain}*
- *mqtt-mtls.{hub-domain}*
- *s3.{hub-domain}*
- *s3console.{hub-domain}*

Zu dieser Aufgabe

XClarity Orchestrator überwacht und verwaltet Einheiten über Ressourcenmanager. Wenn Sie einen Ressourcenmanager verbinden, verwaltet XClarity Orchestrator alle Einheiten, die von diesem Ressourcenmanager verwaltet werden.

Sie können Einheiten auch mit XClarity Orchestrator verwalten. XClarity Orchestrator listet Einheiten auf, die von den Ressourcenmanagern bereits ermittelt (aber nicht verwaltet) wurden. Wenn Sie ermittelte Einheiten mit XClarity Orchestrator verwalten, werden die Einheiten vom Ressourcenmanager verwaltet, der sie ermittelt hat. Wenn Sie Einheiten manuell mithilfe von IP-Adressen, Hostnamen oder Subnetzen ermitteln und verwalten, wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten. XClarity Management Hub kann zur Verwaltung von ThinkEdge Client-Einheiten verwendet werden. XClarity Management Hub 2.0 kann zur Verwaltung von ThinkServer Einheiten verwendet werden. Lenovo XClarity Administrator kann zur Verwaltung von Servern, Speicher, Switches und Gehäusen verwendet werden.

Eine vollständige Liste der unterstützten ThinkEdge Client-Einheiten finden Sie auf der [Lenovo XClarity Unterstützungswebsite](#). Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Anmerkung: ThinkEdge Server (z. B. SE350, SE360 und SE450) verfügen über Baseboard Management Controller und können mithilfe eines Service-Ermittlungsprotokolls ermittelt werden. Informationen zur Verwaltung dieser Einheiten finden Sie unter [Server verwalten](#).

Vorgehensweise

Gehen Sie wie folgt vor, um ThinkEdge Client-Einheiten zu ermitteln und zu verwalten.

1. Installieren Sie den UDC-Agent auf jeder ThinkEdge Client-Einheit.
 - a. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.
 - b. Klicken Sie auf **Manuelle Eingabe**, um das Dialogfenster Neue Einheiten ermitteln anzuzeigen.
 - c. Wählen Sie **Einheiten, die nicht auf das Service-Ermittlungsprotokoll reagieren** aus und klicken Sie auf **Weiter**.
 - d. Wählen Sie die IP-Adresse des XClarity Management Hub Ressourcenmanagers aus, der zum Verwalten der ThinkEdge Client-Einheiten verwendet werden möchte. Es können nur XClarity Management Hub Ressourcenmanager in einem fehlerfreien Zustand ausgewählt werden.
 - e. Wählen Sie den Typ des Betriebssystems aus, das auf dem Server installiert ist.
 - **Linux ARM**
 - **Linux x86**

- **Windows**

- Wählen Sie die Anzahl der Tage aus, bevor das Installationsprogramm für den UDC-Agent nach dem Download nicht mehr benutzbar ist. Der Standardwert beträgt **30** Tage.
- Wählen Sie aus, wie viele Male Sie den UDC-Agent auf einem Server installieren wollen. Dies ist in der Regel die Anzahl der Einheiten, auf denen Sie den UDC-Agent installieren müssen. Sie können bis zu **1.000.000** Verwendungen. Der Standardwert ist **10** Verwendungen.
- Klicken Sie auf **UDC-Agent herunterladen**, um das Installationsprogramm für den UDC-Agent auf Ihr lokales System herunterzuladen. Es wird ein Job erstellt, um den Downloadprozess im Hintergrund abzuschließen. Sie können den Status des Downloadprozesses im Dialog oder im Jobprotokoll überwachen, indem Sie auf **Überwachung** (📄) → **Jobs** klicken (siehe [Jobs überwachen](#)).
- Klicken Sie auf **Schließen**, um das Dialogfenster zu schließen.
- Kopieren Sie das Installationsprogramm für den UDC-Agent zu jeder geeigneten ThinkEdge Client-Einheit. Entpacken Sie das Paket und installieren Sie den UDC-Agent anschließend mithilfe des folgenden Befehls auf diesen Einheiten. Zum Installieren des Agent müssen Sie über **Administrator**-Berechtigungen verfügen.

- **Linux** install.sh

- **Windows** setup.cmd

Nachdem der UDC-Agent erfolgreich auf jeder ThinkEdge Client-Einheit installiert wurde, können die Einheiten automatisch vom ausgewählten XClarity Management Hub Ressourcenmanager ermittelt werden.

- Verwalten Sie die ThinkEdge Client-Einheiten.

- Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.

Anmerkung: Es kann einige Zeit dauern, bis die IP-Adressen in der Tabelle angezeigt werden.

Neue Einheiten ermitteln und verwalten

Klicken Sie **Konfiguration**, um globale Ermittlungseinstellungen zu definieren.
 Klicken Sie auf **Anmeldeinformationen für UDS-Portal**, um die Anmeldeinformationen für das UDS-Portal festzulegen, die zum Herunterladen von UDC-Bereitstellungspaketen für Einheiten erforderlich sind, die nicht auf ein Service-Ermittlungsprotokoll reagieren.
 Wenn die folgende Liste nicht die erwarteten Einheiten enthält, nutzen Sie die Option **Manuelle Eingabe**, um die Einheit zu finden. Weitere Informationen dazu, warum eine Einheit möglicherweise nicht automatisch gefunden wird, finden Sie im folgenden Hilfethema: [Einheit kann nicht erkannt werden](#).

⊕ Manuelle Eingabe
 ⚙️ Konfiguration
 🔒 Anmeldeinformationen für UDS-Portal

Neue Einheiten

🔄 ⊕ 📄 Alle Aktionen ▾
 Filter ▾
 🔍 Suchen ✕

<input type="checkbox"/>	Ermittelte Einhei	IP-Adressen :	Seriennummer :	Typ/Modell :	Typ :	Ermittelt von :
<input type="checkbox"/>	G8052-1	10.241.5.1, 10:	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 1C	1234567890	7D75/CTO1...	Server	10.241.5.134

0 ausgewählt / 3 gesamt Zeilen pro Seite: 10 ▾

- b. Klicken Sie auf das **Alle Aktionen → Aktualisieren**, um alle verwaltbaren Einheiten in der XClarity Orchestrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
- c. Wählen Sie eine oder mehrere zu verwaltende ThinkEdge Client-Einheiten aus.
- d. Klicken Sie auf das Symbol **Verwalten** (⊕), um das Dialogfenster Einheiten verwalten anzuzeigen.
- e. Überprüfen Sie die Liste der ausgewählten Einheiten, die verwaltet werden sollen.
- f. Wählen Sie **Verwalten** aus. Es wird ein Job erstellt, um den Verwaltungsprozess im Hintergrund abzuschließen. Sie können den Status des Verwaltungsprozesses im Dialog oder im Jobprotokoll überwachen, indem Sie auf **Überwachung** (👁️) → **Jobs** klicken (siehe [Jobs überwachen](#)).

Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option Verwaltung erzwingen.

- Der Ressourcenmanager ist fehlgeschlagen und kann nicht wiederhergestellt werden.

Anmerkung: Wenn der Austausch-Ressourcenmanager dieselbe IP-Adresse wie der ausgefallene Ressourcenmanager verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.

- Der Ressourcenmanager wurde heruntergefahren, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Die Verwaltung der Einheiten wurde nicht erfolgreich aufgehoben.
- XClarity Orchestrator zeigt eine verwaltete Einheit als offline an, nachdem die IP-Adresse der Einheit geändert wurde.

Nach dieser Aufgabe

Sie können für die verwaltete Einheit die folgenden Aktionen ausführen.

- Hardwarestatus und die Details überwachen (siehe [Status von Einheiten anzeigen](#) und [Einheitendetails anzeigen](#)).
- Verwaltung einer ausgewählten Einheit aufheben und sie entfernen. Klicken Sie dazu auf **Ressourcen** (⊙) und dann auf den Einheitentyp in der linken Navigation, um eine Übersicht mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs anzuzeigen. Wählen Sie die Einheiten aus, deren Verwaltung aufgehoben werden soll, und klicken Sie auf das Symbol **Verwaltung aufheben** (⏏️).

Anmerkungen:

- Sie können die Verwaltung von maximal **50** Einheiten gleichzeitig aufheben.
- Stellen Sie sicher, dass keine aktiven Jobs auf der Einheit ausgeführt werden.
- Wenn XClarity Orchestrator keine Verbindung zum Ressourcenmanager herstellen kann, weil z. B. wenn die Anmeldeinformationen abgelaufen sind oder es Netzwerkprobleme gibt, wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aus.
- Standardmäßig wird die Verwaltung von Einheiten, die von XClarity Administrator verwaltet werden und 24 Stunden oder länger offline sind, automatisch aufgehoben (siehe [Globale Ermittlungseinstellungen konfigurieren](#)).
- Für die meisten Einheiten werden bestimmte Informationen zur Einheit beibehalten, selbst nachdem ihre Verwaltung aufgehoben wurde. Wenn die Verwaltung der Einheiten aufgehoben wurde:
 - Der Verwaltungsbenutzeraccount sowie die Ereignis- und Metrikabonnements werden von der Einheit entfernt.
 - Bei von XClarity Administrator verwalteten Einheiten: Wenn die Call-Home-Funktion zurzeit auf XClarity Administrator aktiviert ist, ist die Call-Home-Funktion auf der Einheit deaktiviert.

- Bei von XClarity Administrator verwalteten Einheiten: Wenn die Kapselung auf der Einheit aktiviert ist, werden die Firewallregeln der Einheit zu den Einstellungen vor dem Zeitpunkt der Einheitenverwaltung geändert.
- Sensible Informationen, Bestand sowie Ereignisse und Alerts, die von der Einheit ausgelöst wurden, werden vom Verwaltungshub gelöscht.
- Ereignisse und Alerts, die vom Verwaltungshub für die Einheit ausgelöst wurden, bleiben auf dem Verwaltungshub erhalten.

Speichereinheiten verwalten

Lenovo XClarity Orchestrator kann verschiedene Typen von Lenovo Speichereinheiten, Einheiten und Bandbibliotheken verwalten.

Vorbereitende Schritte

Zur Durchführung dieser Aufgabe müssen Sie Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** oder **Sicherheitsadministrator** zugewiesen ist.

Gehen Sie die Verwaltungsaspekte nochmal durch, bevor Sie eine Einheit verwalten (siehe [Hinweise zur Verwaltung von Einheiten](#)).

Informationen zum Ermitteln und Verwalten von Edge-Einheiten, die nicht auf das Service-Ermittlungsprotokoll reagieren, finden Sie unter [ThinkEdge Client-Einheiten verwalten](#).

Die Massenverwaltungsoption ist nur für Server verfügbar. Andere Einheitentypen werden nicht unterstützt.

Zu dieser Aufgabe

XClarity Orchestrator überwacht und verwaltet Einheiten über Ressourcenmanager. Wenn Sie einen Ressourcenmanager verbinden, verwaltet XClarity Orchestrator alle Einheiten, die von diesem Ressourcenmanager verwaltet werden.

Sie können Einheiten auch mit XClarity Orchestrator verwalten. XClarity Orchestrator listet Einheiten auf, die von den Ressourcenmanagern bereits ermittelt (aber nicht verwaltet) wurden. Wenn Sie ermittelte Einheiten mit XClarity Orchestrator verwalten, werden die Einheiten vom Ressourcenmanager verwaltet, der sie ermittelt hat. Wenn Sie Einheiten manuell mithilfe von IP-Adressen, Hostnamen oder Subnetzen ermitteln und verwalten, wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten. XClarity Management Hub kann zur Verwaltung von ThinkEdge Client-Einheiten verwendet werden. XClarity Management Hub 2.0 kann zur Verwaltung von ThinkServer Einheiten verwendet werden. Lenovo XClarity Administrator kann zur Verwaltung von Servern, Speicher, Switches und Gehäusen verwendet werden.

Vorgehensweise

Verwenden Sie eine der folgenden Vorgehensweisen, um Ihre Speichereinheiten zu verwalten.

- [Speichereinheiten manuell ermitteln](#)
- [Ermittelte Speichereinheiten verwalten](#)

Speichereinheiten manuell ermitteln

Gehen Sie wie folgt vor, um bestimmte Speichereinheiten manuell zu ermitteln und dann zu verwalten, die sich nicht im selben Subnetz wie der Orchestrator-Server befinden.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.

2. Klicken Sie auf **Manuelle Eingabe**, um das Dialogfenster Neue Einheiten ermitteln anzuzeigen.
3. Wählen Sie **Einheiten, die auf das Service-Ermittlungsprotokoll reagieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie **Manuell** aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie aus, wie Sie die Einheiten ermitteln möchten, und geben Sie die entsprechenden Werte an.
 - **IP-Adressen/Hostnamen** Geben Sie die IPv4- oder IPv6-IP-Adresse oder den vollständig qualifizierten Domännennamen für jede zu verwaltende Einheit ein (z. B. 192.0.2.0 oder d1.acme.com).
 - **IP-Bereiche**. Geben Sie die Start- und End-IP-Adressen für die zu verwaltenden Einheiten ein.
 - **Subnetze**. Geben Sie die IP-Adresse und die Maske für das Subnetz ein. XClarity Orchestrator scannt das Subnetz nach verwaltbaren Einheiten.
6. Wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten.
7. Klicken Sie auf **Einheiten ermitteln**. Wenn der Ermittlungsprozess abgeschlossen ist, werden die ermittelten Einheiten in der Tabelle „Neue Einheiten“ aufgeführt.

Ermittelte Speichereinheiten verwalten

Gehen Sie wie folgt vor, um bereits ermittelte Einheiten zu verwalten.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.

Neue Einheiten ermitteln und verwalten

Klicken Sie **Konfiguration**, um globale Ermittlungseinstellungen zu definieren.
 Klicken Sie auf **Anmeldeinformationen für UDS-Portal**, um die Anmeldeinformationen für das UDS-Portal festzulegen, die zum Herunterladen von UDC-Bereitstellungspaketen für Einheiten erforderlich sind, die nicht auf ein Service-Ermittlungsprotokoll reagieren.
 Wenn die folgende Liste nicht die erwarteten Einheiten enthält, nutzen Sie die Option **Manuelle Eingabe**, um die Einheit zu finden. Weitere Informationen dazu, warum eine Einheit möglicherweise nicht automatisch gefunden wird, finden Sie im folgenden Hilfethema: [Einheit kann nicht erkannt werden](#).

⊕ Manuelle Eingabe
 ⚙️ Konfiguration
 🔍 Anmeldeinformationen für UDS-Portal

Neue Einheiten

🔄 ⌚ 📄 Alle Aktionen ▾
 Filter ▾
 🔍 Suchen ✕

<input type="checkbox"/>	Ermittelte Einhei	IP-Adressen :	Seriennummer :	Typ/Modell :	Typ :	Ermittelt von :
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.:	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 ausgewählt / 3 gesamt Zeilen pro Seite: 10 ▾

2. Klicken Sie auf das **Alle Aktionen** → **Aktualisieren**, um alle verwaltbaren Einheiten in der XClarity Orchestrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
3. Wählen Sie eine oder mehrere zu verwaltende Speichereinheiten aus.
4. Klicken Sie auf das Symbol **Ausgewählte Einheiten verwalten** (⊕), um das Dialogfenster Ermittelte Einheiten verwalten anzuzeigen.

- Überprüfen Sie die Liste der ausgewählten Einheiten, die verwaltet werden sollen, und klicken Sie auf **Weiter**.
- Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung am Server an.

Tipp: Erwägen Sie, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigung verwendet wird, kann die Verwaltung fehlschlagen, oder sie ist möglicherweise erfolgreich, aber einige Funktionen sind nicht funktional.

- Wählen Sie **Verwalten** aus. Es wird ein Job erstellt, um den Verwaltungsprozess im Hintergrund abzuschließen. Sie können den Status des Verwaltungsprozesses im Dialog oder im Jobprotokoll überwachen, indem Sie auf **Überwachung** (📊) → **Jobs** klicken (siehe [Jobs überwachen](#)).

Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option Verwaltung erzwingen.

- Der Ressourcenmanager ist fehlgeschlagen und kann nicht wiederhergestellt werden.

Anmerkung: Wenn der Austausch-Ressourcenmanager dieselbe IP-Adresse wie der ausgefallene Ressourcenmanager verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.

- Der Ressourcenmanager wurde heruntergefahren, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Die Verwaltung der Einheiten wurde nicht erfolgreich aufgehoben.
- XClarity Orchestrator zeigt eine verwaltete Einheit als offline an, nachdem die IP-Adresse der Einheit geändert wurde.

Nach dieser Aufgabe

Sie können für die verwaltete Einheit die folgenden Aktionen ausführen.

- Hardwarestatus und die Details überwachen (siehe [Status von Einheiten anzeigen](#) und [Einheitendetails anzeigen](#)).
- Verwaltung einer ausgewählten Einheit aufheben und sie entfernen. Klicken Sie dazu auf **Ressourcen** (🔍) und dann auf den Einheitentyp in der linken Navigation, um eine Übersicht mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs anzuzeigen. Wählen Sie die Einheiten aus, deren Verwaltung aufgehoben werden soll, und klicken Sie auf das Symbol **Verwaltung aufheben** (🗑️).

Anmerkungen:

- Sie können die Verwaltung von maximal **50** Einheiten gleichzeitig aufheben.
- Stellen Sie sicher, dass keine aktiven Jobs auf der Einheit ausgeführt werden.
- Wenn XClarity Orchestrator keine Verbindung zum Ressourcenmanager herstellen kann, weil z. B. wenn die Anmeldeinformationen abgelaufen sind oder es Netzwerkprobleme gibt, wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aus.
- Standardmäßig wird die Verwaltung von Einheiten, die von XClarity Administrator verwaltet werden und 24 Stunden oder länger offline sind, automatisch aufgehoben (siehe [Globale Ermittlungseinstellungen konfigurieren](#)).
- Für die meisten Einheiten werden bestimmte Informationen zur Einheit beibehalten, selbst nachdem ihre Verwaltung aufgehoben wurde. Wenn die Verwaltung der Einheiten aufgehoben wurde:
 - Der Verwaltungsbenutzeraccount sowie die Ereignis- und Metrikabonnements werden von der Einheit entfernt.
 - Bei von XClarity Administrator verwalteten Einheiten: Wenn die Call-Home-Funktion zurzeit auf XClarity Administrator aktiviert ist, ist die Call-Home-Funktion auf der Einheit deaktiviert.

- Bei von XClarity Administrator verwalteten Einheiten: Wenn die Kapselung auf der Einheit aktiviert ist, werden die Firewallregeln der Einheit zu den Einstellungen vor dem Zeitpunkt der Einheitenverwaltung geändert.
- Sensible Informationen, Bestand sowie Ereignisse und Alerts, die von der Einheit ausgelöst wurden, werden vom Verwaltungshub gelöscht.
- Ereignisse und Alerts, die vom Verwaltungshub für die Einheit ausgelöst wurden, bleiben auf dem Verwaltungshub erhalten.

Gehäuse verwalten

Lenovo XClarity Orchestrator kann verschiedene Gehäuse- und Gehäusekomponententypen verwalten.

Vorbereitende Schritte

Zur Durchführung dieser Aufgabe müssen Sie Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** oder **Sicherheitsadministrator** zugewiesen ist.

Gehen Sie die Verwaltungsaspekte nochmal durch, bevor Sie eine Einheit verwalten (siehe [Hinweise zur Verwaltung von Einheiten](#)).

Informationen zum Ermitteln und Verwalten von Edge-Einheiten, die nicht auf das Service-Ermittlungsprotokoll reagieren, finden Sie unter [ThinkEdge Client-Einheiten verwalten](#).

Die Massenverwaltungsoption ist nur für Server verfügbar. Andere Einheitentypen werden nicht unterstützt.

Zu dieser Aufgabe

XClarity Orchestrator überwacht und verwaltet Einheiten über Ressourcenmanager. Wenn Sie einen Ressourcenmanager verbinden, verwaltet XClarity Orchestrator alle Einheiten, die von diesem Ressourcenmanager verwaltet werden.

Sie können Einheiten auch mit XClarity Orchestrator verwalten. XClarity Orchestrator listet Einheiten auf, die von den Ressourcenmanagern bereits ermittelt (aber nicht verwaltet) wurden. Wenn Sie ermittelte Einheiten mit XClarity Orchestrator verwalten, werden die Einheiten vom Ressourcenmanager verwaltet, der sie ermittelt hat. Wenn Sie Einheiten manuell mithilfe von IP-Adressen, Hostnamen oder Subnetzen ermitteln und verwalten, wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten. XClarity Management Hub kann zur Verwaltung von ThinkEdge Client-Einheiten verwendet werden. XClarity Management Hub 2.0 kann zur Verwaltung von ThinkServer Einheiten verwendet werden. Lenovo XClarity Administrator kann zur Verwaltung von Servern, Speicher, Switches und Gehäusen verwendet werden.

Vorgehensweise

Verwenden Sie eine der folgenden Vorgehensweisen, um Ihr Gehäuse zu verwalten.

- [Gehäuse manuell ermitteln](#)
- [Ermittelte Gehäuse verwalten](#)

Gehäuse manuell ermitteln

Gehen Sie wie folgt vor, um bestimmte Gehäuse manuell zu ermitteln und dann zu verwalten, die sich nicht im selben Subnetz wie der Orchestrator-Server befinden.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.
2. Klicken Sie auf **Manuelle Eingabe**, um das Dialogfenster Neue Einheiten ermitteln anzuzeigen.

3. Wählen Sie **Einheiten, die auf das Service-Ermittlungsprotokoll reagieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie **Manuell** aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie aus, wie Sie die Einheiten ermitteln möchten, und geben Sie die entsprechenden Werte an.
 - **IP-Adressen/Hostnamen** Geben Sie die IPv4- oder IPv6-IP-Adresse oder den vollständig qualifizierten Domännennamen für jede zu verwaltende Einheit ein (z. B. 192.0.2.0 oder d1.acme.com).
 - **IP-Bereiche**. Geben Sie die Start- und End-IP-Adressen für die zu verwaltenden Einheiten ein.
 - **Subnetze**. Geben Sie die IP-Adresse und die Maske für das Subnetz ein. XClarity Orchestrator scannt das Subnetz nach verwaltbaren Einheiten.
6. Wählen Sie den Ressourcenmanager aus, den Sie für die Verwaltung der Einheiten verwenden möchten.
7. Klicken Sie auf **Einheiten ermitteln**. Wenn der Ermittlungsprozess abgeschlossen ist, werden die ermittelten Einheiten in der Tabelle „Neue Einheiten“ aufgeführt.

Ermittelte Gehäuse verwalten

Gehen Sie wie folgt vor, um bereits ermittelte Einheiten zu verwalten.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) → **Neue Einheiten**, um die Übersicht Neue Einheiten ermitteln und verwalten anzuzeigen.

Neue Einheiten ermitteln und verwalten

Klicken Sie **Konfiguration**, um globale Ermittlungseinstellungen zu definieren.

Klicken Sie auf **Anmeldeinformationen für UDS-Portal**, um die Anmeldeinformationen für das UDS-Portal festzulegen, die zum Herunterladen von UDC-Bereitstellungspaketen für Einheiten erforderlich sind, die nicht auf ein Service-Ermittlungsprotokoll reagieren.

Wenn die folgende Liste nicht die erwarteten Einheiten enthält, nutzen Sie die Option **Manuelle Eingabe**, um die Einheit zu finden. Weitere Informationen dazu, warum eine Einheit möglicherweise nicht automatisch gefunden wird, finden Sie im folgenden HilfetHEMA: [Einheit kann nicht erkannt werden](#).

⊕ Manuelle Eingabe
⚙️ Konfiguration
🔍 Anmeldeinformationen für UDS-Portal

Neue Einheiten

🔄
⊕
📄
Alle Aktionen ▾
Filter ▾
🔍 Suchen ✕

<input type="checkbox"/>	Ermittelte Einhei	IP-Adressen	Seriennummer	Typ/Modell	Typ	Ermittelt von
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.:	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 ausgewählt / 3 gesamt Zeilen pro Seite: 10 ▾

2. Klicken Sie auf das **Alle Aktionen** → **Aktualisieren**, um alle verwaltbaren Einheiten in der XClarity Orchestrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
3. Wählen Sie ein oder mehrere Gehäuse aus, die Sie verwalten möchten.
4. Klicken Sie auf das Symbol **Ausgewählte Einheiten verwalten** (⊕), um das Dialogfenster Ermittelte Einheiten verwalten anzuzeigen.
5. Überprüfen Sie die Liste der ausgewählten Einheiten, die verwaltet werden sollen, und klicken Sie auf **Weiter**.

6. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung am Server an.

Tipp: Erwägen Sie, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigung verwendet wird, kann die Verwaltung fehlschlagen, oder sie ist möglicherweise erfolgreich, aber einige Funktionen sind nicht funktional.

7. **Optional:** Wählen Sie **Wiederherstellungsaccount erstellen und alle lokalen Benutzer deaktivieren** und geben Sie das Wiederherstellungskennwort an. Wenn diese Option deaktiviert ist, werden lokale Benutzeraccounts für die Authentifizierung verwendet.

Wenn diese Option aktiviert ist, erstellt der zugeordnete Ressourcenmanager einen Benutzeraccount für verwaltete Authentifizierung und einen Wiederherstellungsaccount (RECOVERY_ID) auf dem Server, und alle anderen lokalen Benutzeraccounts werden deaktiviert. Der Benutzeraccount für verwaltete Authentifizierung wird vom XClarity Orchestrator Ressourcenmanager für die Authentifizierung verwendet. Wenn ein Problem mit XClarity Orchestrator oder dem Ressourcenmanager auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich auch am Baseboard Management Controller *nicht* mehr mit den normalen Benutzeraccounts anmelden. Sie können sich allerdings über den RECOVERY_ID-Account anmelden.

Wichtig: Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.

Anmerkung: Der Wiederherstellungsaccount wird für ThinkServer- und System x M4-Server nicht unterstützt.

8. **Optional:** Aktivieren Sie **Neues Kennwort festlegen, wenn Anmeldeinformationen abgelaufen sind** und geben Sie dann das neue Serverkennwort an. Wenn das aktuelle Serverkennwort abgelaufen ist, schlägt die Ermittlung bis zur Änderung des Kennworts fehl. Wenn Sie ein neues Kennwort angeben, werden die Anmeldeinformationen geändert und der Verwaltungsprozess kann fortgesetzt werden. Das Kennwort wird nur geändert, wenn das aktuelle Kennwort abgelaufen ist.
9. Wählen Sie **Verwalten** aus. Es wird ein Job erstellt, um den Verwaltungsprozess im Hintergrund abzuschließen. Sie können den Status des Verwaltungsprozesses im Dialog oder im Jobprotokoll überwachen, indem Sie auf **Überwachung** (📧) → **Jobs** klicken (siehe [Jobs überwachen](#)).

Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option Verwaltung erzwingen.

- Der Ressourcenmanager ist fehlgeschlagen und kann nicht wiederhergestellt werden.

Anmerkung: Wenn der Austausch-Ressourcenmanager dieselbe IP-Adresse wie der ausgefallene Ressourcenmanager verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.

- Der Ressourcenmanager wurde heruntergefahren, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Die Verwaltung der Einheiten wurde nicht erfolgreich aufgehoben.
- XClarity Orchestrator zeigt eine verwaltete Einheit als offline an, nachdem die IP-Adresse der Einheit geändert wurde.

Nach dieser Aufgabe

Sie können für die verwaltete Einheit die folgenden Aktionen ausführen.

- Hardwarestatus und die Details überwachen (siehe [Status von Einheiten anzeigen](#) und [Einheitendetails anzeigen](#)).
- Verwaltung einer ausgewählten Einheit aufheben und sie entfernen. Klicken Sie dazu auf **Ressourcen** (🔧) und dann auf den Einheitsentyp in der linken Navigation, um eine Übersicht mit einer Tabellenansicht aller

verwalteten Einheiten dieses Typs anzuzeigen. Wählen Sie die Einheiten aus, deren Verwaltung aufgehoben werden soll, und klicken Sie auf das Symbol **Verwaltung aufheben** (III).

Anmerkungen:

- Sie können die Verwaltung von maximal **50** Einheiten gleichzeitig aufheben.
- Stellen Sie sicher, dass keine aktiven Jobs auf der Einheit ausgeführt werden.
- Wenn XClarity Orchestrator keine Verbindung zum Ressourcenmanager herstellen kann, weil z. B. wenn die Anmeldeinformationen abgelaufen sind oder es Netzwerkprobleme gibt, wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aus.
- Standardmäßig wird die Verwaltung von Einheiten, die von XClarity Administrator verwaltet werden und 24 Stunden oder länger offline sind, automatisch aufgehoben (siehe [Globale Ermittlungseinstellungen konfigurieren](#)).
- Für die meisten Einheiten werden bestimmte Informationen zur Einheit beibehalten, selbst nachdem ihre Verwaltung aufgehoben wurde. Wenn die Verwaltung der Einheiten aufgehoben wurde:
 - Der Verwaltungsbenutzeraccount sowie die Ereignis- und Metrikabonnements werden von der Einheit entfernt.
 - Bei von XClarity Administrator verwalteten Einheiten: Wenn die Call-Home-Funktion zurzeit auf XClarity Administrator aktiviert ist, ist die Call-Home-Funktion auf der Einheit deaktiviert.
 - Bei von XClarity Administrator verwalteten Einheiten: Wenn die Kapselung auf der Einheit aktiviert ist, werden die Firewallregeln der Einheit zu den Einstellungen vor dem Zeitpunkt der Einheitenverwaltung geändert.
 - Sensible Informationen, Bestand sowie Ereignisse und Alerts, die von der Einheit ausgelöst wurden, werden vom Verwaltungshub gelöscht.
 - Ereignisse und Alerts, die vom Verwaltungshub für die Einheit ausgelöst wurden, bleiben auf dem Verwaltungshub erhalten.

Verwaltung von Einheiten aufheben

Mit Lenovo XClarity Orchestrator können Sie die Verwaltung von Einheiten durch den jeweiligen Ressourcenmanager aufheben. Dieser Vorgang wird als *Aufheben der Verwaltung* bezeichnet.

Vorbereitende Schritte

Zur Durchführung dieser Aufgabe müssen Sie Mitglied einer Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** oder **Sicherheitsadministrator** zugewiesen ist.

Stellen Sie sicher, dass keine aktiven Jobs auf der Einheit ausgeführt werden.

Zu dieser Aufgabe


XClarity Orchestrator hebt die Verwaltung von Einheiten automatisch auf, die standardmäßig 24 Stunden oder länger offline sind (siehe [Globale Ermittlungseinstellungen konfigurieren](#)).

Für die meisten Einheiten speichern XClarity Orchestrator und der Ressourcenmanager bestimmte Informationen, selbst nachdem ihre Verwaltung aufgehoben wurde. Diese Informationen werden erneut angewendet, wenn Sie dieselbe Einheit wieder verwalten.

Vorgehensweise

Gehen Sie wie folgt vor, um die Verwaltung von Einheiten aufzuheben.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.

- Schritt 2. Wählen Sie mindestens eine Einheit aus, deren Verwaltung aufgehoben werden soll.
- Schritt 3. Klicken Sie auf das Symbol **Verwaltung aufheben** () , um das Dialogfenster zur Verwaltungsaufhebung anzuzeigen.
- Schritt 4. Wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aus.
- Schritt 5. Klicken Sie auf **Verwaltung aufheben**.

Der Dialog „Verwaltung aufheben“ zeigt den Status jedes Schritts im Verwaltungsaufhebungsprozess an.

VMware Tools verwenden

Das Paket mit VMware Tools wird auf dem Gastbetriebssystem der virtuellen Maschine installiert, wenn Sie Lenovo XClarity Orchestrator in VMware ESXi-basierten Umgebungen installieren. Dieses Paket enthält eine Gruppe von VMware-Tools, die die optimierte Sicherung und Migration von virtuellen Einheiten unterstützen und gleichzeitig den Anwendungszustand und Kontinuität sicherstellen.

Informationen zur Verwendung der VMware-Tools finden Sie unter [Website zum Verwenden des Konfigurationsdienstprogramms für VMware-Tools im VMware vSphere-Dokumentationscenter](#).

Netzwerkeinstellungen konfigurieren

Sie können eine einzelne Netzwerkschnittstelle (mithilfe von IPv4- und IPv6-Einstellungen) und Internet-Routing- sowie Proxy-Einstellungen konfigurieren.

Vorbereitende Schritte

Weitere Informationen:  [Netzwerke konfigurieren und NTP-Server einrichten](#)

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

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.

IPv4-Konfiguration Enabled

Methode Obtain IP from DHCP	IPv4-Netzwerkmaske 255.255.224.0
IPv4-Adresse 10.243.14.36	IPv4-Standard-Gateway 10.243.0.1

Übernehmen Zurücksetzen

IPv6-Konfiguration Enabled

Methode Use stateless address...	IPv6-Präfixlänge 64
IPv6-Adresse fd55:faaf:e1ab:2021:20c:2'	IPv6-Standard-Gateway fe80::5:73ff:fea0:2c

Übernehmen Zurücksetzen

- **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 Proxyserver, 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).

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

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

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** → **Integrationsservices** 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**.

Mit Sicherheitszertifikaten arbeiten

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.

Vorbereitende Schritte

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

Zu dieser Aufgabe

Das eindeutige Standardserverzertifikat, das in jeder Instanz von 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.

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

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

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

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

Sie können festlegen, dass ein extern signiertes Serverzertifikat anstelle des standardmäßig selbst signierten Serverzertifikats verwendet wird, indem Sie eine Zertifikatssignieranforderung (CSR) generieren, die CSR von einer privaten oder kommerziellen Stammzertifizierungsstelle signieren lassen und dann die vollständige Zertifikatskette in XClarity Orchestrator importieren (siehe [Ein vertrauenswürdigen, extern signiertes XClarity Orchestrator-Serverzertifikat installieren](#)).

Wenn Sie das standardmäßig selbst signierte Serverzertifikat verwenden möchten, wird empfohlen, das Serverzertifikat in Ihren Webbrowser als vertrauenswürdige Stammzertifizierungsstelle zu importieren, um Fehlernachrichten im Browser zu vermeiden (siehe [Das Serverzertifikat in einen Webbrowser importieren](#)).

Die folgende Kategorie (Truststores) von Zertifikaten wird von XClarity Orchestrator Clients verwendet.

- **Vertrauenswürdige Zertifikate** Dieser Truststore verwaltet Zertifikate, die zum Herstellen einer sicheren Verbindung zu lokalen Ressourcen verwendet werden, wenn XClarity Orchestrator als Client fungiert. Beispiele für lokale Ressourcen sind verwaltete Ressourcenmanager, lokale Software bei der Ereignisweiterleitung usw.

- **Zertifikate für externe Services.** Dieser Truststore verwaltet Zertifikate, die zum Herstellen einer sicheren Verbindung mit externen Services verwendet werden, wenn XClarity Orchestrator als Client fungiert. Beispiele für externe Services sind Online-Supportdienste von Lenovo, die zum Abrufen von Garantieinformationen oder zum Erstellen von Servicetickets verwendet werden, sowie externe Software (wie Splunk), an die Ereignisse weitergeleitet werden können. Er enthält vorkonfigurierte, vertrauenswürdige Zertifikate von Stammzertifizierungsstellen von bestimmten, allgemein vertrauenswürdigen und weltweit bekannten Zertifizierungsstellen (z. B. Digicert und Globalsign). Wenn Sie XClarity Orchestrator für die Verwendung einer Funktion konfigurieren, die eine Verbindung zu einem anderen externen Service erfordert, lesen Sie die Dokumentation, um herauszufinden, ob Sie manuell ein Zertifikat zu diesem Truststore hinzufügen müssen.

Beachten Sie, dass Zertifikate in diesem Truststore als nicht vertrauenswürdig eingestuft werden, wenn Verbindungen für andere Services (z. B. LDAP) hergestellt werden, es sei denn, Sie fügen sie auch dem grundlegenden Truststore mit vertrauenswürdigen Zertifikaten hinzu. Das Entfernen von Zertifikaten aus diesem Truststore verhindert die erfolgreiche Ausführung der entsprechenden Dienste.

Vertrauenswürdige Zertifikate für externe Dienste hinzufügen

Diese Zertifikate werden verwendet, um Vertrauensstellungen zu externen Services zu etablieren. Beispielsweise werden Zertifikate in diesem Truststore verwendet, wenn Garantieinformationen von Lenovo abgerufen, Tickets erstellt, Ereignisse an eine externe Anwendung (z. B. Splunk) weitergeleitet und externe LDAP-Server verwendet werden.

Vorbereitende Schritte

Zertifikate in diesem Truststore sind nicht vertrauenswürdig, was die Verbindungen für andere Services anbelangt, es sei denn, Sie fügen sie auch dem Haupt-Truststore für vertrauenswürdige Zertifikate hinzu. Das Entfernen von Zertifikaten aus diesem Truststore verhindert die erfolgreiche Ausführung der entsprechenden Dienste.






Vorgehensweise

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Zertifikat hinzuzufügen.

- Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung**  → **Sicherheit** und dann im linken Navigationsbereich auf **Zertifikate für externe Dienste**, um die Übersicht Vertrauenswürdige Zertifikate für externe Dienste anzuzeigen.

Vertrauenswürdige Zertifikate für externe Dienste

Verwalten Sie Zertifikate, die zur Einrichtung von vertrauenswürdige Beziehungen mit externen Diensten verwendet werden, z. B. beim Abrufen von Garantieinformationen von Lenovo, Erstellen von Tickets, Weiterleiten von Ereignissen an externe Software und Verwendung von externen LDAP-Servern.






 Alle Aktionen ▾ Filter ▾ Suchen X

<input type="checkbox"/>	Thema DN :	Aussteller DN :	Nicht vor :	Nicht nach :	Status :
<input type="checkbox"/>	C = US, O = DigiC...	C = US, O = DigiC...	09.11.2006, 19:0...	09.11.2031, 19:0...	Active
<input type="checkbox"/>	OU = GlobalSign...	OU = GlobalSign...	18.03.2009, 06:0...	18.03.2029, 06:0...	Active
<input type="checkbox"/>	CN = Motorola R...	CN = Motorola R...	28.01.2015, 09:5...	28.01.2035, 10:0...	Active
<input type="checkbox"/>	C = US, ST = Illino...	C = BE, O = Globa...	14.11.2019, 08:5...	27.01.2022, 15:0...	Expired

0 Ausgewählt / 4 Gesamt Zeilen pro Seite: 10 ▾

Schritt 2. Klicken Sie auf das Symbol für **Hinzufügen** (+), um ein Zertifikat hinzuzufügen. Das Dialogfenster Zertifikat hinzufügen wird angezeigt.

Schritt 3. Kopieren Sie die Zertifikatsdaten und fügen Sie sie im PEM-Format ein.

Schritt 4. Klicken Sie auf **Hinzufügen**.

Nach dieser Aufgabe

In der Übersicht Vertrauenswürdige Zertifikate für externe Dienste können Sie die folgenden Aktionen ausführen.

- Um Details zu einem ausgewählten vertrauenswürdigen Zertifikat anzuzeigen, klicken Sie auf das Symbol **Anzeigen** (🔍).
- Sie speichern ein ausgewähltes vertrauenswürdigen Zertifikat auf dem lokalen System, indem Sie auf das Symbol **Anzeigen** (🔍) und anschließend auf **Als „PEM“ speichern** klicken.
- Sie löschen ein ausgewähltes vertrauenswürdigen Zertifikat über das Symbol **Löschen** (🗑️).

Vertrauenswürdige Zertifikate für interne Dienste hinzufügen

Diese Zertifikate werden verwendet, um Vertrauensstellungen mit lokalen Ressourcen herzustellen, wenn Lenovo XClarity Orchestrator für diese Ressourcen als Client fungiert, z. B. Ressourcenmanager, Ereignisweiterleitungen an lokale Software und der eingebettete LDAP-Server. Darüber hinaus sind in diesem Truststore das interne CA-Zertifikat sowie das CA-Zertifikat eines angepassten, extern signierten Serverzertifikats (sofern eines installiert ist) gespeichert, um die interne XClarity Orchestrator-Kommunikation zu unterstützen.

Vorgehensweise

Gehen Sie wie folgt vor, um ein vertrauenswürdigen Zertifikat hinzuzufügen.

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

Vertrauenswürdige Zertifikate

Verwalten Sie Zertifikate, die zur Einrichtung von vertrauenswürdigen Beziehungen mit lokalen Ressourcen verwendet werden, wenn XClarity Orchestrator als Client für diese Ressourcen fungiert, z. B. Ressourcenmanager (XClarity Administrator), die Ereignisse an lokale Software und den LDAP-Server weiterleiten.

🔄 + - 🗑️ 📄 📄 Alle Aktionen Filter 🔍 Suchen ✕

	Thema DN :	Aussteller DN :	Nicht vor :	Nicht nach :	Status :
<input type="radio"/>	C = US, ST = Nort...	C = US, ST = Nort...	31.12.1969, 19:0...	31.12.2069, 18:5...	Active
<input type="radio"/>	C = US, ST = NC, L...	C = US, ST = NC, L...	03.10.2022, 11:1...	03.10.2023, 11:1...	Active

0 Ausgewählt / 2 Gesamt Zeilen pro Seite: 10

Schritt 2. Klicken Sie auf das Symbol für **Hinzufügen** (+), um ein Zertifikat hinzuzufügen. Das Dialogfenster Zertifikat hinzufügen wird angezeigt.

Schritt 3. Kopieren Sie die Zertifikatsdaten und fügen Sie sie im PEM-Format ein.

Schritt 4. Klicken Sie auf **Hinzufügen**.

Nach dieser Aufgabe

In der Übersicht Vertrauenswürdiges Zertifikat können Sie die folgenden Aktionen ausführen.

- Um Details zu einem ausgewählten vertrauenswürdigen Zertifikat anzuzeigen, klicken Sie auf das Symbol **Anzeigen** (🔍).
- Sie speichern ein ausgewähltes vertrauenswürdigen Zertifikat auf dem lokalen System, indem Sie auf das Symbol **Anzeigen** (🔍) und anschließend auf **Als „PEM“ speichern** klicken.
- Sie löschen ein ausgewähltes vertrauenswürdigen Zertifikat über das Symbol **Löschen** (🗑️).

Ein vertrauenswürdigen, extern signiertes XClarity Orchestrator-Serverzertifikat installieren

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

Zu dieser Aufgabe

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

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

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

Wenn das neue Serverzertifikat nicht von einem vertrauenswürdigen Drittanbieter signiert wurde, wird das nächste Mal, wenn Sie eine Verbindung mit XClarity Orchestrator herstellen, im Webbrowser eine Sicherheitsnachricht angezeigt. In einem Dialogfeld werden Sie aufgefordert, das neue Zertifikat im Browser zu akzeptieren. Sie können das Serverzertifikat in die Liste vertrauenswürdiger Zertifikate Ihres Webbrowsers importieren, um die Sicherheitsnachrichten zu vermeiden (siehe [Das Serverzertifikat in einen Webbrowser importieren](#)).

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

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

Vorgehensweise

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

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

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

Zertifikatssignieranforderung (CSR) generieren

Erstellen und speichern Sie eine Zertifikatssignieranforderung mit von Nutzern zur Verfügung gestellten Werten.

Land/Region* <input type="text" value="UNITED STATES"/>	Anordnung* <input type="text" value="Lenovo"/>
Bundesland* <input type="text" value="NC"/>	Organisationseinheit* <input type="text" value="DCG"/>
Stadt* <input type="text" value="Raleigh"/>	Allgemeiner Name* <input type="text" value="Generated by Lenovo Management Ecosystem"/>

Alternative Antragstellernamen ?

Um einen neuen alternativen Antragstellernamen hinzuzufügen, klicken Sie auf +

CSR-Datei generieren
Zertifikat importieren

2. Geben Sie in der Übersicht „Zertifikatssignieranforderung (CSR) generieren“ Daten in die Felder für die Anforderung ein.
 - Zweistelliger ISO 3166-Code für das ursprüngliche Land oder die ursprüngliche Region, der der Zertifizierungsorganisation zugeordnet ist (z. B. US für die Vereinigten Staaten).
 - Vollständiger Name des Bundesstaats/-lands, das dem Zertifikat zugeordnet werden soll (z. B. Kalifornien oder New Brunswick).
 - Vollständiger Name der Stadt, die dem Zertifikat zugeordnet werden soll (z. B. San Jose). Die Länge des Werts darf 50 Zeichen nicht überschreiten.
 - Unternehmen, dem das Zertifikat gehören soll. In der Regel handelt es sich hierbei um den eingetragenen Namen eines Unternehmens. Dies sollte alle Suffixe umfassen wie etwa Ltd., Inc. oder GmbH (z. B. ACME International Ltd.). Die Länge des Werts darf 60 Zeichen nicht überschreiten.
 - (Optional) Organisationseinheit, der das Zertifikat gehören soll (z. B. Sparte ABC). Die Länge des Werts darf 60 Zeichen nicht überschreiten.
 - Allgemeiner Name des Zertifikatsinhabers. Dies muss der Hostname des Servers sein, der das Zertifikat verwendet. Die Länge des Werts darf 63 Zeichen nicht überschreiten.
 - (Optional) Alternative Namen, die beim Generieren der Zertifikatssignieranforderung zur Erweiterung X.509 „subjectAltName“ hinzugefügt werden. Standardmäßig definiert XClarity Orchestrator automatisch alternative Namen für die Zertifikatssignieranforderung auf Basis der IP-Adresse und des Hostnamens, die von den Netzwerkschnittstellen des Gastbetriebssystems von XClarity Orchestrator erkannt werden. Sie können die Werte alternativer Namen anpassen, löschen oder ergänzen. Die alternativen Namen müssen jedoch den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers haben und der Name muss auf den FQDN festgelegt sein.

Der von Ihnen angegebene Name muss für den ausgewählten Typ gültig sein.

 - **DNS** (FQDN verwenden, z. B. hostname.labs.company.com)
 - **IP-Adresse** (z. B. 192.0.2.0)
 - **E-Mail** (z. B. example@company.com)

Anmerkung: Alle alternativen Namen, die in der Tabelle aufgelistet sind, werden überprüft, gespeichert und zur Zertifikatssignieranforderung hinzugefügt, nachdem Sie diese im nächsten Schritt generiert haben.

- Schritt 2. Übermitteln Sie die Zertifikatssignieranforderung an eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA). Die Zertifizierungsstelle signiert die Zertifikatssignieranforderung und gibt ein Serverzertifikat zurück.
- Schritt 3. Importieren Sie das extern signierte Serverzertifikat und das Zertifizierungsstellenzertifikat in XClarity Orchestrator und ersetzen Sie das aktuelle Serverzertifikat.
1. Klicken Sie in der Übersicht „Zertifikatssignieranforderung (CSR) generieren“ auf **Zertifikat importieren**, um das Dialogfeld Zertifikat importieren anzuzeigen.
 2. Kopieren Sie das Serverzertifikat und das Zertifizierungsstellenzertifikat im PEM-Format und fügen Sie sie ein. Sie müssen die gesamte Zertifikatskette angeben, beginnend mit dem Serverzertifikat und endend mit dem Zertifizierungsstellenzertifikat.
 3. Klicken Sie auf **Importieren**, um das Serverzertifikat im XClarity Orchestrator-Truststore zu speichern.
- Schritt 4. Akzeptieren Sie das neue Zertifikat, indem Sie Strg + F5 drücken, um den Browser zu aktualisieren, und dann die Verbindung zur Webschnittstelle wiederherstellen. Dies muss von allen bestehenden Benutzersitzungen durchgeführt werden.

Intern signiertes XClarity Orchestrator-Serverzertifikat neu generieren

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

Zu dieser Aufgabe

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

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

Vorgehensweise

Gehen Sie wie folgt vor, um ein intern signiertes XClarity Orchestrator-Serverzertifikat zu generieren.

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

Serverzertifikat neu generieren

Erstellen Sie mit den zur Verfügung gestellten Zertifikatsdaten einen neuen Schlüssel und ein Zertifikat.

Land/Region* UNITED STATES	Anordnung* Lenovo
Bundesland* NC	Organisationseinheit* DCG
Stadt* Raleigh	Allgemeiner Name* Generated by Lenovo Management Ecosystem
Ungültig vor Datum 03. Oktober.2022 13:21	Ungültig nach Datum* 30. September.2032 13:21

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

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

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

Schritt 3. Klicken Sie auf **Zertifikat neu generieren**, um das intern signierte Zertifikat neu zu generieren. Klicken Sie zur Bestätigung dann auf **Zertifikat neu generieren**.

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

Nach dieser Aufgabe

In der Übersicht „Serverzertifikat neu generieren“ können Sie die folgenden Aktionen ausführen.

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

Das Serverzertifikat in einen Webbrowser importieren

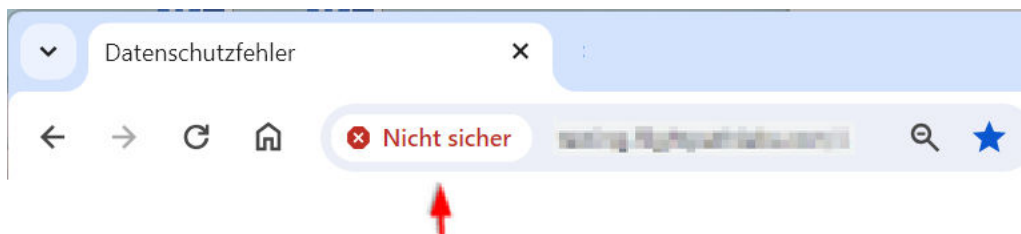
Sie können eine Kopie des aktuellen Serverzertifikats im PEM-Format auf dem lokalen System speichern. Anschließend können Sie das Zertifikat in die Liste vertrauenswürdiger Zertifikate des Webbrowsers oder in andere Anwendungen (z. B. Lenovo XClarity Mobile oder Lenovo XClarity Integrator) importieren,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

Vorgehensweise

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

• Chrome

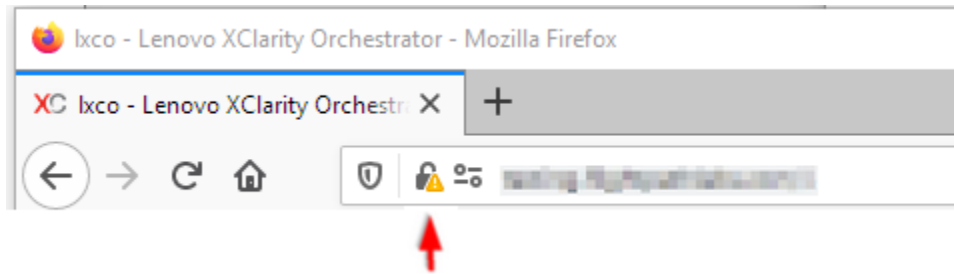
1. Exportieren Sie das XClarity Orchestrator-Serverzertifikat.
 - a. Klicken Sie oben in der Adressleiste auf das Warnsymbol „Nicht sicher“, z. B.:



- b. Klicken Sie auf **Zertifikat (ungültig)**, um das gleichnamige Dialogfeld anzuzeigen.
 - c. Klicken Sie auf die Registerkarte **Details**.
 - d. Wenn Sie auf **In Datei kopieren** klicken, wird der Zertifikatexport-Assistent gestartet.
 - e. Wählen Sie **Cryptographic Message Syntax** aus und klicken Sie auf **Weiter**.
 - f. Geben Sie Name und Speicherort der Zertifikatsdatei an und klicken Sie dann auf **Fertigstellen**, um das Zertifikat zu exportieren.
 - g. Klicken Sie auf **OK**, um das Dialogfenster „Zertifikat“ zu schließen.
2. Importieren Sie das XClarity Orchestrator-Serverzertifikat in die Liste der vertrauenswürdigen Stammzertifizierungsstellen für Ihren Browser.
 - a. Klicken Sie im Chrome-Browser auf die drei Punkte in der oberen rechten Ecke des Fensters und klicken Sie dann auf **Einstellungen**.
 - b. Blättern Sie zum Abschnitt **Datenschutz & Sicherheit** und klicken Sie auf **Zertifikate verwalten**, um das Dialogfeld „Zertifikate“ anzuzeigen.
 - c. Klicken Sie auf **Importieren** und wählen Sie die Zertifikatsdatei aus, die Sie zuvor exportiert haben. Klicken Sie dann auf **Weiter**.
 - d. Klicken Sie neben **Zertifikatspeicher** auf **Durchsuchen** und wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen** aus. Klicken Sie dann auf **OK**.
 - e. Klicken Sie auf **Fertig stellen**.
 - f. Schließen Sie den Chrome-Browser, öffnen Sie ihn erneut und öffnen Sie XClarity Orchestrator.

• Firefox

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



- b. Erweitern Sie „Verbindung nicht sicher“ und klicken Sie dann auf „Weitere Informationen“, um ein Dialogfenster anzuzeigen.
 - c. Klicken Sie auf **Zertifikate anzeigen**.
 - d. Blättern Sie nach unten zum Abschnitt „Speichern“ und klicken Sie auf den Link **PEM (Zertifikat)**.
 - e. Wählen Sie **Datei speichern** aus und klicken Sie auf **OK**.
2. Importieren Sie das XClarity Orchestrator-Serverzertifikat in die Liste der vertrauenswürdigen Stammzertifizierungsstellen für Ihren Browser.
 - a. Öffnen Sie den Browser und klicken Sie auf **Extras → Einstellungen → Erweitert**.
 - b. Wählen Sie **Zertifikate** aus.
 - c. Klicken Sie auf **Zertifikate anzeigen**.
 - d. Wählen Sie **Importieren** aus und navigieren Sie zur Position des heruntergeladenen Zertifikats.
 - e. Markieren Sie das Zertifikat und klicken Sie auf **Öffnen**.

Authentifizierung verwalten

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.

Externen LDAP-Authentifizierungsserver konfigurieren

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

Vorbereitende Schritte

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](#) in der Onlinedokumentation zu XClarity Orchestrator.

Es wird nur Microsoft Active Directory als externer LDAP-Server unterstützt.

XClarity Orchestrator kloniert nicht automatisch Benutzergruppen, die auf dem externen LDAP-Server definiert sind. Sie können die LDAP-Benutzergruppe jedoch manuell klonen (siehe [Benutzergruppen erstellen](#)).

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.

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

Sie können eine LDAP-Serverkonfiguration entfernen, indem Sie auf das Symbol **Löschen** (🗑️) neben der Konfiguration klicken. Wenn Sie eine LDAP-Serverkonfiguration löschen und keine anderen LDAP-Serverkonfigurationen in derselben Domäne vorhanden sind, werden auch die geklonten Benutzer und geklonten Benutzergruppen in dieser Domäne entfernt.

Benutzer und Benutzersitzungen verwalten

Benutzeraccounts werden für die Anmeldung bei und Verwaltung von Lenovo XClarity Orchestrator verwendet.

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

Benutzer in einem externen LDAP-Server werden bei ihrer ersten Anmeldung automatisch auf dem lokalen Authentifizierungsserver geklont und erhalten den Namen *{username}@{domain}*. Dieser geklonte Benutzeraccount kann nur verwendet werden, um den Zugriff auf Ressourcen zu genehmigen. Die Authentifizierung dieser Benutzer erfolgt weiterhin über den LDAP-Authentifizierungsserver und Änderungen am Benutzeraccount (ausgenommen Beschreibung und Rollen) müssen über LDAP durchgeführt werden.

XClarity Orchestrator steuert den Zugriff auf Funktionen (Aktionen) mithilfe von Rollen. Sie können lokalen und geklonten Benutzern eine andere Rolle zuweisen, indem Sie diese Benutzer einer oder mehreren Benutzergruppen hinzufügen, die den gewünschten Rollen zugeordnet sind. Standardmäßig sind alle Benutzer Mitglieder der Benutzergruppe **OperatorGroup** (siehe [Benutzergruppen erstellen](#)).

Mindestens ein Benutzer muss Mitglied einer *lokalen* Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** zugewiesen ist (siehe [Zugriff auf Funktionen steuern](#)).

Achtung: 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.

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

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

- Benutzereigenschaften anzeigen, indem Sie auf die Zeile in der Tabelle klicken, damit ein Benutzer das Dialogfeld Benutzerdetails anzeigen kann
- Die Eigenschaften eines ausgewählten Benutzers ändern, einschließlich Kennwort und Benutzergruppen, indem Sie auf das Symbol **Bearbeiten** klicken (✎)
- Sie löschen einen ausgewählten Benutzer über das Symbol **Löschen** (🗑️). Sie können die vorhandene LDAP-Benutzergruppe nicht aus LDAP-Benutzern löschen.
- Sie können Benutzerdetails, z. B. Benutzername, Vorname und Nachname, durch einen Klick auf das Symbol **Exportieren** (📄) exportieren.

Benutzergruppen erstellen

Benutzergruppen werden verwendet, um den Zugriff auf Ressourcen zu genehmigen.

Vorbereitende Schritte

Weitere Informationen:  [Benutzergruppe erstellen](#)

Sie können Benutzergruppen manuell im lokalen Repository erstellen. Lokale Benutzergruppen enthalten lokale und geklonte Benutzer.

Sie können alle Benutzergruppen klonen, die in einem externen LDAP-Server definiert sind. Die geklonte LDAP-Benutzergruppe hat im lokalen Repository den Namen `{domain}\{groupName}`. Diese geklonte Benutzergruppe kann nur verwendet werden, um den Zugriff auf Ressourcen zu genehmigen. Änderungen am Gruppennamen und an der Beschreibung und Mitgliedschaft müssen über LDAP durchgeführt werden.

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.

Wenn die LDAP-Serverkonfiguration für die Verwendung von Anmeldeinformationen konfiguriert ist und Sie bei XClarity Orchestrator mit einer lokalen XClarity Orchestrator Benutzer-ID angemeldet sind, werden Sie beim Klonen einer LDAP-Benutzergruppe dazu aufgefordert, LDAP-Benutzeranmeldeinformationen anzugeben. In allen anderen Fällen sind Ihre Anmeldeinformationen nicht erforderlich.

Zu dieser Aufgabe

XClarity Orchestrator stellt die folgenden vordefinierten Benutzergruppen bereit, eine für jede vordefinierte Rolle. Weitere Informationen zu Rollen finden Sie unter [Zugriff auf Funktionen steuern](#).

- **Supervisor-Gruppe.** Allen Benutzern in dieser Benutzergruppe wird die Rolle **Supervisor** zugeordnet.
- **Hardwareadministrator-Gruppe.** Allen Benutzern in dieser Benutzergruppe wird die Rolle **Hardwareadministrator** zugeordnet.
- **Sicherheitsadministrator-Gruppe.** Allen Benutzern in dieser Benutzergruppe wird die Rolle **Sicherheitsadministrator** zugeordnet.
- **Reporter-Gruppe:** Allen Benutzern in dieser Benutzergruppe wird die Rolle **Reporter** zugeordnet.
- **Aktualisierungsadministrator-Gruppe.** Allen Benutzern in dieser Benutzergruppe wird die Rolle **Administrator für Aktualisierungen** zugeordnet.
- **Operator-Gruppe.** Allen Benutzern in dieser Benutzergruppe wird die Rolle **Bediener** zugeordnet.
- **Legacy-Operator-Gruppe.** Allen Benutzern in dieser Benutzergruppe wird die Rolle **OperatorLegacy** zugeordnet. Beachten Sie, dass diese Benutzergruppe in zukünftigen Versionen nicht mehr unterstützt wird.

Mindestens ein Benutzer muss Mitglied einer *lokalen* Benutzergruppe sein, der die vordefinierte Rolle **Supervisor** zugewiesen ist (siehe [Zugriff auf Funktionen steuern](#)).

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.





Vorgehensweise

Gehen Sie wie folgt vor, um eine Benutzergruppe zu erstellen.

- **Lokale Benutzergruppe erstellen**

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

Benutzergruppen
Gruppen von Benutzern verwalten.





 Alle Aktionen ▾ Filter ▾ Suchen X

Name	Beschreibung	Rollen
<input type="radio"/> Configuration Patterns Administra...	Allows users to configure servers u...	Configuration Patterns Administrato
<input type="radio"/> Hardware Administrator Group	Allows users to view data, manage ...	Hardware Administrator
<input type="radio"/> OS Administrator Group	Allows users to deploy operating s...	OS Administrator
<input type="radio"/> Operator Group	Allows user to only view the orches...	Operator
<input type="radio"/> Operator Legacy Group	Allows user to view the orchestrat...	Operator Legacy
<input type="radio"/> Reporter Group	Allows users to view the orchestrat...	Reporter
<input type="radio"/> Security Administrator Group	Allows user to modify security setti...	Security Administrator
<input type="radio"/> Supervisor Group	Allows user to view data about and...	Supervisor
<input type="radio"/> Updates Administrator Group	Allows user to manage the updates...	Updates Administrator

0 Ausgewählt / 9 Gesamt Zeilen pro Seite: 10 ▾

2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Gruppe erstellen anzuzeigen.
3. Wählen Sie **Lokale Benutzergruppe** als Gruppentyp aus.
4. Geben Sie den Namen und optional eine Beschreibung für diese Benutzergruppe ein.
5. Klicken Sie auf die Registerkarte **Verfügbare Benutzer** und wählen Sie die Benutzer aus, die in diese Benutzergruppe aufgenommen werden sollen.
6. Klicken Sie auf die Registerkarte **Rollen** und wählen Sie die Rollen aus, die dieser Benutzergruppe zugewiesen werden sollen. Wenn keine Rolle ausgewählt wird, wird standardmäßig die Rolle **Bediener** zugewiesen.
7. Klicken Sie auf **Erstellen**.

- **Benutzergruppe von einem externen LDAP-Server klonen**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⚙️) → **Sicherheit** und dann im linken Navigationsbereich auf **Benutzergruppen**, um die Übersicht Benutzergruppen anzuzeigen.
2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Gruppe erstellen anzuzeigen.
3. Wählen Sie **LDAP-Benutzergruppe** als Gruppentyp aus.
4. Geben Sie optional eine Beschreibung für die Gruppe ein.
5. Wählen Sie die LDAP-Konfiguration für den externen LDAP-Server aus, der die Benutzergruppe enthält, die Sie hinzufügen möchten.

Tipp: Beginnen Sie mit der Eingabe, um alle Gruppennamen zu finden, die ein angegebenes Schlüsselwort enthalten.

6. Wenn der externe LDAP-Server mit Anmeldeinformationen konfiguriert ist, geben Sie den Benutzernamen und das Kennwort an, um sich beim externen LDAP-Server anzumelden.

7. Geben Sie im Feld **Gruppe durchsuchen** einen Suchbegriff (mit mindestens drei Zeichen) ein und klicken Sie auf **Suchen**, um Benutzergruppen im externen LDAP-Server zu finden, die mit dem Suchbegriff übereinstimmen. Wählen Sie dann die Gruppe aus, die Sie hinzufügen möchten.
8. Klicken Sie auf die Registerkarte **Rollen** und wählen Sie die Rollen aus, die dieser Benutzergruppe zugewiesen werden sollen. Wenn keine Rolle ausgewählt wird, wird standardmäßig die Rolle **Bediener** zugewiesen.
9. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

In der Übersicht „Benutzergruppen“ können Sie die folgenden Aktionen ausführen.

- Sie bearbeiten die Eigenschaften, die lokale Mitgliedschaft und die Rollen einer ausgewählten Benutzergruppe, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
 - Wenn Sie einen Benutzer einer Gruppe hinzufügen oder daraus entfernen, wird der Benutzer automatisch abgemeldet, wenn sich die Rollen (Berechtigungen) nach der Zuweisung neuer Gruppen geändert haben. Wenn sich der Benutzer erneut anmeldet, kann er Aktionen basierend auf den aggregierten Rollen der zugewiesenen Benutzergruppen ausführen.
 - Jeder Benutzer muss in mindestens einer Benutzergruppe Mitglied sein. Wenn Sie dieses Attribut auf ein leeres Array oder null festlegen, wird standardmäßig **OperatorGroup** zugewiesen.
 - Bei vordefinierten Benutzergruppen können Sie nur die Gruppenmitgliedschaft ändern.
 - Bei LDAP-Benutzergruppen können Sie nur die Beschreibung und Rollen ändern. Verwenden Sie den externen LDAP-Server, um andere Eigenschaften und Mitgliedschaften zu ändern.
 - Sie löschen eine ausgewählte Benutzergruppe über das Symbol **Löschen** (🗑).
- Anmerkung:** Vordefinierte Benutzergruppen können nicht gelöscht werden.
- Sie können die Mitglieder einer Benutzergruppe anzeigen, indem Sie auf den Gruppennamen klicken, um das Dialogfenster Gruppe anzeigen zu öffnen, und dann auf die Registerkarte **Mitgliedsübersicht** klicken.

Details für Ihren Benutzeraccount ändern

Sie können Kennwort, vollständigen Namen, E-Mail-Adresse und Telefonnummer für Ihren Benutzeraccount ändern.

Zu dieser Aufgabe

Benutzerkennwörter laufen standardmäßig nach **0** Tagen ab.

Vorgehensweise

Gehen Sie wie folgt vor, um Ihr Kennwort und andere Attribute zu ändern.

Schritt 1. Klicken Sie in der Titelleiste von XClarity Orchestrator oben rechts auf das Menü **Benutzerkonto** (👤) und dann auf **Kennwort ändern**. Das Dialogfenster Kennwort ändern wird angezeigt.

Schritt 2. Geben Sie das aktuelle Kennwort ein.

Schritt 3. Geben Sie das neue Kennwort ein und bestätigen Sie es. Standardmäßig müssen Kennwörter **8 – 256** Zeichen enthalten und die folgenden Kriterien erfüllen.

- 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).

Schritt 4. Ändern Sie ggf. Ihren vollständigen Namen, Ihre E-Mail-Adresse und Telefonnummer.

Schritt 5. Klicken Sie auf **Ändern**.

Details für einen anderen Benutzer ändern

Benutzer mit Supervisor-Berechtigungen können Details ändern, darunter auch das Kennwort für einen anderen Benutzer.

Zu dieser Aufgabe

Benutzerkennwörter laufen standardmäßig nach **0** Tagen ab.

Sie können die Zeit für den Kennwortablauf und auch Komplexitätsregeln für Kennwörter konfigurieren (siehe [Benutzersicherheitseinstellungen konfigurieren](#)).

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.

Benutzername	Voller Name	Rollen	Benutzergruppen
userid	Nicht verfügbar	Supervisor	Supervisor Group

Schritt 2. Wählen Sie den Benutzeraccount aus.

Schritt 3. Klicken Sie auf das Symbol **Bearbeiten** (✎), um die Eigenschaften des Benutzers zu ändern. Das Dialogfenster Benutzer bearbeiten wird angezeigt.

Schritt 4. Geben Sie das neue Kennwort ein und bestätigen Sie es. Standardmäßig müssen Kennwörter **8 – 256** Zeichen enthalten und die folgenden Kriterien erfüllen.

- 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).

Schritt 5. Klicken Sie auf **Bearbeiten**.

Benutzersicherheitseinstellungen konfigurieren

Über die Sicherheitseinstellungen für den Benutzeraccount werden die Einstellungen für das Kennwort, die Anmeldung und die Benutzersitzung für lokale Benutzer konfiguriert.

Weitere Informationen:  [Benutzersicherheitseinstellungen konfigurieren](#)

Vorgehensweise

So konfigurieren Sie Sicherheitseinstellungen für lokale Benutzer:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung**  → **Sicherheit** und dann im linken Navigationsbereich auf **Sicherheitseinstellungen für Account**, um die Übersicht Sicherheitseinstellungen für Account anzuzeigen.

Schritt 2. Konfigurieren Sie die folgenden globalen Einstellungen:

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standardwerte
Kennwortablaufdauer	Benutzungszeitraum (in Tagen) eines Kennworts, bevor es geändert werden muss. Kleinere Werte verringern den Zeitraum, in dem Angreifer Passwörter herausfinden können. Beträgt dieser Wert 0, laufen Kennwörter nie ab.	0 – 365	0
Warndauer vor Kennwortablauf	Zeitraum (in Tagen) vor Ablauf des Kennworts, ab dem Nutzer Warnungen über einen bevorstehenden Ablauf des Benutzerkennworts erhalten. Beträgt dieser Wert 0, werden Benutzer nicht gewarnt.	0 – 30	0
Mindestwiederverwendungszyklus des Kennworts	Mindestanzahl der Male, bei denen ein Benutzer bei der Änderung des Kennworts ein einzigartiges Kennwort eingeben muss, bevor ein Kennwort erneut verwendet werden kann. Wird dieser Wert auf 0 festgelegt, können die Benutzer die Kennwörter umgehend wiederverwenden.	0 – 10	5

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standardwerte
Mindestintervall für Kennwortänderung	<p>Mindestzeitspanne (in Stunden), die vergehen muss, bevor ein Benutzer ein Kennwort erneut ändern kann. Der festgelegte Wert für diese Einstellung darf den Wert der Einstellung Kennwortablaufdauer nicht überschreiten.</p> <p>Wird dieser Wert auf 0 festgelegt, können die Benutzer die Kennwörter umgehend ändern.</p>	0 – 240	1
Maximale Anzahl an Anmeldefehlern	<p>Maximale Anzahl fehlgeschlagener Anmeldeversuche, bevor der Benutzeraccount gesperrt wird. Anmerkung: Aufeinanderfolgende Anmeldeversuche mit demselben Benutzernamen und demselben Kennwort gelten als einzelne fehlgeschlagene Anmeldung. Beträgt dieser Wert 0, werden Konten niemals gesperrt.</p>	0 – 10	5
Rücksetzdauer des Zählers für fehlgeschlagene Anmeldungen	<p>Zeitraum seit dem letzten fehlgeschlagenen Anmeldeversuch, bevor der Zähler für die Maximale Anzahl fehlgeschlagener Anmeldeversuche auf 0 zurückgesetzt wird. Wenn dieser Wert auf „0“ festgelegt ist, wird der Zähler nie zurückgesetzt. Wenn zum Beispiel die maximale Anzahl fehlgeschlagener Anmeldeversuche 2 beträgt und Sie sich einmal nicht anmelden können und dann 24 Stunden später ein weiterer Versuch fehlschlägt, registriert das System, dass Sie sich zweimal nicht anmelden konnten, und Ihr Account wird gesperrt. Anmerkung: Diese Einstellung gilt nur, wenn die Einstellung für die Maximale Anzahl fehlgeschlagener Anmeldeversuche auf 1 oder höher festgelegt wird.</p>	0 – 60	15
Sperrzeitraum nach maximaler Anzahl von fehlgeschlagenen Anmeldeversuchen	<p>Mindestdauer in Minuten, nach der sich ein gesperrter Benutzer erneut anmelden kann. Gesperrte Benutzeraccounts können nicht verwendet werden, um auf XClarity Orchestrator zuzugreifen, auch wenn ein gültiges Kennwort eingegeben wird. Beträgt dieser Wert 0, werden Benutzeraccounts niemals gesperrt. Anmerkung: Diese Einstellung gilt nur, wenn die Einstellung für die Maximale Anzahl fehlgeschlagener Anmeldeversuche auf 1 oder höher festgelegt wird.</p>	0 – 2880	60

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standardwerte
Sitzungszeitlimit bei Webinaktivität	<p>Zeitraum in Minuten, über den eine Benutzersitzung mit dem Orchestrator-Server inaktiv sein kann, bevor die Benutzersitzung abläuft und der Benutzer automatisch abgemeldet wird. Dieses Zeitlimit gilt für alle Aktionen (z. B. Öffnen einer Seite, Aktualisieren der aktuellen Seite oder Ändern von Daten).</p> <p>Dies ist das primäre Zeitlimit für die Benutzersitzung.</p> <p>Bei einer aktiven Sitzung wird der Timer jedes Mal zurückgesetzt, wenn der Benutzer eine Aktion ausführt. Nachdem der Zeitlimitwert überschritten wurde, wird dem Benutzer die Anmeldeseite angezeigt, wenn er versucht, eine Aktion auszuführen.</p> <p>Wenn dieser Wert auf 0 festgelegt ist, ist dieses Zeitlimit deaktiviert.</p> <p>Anmerkung: Eine Änderung dieser Einstellung wirkt sich unabhängig vom Authentifizierungstyp sofort auf alle Benutzersitzungen aus. Vorhandene Sitzungen, die bereits länger als der neue Zeitlimitwert inaktiv waren, sind abgelaufen.</p>	0, 60 – 1440	1440
Zeitlimit bei Webinaktivität für Vollbetrieb	<p>Zeitraum in Minuten, den eine Benutzersitzung auf dem Orchestrator-Server inaktiv sein kann, bevor Aktionen zum Verändern von Daten (z. B. Erstellen, Aktualisieren oder Löschen einer Ressource) deaktiviert werden.</p> <p>Hierbei handelt es sich um ein optionales sekundäres Zeitlimit, das kürzer als der primäre Wert des Sitzungszeitlimits bei Webinaktivität ist.</p> <p>Bei einer aktiven Sitzung wird der Timer jedes Mal zurückgesetzt, wenn der Benutzer eine Aktion ausführt. Wenn dieser Zeitlimitwert überschritten wird, aber der primäre Wert Sitzungszeitlimit bei Webinaktivität <i>nicht</i> überschritten wird, verfügt der Benutzer nur über Lesezugriff und kann nur Aktionen durchführen wie z. B. das Öffnen oder Aktualisieren einer Seite, bis der primäre Wert Sitzungszeitlimit bei Webinaktivität überschritten wird. Wenn der Benutzer jedoch versucht, eine Aktion auszuführen, bei der Daten geändert werden, läuft die Benutzersitzung ab und die Anmeldeseite wird angezeigt.</p> <p>Wenn dieser Wert auf 0 festgelegt ist, ist dieses Zeitlimit deaktiviert.</p>	0, 15 – 60	30

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standardwerte
	<p>Anmerkung: Eine Änderung dieser Einstellung wirkt sich unabhängig vom Authentifizierungstyp sofort auf alle Benutzersitzungen aus. Vorhandene Sitzungen, die bereits länger als der neue Zeitlimitwert inaktiv waren, sind abgelaufen.</p>		
Obligatorische Ablaufzeit einer webbasierten Sitzung	<p>Zeitraum in Stunden, über den eine Benutzersitzung mit dem Orchestrator-Server offen sein kann, bevor der Benutzer automatisch und unabhängig von der Benutzeraktivität abgemeldet wird.</p> <p>Anmerkung: Eine Änderung dieser Einstellung wirkt sich unabhängig vom Authentifizierungstyp sofort auf alle Benutzersitzungen aus. Vorhandene Sitzungen, die bereits länger als der neue Zeitlimitwert inaktiv waren, sind abgelaufen.</p>	24 – 240	24
Mindestlänge des Kennworts	Mindestanzahl von Zeichen, die für ein gültiges Passwort verwendet werden können.	8 – 256	256
Maximale Länge des Kennworts	Maximale Anzahl von Zeichen, die für ein gültiges Kennwort verwendet werden können.	8 – 128	128
Maximale Anzahl aktiver Sitzungen für einen bestimmten Benutzer	<p>Maximale Anzahl aktiver Sitzungen für einen bestimmten Benutzer, die zu einem bestimmten Zeitpunkt zulässig sind. Wenn die maximale Anzahl erreicht ist, wird die älteste aktive Sitzung eines Benutzers (basierend auf dem Erstellungszeitstempel) entfernt, bevor eine neue Sitzung für diesen Benutzer erstellt wird.</p> <p>Ist dieser Wert auf 0 festgelegt, ist die Anzahl zulässiger aktiver Sitzungen für einen bestimmten Benutzer unbegrenzt.</p> <p>Anmerkung: Sie wirkt sich nur auf Benutzersitzungen aus, die gestartet werden, nachdem die Einstellung geändert wurde.</p>	0 – 20	20

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standardwerte
Anzahl der Komplexitätsregeln, die bei der Erstellung eines neuen Kennworts befolgt werden müssen	<p>Anzahl der Komplexitätsregeln, die bei der Erstellung eines neuen Kennworts befolgt werden müssen</p> <p>Die Regeln werden beginnend mit Regel 1 bis zu der angegebenen Anzahl erzwungen. Beispiel: Wenn die Kennwortkomplexität auf 4 festgelegt ist, müssen die Regeln 1, 2, 3 und 4 befolgt werden. Wenn die Kennwortkomplexität auf 2 festgelegt ist, müssen die Regeln 1 und 2 befolgt werden.</p> <p>XClarity Orchestrator unterstützt die folgenden Komplexitätsregeln für Kennwörter.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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). <p>Wenn der Wert auf 0 festgelegt ist, müssen die Kennwörter keine der Komplexitätsregeln einhalten.</p>	0 – 5	4
Benutzer zwingen, das Kennwort beim ersten Zugriff zu ändern	Mit dieser Einstellung wird festgelegt, ob ein Benutzer das Kennwort ändern muss, wenn er sich erstmalig bei XClarity Orchestrator anmeldet.	Ja oder Nein	Ja

Schritt 3. Klicken Sie auf **Übernehmen**.

Nachdem die Änderungen übernommen wurden, werden die neuen Einstellungen sofort wirksam. Wenn Sie Kennwortrichtlinien ändern, werden diese Richtlinien beim nächsten Anmelden eines Benutzers oder bei einer Kennwortänderung aktiv.

Nach dieser Aufgabe

In der Übersicht Sicherheitseinstellungen für Account können Sie die folgenden Aktionen ausführen.

- Klicken Sie zum Zurücksetzen der Einstellungen auf die Standardwerte auf **Standardwerte wiederherstellen**.

Aktive Benutzersitzungen überwachen

Sie können feststellen, wer an der XClarity Orchestrator-Webschnittstelle angemeldet ist.

Vorbereitende Schritte

Standardmäßig werden Benutzersitzungen, die länger als 24 Stunden keine Aktivitäten verzeichnen, automatisch abgemeldet. Sie können das Sitzungszeitlimit bei Webinaktivität konfigurieren (siehe [Benutzersicherheitseinstellungen konfigurieren](#)).

Vorgehensweise

Um eine Liste aller aktiven Benutzersitzungen (einschließlich der aktuellen Sitzung) abzurufen, klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⚙️) → **Sicherheit** und dann im linken Navigationsbereich auf **Aktive Sitzungen**, um die Übersicht Aktive Sitzungen anzuzeigen.

Benutzername	IP-Adresse	Zuletzt angemeldet
userid	Nicht verfügbar	04.10.22, 08:36
userid	Nicht verfügbar	04.10.22, 13:25

Nach dieser Aufgabe

In der Übersicht Aktive Sitzungen können Sie die folgenden Aktionen ausführen.

- Trennen Sie eine ausgewählte Benutzersitzung über das Symbol **Löschen** (🗑️).

Anmerkung: Sie können die aktuelle Sitzung nicht trennen.

Zugriff auf Funktionen steuern

Lenovo XClarity Orchestrator verwendet *Rollen* und *Benutzergruppen*, um zu steuern, welche Funktionen (Aktionen) ein Benutzer ausführen darf.

Zu dieser Aufgabe

Eine *Rolle* umfasst eine Reihe von Funktionen. Wenn eine Rolle einer Benutzergruppe zugewiesen ist, können alle Benutzer in dieser Gruppe die Funktionen ausführen, die in dieser Rolle enthalten sind.

Die folgenden Rollen sind in XClarity Orchestrator vordefiniert.

- **Supervisor:** Benutzer können Daten über alle verfügbaren Aktionen auf dem Orchestrator-Server und alle verwalteten Ressourcen (Ressourcenmanager und Einheiten) anzeigen und alle verfügbaren Aktionen ausführen. Benutzer mit dieser Rolle haben immer Zugriff auf alle Ressourcen (Einheiten und Ressourcenmanager) sowie alle Funktionen. Sie können den Zugriff auf Ressourcen oder Funktionen für diese Rolle nicht einschränken.

Sie müssen über Supervisor-Berechtigungen verfügen, um die folgenden Aktionen durchführen zu können.

- Orchestrator-Server neu starten
- Wartungsaufgaben ausführen, z. B. Lizenzen installieren und auf eine neuere Version aktualisieren
- Ressourcenmanager verbinden und trennen
- Systemeinstellungen ändern, z. B. Netzwerkeinstellungen sowie Datum und Uhrzeit
- Zustimmung, dass regelmäßig Daten an Lenovo gesendet werden

Es muss mindestens ein Benutzer mit Supervisor-Berechtigungen vorhanden sein.

Wichtig: Bei der Aktualisierung von XClarity Orchestrator v1.0 auf eine neuere Version erhalten alle in XClarity Orchestrator v1.0 erstellten Benutzer standardmäßig Supervisor-Berechtigungen. Ein Supervisor-Benutzer kann die Supervisor-Berechtigungen für Benutzer entfernen, die nicht über diese Berechtigungen verfügen sollten.

- **Hardwareadministrator.** Benutzer können Daten anzeigen, Konfigurationsmuster verwalten und implementieren, Betriebssysteme mithilfe von BS-Profilen verwalten und implementieren, Analysen anzeigen und anpassen und Aktionen auf zugänglichen Ressourcen durchführen. Diese Rolle verbietet Benutzern die Aktualisierung von Software oder Firmware auf verwalteten Ressourcen sowie die Verwaltung von Ressourcengruppen.
- **Serverkonfigurationsadministrator.** Benutzer können Server mithilfe von Konfigurationsmustern konfigurieren, vordefinierte Analysen anzeigen und Daten für zugängliche Ressourcen anzeigen. Diese Rolle verhindert, dass Benutzer per Fernsteuerung auf die Einheiten zugreifen und Einheiten ein- und ausschalten.
- **BS-Administrator.** Benutzer können Betriebssysteme mithilfe von BS-Profilen implementieren, vordefinierte Analysen anzeigen und Daten für zugängliche Ressourcen anzeigen. Diese Rolle verhindert, dass Benutzer per Fernsteuerung auf die Einheiten zugreifen und Einheiten ein- und ausschalten.
- **Administrator für Aktualisierungen:** Benutzer können Firmware auf Einheiten und Software auf Ressourcenmanagern aktualisieren, Daten für zugängliche Ressourcen anzeigen und vordefinierte Analysen anzeigen.
- **Sicherheitsadministrator:** Benutzer können Sicherheitseinstellungen ändern und sicherheitsbezogene Aktionen auf dem Orchestrator-Server ausführen, Daten für alle verwalteten Ressourcen anzeigen, die Ressourcengruppe verwalten und vordefinierte Analysen einsehen. Benutzer mit dieser Rolle haben immer Zugriff auf alle Ressourcen (Geräte und Ressourcenmanager). Sie können den Zugriff auf Ressourcen für diese Rolle nicht einschränken.
- **Reporter:** Benutzer können die Konfiguration des Orchestrator-Servers anzeigen, Daten zu zugänglichen Ressourcen anzeigen, Abfragen zur Generierung von angepassten Berichten erstellen und Datenweiterleiter zur Planung und Versendung von Berichten per E-Mail erstellen. Diese Rolle verhindert, dass Benutzer Ressourcen bereitstellen und Einheiten ein- und ausschalten.
- **Bediener.** Benutzer können die Konfiguration des Orchestrator-Servers sowie Daten für zugängliche Ressourcen anzeigen. Diese Rolle enthält nicht die Berechtigung zum Ausführen von Aktionen oder Ändern von Konfigurationseinstellungen auf dem Orchestrator-Server und den verwalteten Ressourcen, zum Erstellen und Anzeigen von Analyseberichten oder zum Erstellen benutzerdefinierter Warnungen.
- **Bediener (veraltet):** Benutzer können Daten anzeigen und bestimmte Aktionen auf zugänglichen Ressourcen ausführen, z. B. Bestand, Alerts und Service-Tickets verwalten. Diese Rolle ermöglicht es Benutzern nicht, Software oder Firmware für verwaltete Ressourcen zu aktualisieren, Ressourcengruppen zu erstellen, Analyseberichte zu erstellen und anzuzeigen und benutzerdefinierte Warnungen zu erstellen.

Achtung: Beim Upgrade von XClarity Orchestrator v1.2 auf eine spätere Version erhalten Benutzer, denen die Rolle **Bediener** zugewiesen ist, automatisch die Rolle **Bediener (veraltet)** und werden der Benutzergruppe **OperatorLegacyGroup** hinzugefügt. Die Rolle **Bediener (veraltet)** und die Benutzergruppe **OperatorLegacyGroup** werden ab einer künftigen Version nicht mehr unterstützt.

Wenn ein Benutzer keine Berechtigung zum Ausführen bestimmter Aktionen hat, sind die Menüelemente, Symbolleistensymbole und Schaltflächen, über die diese Aktionen ausgeführt werden, deaktiviert (abgeblendet).

Anmerkung: Die Anzeige ressourcenbezogener Daten ist nicht je nach Rolle eingeschränkt. Alle Benutzer können ressourcenbezogene Daten (z. B. Bestände, Warnungen, Aufträge und Service-Tickets) für Ressourcen anzeigen, auf die sie Zugriff haben.

Vorgehensweise

Um Informationen zu den vordefinierten Rollen anzuzeigen, klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (🔗) → **Sicherheit** und dann im linken Navigationsbereich auf **Rollen**.

Klicken Sie auf die Zeile für eine Rolle, um das Dialogfeld Rollen mit Informationen zu den Rolleneigenschaften, eine Liste der Funktionen in der Rolle und eine Liste der Benutzergruppen anzuzeigen, denen die Rolle zugewiesen ist.

Rollen Benutzern zuweisen

Lenovo XClarity Orchestrator verwendet *Rollen* und *Benutzergruppen*, um zu steuern, welche Funktionen (Aktionen) ein Benutzer ausführen darf.

Vorbereitende Schritte

Wenn sich die Rollenzuweisung für einen Benutzer ändert, während er bei einer aktiven Sitzung angemeldet ist, wird die Sitzung des Benutzers automatisch beendet und er wird von der Benutzerschnittstelle abgemeldet. Wenn sich der Benutzer dann erneut anmeldet, kann er die Funktionen entsprechend den neuen Rollen ausführen.

Zu dieser Aufgabe

Wenn Sie einer Benutzergruppe mehrere Rollen zuweisen, werden die Funktionen jeder Rolle aggregiert.

Alle Benutzer, die einer Benutzergruppe angehören, dürfen die Funktionen ausführen, die in den dieser Benutzergruppe zugewiesenen Rollen enthalten sind.

Sie können die Rollen eines Benutzers durch folgende Aktionen ändern:

- Benutzer einer Benutzergruppe hinzufügen oder daraus entfernen
- Rollen zu einer Benutzergruppe hinzufügen, der der Benutzer angehört, oder daraus entfernen
- Eine Benutzergruppe löschen, der der Benutzer angehört

Anmerkungen:

- Wenn LDAP-Benutzer zu LDAP-Benutzergruppen auf dem LDAP-Server hinzugefügt oder daraus entfernt werden, werden die Änderungen an den Zuordnungen zwischen LDAP-Benutzer und LDAP-Benutzergruppe basierend auf vorhandenen geklonten LDAP-Benutzergruppen in XClarity Orchestrator automatisch aktualisiert.
- Wenn sich die Rollen, die einer Benutzergruppe zugewiesen sind, ändern, muss sich der Benutzer erneut anmelden, damit die Rollenänderungen wirksam werden.

Zugriff auf Ressourcen steuern

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.

Vorgehensweise

Gehen Sie wie folgt vor, um den Zugriff auf Ressourcen zu steuern.

Schritt 1. Erstellen Sie eine Benutzergruppe, die auf die Ressourcen zugreifen kann.

Schritt 2. Erstellen Sie mindestens eine Ressourcengruppe, für die der Zugriff gesteuert werden soll.

Schritt 3. Erstellen Sie eine Zugriffssteuerungsliste, die die Benutzergruppe und mindestens eine Ressourcengruppe enthält.

Schritt 4. Aktivieren Sie die ressourcenbasierte Zugriffssteuerung.

Ressourcenbasierten Zugriff aktivieren

Wenn Sie die Ressourcen einschränken möchten, auf die Benutzer zugreifen können, aktivieren Sie den ressourcenbasierten Zugriff.

Zu dieser Aufgabe

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.

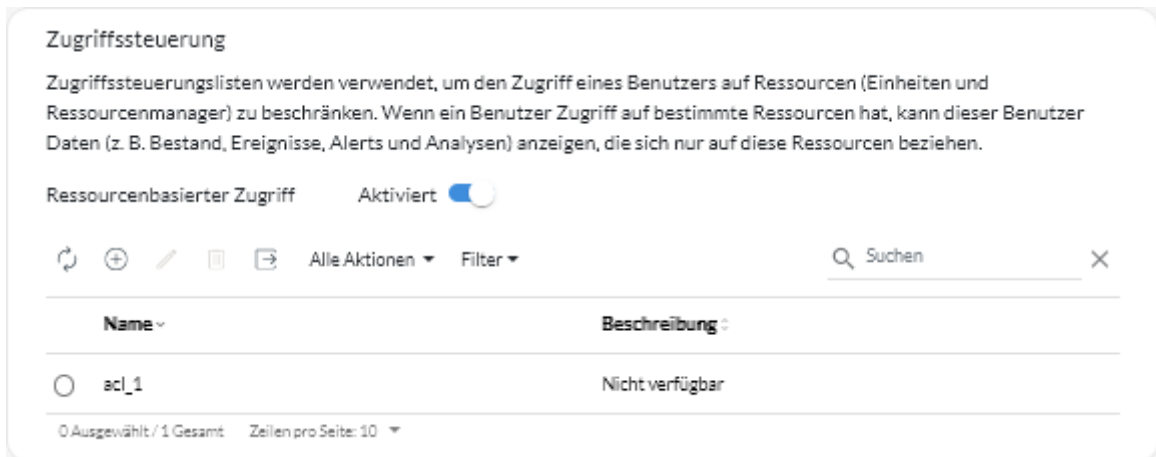
Wenn der ressourcenbasierte Zugriff aktiviert ist, haben Benutzer, die *nicht* Mitglied einer Gruppe sind, der die vordefinierte Rolle **Supervisor** zugewiesen ist, standardmäßig keinen Zugriff auf Ressourcen (Einheiten und Ressourcenmanager). Sie müssen Benutzer ohne Supervisor-Berechtigungen zu einer 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).

Vorgehensweise

Gehen Sie wie folgt vor, um den ressourcenbasierten Zugriff zu aktivieren.

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



Schritt 2. Klicken Sie auf die Umschalt-Schaltfläche **Ressourcenbasierter Zugriff**, um den ressourcenbasierten Zugriff über Zugriffssteuerungslisten zu aktivieren.

Zugriffssteuerungslisten erstellen

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.

Vorbereitende Schritte

Weitere Informationen:  [Zugriffssteuerungslisten erstellen](#)

Stellen sie sicher, dass die Benutzergruppen, die Sie der ACL zuordnen möchten, definiert sind (siehe [Benutzergruppen erstellen](#)).

Stellen sie sicher, dass alle Ressourcengruppen, die Sie dieser ACL zuordnen möchten, definiert sind (siehe [Ressourcengruppen erstellen](#)).

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).

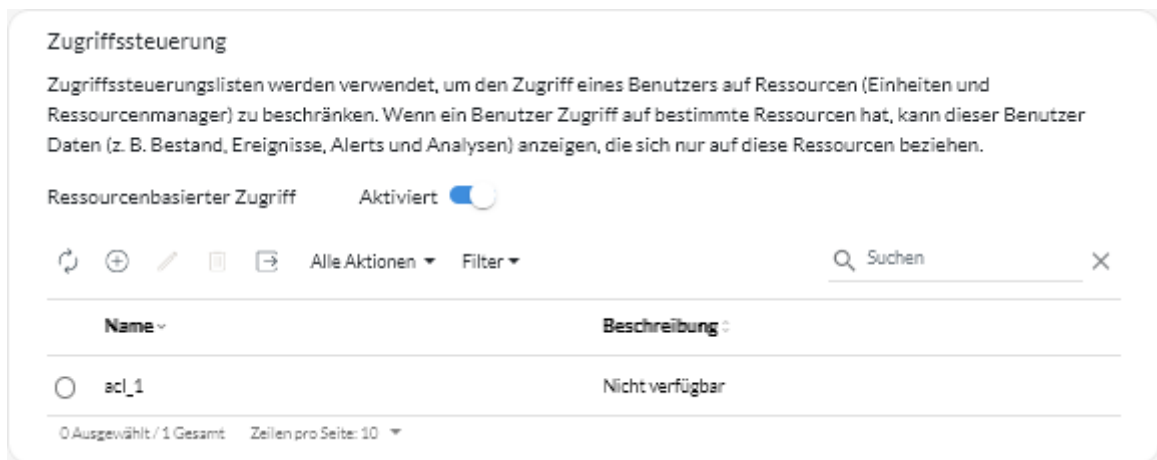
- *Ressourcengruppen* identifizieren die Ressourcen (Einheiten, Ressourcenmanager und XClarity Orchestrator), auf die zugegriffen werden kann. Die ACL muss mindestens eine Ressourcengruppe enthalten.

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.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Zugriffssteuerungsliste zu erstellen.

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



- Schritt 2. Klicken Sie auf das Symbol **Hinzufügen** (+), um eine ACL hinzuzufügen. Der Dialog Zugriffssteuerung erstellen wird angezeigt.
- Schritt 3. Geben Sie den Namen und optional eine Beschreibung für die ACL ein.
- Schritt 4. Klicken Sie auf **Benutzergruppe** und wählen Sie die Benutzergruppe aus, die in die ACL aufgenommen werden soll.
- Schritt 5. Klicken Sie auf **Ressourcengruppen** und wählen Sie die Ressourcengruppe aus, die in die ACL aufgenommen werden soll.
- Schritt 6. Klicken Sie auf **Erstellen**.

Die Zugriffssteuerungsliste wird zur Tabelle hinzugefügt.

Nach dieser Aufgabe

Auf dieser Seite können Sie die folgenden Aktionen ausführen.

- Zeigen Sie die Benutzergruppe und Ressourcengruppen in einer bestimmten ACL an, indem Sie auf eine beliebige Stelle in der Zeile dieser ACL klicken.

- Bearbeiten Sie die Eigenschaften und Mitgliedschaft einer ausgewählten ACL, indem Sie auf das Symbol **Bearbeiten** klicken (✎).
- Sie löschen eine ausgewählte ACL über das Symbol **Löschen** (🗑️).
- Wenn ein Benutzer nicht auf Daten für eine bestimmte Ressource zugreifen kann oder wenn ein Benutzer auf Daten für eine bestimmte Ressource zugreifen kann, auf die er nicht zugreifen können sollte, identifizieren Sie die Zugriffssteuerungslisten, die dem Benutzer zugeordnet sind, und zeigen Sie dann die Mitgliedschaft jeder Ressourcengruppe an, die auch diesen Zugriffssteuerungslisten zugeordnet ist. Stellen Sie sicher, dass die fragliche Ressource (nicht) in diesen Ressourcengruppen enthalten ist.

Plattenspeicher verwalten

Sie können die von Lenovo XClarity Orchestrator verwendete Plattenspeicherbelegung verwalten, indem Sie Dateien löschen, die nicht mehr benötigt werden.

Zu dieser Aufgabe

Vorgehensweise

Wählen Sie eine der folgenden Vorgehensweisen, um nicht mehr benötigte Dateien zu löschen.

Service-dateien von Einheiten

1. Klicken Sie in der Menüleiste von Lenovo XClarity Orchestrator auf **Verwaltung** (⚙️) → **Service und Support** und dann auf die Registerkarte **Service-dateien**, um die Übersicht Einheiten-Service-dateien aufzurufen.
2. Wählen Sie beliebig viele zu löschende Service-dateien aus und klicken Sie auf das Symbol **Löschen** (🗑️).

Betriebssystem-Images

1. Klicken Sie in der Menüleiste von Lenovo XClarity Orchestrator auf **Verwaltung** (⚙️) → **BS-Implementierung** und dann auf die Registerkarte **BS-Verwaltung**, um die Übersicht BS-Images anzuzeigen.
2. Wählen Sie mindestens ein zu löschendes BS-Image aus und klicken Sie auf das Symbol **Löschen** (🗑️).

Nutzlastdateien aktualisieren

Stellen Sie sicher, dass die Aktualisierungen nicht in einer Updates-Konformitätsrichtlinie verwendet werden. Sie können eine Aktualisierung auf der Übersicht „Übernehmen und aktivieren“ aus einer Richtlinie entfernen (siehe [Aktualisierungskonformitätsrichtlinien erstellen und zuordnen](#)).

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (📦) → **Aktualisierungen** und dann auf die Registerkarte **Repository-Verwaltung**, um die Übersicht Repository-Verwaltung aufzurufen.
2. Wählen Sie eine oder mehrere zu löschende Aktualisierungspakete aus.
3. Klicken Sie auf das Symbol **Nur Nutzlastdateien löschen** (🗑️), um nur die Image-Datei (Nutzlastdatei) für die einzelnen ausgewählten Aktualisierungen zu löschen. Informationen zur Aktualisierung (die XML-Metadatei) verbleiben im Repository und der Downloadstatus ändert sich zu „Nicht heruntergeladen“.

XClarity Orchestrator-Aktualisierungen

Sie können Orchestrator-Serveraktualisierungen löschen, die den Status „Heruntergeladen“ aufweisen. In der Tabellenspalte **Angewendeter Status** wird der Status der Aktualisierung angegeben.

1. Klicken Sie auf der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⌘) und dann auf die Registerkarte **Orchestrator-Serveraktualisierung**, um die Übersicht „Orchestrator-Serveraktualisierung“ aufzurufen.
2. Wählen Sie beliebig viele zu löschende Aktualisierungen aus und klicken Sie auf das Symbol **Löschen** (🗑️). Die Angabe in der Spalte **Abgerufener Status** für die gelöschten Updates ändert sich in „Nicht heruntergeladen“.

Neustart von XClarity Orchestrator

Es gibt bestimmte Situationen, in denen Sie Lenovo XClarity Orchestrator möglicherweise neu starten müssen, z. B. beim Neugenerieren oder Hochladen eines Serverzertifikats. Sie können Lenovo XClarity Orchestrator über die Webschnittstelle neu starten.

Vorbereitende Schritte

Für den Neustart von XClarity Orchestrator benötigen Sie **Supervisor**-Berechtigungen.

Sie sollten den Orchestrator-Server vor dem Neustart sichern (siehe [Orchestrator-Serverdaten sichern und wiederherstellen](#)).

Stellen Sie sicher, dass aktuell keine Jobs laufen. Alle aktuell laufenden Jobs werden beim Neustart abgebrochen. Weitere Informationen zum Anzeigen des Jobprotokolls finden Sie unter [Jobs überwachen](#).

Während des Neustarts werden Jobs angehalten, alle Benutzer abgemeldet und die Verbindung zum Orchestrator-Server geht verloren. Warten Sie 15 Minuten oder länger (je nach Anzahl der verwalteten Einheiten) auf den Neustart des Orchestrator-Servers, bevor Sie sich erneut anmelden ([Bei XClarity Orchestrator anmelden](#)).

Nach dem Neustart erfasst XClarity Orchestrator für jede verwaltete Einheit neue Bestandsdaten. Warten Sie ca. 30-45 Minuten (je nach Anzahl der verwalteten Einheiten), bevor Sie Firmwareaktualisierungen, die Bereitstellung von Konfigurationsmustern oder Betriebssystembereitstellungen durchführen.

Vorgehensweise

Schließen Sie eine der folgenden Vorgehensweisen ab, um XClarity Orchestrator neu zu starten.

Aus der Benutzerschnittstelle

1. Navigieren Sie in der Menüleiste von XClarity Orchestrator zu **Wartung** → **Einheit neu starten**.
2. Klicken Sie auf **Neu starten**.
3. Klicken Sie auf **Ja**.
4. Aktualisieren Sie den Browser.

Aus dem Hypervisor

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. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Zurücksetzen**.

VMware ESXi

1. Stellen Sie über VMware vSphere Client eine Verbindung zum Host her.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und navigieren Sie dann zu **Ein/Aus → Zurücksetzen**.
3. Klicken Sie auf die Registerkarte **Konsole**.

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
... ..
```

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.

Orchestrator-Serverdaten sichern und wiederherstellen

Lenovo XClarity Orchestrator enthält keine integrierten Sicherungs- und Wiederherstellungsfunktionen. Stattdessen werden Sicherungsfunktionen verwendet, die basierend auf dem virtuellen Hostbetriebssystem verfügbar sind, auf dem XClarity Orchestrator installiert ist.

Zu dieser Aufgabe

Sichern Sie XClarity Orchestrator immer nach der Erstkonfiguration und nachdem wesentliche Konfigurationsänderungen durchgeführt wurden, einschließlich:

- Vor der Aktualisierung von XClarity Orchestrator
- Nach Netzwerkänderungen
- Nach dem Hinzufügen von Benutzern zum lokalen Authentifizierungsserver von XClarity Orchestrator

- Nach der Verwaltung neuer Ressourcenmanager

Wenn Sicherungs- und Wiederherstellungsverfahren für virtuelle Hosts vorhanden sind, stellen Sie sicher, dass Ihre Verfahren XClarity Orchestrator berücksichtigen.

Wichtig:

- Stellen Sie sicher, dass alle laufenden Jobs abgeschlossen sind und dass XClarity Orchestrator heruntergefahren wird, bevor Sie eine Sicherung erstellen.
- Stellen Sie sicher, dass Sie XClarity Orchestrator regelmäßig sichern. Wenn das Hostbetriebssystem unerwartet herunterfährt, ist eine Authentifizierung bei XClarity Orchestrator eventuell nicht möglich, nachdem das Hostbetriebssystem neu gestartet wurde. Sie können dieses Problem lösen, indem Sie XClarity Orchestrator aus der letzten Sicherung wiederherstellen.

Orchestrator-Serverdaten auf einem VMware ESXi-Host sichern und wiederherstellen

Hin und wieder müssen Sie möglicherweise Orchestrator-Serverdaten aus einer Sicherung wiederherstellen. Es gibt mehrere Möglichkeiten, eine virtuelle XClarity Orchestrator-Einheit, die auf einem VMware ESXi-Host ausgeführt wird, zu sichern und wiederherzustellen. Der spezifische Prozess, der zur Wiederherstellung aus einer Sicherung verwendet wird, basiert auf dem Prozess, der zum Erstellen der Sicherung verwendet wurde. In diesem Abschnitt wird erläutert, wie Sie mit dem VMware vSphere Client Sicherungen und Wiederherstellungen durchführen.

Zu dieser Aufgabe

Wenn VMware vCenter Server installiert ist, können Sie die Sicherungsfunktion verwenden, die mit VMware vCenter bereitgestellt wird, um XClarity Orchestrator zu sichern.

Wenn VMware vCenter Server nicht installiert ist, können Sie den VMware vSphere Client verwenden, um eine Sicherung der virtuellen Maschinen zu erstellen, indem Sie die Dateien aus dem XClarity Orchestrator-Ordner in einen anderen Ordner im gleichen Datenspeicher kopieren. Sie können auch die Dateien in einen anderen Datenspeicher oder sogar in einen anderen Host kopieren, um zusätzlichen Sicherungsschutz zu erhalten.

Anmerkung: Es ist nicht erforderlich, dass VMware vCenter Server eine Sicherung mithilfe dieses Verfahrens ausführt.

Vorgehensweise

- **XClarity Orchestrator sichern** Gehen Sie wie folgt vor, um mithilfe von VMware vSphere Client eine Sicherung von XClarity Orchestrator zu erstellen.
 1. Fahren Sie XClarity Orchestrator herunter.
 2. Starten Sie den VMware vSphere Client und stellen Sie eine Verbindung mit dem ESXi-Host her, auf dem sich XClarity Orchestrator befindet.
 3. Erstellen Sie einen neuen Ordner im Datenspeicher, der auch von XClarity Orchestrator verwendet wird.
 - a. Wählen Sie den ESXi-Host in der Navigationsstruktur und klicken Sie anschließend auf die Registerkarte **Konfigurieren** im rechten Fenster.
 - b. Klicken Sie auf **Hardware → Speicher**.
 - c. Klicken Sie mit der rechten Maustaste auf den Datenspeicher für XClarity Orchestrator und klicken Sie auf **Datenspeicher durchsuchen**.

- d. Wählen Sie den Stammordner aus und erstellen Sie dann einen neuen Ordner, der eine Kopie der XClarity Orchestrator-Dateien enthalten soll.
 4. Klicken Sie auf den Ordner XClarity Orchestrator.
 5. Wählen Sie alle Dateien im Ordner aus und kopieren Sie die Dateien in den Sicherungsordner, den Sie gerade erstellt haben.
 6. Führen Sie für XClarity Orchestrator einen Neustart durch.
- **XClarity Orchestrator wiederherstellen** Gehen Sie wie folgt vor, um XClarity Orchestrator mithilfe der im vorherigen Schritt erstellten Sicherung wiederherzustellen.
 1. Starten Sie den VMware vSphere Client und stellen Sie eine Verbindung mit dem ESXi-Host her, auf dem XClarity Orchestrator installiert ist.
 2. Klicken Sie mit der rechten Maustaste auf XClarity Orchestrator in der linken Navigationsstruktur und klicken Sie anschließend auf **Strom → Ausschalten**.
 3. Klicken Sie mit der rechten Maustaste erneut auf XClarity Orchestrator in der linken Navigationsstruktur und klicken Sie anschließend auf **Aus Inventar entfernen**.
 4. Löschen Sie die Dateien aus dem XClarity Orchestrator-Ordner im Datenspeicher, der vom XClarity Orchestrator verwendet wird.
 - a. Wählen Sie den ESXi-Host in der Navigationsstruktur und klicken Sie anschließend auf die Registerkarte **Konfigurieren** im rechten Fenster.
 - b. Klicken Sie auf **Hardware → Speicher**.
 - c. Klicken Sie mit der rechten Maustaste auf den Datenspeicher für XClarity Orchestrator und klicken Sie auf **Datenspeicher durchsuchen**.
 - d. Wählen Sie den Ordner XClarity Orchestrator aus.
 - e. Wählen Sie alle Dateien im Ordner aus, klicken Sie mit der rechten Maustaste darauf und klicken Sie anschließend auf **Ausgewählte Elemente löschen**.
 5. Wählen Sie den Ordner aus, in dem die Sicherungsdateien gespeichert sind.
 6. Wählen Sie alle Dateien im Ordner aus und kopieren Sie sie in den Ordner XClarity Orchestrator.
 7. Klicken Sie im Ordner XClarity Orchestrator mit der rechten Maustaste auf die VMX-Datei und klicken Sie anschließend auf **Zu Bestand hinzufügen**.
 8. Schließen Sie den Vorgang im Assistenten ab, um XClarity Orchestrator-Daten hinzuzufügen.
 9. Führen Sie über VMware vSphere Client einen Neustart von XClarity Orchestrator durch.
 10. Wenn Sie aufgefordert werden, auszuwählen, ob die VM verschoben oder kopiert wurde, wählen Sie **verschoben** aus.

Wichtig: Wenn Sie **kopiert** auswählen, bekommt die VM eine UUID zugewiesen, die sich von der ursprünglichen VM unterscheidet. Die VM agiert wie eine neue Instanz und zuvor verwaltete Einheiten können nicht angezeigt werden.

Orchestrator-Serverdaten auf einem Microsoft Hyper-V-Host sichern und wiederherstellen

Hin und wieder müssen Sie möglicherweise Lenovo XClarity Orchestrator Orchestrator-Serverdaten aus einer Sicherung wiederherstellen. Es gibt mehrere Möglichkeiten, eine virtuelle XClarity Orchestrator-Einheit, die auf einem Microsoft Hyper-V-Host ausgeführt wird, zu sichern und wiederherzustellen. Der spezifische Prozess, der zur Wiederherstellung aus einer Sicherung verwendet wird, basiert auf dem Prozess, der zum Erstellen der Sicherung verwendet wurde. In diesem Abschnitt wird erläutert, wie Sie mit Windows Server Backup Sicherungen und Wiederherstellungen durchführen.

Vorbereitende Schritte

Stellen Sie sicher, dass Windows Server Backup ordnungsgemäß konfiguriert ist, indem Sie die folgenden Schritte ausführen.

1. Starten Sie Windows Server Manager.
2. Klicken Sie auf **Verwalten → Rollen und Funktionen hinzufügen**.
3. Überspringen Sie den Assistenten, bis Sie die Seite **Funktionen auswählen** erreichen.
4. Aktivieren Sie das Kontrollkästchen **Windows Server Backup**.
5. Beenden Sie den Assistenten.

Vorgehensweise


- **XClarity Orchestrator sichern** Gehen Sie wie folgt vor, um mithilfe von Windows Server Backup eine Sicherung von XClarity Orchestrator zu erstellen.
 1. Starten Sie Windows Server Backup und navigieren Sie zu **Lokale Sicherung**.
 2. Klicken Sie im Aktionsfenster auf **Einmal sichern**, um den Einmal sichern-Assistenten zu starten.
 3. Klicken Sie auf der Seite mit den Sicherungsoptionen auf **Verschiedene Optionen** und anschließend auf **Weiter**.
 4. Klicken Sie auf der Seite „Sicherungskonfiguration“ auf **Angepasst** und anschließend auf **Weiter**.
 5. Klicken Sie auf der Seite „Elemente für Sicherung auswählen“ auf **Elemente hinzufügen**, um das Fenster „Elemente auswählen“ anzuzeigen.
 6. Erweitern Sie das Element „Hyper-V“, klicken Sie auf die virtuelle XClarity Orchestrator-Maschine und anschließend auf **OK**.
 7. Klicken Sie zum Fortfahren auf **Weiter**.
 8. Wählen Sie auf der Seite „Zieltyp angeben“ den Speichertyp für die Sicherung (entweder ein lokales Laufwerk oder ein entfernter gemeinsam genutzter Ordner) und klicken Sie auf **Weiter**.
 9. Geben Sie auf der Seite „Sicherungsziel auswählen“ oder „Fernordner angeben“ die Position an, in der Sie die Sicherung speichern möchten, und klicken Sie auf **Weiter**.
 10. Klicken Sie auf **Sicherung**, um den Sicherungsprozess zu starten.
- **XClarity Orchestrator wiederherstellen** Gehen Sie wie folgt vor, um XClarity Orchestrator mithilfe der im vorherigen Schritt erstellten Sicherung wiederherzustellen.
 1. Starten Sie Windows Server Backup und navigieren Sie zu **Lokale Sicherung**.
 2. Klicken Sie im Aktionsfenster auf **Wiederherstellen**, um den Wiederherstellungsassistenten zu starten.
 3. Geben Sie auf der Seite „Erste Schritte“ die Position an, an der die Sicherung gespeichert ist, und klicken Sie auf **Weiter**.
 4. Wählen Sie auf der Seite „Sicherungsdatum auswählen“ die Sicherung, die Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.
 5. Wählen Sie auf der Seite „Wiederherstellungstyp auswählen“ die Option **Hyper-V** aus und klicken Sie auf **Weiter**.
 6. Erweitern Sie auf der Seite „Wiederherzustellende Elemente auswählen“ das Element „Hyper-V“ und wählen Sie die XClarity Orchestrator-VM aus. Klicken Sie anschließend auf **Weiter**.
 7. Wählen Sie auf der Seite „Wiederherstellungsoptionen angeben“, dass die VM in ihrer ursprünglichen Position wiederhergestellt werden soll, und klicken Sie anschließend auf **Weiter**.
 8. Klicken Sie auf der Bestätigungsseite auf **Wiederherstellen**. Die virtuelle Maschine wird in Hyper-V wiederhergestellt und registriert.
 9. Starten Sie XClarity Orchestrator über Hyper-V-Manager neu.

Kapitel 3. Ressourcen und Aktivitäten überwachen

Sie können Lenovo XClarity Orchestrator verwenden, um Ressourcenbestände, Firmware- und Konfigurationskonformität, den Integritätsstatus und den Ereignisverlauf Ihrer verwalteten Einheiten zu überwachen.

Übersicht über Ihre Umgebung anzeigen

Das Dashboard ist der Hub von Lenovo XClarity Orchestrator, der Ihnen den Zugriff auf Informationen bietet, die für Sie von Bedeutung sind. Er enthält Berichtskarten, die jeweils den Status von Ressourcen und Aktivitäten in Ihrer Umgebung zusammenfassen, einschließlich Einheitenzustand, Konformität und Alerts.

Klicken Sie für den Zugriff auf das Dashboard auf **Dashboard**  in der Menüleiste von XClarity Orchestrator.

Sie können den Umfang der Zusammenfassung nur auf Einheiten ändern, die von einem bestimmten Ressourcenmanager oder in einer bestimmten Ressourcengruppe verwaltet werden, indem Sie das Dropdown-Menü **Manager auswählen** verwenden.

Sie können auf eine der verknüpften Statistiken im Dashboard klicken, um eine gefilterte Liste der Daten anzuzeigen, die den Kriterien entsprechen.

Garantie

Die Übersicht Garantie enthält eine Zusammenfassung des Garantiezeitraums für verwaltete Einheiten, einschließlich der folgenden Daten.

- Anzahl der Einheiten, für die die Garantie abgelaufen ist
- Anzahl der Einheiten mit aktiver Garantie
- Anzahl der Einheiten, für die keine Garantiedaten verfügbar sind

Service-Tickets

Die Übersicht Service-Tickets enthält eine Zusammenfassung der Service-Tickets, einschließlich der folgenden Daten.

- Gesamtzahl der aktiven Service-Tickets
- Anzahl der offenen Service-Tickets
- Anzahl der Service-Tickets in Bearbeitung
- Anzahl der Service-Tickets in der Warteschleife
- Anzahl der geschlossenen Service-Tickets
- Anzahl der Service-Tickets in anderen Zuständen

Firmwarekonformität

Die Übersicht Firmware-Konformität fasst die Einhaltung der Firmwarekonformitätsrichtlinie, die verwalteten Einheiten in XClarity Orchestrator zugewiesen ist, zusammen und enthält die folgenden Daten.

- Anzahl der *nicht* konformen Einheiten
- Anzahl der konformen Einheiten
- Anzahl der Einheiten, denen *keine* Firmwarekonformitätsrichtlinie zugeordnet ist.
- Anzahl der Einheiten, für die keine Konformität unterstützt wird.
- Anzahl der Einheiten, für die die Konformität mit der zugeordneten Richtlinie überprüft wird

Anmerkung: Diese Daten stellen die Firmwarekonformität für alle Einheiten dar, die auf Richtlinien basieren, die von XClarity Orchestrator zugewiesen werden. Sie stellen keine Richtlinien dar, die von Lenovo XClarity Administrator-Ressourcenmanagern zugewiesen werden.

Konfigurationskonformität

Die Übersicht Konfigurationskonformität fasst die Einhaltung der Serverkonfigurationsmuster auf verwalteten Einheiten zusammen und enthält die folgenden Daten.

- Anzahl der Einheiten, die *nicht* mit ihrem zugewiesenen Muster kompatibel sind
- Anzahl der Einheiten, die mit ihrem zugewiesenen Muster kompatibel sind
- Anzahl der Einheiten, denen *kein* Muster zugewiesen ist
- Anzahl der Einheiten, bei denen gerade eine Prüfung der Konfigurationskonformität stattfindet
- Anzahl der Einheiten, für die ein manueller Neustart erforderlich ist, um die Musterbereitstellung abzuschließen (ausstehender Neustart)
- Anzahl der Einheiten, bei denen die letzte Musterimplementierung fehlgeschlagen ist

Anmerkung: Diese Daten stellen die Konformität der Serverkonfiguration für alle Einheiten dar, die auf Mustern basieren, die von XClarity Orchestrator zugeordnet werden. Sie stellen keine Muster dar, die von verwalteten XClarity Administrator Ressourcenmanagern zugeordnet werden.

Sicherheitskorrekturen

Die Übersicht Sicherheitskorrekturen fasst die Anzahl der verwalteten Einheiten mit allgemeinen Sicherheitsrisiken und -lücken (CVEs) zusammen, für die eine Sicherheitskorrektur verfügbar ist, sortiert nach dem höchsten CVE-Schweregrad.

- Anzahl der Einheiten, die mindestens kritische Sicherheitsrisiken aufweisen
- Anzahl der Einheiten, die mindestens ein hohes, mittleres oder niedriges Sicherheitsrisiko, aber keine kritischen Sicherheitsrisiken aufweisen
- Anzahl der Einheiten, die keine bekannten Sicherheitsrisiken aufweisen und geschützt sind

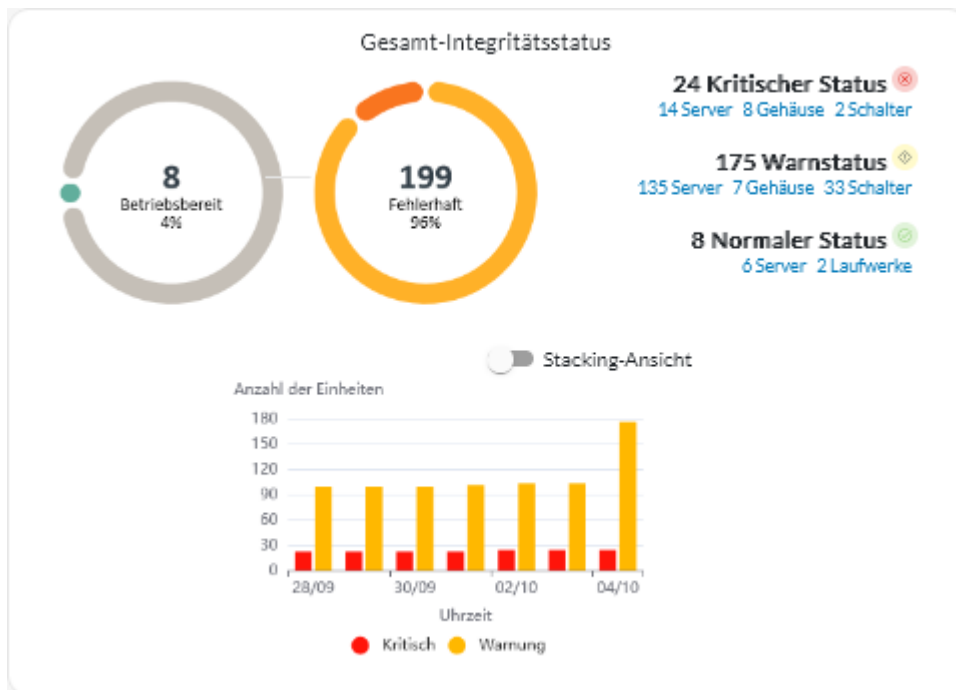
Firmwarealter

Auf der Karte Firmwarealter ist das Alter der Firmware für jeden Komponententyp zusammengefasst.

- Anzahl der Firmware, die für jeden Komponententyp älter als 2 Jahre ist
- Anzahl der Firmware, die für jeden Komponententyp zwischen 1 und 2 Jahre alt ist
- Anzahl der Firmware, die für jeden Komponententyp zwischen 6 Monaten und 1 Jahr alt ist
- Anzahl der Firmware, die für jeden Komponententyp jünger als 6 Monate ist

Gesamt-Integritätsstatus

In der Übersicht Gesamt-Integritätsstatus werden die verwalteten Einheiten zusammengefasst, die derzeit in Ihrer Umgebung fehlerfrei bzw. fehlerhaft sind.



Es werden u. a. die folgenden Informationen angezeigt.

- Ein Kreisdiagramm, das den Prozentsatz der Einheiten zeigt, die einen fehlerfreien Status (normal) und einen fehlerhaften Status („Kritisch“, „Warnung“ und „Unbekannt“) haben

Tipp: Jeder farbige Balken im Kreisdiagramm zeigt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten.

- Gesamtzahl und Prozentsatz der fehlerfreien und fehlerhaften Einheiten
- Anzahl der Einheiten jedes Typs, die derzeit den Status „Kritisch“, „Warnung“, „Normal“ und „Unbekannt“ haben

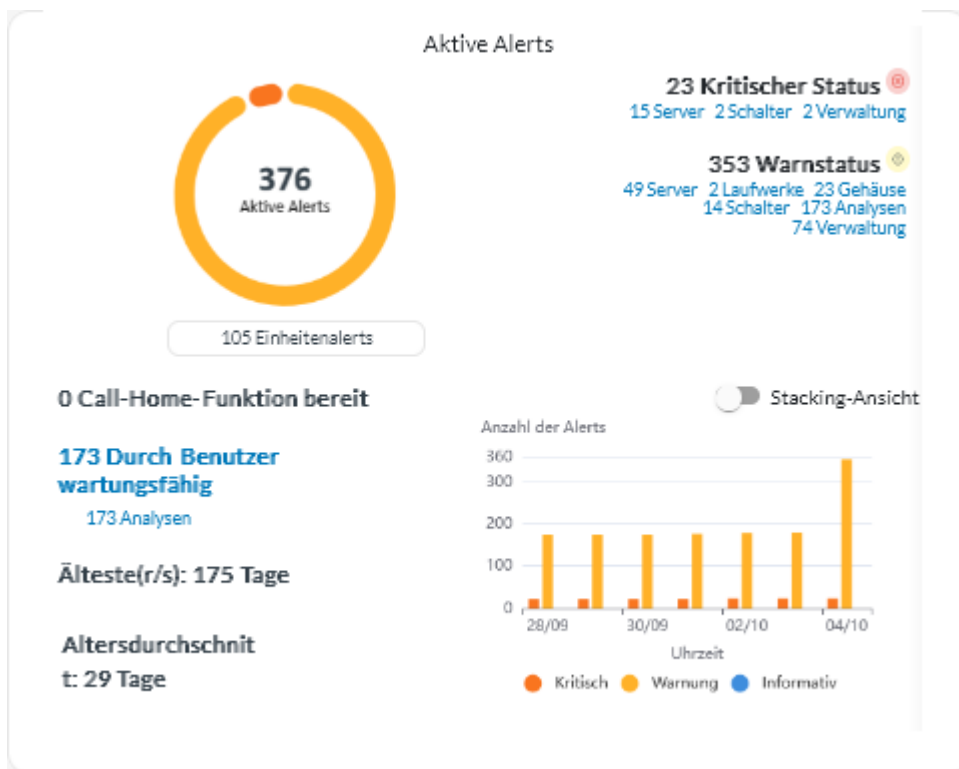
Tipp: Sie können auf die Anzahl der Einheiten mit einem bestimmten Status klicken, um eine Seite mit einer gefilterten Liste der Einheiten zu öffnen, die den Kriterien entsprechen.

- Ein Liniendiagramm, das die Anzahl der Einheiten mit fehlerhaftem Status im Laufe der Zeit zeigt

Tipp: Jeder farbige Balken im Balkendiagramm zeigt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten.

Aktive Alerts

Die Übersicht Aktive Alerts für Einheiten enthält eine Zusammenfassung der aktiven Alerts, die von den verwalteten Einheiten ausgelöst wurden.



Es werden u. a. die folgenden Informationen angezeigt.

- Ein Kreisdiagramm, das den Prozentprozent der aktiven Alerts für jeden Schweregrad („Kritisch“, „Warnung“, „Information“ und „Unbekannt“) zeigt

Tipp: Jeder farbige Balken im Kreisdiagramm zeigt die Anzahl der Alerts mit einem bestimmten Schweregrad an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Schweregrad zu erhalten.

- Gesamtzahl der aktiven Alerts
- Anzahl der Einheiten, die über aktive Alerts verfügen
- Gesamtzahl der aktiven Alerts für jeden Schweregrad und die Anzahl der Einheiten jedes Typs, die aktive Alerts aufweisen (je Schweregrad)

Tipp: Sie können auf die Anzahl der Einheiten mit einem bestimmten Status klicken, um eine Seite mit einer gefilterten Liste der Einheiten zu öffnen, die den Kriterien entsprechen.

- Ein Liniendiagramm, das die Anzahl der Einheiten mit fehlerhaftem Status im Laufe der Zeit zeigt

Tipp: Jeder farbige Balken im Balkendiagramm zeigt die Anzahl der Alerts mit einem bestimmten Schweregrad an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Schweregrad zu erhalten.

- Anzahl der aktiven Alerts, die ein Service-Ticket beim Lenovo Support-Center geöffnet haben (Call-Home-Funktion)
- Gesamtzahl der aktiven Alerts, die eine Benutzeraktion erfordern (durch Benutzer zu warten) und die Anzahl von Einheiten jedes Typs, die vom Benutzer wartbare Alerts haben
- Alter des ältesten aktiven Alerts
- Durchschnittsalter aller aktiven Alerts

Status und Details von Ressourcenmanagern anzeigen

Sie können den Typ, die Version, den Status und die Verbindungen jedes Ressourcenmanagers anzeigen.

Zu dieser Aufgabe

In der Spalte **Integritätsstatus** wird der allgemeine Zustand eines Ressourcenmanagers angegeben. Die folgenden Integritätsstatus werden verwendet:

- (🟢) Normal
- (🟡) Warnung
- (🔴) Kritisch

Vorgehensweise

Klicken Sie zum Anzeigen von Details zu Ressourcenmanagern in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) → **Ressourcenmanager**, um die Übersicht Ressourcenmanager zu öffnen.

<input type="checkbox"/>	Ressourcenn	Allgemeinzus	Typ	Version	Build	Verbunden	Daten der La	Gruppen
<input type="checkbox"/>	XClarity...	🟢 No...	XClarity...	2.0.0	279	Nicht verfü.	Nicht verfü.	Nicht verfü.
<input type="checkbox"/>	host-10...	🟢 No...	XClarity...	3.6.0	108	16.02.23, 1	<input type="checkbox"/>	Nicht verfü.

Nach dieser Aufgabe

In der Übersicht Ressourcenmanager können Sie die folgenden Aktionen ausführen.

- Sie können einen Ressourcenmanager verbinden, indem Sie auf das Symbol **Verbinden** (⊕) klicken (siehe [Ressourcenmanager verbinden](#)).
- Sie können einen bestimmten Ressourcenmanager trennen und löschen, indem Sie auf das Symbol **Löschen** (🗑️) klicken.

Anmerkung: Wenn XClarity Orchestrator keine Verbindung zum Ressourcenmanager herstellen kann, weil z. B. wenn die Anmeldeinformationen abgelaufen sind oder es Netzwerkprobleme gibt, wählen Sie **Trennen erzwingen** aus.

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).

Wenn der Ressourcenmanager entfernt wird, werden alle von diesem Ressourcenmanager verwalteten Geräte ebenfalls entfernt. Dazu gehören Einheitenbestand, Protokolle, Metrikdaten und analytische Berichte.

- Zeigen Sie eine Statuszusammenfassung aller Ressourcenmanager oder eines bestimmten Ressourcenmanagers an. Klicken Sie dazu auf **Dashboard** (☰) in der Menüleiste von XClarity Orchestrator. Sie können den Bereich mithilfe des Dropdown-Menüs **Manager auswählen** auf einen einzelnen Ressourcenmanager oder eine Ressourcengruppe eingrenzen.

Status von Einheiten anzeigen

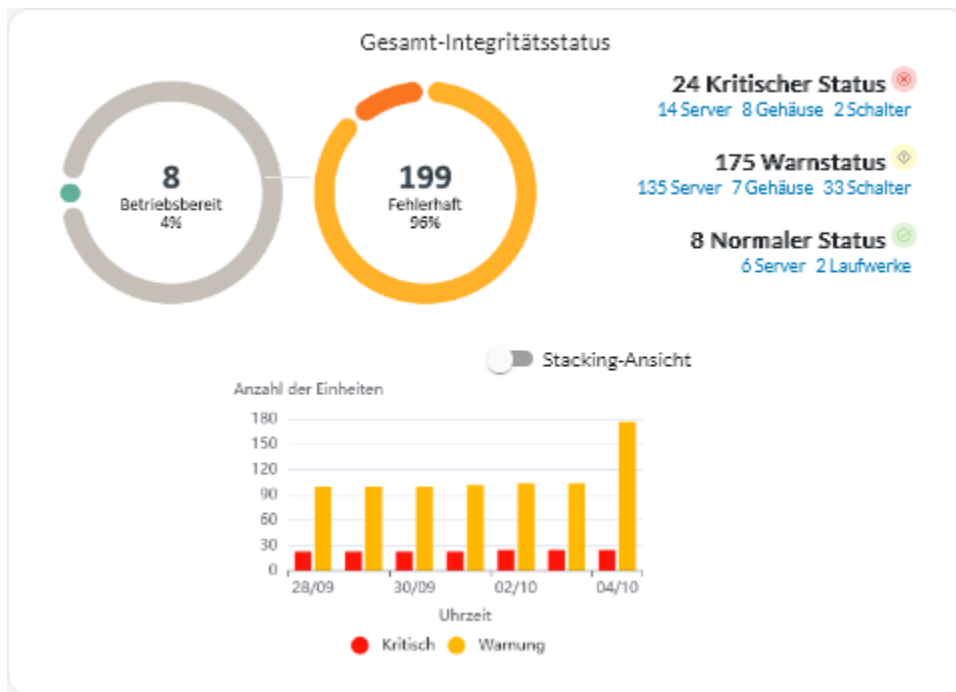
Sie können den Status aller Einheiten anzeigen, die von allen Ressourcenmanagern verwaltet werden.

Vorgehensweise

Gehen Sie wie folgt vor, um den Status der verwalteten Einheiten anzuzeigen.

- **Statusübersicht aller Einheiten** Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Dashboard** (☰), um die Dashboard-Karten wird mit einer Übersicht und dem Status aller verwalteten Einheiten und anderen Ressourcen anzuzeigen (siehe [Übersicht über Ihre Umgebung anzeigen](#)).

Sie können den Umfang der Zusammenfassung nur auf Einheiten ändern, die von einem bestimmten Ressourcenmanager oder in einer bestimmten Ressourcengruppe verwaltet werden, indem Sie das Dropdown-Menü **Manager auswählen** verwenden.

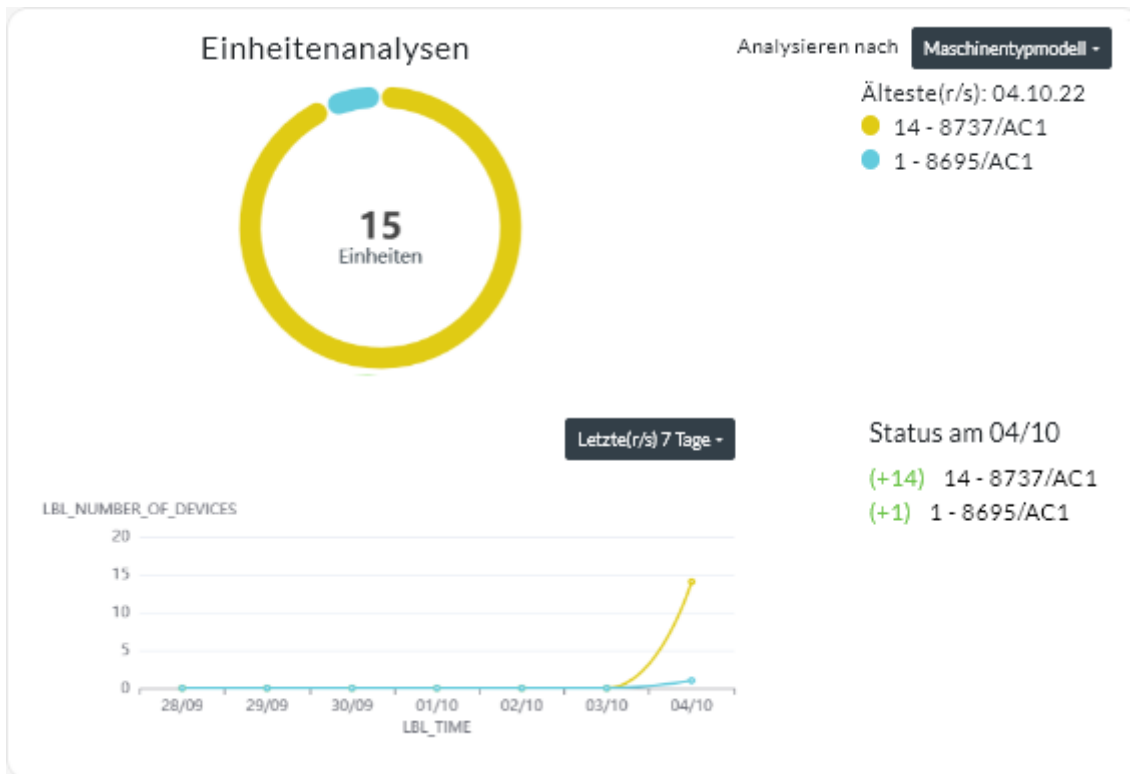


Jeder farbige Balken in den Kreis- und Balkendiagrammen zeigt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten. Sie können auch auf die Anzahl der Einheiten in jedem Status klicken, um eine Liste aller Einheiten anzuzeigen, die den Kriterien entsprechen.

- **Status für alle Einheiten eines bestimmten Typs** Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen. Wenn Sie beispielsweise **Server** auswählen, wird eine Liste aller Rack-, Tower- und Density-Server sowie aller Flex System- und ThinkSystem-Server in einem Gehäuse angezeigt.

Sie können den Umfang der Zusammenfassung basierend auf der Eigenschaft der Einheit in der Dropdown-Liste **Analysieren nach** ändern.

- **Maschinentypmodell.** (Standardeinstellung) In diesem Bericht wird der Zustand der Einheit nach Maschinentypmodell (MTM) zusammengefasst.
- **Maschinentyp.** In diesem Bericht wird der Zustand der Einheit nach Maschinentyp zusammengefasst.
- **Produktname.** In diesem Bericht wird der Zustand der Einheit nach Produkt zusammengefasst.



XClarity Orchestrator fasst den Zustand der Einheit basierend auf bestimmten Kriterien zusammen. Jede Zusammenfassung enthält die folgenden Informationen:

- Ein Kreisdiagramm, das die Gesamtzahl der fehlerhaften Einheiten sowie den Prozentsatz der Einheiten in jedem fehlerhaften Zustand anzeigt („Kritisch“, „Warnung“ und „Unbekannt“).

Jeder farbige Balken im Kreisdiagramm gibt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten.

- Ein Liniendiagramm, das die Anzahl der Einheiten in jedem Integritätsstatus pro Tag über die angegebene Anzahl an Tagen zeigt.

Jeder farbige Balken im Liniendiagramm gibt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten.

- Die Anzahl der Einheiten jedes Typs, die an einem bestimmten Tag fehlerhaft sind. Der aktuelle Tag wird standardmäßig angezeigt. Sie können den Tag ändern, indem Sie den Mauszeiger über jeden Tag im Liniendiagramm bewegen.

- **Status für eine bestimmte Einheit** Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen. Wenn Sie beispielsweise **Server** auswählen, wird eine Liste aller Rack-,

Tower- und Density-Server sowie aller Flex System- und ThinkSystem-Server in einem Gehäuse angezeigt.

Server

Suchen

Fernsteuerung starten
 Stromversorgungsaktionen

 Alle Aktionen
 Filter

<input type="checkbox"/>	Server	Status	Konnekti	Energie	IP-Adres	Produkt	Typ/Mod	Systemfi	Empfehl	Gruppen
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Nich...	Nicht\
<input type="checkbox"/>	ite-b...				10.24:	Leno...	716...	CGE1:	Nich...	Nicht\
<input type="checkbox"/>	Blac...				10.24:	Leno...	716...	A3EG:	Nich...	Nicht\
<input type="checkbox"/>	nod...				10.24:	IBM...	791...	Nicht\	Nich...	Nicht\
<input type="checkbox"/>	Cara...				10.24:	Eagl...	791...	Nicht\	Nich...	Nicht\
<input type="checkbox"/>	blad...				10.24:	IBM...	790...	Nicht\	Nich...	Nicht\
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Nich...	Nicht\
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Nich...	Nicht\
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Nich...	Nicht\
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Nich...	Nicht\

0 ausgewählt / 60 gesamt Zeilen pro Seite: 10

In der Spalte **Status** wird der allgemeine Zustand einer Einheit angegeben. Die folgenden Integritätsstatus werden verwendet: Wenn sich eine Einheit in einem fehlerhaften Zustand befindet, nehmen Sie das Alertprotokoll zu Hilfe, um die Probleme zu identifizieren und zu beheben (siehe [Aktive Alerts überwachen](#)).

- Normal
- Warnung
- Kritisch

In der Spalte **Verbindung** wird der Verbindungsstatus zwischen dem Gerät und XClarity Orchestrator angegeben. Es werden die folgenden Verbindungsstatus verwendet.

- Offline
- Offline verwaltet
- Online
- Teilweise
- Ausstehend

In der Spalte **Strom** wird der Stromversorgungsstatus angezeigt. Die folgenden Stromversorgungsstatus werden verwendet:

- Ein

– (⬇️) Aus

In der Spalte **Empfehlung** sehen Sie die Anzahl der Onlinehinweise für Kunden (technische Tipps), die sich auf die einzelnen Server beziehen. Klicken Sie auf die Zahl, um die Übersicht Empfehlung auf der Seite „Einheitendetails“ anzuzeigen. Diese Übersicht enthält eine Liste der Onlinehinweise für Kunden, einschließlich einer Zusammenfassung und eines Links für jede Empfehlung. Klicken Sie auf einen Link, um eine Webseite mit Details zu dieser Empfehlung zu öffnen.

Nach dieser Aufgabe

Über die Einheitenübersichten können Sie die folgende Aktion ausführen.

- Fügen Sie eine ausgewählte Einheit zu einer Gruppe hinzu, indem Sie auf **Alle Aktionen → Elemente zur Gruppe hinzufügen** klicken.
- Leiten Sie Berichte über bestimmte Einheitentypen regelmäßig an eine oder mehrere E-Mail-Adressen weiter, indem Sie auf das Symbol **Berichtsweiterleiter erstellen** (⊕) klicken. Der Bericht wird mithilfe der Datenfilter gesendet, die derzeit auf die Tabelle angewendet werden. Alle ein- und ausgeblendeten Tabellenspalten werden in den Bericht einbezogen. Siehe [Berichte weiterleiten](#) für weitere Informationen.
- Fügen Sie einem bestimmten Berichtsweiterleiter einen Bericht über einen bestimmten Einheitentyp hinzu, indem Sie die Datenfilter verwenden, die derzeit auf die Tabelle angewendet werden. Klicken Sie dazu auf das Symbol **Zu Berichtsweiterleiter hinzufügen** (↗️). Wenn der Berichtsweiterleiter bereits einen Bericht über diesen Einheitentyp enthält, wird der Bericht so aktualisiert, dass die aktuellen Datenfilter angewendet werden.

Einheitendetails anzeigen

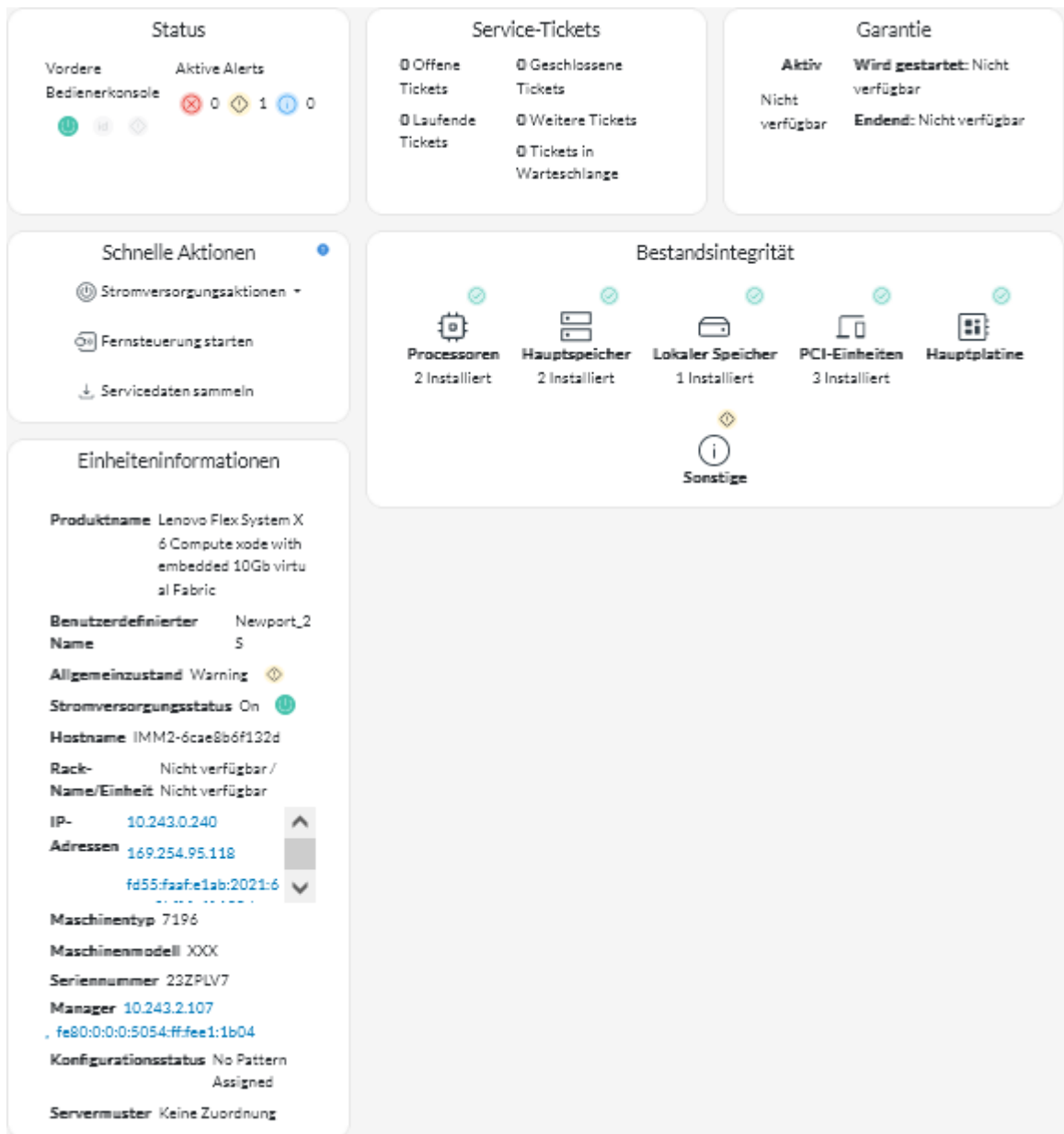
Sie können ausführliche Informationen zu jeder Einheit anzeigen, darunter eine Gesamtübersicht über den Zustand und den Status von Einheiten, den Bestand, Alerts und Ereignisse, Systemmetriken und Firmware.

Vorgehensweise

Gehen Sie wie folgt vor, um die Details für eine Einheit anzuzeigen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.

Schritt 2. Klicken Sie auf die Zeile für die Einheit, um die Übersichten für diese Einheit anzuzeigen.








Schritt 3. Führen Sie eine oder mehrere der folgenden Aktionen aus:

Die Details auf den einzelnen Übersichten können je nach Einheitentyp unterschiedlich sein.

- Klicken Sie auf **Zusammenfassung**, um eine Gesamtübersicht der Einheit anzuzeigen, einschließlich Informationen zu Einheit, Bestand, Zustand, BS-Informationen, Systemmetriken, Service-Tickets und Garantie. Diese Seite enthält außerdem die Übersicht **Schnelle Aktionen**, auf der Aktionen aufgeführt sind, die Sie auf der Einheit ausführen können (z. B. Stromversorgungsaktionen ausführen, Servicedaten sammeln und eine Fernsteuerungssitzung starten). Auf dieser Seite wird der Status der einzelnen Anzeigen auf der vorderen Bedienerkonsole angezeigt.

– **Betriebsanzeige**

- **Ein** (🔌). Die Einheit ist eingeschaltet.
- **Aus** (🔌). Die Einheit ist ausgeschaltet.

- **Positionsanzeige**
 - **Ein** (). Die Positionsanzeige an der Systemsteuerung leuchtet.
 - **Blinkt** (). Die Positionsanzeige an der Systemsteuerung leuchtet oder blinkt.
 - **Aus** (). Die Positionsanzeige an der Systemsteuerung leuchtet nicht.
- **Fehleranzeige**
 - **Ein** (). Die Fehleranzeige an der Systemsteuerung leuchtet.
 - **Aus** (). Die Fehleranzeige an der Systemsteuerung leuchtet nicht.
- Klicken Sie auf **Bestand**, um Details zu Hardwarekomponenten in der Einheit anzuzeigen (z. B. Prozessoren, Speichermodule, Laufwerke, Netzteile, Lüfter, PCI-Einheiten und Systemplatine).

Anmerkungen:

- Bestand wird *nicht* für diese Speichereinheiten unterstützt: ThinkSystem DS2200, Lenovo Storage S2200 und S3200 und Flex System V7000 Speicherknoten.
- Firmwaredetails stehen *nicht* für diese Speichereinheiten zur Verfügung: ThinkSystem DS4200 und DS6200 und Lenovo Storage DX8200C, DX8200D und DX8200N.
- Klicken Sie auf **Alertprotokoll**, um die Liste der aktiven Alerts und Alert-Statistiken für die Einheit anzuzeigen (siehe [Aktive Alerts überwachen](#)).
- Klicken Sie auf **Ereignisprotokoll**, um die Liste der Ereignisse für diese Einheit anzuzeigen (siehe [Überwachen von Ereignissen](#)).
- Klicken Sie auf **Firmware**, um eine Liste der aktuellen Firmwareversionen für Einheiten und Einheitenkomponenten anzuzeigen.
- Klicken Sie auf **Service**, um Informationen zu Servicedatenarchiven und Service-Tickets für die Einheit anzuzeigen.
- Klicken Sie auf **Auslastung**, um die Metriken zu Systemauslastung, Temperatur und Stromversorgung im Laufe der Zeit für ThinkAgile und ThinkSystem Einheiten aufzurufen.
- Klicken Sie auf **Empfehlung**, um eine Liste der Onlinehinweise für Kunden anzuzeigen, einschließlich einer Zusammenfassung und eines Link für jede Empfehlung. Klicken Sie auf einen Link, um eine Webseite mit Details zu dieser Empfehlung zu öffnen.

Nach dieser Aufgabe

Außer der Anzeige von Übersichts- und Detailinformationen zu einer Einheit können Sie über diese Seite die folgenden Aktionen auf einer Einheit durchführen:

- Starten Sie die Webschnittstelle für Baseboard Management Controller über die Registerkarte **Zusammenfassung**, indem Sie auf die hauptsächliche IP-Adresse für dieses Gerät klicken.
- Starten Sie die Webschnittstelle für die Einheit über die Registerkarte **Zusammenfassung**, indem Sie auf die IP-Adresse klicken.
- Starten Sie die Webschnittstelle für den Ressourcenmanager, der die Einheit verwaltet, über die Registerkarte **Zusammenfassung**, indem Sie auf Name oder IP-Adresse des Ressourcenmanagers klicken.

Status und Details zu Infrastrukturressourcen anzeigen

Sie können den Status sowie ausführliche Informationen zu Ressourcen der Rechenzentrumsinfrastruktur (z. B. PDUs und USVs) aufrufen, die über einen Schneider Electric EcoStruxure IT Expert Ressourcenmanager verwaltet werden.

Vorbereitende Schritte

In der Spalte **Status** wird der allgemeine Zustand einer Infrastrukturressource angegeben. Die folgenden Integritätsstatus werden verwendet: Wenn sich Infrastrukturressourcen in einem fehlerhaften Zustand befinden, nehmen Sie das Alertprotokoll zu Hilfe, um die Probleme zu identifizieren und zu beheben (siehe [Aktive Alerts überwachen](#)).


- (🟢) Normal
- (🟡) Warnung
- (🔴) Kritisch

Vorgehensweise

- **Status für eine bestimmte Infrastrukturressource** Klicken Sie zum Anzeigen des Status von Infrastrukturressourcen in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) → **Infrastruktur**, um die Übersicht Infrastruktur zu öffnen. Wenn sich eine Infrastrukturressource in einem fehlerhaften Zustand befindet, nehmen Sie das Alertprotokoll zu Hilfe, um die Probleme zu identifizieren und zu beheben (siehe [Aktive Alerts überwachen](#)).

Name	Status	Hostname	Hersteller	Modell	Typ	Gruppen
APC_R18	Normal	APC_R18	Server Tech...	Sentry Swit...	Rack PDU	Yacheng Test
APC_R19	Normal	APC_R19	Server Tech...	Sentry Swit...	Rack PDU	Nicht verfügbar
EcoStruxur...	Normal	Nicht verfü...	Schneider ...	EcoStruxur...	Gateway	Nicht verfügbar
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	bangalore-grj
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	DemoGroup
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	Romania-PDI
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	Test Group
Sentry3_53...	Normal	Sentry3_53...	Server Tech...	Sentry Swit...	Rack PDU	New Group
UPSR11	Kritisch	UPSR11	MGE	9135 6000	UPS	Yacheng Test

- **Details einer bestimmten Infrastrukturressource**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) → **Infrastruktur**, um die Übersicht „Infrastruktur“ anzuzeigen.
 2. Klicken Sie auf die Zeile der Infrastrukturressource, um die Zusammenfassung für diese Ressource anzuzeigen.
 3. Führen Sie eine oder mehrere der folgenden Aktionen aus:
 - Klicken Sie auf **Zusammenfassung**, um eine Gesamtübersicht über die Ressource anzuzeigen, einschließlich Informationen zur Einheit sowie Status.

- Klicken Sie auf **Alertprotokoll**, um die Liste der aktiven Alerts und Alert-Statistiken für die Ressource anzuzeigen (siehe [Aktive Alerts überwachen](#)).
- Klicken Sie auf **Ereignisprotokoll**, um die Liste der Ereignisse für diese Ressource anzuzeigen (siehe [Überwachen von Ereignissen](#)).
- Klicken Sie auf **Sensoren**, um die Liste der Sensoren in der Ressource anzuzeigen. Sie können die letzten Messwerte des Sensor in der Übersicht „Sensor“ ermitteln oder einen oder mehrere Sensoren auswählen und dann auf das Symbol **Diagramm** () klicken, um die Liniendiagramme im Laufe der Zeit für jeden ausgewählten Sensor anzuzeigen. Sensoren mit derselben Einheit (z. B. Watt oder Ampere) werden im selben Diagramm dargestellt.

Anmerkung: Schneider Electric EcoStruxure IT Expert erfasst alle 5 Minuten Sensordaten und XClarity Orchestrator synchronisiert diese Daten einmal stündlich. Aktuell speichert XClarity Orchestrator nur die letzten 60 Minuten an Daten.

Nach dieser Aufgabe

Außer der Anzeige von Zusammenfassungs- und ausführlichen Informationen zu einer Infrastrukturressource können Sie über diese Seite die folgenden Aktionen durchführen.

- Starten der Webschnittstelle für bestimmte Infrastrukturressourcen über die Registerkarte **Zusammenfassung**, indem Sie auf die IP-Adresse für die Ressource klicken.

Jobs überwachen

Jobs sind Aufgaben mit langer Laufzeit, die im Hintergrund ausgeführt werden. Sie können ein Protokoll aller Jobs anzeigen, die von Lenovo XClarity Orchestrator gestartet wurden.

Zu dieser Aufgabe



Wenn eine Aufgabe mit langer Laufzeit auf mehrere Ressourcen abzielt, wird für jede Ressource ein separater Job erstellt.

Sie können Status und Details zu jedem Job im Jobprotokoll anzeigen. Das Jobprotokoll kann maximal 500 Jobs oder 1 GB enthalten. Wenn die maximale Größe erreicht ist, werden die ältesten Jobs, die erfolgreich abgeschlossen wurden, gelöscht. Wenn es keine Jobs gibt, die erfolgreich im Protokoll abgeschlossen wurden, werden die ältesten Jobs, die mit Warnungen abgeschlossen wurden, gelöscht. Wenn es keine Jobs gibt, die erfolgreich oder mit Warnungen im Protokoll abgeschlossen wurden, werden die ältesten Jobs, die mit Fehlern abgeschlossen wurden, gelöscht.

Anmerkung: Jobs, die länger als 24 Stunden ausgeführt werden, werden gestoppt und erhalten den Status „Abgelaufen“.

Vorgehensweise

Führen Sie einen oder mehrere der folgenden Schritte aus, um Jobs anzuzeigen.

- **Geplante Jobs anzeigen** Navigieren Sie in der Menüleiste von XClarity Orchestrator zu **Überwachung** () → **Jobs** und klicken Sie anschließend auf die Registerkarte **Geplante Jobs**, um die Übersicht Geplante Jobs anzuzeigen. Diese Übersicht listet Informationen zu jedem geplanten Job auf, darunter Status, Zeitstempel für die geplante Ausführung des Jobs und Zeitstempel für den Start des Jobs.
- **Job anzeigen** Klicken Sie auf **Überwachung** () → **Jobs**, um in der Menüleiste von XClarity Orchestrator die Übersicht Jobs aufzurufen. Es werden Informationen zu den einzelnen Jobs angezeigt, einschließlich Status, Fortschritt, Start- und Endzeit sowie Zielressource.

Jobs

Jobs sind länger laufende Tasks, die für mindestens ein Zielsystem ausgeführt werden. Sie können einen Job löschen oder seine Details anzeigen.

Alle Aktionen ▾ Filter ▾ Suchen

Jobname	Status	Fortschritt	Startzeit	Abschlusszeit	Ziel	Kategorie	Erstellt von
<input type="radio"/> Richtlinie	✓ Abge	100%	05.10.2021	05.10.2021	Nicht v...	Aktuali...	Orches...
<input type="radio"/> Richtlinie	✓ Abge	100%	05.10.2021	05.10.2021	Nicht v...	Aktuali...	Orches...
<input type="radio"/> Richtlinie	✓ Abge	100%	05.10.2021	05.10.2021	Nicht v...	Aktuali...	Orches...
<input type="radio"/> Richtlinie	✓ Abge	100%	05.10.2021	05.10.2021	Nicht v...	Aktuali...	Orches...
<input type="radio"/> Richtlinie	✓ Abge	100%	05.10.2021	05.10.2021	Nicht v...	Aktuali...	Orches...
<input type="radio"/> Serviceda	✗ Abge	100%	05.10.2021	05.10.2021	SN#Y0...	Service	Orches...
<input type="radio"/> Serviceda	✗ Abge	100%	04.10.2021	04.10.2021	SN#Y0...	Service	Orches...
<input type="radio"/> Serviceda	✗ Abge	100%	04.10.2021	04.10.2021	SN#Y0...	Service	Orches...
<input type="radio"/> Serviceda	✗ Abge	100%	04.10.2021	04.10.2021	SN#Y0...	Service	Orches...
<input type="radio"/> Mehrere I	✓ Abge	100%	04.10.2021	04.10.2021	XClarit...	Aktuali...	Orches...

0 Ausgewählt / 15 Gesamt Zeilen pro Seite: 10 ▾ ◀ 1 2 ▶

Um detaillierte Informationen zu einem Job anzuzeigen, klicken Sie in der Tabelle auf die Zeile für den Job. Es werden Übersichten angezeigt, die Informationen zu jeder Unteraufgabe im Job enthalten (z. B. Status, Fortschritt, Start- und Endzeit, Zieleinheiten und Jobprotokoll).

Manager 10.243.10.122 verbinden

Alle Aktionen ▾ Filter ▾ Suchen

Jobname	Status	Fortschritt	Startzeit	Abschlusszeit	Ziel
▼ Manager 10.2	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar
SSL-Zertif	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar
Verbindung	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar
Authentifiz	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar
Duplikatür	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar
> Konfigurati	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar
Konfigurati	ⓘ Abgeschlossen	100%	04.10.2022, 09:2	04.10.2022, 09:2	Nicht verfügbar

7 Gesamt Zeilen pro Seite: 10 ▾

Nach dieser Aufgabe

In der Übersicht „Jobs“ können Sie die folgenden Aktionen ausführen:

- Einen *abgeschlossenen* oder *abgelaufenen* Job oder eine abgeschlossene/abgelaufene Unteraufgabe aus dem Jobprotokoll löschen, indem Sie Job oder Unteraufgabe auswählen und auf das Symbol **Löschen** (🗑️) klicken.

Aktive Alerts überwachen

Alerts sind Hardware- oder Orchestrator-Ereignisse, die eine Überprüfung und Benutzeraktion erfordern. Lenovo XClarity Orchestrator ruft die Ressourcenmanager asynchron ab und zeigt Alerts an, die von diesen Ressourcenmanagern empfangen wurden.

Zu dieser Aufgabe

Es gibt keine Begrenzung für die Anzahl der aktiven Alerts, die im lokalen Repository gespeichert sind.

Über die Übersicht „Alerts“ können Sie eine Liste aller aktiven Alerts anzeigen.

Datum und	Dringlichkeit	Alert	Ressource	Wartbarkeit	Ressourcen	Qualitätstyp	Gruppen
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Gehäuse	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Gehäuse	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert
05.10.2...	W...	Die Verbi	XClarit...	Kei...	Schalter	Verwalt...	Nicht vert

Die Spalte **Wertigkeit** gibt den Schweregrad des Alerts an. Die folgenden Wertigkeiten werden verwendet:

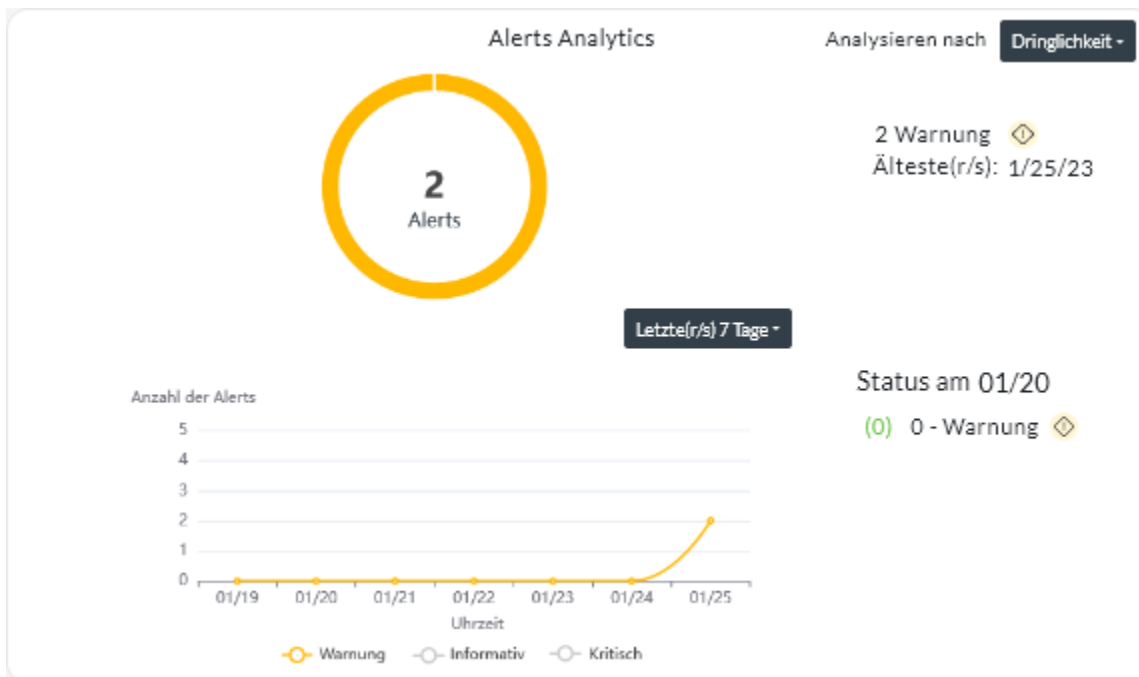
- (i) **Information**. Es ist keine Aktion erforderlich.
- (⚠️) **Warnung**. Die Aktion kann verzögert werden oder es ist keine Aktion erforderlich.

- (⊗) **Kritisch**. Es ist eine sofortige Maßnahme erforderlich.

Die Spalte **Wartbarkeit** gibt an, ob die Einheit gewartet werden muss und wer diese Service normalerweise durchführt. Die folgenden Wartbarkeitstypen werden verwendet:

- **Keine Angabe**. Der Alert ist informativ und erfordert keine Aktion.
- (👤) **Benutzer**. Führen Sie die entsprechende Wiederherstellungsaktion durch, um das Problem zu beheben.
- (🔧) **Support**. Wenn die Call-Home-Funktion für XClarity Orchestrator oder für den Ressourcenmanager aktiviert ist, der die zugeordnete Einheit verwaltet, wird der Alert normalerweise an das Lenovo Support-Center gesendet, es sei denn, es existiert bereits ein offenes Service-Ticket für dieselbe Alert-ID für die Einheit (siehe [Service-Tickets mit Call-Home-Funktion automatisch öffnen](#) in der Onlinedokumentation zu XClarity Orchestrator). Wenn die Call-Home-Funktion nicht aktiviert ist, wird empfohlen, manuell ein Service-Ticket zu öffnen, um das Problem zu beheben (siehe [Service-Ticket im Lenovo Unterstützungszentrum manuell öffnen](#) in der Onlinedokumentation zu XClarity Orchestrator).

Wenn aktive Alerts vorhanden sind, werden Alert-Statistiken auf der Karte Alerts Analytics angezeigt. Sie können Alertstatistiken nach Schweregrad, Quelle, Ressource und Wartbarkeit für den aktuellen Tag und über einen bestimmten Zeitraum aufrufen (siehe [Aktive Alerts analysieren](#)).




Vorgehensweise

Führen Sie einen oder mehrere der folgenden Schritte durch, um aktive Alerts anzuzeigen.

- **Alle aktiven Alerts anzeigen** Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📧) → **Alerts**, um die Übersicht Alerts anzuzeigen.

Um Informationen über einen bestimmte Alert anzuzeigen, klicken Sie auf die Beschreibung in der Spalte **Alert**. Ein Dialogfenster mit Informationen zur Quelle der Alerts, Erläuterungen und Wiederherstellungsaktionen wird angezeigt.

- **Aktive Alerts für eine bestimmte Einheit anzeigen**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen**  und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.
2. Klicken Sie auf die Zeile für eine Einheit, um die Übersichtskarten für diese Einheit anzuzeigen.
3. Klicken Sie auf **Alertprotokoll**, um die Liste der aktiven Alerts für die Einheit und die Alerts Analytics-Karte anzuzeigen. Um Informationen über einen bestimmte Alert anzuzeigen, klicken Sie auf die Beschreibung in der Spalte **Alert**. Ein Dialogfenster mit Informationen zur Quelle der Alerts, Erläuterungen und Wiederherstellungsaktionen wird angezeigt.

Überwachen von Ereignissen

Über Lenovo XClarity Orchestrator haben Sie Zugriff auf eine Verlaufsliste aller Ressourcen- und Prüfereignisse.

Weitere Informationen:  [Ereignisse für eine bestimmte Einheit überwachen](#)




Zu dieser Aufgabe

Ein *Ressourcenereignis* identifiziert eine Hardware- oder Orchestrator-Bedingung, die auf einer verwalteten Einheit, einem Ressourcenmanager oder XClarity Orchestrator aufgetreten ist. Sie können diese Ereignisse verwenden, um Probleme im Zusammenhang mit der Hardware oder dem Orchestrator-Server nachzuerfolgen und zu analysieren.



Ein *Prüfereignis* ist eine Aufzeichnung von Benutzeraktivitäten, die über einen Ressourcenmanager oder XClarity Orchestrator durchgeführt wurden. Sie können diese Prüfereignisse verwenden, um authentifizierungsbezogene Probleme nachzuerfolgen und zu analysieren.

Das Ereignisprotokoll enthält sowohl Ressourcen- als auch Prüfereignisse. Sie kann maximal 100.000 Ereignisse aus allen Quellen enthalten. Maximal 50.000 Ereignisse können von einem einzelnen Ressourcenmanager und dessen verwalteten Einheiten stammen. Maximal 1.000 Ereignisse können von einer einzelnen verwalteten Einheit stammen. Wenn die maximale Anzahl an Ereignissen erreicht ist, wird das älteste Ereignis im Protokoll gelöscht, wenn das nächste Ereignis empfangen wird.

Die Spalte **Wertigkeit** gibt den Schweregrad des Ereignisses an. Die folgenden Wertigkeiten werden verwendet:

-  **Information.** Es ist keine Aktion erforderlich.
-  **Warnung.** Die Aktion kann verzögert werden oder es ist keine Aktion erforderlich.
-  **Kritisch.** Es ist eine sofortige Maßnahme erforderlich.

Die Spalte **Wartbarkeit** gibt an, ob die Einheit gewartet werden muss und wer diese Service normalerweise durchführt. Die folgenden Wartbarkeitstypen werden verwendet:

- **Keine Angabe.** Der Alert ist informativ und erfordert keine Aktion.
-  **Benutzer.** Führen Sie die entsprechende Wiederherstellungsaktion durch, um das Problem zu beheben.
-  **Support.** Wenn die Call-Home-Funktion für XClarity Orchestrator oder für den Ressourcenmanager aktiviert ist, der die zugeordnete Einheit verwaltet, wird der Alert normalerweise an das Lenovo Support-Center gesendet, es sei denn, es existiert bereits ein offenes Service-Ticket für dieselbe Alert-ID für die Einheit (siehe [Service-Tickets mit Call-Home-Funktion automatisch öffnen](#) in der Onlinedokumentation zu XClarity Orchestrator). Wenn die Call-Home-Funktion nicht aktiviert ist, wird empfohlen, manuell ein Service-Ticket zu öffnen, um das Problem zu beheben (siehe [Service-Ticket im Lenovo Unterstützungszentrum manuell öffnen](#) in der Onlinedokumentation zu XClarity Orchestrator).

Vorgehensweise

Führen Sie einen oder mehrere der folgenden Schritte aus, um Ereignisse anzuzeigen.

- **Alle Ressourcen- oder Prüfereignisse anzeigen** Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Ereignisse**, um die Übersicht „Ereignisse“ anzuzeigen. Klicken Sie anschließend auf die Registerkarte **Ressourcenereignisse** oder **Prüfereignisse**, um die Protokolleinträge anzuzeigen.

Ereignisse

Das Ereignisprotokoll enthält einen Verlauf der ermittelten Hardware- und Verwaltungsbedingungen (Ressourcenereignisse) und ein Prüfprotokoll der Benutzeraktionen (Prüfereignisse).

Ressourcenereignisse **Prüfereignisse**

🔄 📄 🗑️ → 📄 📄 Alle Aktionen ▾ Filter ▾ ✕

Datum und UI	Dringlichkeit	Ereignis	Ressource	Wartbarkeit	Ressourcen	Gruppen
05.10.22, ...	📘 Informativ	Einheit IOI	IO Module	Kei...	Schalter	Nicht verf.
05.10.22, ...	⚠️ Warnung	Der Integri	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	⚠️ Warnung	Auf der Ein	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	📘 Informativ	Auf der Ein	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	📘 Informativ	Einheit IOI	IO Module	Kei...	Schalter	Nicht verf.
05.10.22, ...	📘 Informativ	Auf der Ein	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	⚠️ Warnung	Der Integri	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	⚠️ Warnung	Auf der Ein	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	📘 Informativ	Auf der Ein	Not Availal	Kei...	Nicht verf.	Nicht verf.
05.10.22, ...	📘 Informativ	Einheit IOI	IO Module	Kei...	Schalter	Nicht verf.

9308 Gesamt Zeilen pro Seite: 10 ▾

⏪ < 1 2 3 4 5 > ⏩

- **Ressourcen- oder Prüfereignisse für eine bestimmte Einheit anzeigen**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (📊) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.
 2. Klicken Sie auf die Zeile für eine Einheit, um die Übersichtskarten für diese Einheit anzuzeigen.
 3. Klicken Sie auf die Registerkarte **Ereignisprotokoll**, um die Seite Ereignisse für dieses Gerät anzuzeigen.

Ereignisse und Alerts ausschließen

Wenn bestimmte Ereignisse und aktive Alerts für Sie nicht relevant sind, können Sie diese Ereignisse und aktiven Alerts auf allen Seiten und Übersichten ausschließen, auf denen Ereignisse und Alerts angezeigt werden. Ausgeschlossene Ereignisse und Alerts werden zwar weiterhin im Protokoll festgehalten, aber auf den Seiten mit Ereignissen und Alerts ausgeblendet, einschließlich Protokollansichten und Ressourcenstatus.

Zu dieser Aufgabe

Ausgeschlossene Ereignisse werden für alle Benutzer ausgeblendet, nicht nur für den Benutzer, der die Konfiguration festgelegt hat.

Wenn Sie ein Ereignis ausschließen, dem ein Alert zugeordnet ist, wird dieser Alert ebenfalls ausgeschlossen.

Vorgehensweise

Gehen Sie wie folgt vor, um Alerts und Ereignisse auszuschließen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Alerts** oder **Überwachung** (📊) → **Ereignisse**, um die Übersicht „Alerts“ oder „Ereignisse“ anzuzeigen.

Schritt 2. Wählen Sie die auszuschließenden Alerts oder Ereignisse aus und klicken Sie auf das Symbol **Ausschließen** (🗑️). Das Dialogfenster „Alerts ausschließen“ oder „Ereignisse ausschließen“ wird angezeigt.

Schritt 3. Wählen Sie eine der folgenden Optionen.

- **Ausgewählte Ereignisse von allen Einheiten ausschließen.** Schließt die ausgewählten Ereignisse von allen verwalteten Einheiten aus.
- **Nur Ereignisse von Einheiten im Bereich der ausgewählten Instanzen ausschließen.** Schließt die ausgewählten Ereignisse von den verwalteten Einheiten aus, auf die sich die ausgewählten Ereignisse beziehen.

Schritt 4. Klicken Sie auf **Speichern**.

Nach dieser Aufgabe

Wenn Sie Ereignisse ausschließen, erstellt XClarity Orchestrator Ausschlussregeln basierend auf den von Ihnen bereitgestellten Angaben.

- Zeigen Sie eine Liste der Ausschlussregeln und ausgeschlossenen Ereignisse und Alerts an. Klicken Sie dazu auf das Symbol **Ausschlüsse anzeigen** (🔍), um das Dialogfenster „Ausgeschlossene Alerts“ oder „Ausgeschlossene Ereignisse“ anzuzeigen. Klicken Sie auf die Registerkarte **Ausschlussregeln**, um die Ausschlussregeln anzuzeigen, oder klicken Sie auf die Registerkarte **Ausgeschlossene Alerts** oder **Ausgeschlossene Ereignisse**, um ausgeschlossene Alerts oder Ereignisse anzuzeigen.

Ausgeschlossene Ereignisse

Verwenden Sie die Schaltfläche "Entfernen", um Ausschlussregeln zu entfernen und ausgeschlossene Ereignisse im Ereignisprotokoll wiederherzustellen.

Ausschlussregeln | **Ausgeschlossene Ereignisse**

🔄 🗑️ 📄 Alle Aktionen ▾ Filter ▾ ✕

Ereignis	System	Ereignis-ID
Power supply Power Supply 04 power meter is offli	Alle betroffenen Systeme	00038504

0 Ausgewählt / 1 Gesamt Zeilen pro Seite: 10 ▾

Schließen

- Stellen Sie Ereignisse wieder her, die aus Protokollen ausgeschlossen wurden, indem Sie die entsprechende Ausschlussregel entfernen. Um eine Ausschlussregel zu entfernen, klicken Sie auf das Symbol **Ausschlüsse anzeigen** (🗖). Das Dialogfenster „Ausgeschlossene Alerts“ oder „Ausgeschlossene Ereignisse“ wird angezeigt. Wählen Sie die wiederherzustellenden Ausschlussregeln aus und klicken Sie auf das Symbol **Löschen** (🗑).

Ereignis-, Bestands- und Metrikdaten weiterleiten

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](#)

Vorgehensweise

Gehen Sie wie folgt vor, um Daten weiterzuleiten.

Schritt 1. Erstellen Sie ein Weiterleiterziel.

Weiterleiterziele sind gemeinsame Konfigurationen, die von mehreren Datenweiterleitern verwendet werden können. Das Weiterleiterziel bestimmt, wohin die Daten für einen bestimmten Weiterleitertyp gesendet werden sollen.

Schritt 2. Erstellen Sie Ereignis- und Ressourcenfilter (nur für Ereignisweiterleiter).

Optional können Sie gemeinsame *Datenweiterleitungsfilter* zu mehreren Datenweiterleitern zuordnen. Diese Filter werden verwendet, um bestimmte Kriterien zu definieren, um zu bestimmen, welche Ereignisse für welche Ressourcen weitergeleitet werden sollen.

Wenn Sie dem Datenweiterleiter keine Filter zuordnen, werden alle Ereignisse für alle Ressourcen an das ausgewählte Weiterleiterziel weitergeleitet.

Schritt 3. Erstellen und aktivieren Sie einen Datenweiterleiter.

Sie können Datenweiterleiter erstellen und aktivieren, damit sie Ereignisdaten an eine bestimmte externen Anwendung weiterleiten. Sie müssen ein Weiterleiterziel auswählen, das dem Typ des zu erstellenden Weiterleiters entspricht.

Filter für die Datenweiterleitung erstellen

Sie können häufige *Filter für die Datenweiterleitung* definieren, die von mehreren Weiterleitern verwendet werden können, um die Weiterleitung von Daten auszulösen, die bestimmte Kriterien erfüllen.

Zu dieser Aufgabe

Sie können die folgenden Arten von Filtern erstellen.

- *Ereignisfilter* leiten Ereignisse weiter, die bestimmten Ereigniscodes oder -eigenschaften entsprechen (z. B. Ereignisklassen, Ereignisschweregrade und Servicetypen).
 - Alle Codes und Eigenschaften gelten für alle Ereignisquellen.
 - Wenn keine Klasseneigenschaften ausgewählt sind, werden alle Klasseneigenschaften abgeglichen.
 - Wenn keine Wartbarkeitseigenschaften ausgewählt sind, werden alle Wartbarkeitseigenschaften abgeglichen.
 - Wenn keine Schweregradeigenschaften ausgewählt sind, werden alle Schweregradeigenschaften abgeglichen.
 - Wenn kein Ereigniscode angegeben ist, werden alle Ereigniscodes abgeglichen.
- *Ressourcenfilter* leiten Daten weiter, die von bestimmten Ressourcen (XClarity Orchestrator, Ressourcenmanagern und Einheiten) generiert werden. Sie können eine Teilmenge der Ressourcen auswählen, indem Sie eine oder mehrere Ressourcengruppen wählen.
 - Wenn ein Ressourcentyp deaktiviert ist, werden keine Daten dieses Ressourcentyps weitergeleitet.
 - Wenn ein Ressourcentyp aktiviert ist, aber keine Gruppen ausgewählt sind, werden alle Daten dieses Ressourcentyps weitergeleitet.
 - Wenn ein Ressourcentyp aktiviert ist und mindestens eine Gruppe ausgewählt ist, werden nur Daten weitergeleitet, die von den Ressourcen in den ausgewählten Gruppen generiert werden.

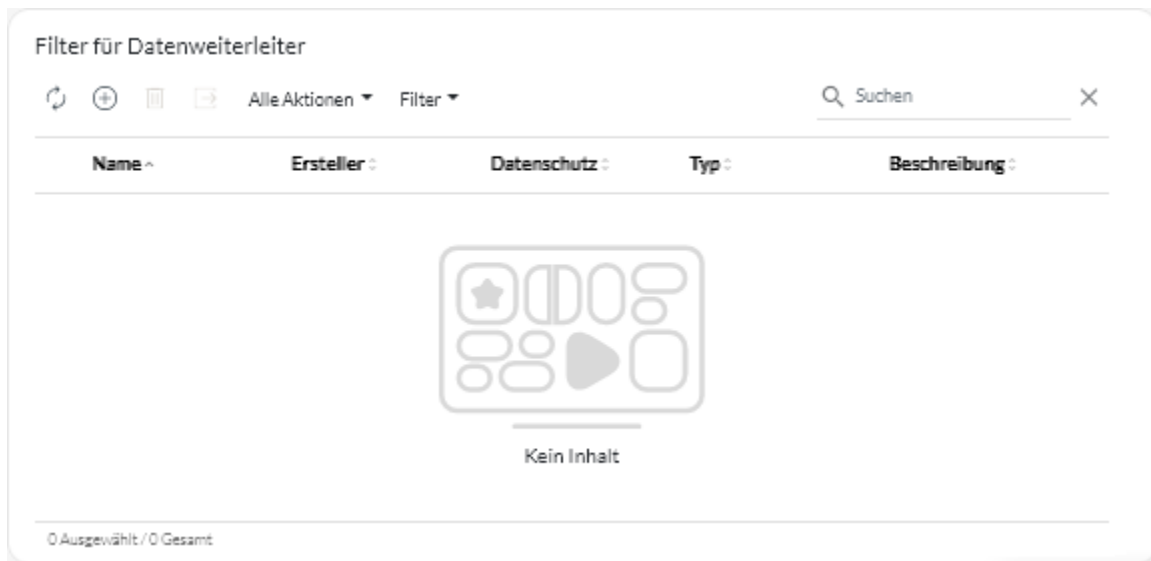
Sie können Ereignis- und Ressourcenfilter in mehreren Weiterleitern wiederverwenden. Sie können allerdings jedem Weiterleiter höchstens einen Ereignisfilter und einen Ressourcenfilter hinzufügen.

Vorgehensweise

Gehen Sie je nach Filtertyp, den Sie erstellen möchten, wie folgt vor, um einen Filter für die Datenweiterleitung zu erstellen.

- **Ereignisfilter**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Weiterleitung** und dann im linken Navigationsbereich auf **Filter für Datenweiterleiter**, um die Übersicht Filter für Datenweiterleiter anzuzeigen.



2. Wählen Sie das Symbol **Erstellen** (+) aus, um das Dialogfeld Filter für Datenweiterleiter erstellen anzuzeigen.

3. Geben Sie den Filternamen und optional eine Beschreibung ein.
 4. Wählen Sie **Ereignisfilter** als Filtertyp aus.
 5. Wählen Sie den Datenschutztyp aus.
 - **Privat**. Der Filter kann nur von Benutzern verwendet werden, die den Filter erstellt haben.
 - **Öffentlich**. Jeder Benutzer kann den Filter verwenden.
 6. Wählen Sie Ereigniseigenschaften oder Ereigniscodes als Kriterien für diesen Filter aus.
 7. Klicken Sie auf **Regeln** und wählen Sie die Kriterien für diesen Filter basierend auf dem Kriterientyp aus, den Sie im vorherigen Schritt ausgewählt haben.
 - **Nach Ereigniseigenschaften abgleichen**. Wählen Sie einen oder mehrere Eigenschaften für Schweregrad, Wartbarkeit und Klasse aus. Es werden nur Ereignisse weitergeleitet, die mit den ausgewählten Eigenschaften übereinstimmen. Wenn Sie beispielsweise die Schweregrade „Warnung“ und „Kritisch“ und die Klassen „Adapter“ und „Speicher“ auswählen, werden Ereignisdaten nur für Warnungsereignisse für Speicher, kritische Speicherereignisse, Warnungsereignisse für Adapter und kritische Adapterereignisse weitergeleitet, unabhängig von der Wartbarkeit des Ereignisses. Wenn Sie nur Benutzerwartbarkeit auswählen, werden Ereignisdaten nur für Ereignisse weitergeleitet, die vom Benutzer gewartet werden können, unabhängig von Schweregrad oder Klasse.
- Anmerkungen:**
- Wenn keine Klasseneigenschaft ausgewählt ist, werden alle Klasseneigenschaften abgeglichen.
 - Wenn keine Wartbarkeitseigenschaft ausgewählt ist, werden alle Wartbarkeitseigenschaften abgeglichen.
 - Wenn keine Schweregradeigenschaft ausgewählt ist, werden alle Schweregradeigenschaften abgeglichen.
 - **Nach Ereignis-Code abgleichen**. Geben Sie einen Ereigniscode ein, nach dem Sie filtern möchten. Klicken Sie dann auf das Symbol **Hinzufügen** (+), um den Ereigniscode zur Liste

hinzuzufügen. Wiederholen Sie dies für jeden Ereigniscode, den Sie hinzufügen möchten. Sie können einen Ereigniscode löschen, indem Sie auf das Symbol **Löschen** (🗑️) neben dem entsprechenden Code klicken. Es werden nur Ereignisse weitergeleitet, die mit einem der aufgelisteten Ereigniscodes übereinstimmen.

Sie können einen vollständigen oder einen teilweisen Ereigniscode angeben. Beispiel: FQXXOCO00011 stimmt mit dem spezifischen Ereignis überein, FQXXOSE stimmt mit allen XClarity Orchestrator-Sicherheitsereignissen überein und CO001 stimmt mit allen Ereignissen überein, die diese Zeichen enthalten.

Wenn Sie keinen Ereigniscode angeben, werden alle Ereigniscodes abgeglichen.

Eine Liste der verfügbaren Ereigniscodes finden Sie unter [Ereignis- und Alertmeldungen](#) in der Onlinedokumentation zu XClarity Orchestrator.

8. Klicken Sie auf **Erstellen**, um den Filter zu erstellen. Der Filter wird zur Tabelle hinzugefügt.

• **Ressourcenfilter**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Weiterleitung** und dann im linken Navigationsbereich auf **Filter für Datenweiterleiter**, um die Übersicht Filter für Datenweiterleiter anzuzeigen.

2. Wählen Sie das Symbol **Erstellen** (+) aus, um das Dialogfeld Filter für Datenweiterleiter erstellen anzuzeigen.

3. Geben Sie den Filternamen und optional eine Beschreibung ein.

4. Wählen Sie **Ressourcenfilter** als Filtertyp aus.

5. Wählen Sie den Datenschutztyp aus.

– **Privat**. Der Filter kann nur von Benutzern verwendet werden, die den Filter erstellt haben.

– **Öffentlich**. Jeder Benutzer kann den Filter verwenden.

6. Klicken Sie auf **Ressourcen** und wählen Sie die Ereignisquelle für diesen Filter aus.

– **Beliebige XClarity Orchestrator-Ereignisse abgleichen**. Leitet Ereignisse weiter, die von diesem XClarity Orchestrator generiert werden. Diese Option ist standardmäßig deaktiviert.

– **Beliebige Ressourcenmanager-Ereignisse abgleichen**. Leitet Ereignisse weiter, die von einem Ressourcenmanager generiert werden. Diese Option ist standardmäßig deaktiviert.

– Wenn Sie diese Option deaktivieren, werden Ereignisse nicht von beliebigen Ressourcenmanagern weitergeleitet.

– Wenn Sie diese Option aktivieren, aber keine Managergruppen auswählen, werden Ereignisse, die von allen Ressourcenmanagern generiert werden, weitergeleitet.

– Wenn Sie diese Option aktivieren und eine oder mehrere Managergruppen auswählen, werden nur Ereignisse weitergeleitet, die von Ressourcenmanagern in den ausgewählten Gruppen generiert werden.

Tipp: Sie können Managergruppen von dieser Übersicht aus erstellen, indem Sie auf das Symbol **Erstellen** (+) klicken.

– **Alle Einheitenereignisse abgleichen**. Leitet Ereignisse weiter, die von einer Einheit generiert werden. Diese Option ist standardmäßig aktiviert.

– Wenn Sie diese Option deaktivieren, werden Ereignisse nicht von allen Einheiten weitergeleitet.

– Wenn Sie diese Option aktivieren, aber keine Einheitengruppen auswählen, werden Ereignisse, die von allen Einheiten generiert werden, weitergeleitet.

– Wenn Sie diese Option aktivieren und eine oder mehrere Einheitengruppen auswählen, werden nur Ereignisse weitergeleitet, die von Einheiten in den ausgewählten Gruppen generiert werden.

Tipp: Sie können Einheitengruppen von dieser Übersicht aus erstellen, indem Sie auf das Symbol **Erstellen** (+) klicken.

7. Klicken Sie auf **Erstellen**, um den Filter zu erstellen. Der Filter wird zur Tabelle hinzugefügt.

Nach dieser Aufgabe

In der Übersicht Filter für die Datenweiterleitung können Sie die folgenden Aktionen ausführen.

- Um einen ausgewählten Filter zu entfernen, klicken Sie auf das Symbol **Löschen** (🗑️). Sie können keinen Filter löschen, der einem Weiterleiter zugewiesen ist.

Ereignisse an SAP Data Intelligence weiterleiten

Sie können Lenovo XClarity Orchestrator für die Weiterleitung von Ereignissen an SAP Data Intelligence (Intelligent Insights) konfigurieren.

Vorbereitende Schritte

Achtung: Die Verbindung zwischen XClarity Orchestrator und SAP Data Intelligence ist verschlüsselt, das TLS-Zertifikat des fernen Systems wird jedoch nicht überprüft.

Zu dieser Aufgabe

Wenn die ressourcenbasierte Zugriffssteuerung aktiviert ist, werden nur für die Ressourcen Daten weitergeleitet, auf die Sie über Zugriffssteuerungslisten zugreifen können. Wenn Sie keiner Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, müssen Sie den von Ihnen erstellten Weiterleitungen eine oder mehrere Zugriffssteuerungslisten zuweisen. Wenn Sie Daten für alle Ressourcen senden möchten, auf die Sie zugreifen können, wählen Sie alle Zugriffssteuerungslisten aus, die Ihnen zur Verfügung stehen. Wenn Sie einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können Sie Daten für alle Ressourcen senden oder Zugriffssteuerungslisten zuweisen, um die Ressourcen einzuschränken.

Sie können keine Daten filtern, die an SAP Data Intelligence weitergeleitet werden.

Im folgenden Beispiel wird das Standardformat für Daten dargestellt, die an SAP Data Intelligence weitergeleitet werden. Worte in doppelten eckigen Klammern sind Attribute, die bei der Weiterleitung von Daten durch tatsächliche Werte ersetzt werden.

```
{ "msg": "[EventMessage]", "eventID": "[EventID]", "serialnum": "[EventSerialNumber]", "senderUUID": "[EventSenderUUID]", "flags": "[EventFlags]", "userid": "[EventUserName]", "localLogID": "[EventLocalLogID]", "systemName": "[DeviceFullPathName]", "action": "[EventActionNumber]", "failFRUNumbers": "[EventFailFRUs]", "severity": "[EventSeverityNumber]", "sourceID": "[EventSourceUUID]", "sourceLogSequence": "[EventSourceLogSequenceNumber]", "failFRUSNs": "[EventFailSerialNumbers]", "failFRUUUIDs": "[EventFailFRUUUIDs]", "eventClass": "[EventClassNumber]", "componentID": "[EventComponentUUID]", "mtm": "[EventMachineTypeModel]", "msgID": "[EventMessageID]", "sequenceNumber": "[EventSequenceID]", "timeStamp": "[EventTimeStamp]", "args": "[EventMessageArguments]", "service": "[EventServiceNumber]", "commonEventID": "[CommonEventID]", "eventDate": "[EventDate]" }
```

Vorgehensweise

Gehen Sie wie folgt vor, um Ereignisdaten an SAP Data Intelligence weiterzuleiten.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Weiterleitung** und dann im linken Navigationsbereich auf **Datenweiterleiter**, um die Übersicht Datenweiterleiter anzuzeigen.

- Schritt 2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Datenweiterleiter erstellen anzuzeigen.
- Schritt 3. Geben Sie den Weiterleiternamen und optional eine Beschreibung ein.
- Schritt 4. Aktivieren oder deaktivieren Sie den Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten auswählen.
- Schritt 5. Wählen Sie **Intelligent Insights** als Weiterleitertyp aus.
- Schritt 6. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.
- Geben Sie den Hostnamen oder die IP-Adresse von SAP Data Intelligence ein.
 - Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 443.
 - Geben Sie den Ressourcenpfad ein, auf dem der Weiterleiter die Ereignisse senden soll (z. B. /rest/test).
 - Wählen Sie die REST-Methode aus. Es kann einen der folgenden Werte aufweisen.
 - **PUT**
 - **POST**
 - Wählen Sie das Protokoll aus, das für die Ereignisweiterleitung verwendet werden soll. Es kann einen der folgenden Werte aufweisen.
 - **HTTP**
 - **HTTPS**
 - Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
 - Wenn eine Authentifizierung erforderlich ist, wählen Sie einen der folgenden Authentifizierungstypen aus.
 - **Allgemein**. Authentifiziert den angegebenen Server mithilfe des angegebenen Tenant, der Benutzer-ID und des Kennworts.
 - **Token**. Authentifiziert den angegebenen Server mithilfe des angegebenen Token-Header-Namens und -Werts.
- Schritt 7. Klicken Sie auf **Zugriffssteuerungslisten** und wählen Sie eine oder mehrere Zugriffssteuerungslisten aus, die diesem Weiterleiter zugeordnet werden sollen.

Wenn der ressourcenbasierte Zugriff aktiviert ist, müssen Sie mindestens eine Zugriffssteuerungsliste auswählen.

Tipp: Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können optional **Alles abgleichen** auswählen, anstatt eine Zugriffssteuerungsliste auszuwählen, sodass weitergeleitete Daten nicht eingeschränkt sind.

- Schritt 8. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

In der Übersicht Datenweiterleiter können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie einen ausgewählten Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten wählen.
- Ändern Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Löschen** (🗑) klicken.

Ereignisse an einen REST-Webservice weiterleiten

Sie können Lenovo XClarity Orchestrator für die Weiterleitung bestimmter Ereignisse an einen REST-Webservice konfigurieren.

Vorbereitende Schritte

Achtung: Bei der Weiterleitung von Daten an diesen Service wird keine sichere Verbindung hergestellt. Die Daten werden über ein Klartextprotokoll gesendet.

Zu dieser Aufgabe

Wenn die ressourcenbasierte Zugriffssteuerung aktiviert ist, werden nur für die Ressourcen Daten weitergeleitet, auf die Sie über Zugriffssteuerungslisten zugreifen können. Wenn Sie keiner Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, müssen Sie den von Ihnen erstellten Weiterleitungen eine oder mehrere Zugriffssteuerungslisten zuweisen. Wenn Sie Daten für alle Ressourcen senden möchten, auf die Sie zugreifen können, wählen Sie alle Zugriffssteuerungslisten aus, die Ihnen zur Verfügung stehen. Wenn Sie einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können Sie Daten für alle Ressourcen senden oder Zugriffssteuerungslisten zuweisen, um die Ressourcen einzuschränken.



Gängige *Filter für die Datenweiterleitung* werden verwendet, um den Umfang der weiterzuleitenden Ereignisse anhand von Ereigniscodes, Ereignisklassen, Ereignisschweregraden, Servicetypen und Ressourcen zu definieren, die das Ereignis generiert haben. Stellen Sie sicher, dass die Ereignis- und Ressourcenfilter, die Sie für diesen Weiterleiter verwenden möchten, bereits erstellt wurden (siehe [Filter für die Datenweiterleitung erstellen](#)).

Im folgenden Beispiel wird das Standardformat für Daten dargestellt, die zu einem REST-Webservice weitergeleitet werden. Worte in doppelten eckigen Klammern sind Attribute, die bei der Weiterleitung von Daten durch tatsächliche Werte ersetzt werden.

```
{ "msg": "[[EventMessage]]", "eventID": "[[EventID]]", "serialnum": "[[EventSerialNumber]]", "senderUUID": "[[EventSenderUUID]]", "flags": "[[EventFlags]]", "userid": "[[EventUserName]]", "localLogID": "[[EventLocalLogID]]", "systemName": "[[DeviceFullPathName]]", "action": "[[EventActionNumber]]", "failFRUNumbers": "[[EventFailFRUs]]", "severity": "[[EventSeverityNumber]]", "sourceID": "[[EventSourceUUID]]", "sourceLogSequence": "[[EventSourceLogSequenceNumber]]", "failFRUSNs": "[[EventFailSerialNumbers]]", "failFRUUUIDs": "[[EventFailFRUUUIDs]]", "eventClass": "[[EventClassNumber]]", "componentID": "[[EventComponentUUID]]", "mtm": "[[EventMachineTypeModel]]", "msgID": "[[EventMessageID]]", "sequenceNumber": "[[EventSequenceID]]", "timeStamp": "[[EventTimeStamp]]", "args": "[[EventMessageArguments]]", "service": "[[EventServiceNumber]]", "commonEventID": "[[CommonEventID]]", "eventDate": "[[EventDate]]" }
```

Vorgehensweise

Gehen Sie wie folgt vor, um Daten an einen REST-Webservice weiterzuleiten.

- Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung**  → **Weiterleitung** und dann im linken Navigationsbereich auf **Datenweiterleiter**, um die Übersicht Datenweiterleiter anzuzeigen.
- Schritt 2. Klicken Sie auf das Symbol **Erstellen** , um das Dialogfenster Datenweiterleiter erstellen anzuzeigen.
- Schritt 3. Geben Sie den Weiterleiternamen und optional eine Beschreibung ein.
- Schritt 4. Aktivieren oder deaktivieren Sie den Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten auswählen.

Schritt 5. Wählen Sie **REST** als Weiterleitertyp aus.

Schritt 6. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.

- Geben Sie den Hostnamen oder die IP-Adresse des REST-Servers ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 80.
- Geben Sie den Ressourcenpfad ein, auf dem der Weiterleiter die Ereignisse senden soll (z. B. /rest/test).
- Wählen Sie die REST-Methode aus. Es kann einen der folgenden Werte aufweisen.
 - **PUT**
 - **POST**
- Wählen Sie das Protokoll aus, das für die Ereignisweiterleitung verwendet werden soll. Es kann einen der folgenden Werte aufweisen.
 - **HTTP**
 - **HTTPS**
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- Wenn eine Authentifizierung erforderlich ist, wählen Sie einen der folgenden Authentifizierungstypen aus.
 - **Allgemein**. Authentifiziert den angegebenen Server mithilfe der angegebenen Benutzer-ID und des Kennworts.
 - **Token**. Authentifiziert den angegebenen Server mithilfe des angegebenen Token-Header-Namens und -Werts.

Schritt 7. Klicken Sie auf **Filter** und wählen Sie optional die Filter aus, die für diesen Weiterleiter verwendet werden sollen.

Sie können höchstens einen Ereignisfilter und einen Ressourcenfilter auswählen.

Wenn Sie keinen Filter auswählen, werden die Daten für alle Ereignisse weitergeleitet, die von allen Ressourcen generiert werden (Einheiten, Ressourcenmanager und XClarity Orchestrator).

Auf dieser Registerkarte können Sie auch ausgeschlossene Ereignisse weiterleiten, indem Sie die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse** auf **Ja** setzen.

Schritt 8. Klicken Sie auf **Zugriffssteuerungslisten** und wählen Sie eine oder mehrere Zugriffssteuerungslisten aus, die diesem Weiterleiter zugeordnet werden sollen.

Wenn der ressourcenbasierte Zugriff aktiviert ist, müssen Sie mindestens eine Zugriffssteuerungsliste auswählen.

Tipp: Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können optional **Alles abgleichen** auswählen, anstatt eine Zugriffssteuerungsliste auszuwählen, sodass weitergeleitete Daten nicht eingeschränkt sind.

Schritt 9. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

In der Übersicht Datenweiterleiter können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie einen ausgewählten Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten wählen.
- Ändern Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.

- Entfernen Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Löschen** (🗑️) klicken.

Ereignisse an einen E-Mail-Service über SMTP weiterleiten

Sie können Lenovo XClarity Orchestrator so konfigurieren, dass bestimmte Ereignisse an eine oder mehrere E-Mail-Adressen über SMTP weitergeleitet werden.

Vorbereitende Schritte

Achtung: Bei der Weiterleitung von Daten an diesen Service wird keine sichere Verbindung hergestellt. Die Daten werden über ein Klartextprotokoll gesendet.

Wenn Sie E-Mails an einen webbasierten E-Mail-Service (wie Gmail, Hotmail oder Yahoo) weiterleiten möchten, muss Ihr SMTP-Server die Weiterleitung von Web-Mails unterstützen.

Lesen Sie sich vor der Einrichtung eines Ereignisweiterleiters an einen Gmail-Webservice die Informationen in [Ereignisse an einen Gmail-SMTP-Service weiterleiten](#) durch.

Zu dieser Aufgabe

Wenn die ressourcenbasierte Zugriffssteuerung aktiviert ist, werden nur für die Ressourcen Daten weitergeleitet, auf die Sie über Zugriffssteuerungslisten zugreifen können. Wenn Sie keiner Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, müssen Sie den von Ihnen erstellten Weiterleitungen eine oder mehrere Zugriffssteuerungslisten zuweisen. Wenn Sie Daten für alle Ressourcen senden möchten, auf die Sie zugreifen können, wählen Sie alle Zugriffssteuerungslisten aus, die Ihnen zur Verfügung stehen. Wenn Sie einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können Sie Daten für alle Ressourcen senden oder Zugriffssteuerungslisten zuweisen, um die Ressourcen einzuschränken.

Gängige *Filter für die Datenweiterleitung* werden verwendet, um den Umfang der weiterzuleitenden Ereignisse anhand von Ereigniscodes, Ereignisklassen, Ereignisschweregraden, Servicetypen und Ressourcen zu definieren, die das Ereignis generiert haben. Stellen Sie sicher, dass die Ereignis- und Ressourcenfilter, die Sie für diesen Weiterleiter verwenden möchten, bereits erstellt wurden (siehe [Filter für die Datenweiterleitung erstellen](#)).

Im folgenden Beispiel wird das Standardformat für Daten dargestellt, die zu einem E-Mail-Service weitergeleitet werden. Worte in doppelten eckigen Klammern sind Attribute, die bei der Weiterleitung von Daten durch tatsächliche Werte ersetzt werden.

E-Mail-Betreff

Event Forwarding

E-Mail-Text

```
{
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXHMEMO216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event based on the eventID. At the moment the orchestrator server can not offer more
```

```

        information.",
    "recoveryURL": null,
    "flags": [],
    "userid": null,
    "action": "None",
    "eventClass": "System",
    "args": [],
    "service": "None",
    "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
    "managerID": "23C87F0A2CB6491097489193447A655C",
    "failFRUNumbers": null,
    "failFRUSNs": null,
    "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
    "msgID": null,
    "timeStamp": "2021-03-12T18:32:14.000Z",
    "eventDate": "2021-03-12T18:32:14Z",
    "commonEventID": "FQXHMEMO216I",
    "sequenceNumber": "17934247",
    "details": null,
    "device": {
        "name": "xhmc194.labs.lenovo.com",
        "mtm": null,
        "serialNumber": null
    },
    "resourceType": "XClarity Administrator",
    "componentType": "XClarity Administrator",
    "sourceType": "Management",
    "resourceName": "xhmc194.labs.lenovo.com",
    "fruType": "other",
    "ipAddress": "10.243.2.107",
    "_id": 252349
}

```

Vorgehensweise

Gehen Sie wie folgt vor, um Daten per SMTP an einen E-Mail-Service weiterzuleiten.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📧) → **Weiterleitung** und dann im linken Navigationsbereich auf **Datenweiterleiter**, um die Übersicht Datenweiterleiter anzuzeigen.

Schritt 2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Datenweiterleiter erstellen anzuzeigen.

Schritt 3. Geben Sie den Weiterleiternamen und optional eine Beschreibung ein.

Schritt 4. Aktivieren oder deaktivieren Sie den Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten auswählen.

Schritt 5. Wählen Sie **E-Mail** als Weiterleitertyp aus.

Schritt 6. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.

- Geben Sie den Hostnamen oder die IP-Adresse des SMTP-Servers ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 25.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- Geben Sie die E-Mail-Adresse für die einzelnen Empfänger ein. Trennen Sie mehrere E-Mail-Adressen, indem Sie ein Komma verwenden.

- **Optional:** Geben Sie die E-Mail-Adresse des Absenders der E-Mail (z. B. john@company.com) und die Domäne des Absenders ein. Wenn Sie keine E-Mail-Adresse angeben, wird standardmäßig LXCO.<source_identifizier>@<smtp_host> als Absenderadresse verwendet.

Wenn Sie nur die Absenderdomäne angeben, wird <LXCO_host_name>@<sender_domain> (zum Beispiel XClarity1@company.com) als das Format der Absenderadresse verwendet.

Anmerkungen:

- Wenn Sie festgelegt haben, dass Ihr SMTP-Server für das Weiterleiten von E-Mails einen Hostnamen benötigt und Sie keinen Hostnamen für XClarity Orchestrator definiert haben, lehnt der SMTP-Server unter Umständen weitergeleitete Ereignisse ab. Wenn XClarity Orchestrator nicht über einen Hostnamen verfügt, wird das Ereignis zusammen mit der IP-Adresse weitergeleitet. Wenn die IP-Adresse nicht abgerufen werden kann, wird stattdessen „localhost“ gesendet. Dies könnte dazu führen, dass der SMTP-Server das Ereignis ablehnt.
- Wenn Sie die Absenderdomäne angeben, wird die Quelle in der Absenderadresse nicht identifiziert. Stattdessen werden Informationen über die Quelle des Ereignisses in den Text der E-Mail geschrieben, darunter Systemname, IP-Adresse, Typ/Modell und Seriennummer.
- Wenn der SMTP-Server nur E-Mails akzeptiert, die von einem registrierten Benutzer gesendet wurden, wird die Standardabsenderadresse (LXCO.<source_identifizier>@<smtp_host>) abgelehnt. In diesem Fall müssen Sie im Feld **Von Benutzer** mindestens einen Domännennamen angeben.
- Um eine sichere Verbindung zum SMTP-Server herzustellen, wählen Sie einen der folgenden Verbindungstypen aus.
 - **SSL.** Verwendet das SSL-Protokoll, um eine sichere Kommunikation herzustellen.
 - **STARTTLS.** Verwendet das TLS-Protokoll, um eine sichere Kommunikation über einen unsicheren Kanal herzustellen.

Wenn einer dieser Verbindungstypen ausgewählt ist, versucht XClarity Orchestrator, das Zertifikat des SMTP-Servers herunterzuladen und in den XClarity Orchestrator-Truststore zu importieren. Sie werden aufgefordert, dieses Zertifikat zu akzeptieren.
- Wenn eine Authentifizierung erforderlich ist, wählen Sie einen der folgenden Authentifizierungstypen aus.
 - **Regulär.** Authentifiziert den angegebenen SMTP-Server mithilfe der angegebenen Benutzer-ID und des Kennworts.
 - **OAUTH2.** Verwendet das Protokoll „Simple Authentication and Security Layer (SASL)“, um sich mithilfe des angegebenen Benutzernamens und Sicherheitstokens am angegebenen SMTP-Server zu authentifizieren. Gewöhnlich entspricht der Benutzername Ihrer E-Mail-Adresse.

Achtung: Das Sicherheitstoken läuft nach einer kurzen Zeit ab. Sie sind selber dafür verantwortlich, das Sicherheitstoken zu aktualisieren.

 - **Keine Angabe.** Es wird keine Authentifizierung verwendet.

Schritt 7. Klicken Sie auf **Filter** und wählen Sie optional die Filter aus, die für diesen Weiterleiter verwendet werden sollen.

Sie können höchstens einen Ereignisfilter und einen Ressourcenfilter auswählen.

Wenn Sie keinen Filter auswählen, werden die Daten für alle Ereignisse weitergeleitet, die von allen Ressourcen generiert werden (Einheiten, Ressourcenmanager und XClarity Orchestrator).

Auf dieser Registerkarte können Sie auch ausgeschlossene Ereignisse weiterleiten, indem Sie die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse** auf **Ja** setzen.

Schritt 8. Klicken Sie auf **Zugriffssteuerungslisten** und wählen Sie eine oder mehrere Zugriffssteuerungslisten aus, die diesem Weiterleiter zugeordnet werden sollen.

Wenn der ressourcenbasierte Zugriff aktiviert ist, müssen Sie mindestens eine Zugriffssteuerungsliste auswählen.

Tipp: Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können optional **Alles abgleichen** auswählen, anstatt eine Zugriffssteuerungsliste auszuwählen, sodass weitergeleitete Daten nicht eingeschränkt sind.

Schritt 9. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

In der Übersicht Datenweiterleiter können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie einen ausgewählten Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten wählen.
- Ändern Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Löschen** (🗑️) klicken.

Ereignisse an einen Gmail-SMTP-Service weiterleiten

Sie können Lenovo XClarity Orchestrator so einrichten, dass Ereignisse an einen webbasierten E-Mail-Service wie z. B. Gmail weitergeleitet werden.

Die folgenden Konfigurationsbeispiele unterstützen Sie dabei, die Ereignisweiterleitung für den SMTP-Service von Gmail einzurichten.

Anmerkung: Gmail empfiehlt die Verwendung der OAUTH2-Authentifizierung als sicherste Kommunikationsmethode. Wenn Sie die Standardauthentifizierung verwenden, werden Sie in einer E-Mail darauf hingewiesen, dass eine Anwendung versucht hat, ohne Nutzung aktueller Sicherheitsstandards auf Ihr Account zuzugreifen. Diese E-Mail enthält Anweisungen zum Konfigurieren Ihres E-Mail-Accounts, um diese Arten von Anwendungen zu akzeptieren.

Informationen zum Konfigurieren eines SMTP-Servers für Gmail finden Sie unter <https://support.google.com/a/answer/176600?hl=en>.

Standardauthentifizierung über SSL auf Port 465

In diesem Beispiel erfolgt die Kommunikation mit dem Gmail-SMTP-Server per SSL-Protokoll über Port 465. Für die Authentifizierung werden ein gültiger Benutzeraccount mit passendem Kennwort für Gmail verwendet.

Parameter	Wert
Host	smtp.gmail.com
Port	465
SSL	Auswählen
STARTTLS	Löschen
Authentifizierung	Standard
Benutzer	Gültige E-Mail-Adresse für Gmail

Parameter	Wert
Kennwort	Authentifizierungskennwort für Gmail
Absenderadresse	(optional)

Standardauthentifizierung über TLS auf Port 587

In diesem Beispiel erfolgt die Kommunikation mit dem Gmail-SMTP-Server per TLS-Protokoll über Port 587. Für die Authentifizierung werden ein gültiger Benutzeraccount mit passendem Kennwort für Gmail verwendet.

Parameter	Wert
Host	smtp.gmail.com
Port	587
SSL	Löschen
STARTTLS	Auswählen
Authentifizierung	Standard
Benutzer	Gültige E-Mail-Adresse für Gmail
Kennwort	Authentifizierungskennwort für Gmail
Absenderadresse	(optional)

OAuth2-Authentifizierung über TLS auf Port 587

In diesem Beispiel erfolgt die Kommunikation mit dem Gmail-SMTP-Server per TLS-Protokoll über Port 587. Für die Authentifizierung werden ein gültiger Benutzeraccount und ein Sicherheitstoken für Gmail verwendet.

Verwenden Sie das folgende Beispielverfahren, um ein Sicherheitstoken zu erhalten.

1. Erstellen Sie ein Projekt in der Google-Entwicklerkonsole und rufen Sie die Client-ID und den geheimen Clientschlüssel ab. Weitere Informationen finden Sie auf der [Website zur Google-Anmeldung bei Websites-Website](#).
 - a. Öffnen Sie in einem Webbrowser die [Website zu Google-APIs](#).
 - b. Klicken Sie im Menü dieser Webseite auf **Projekt auswählen** → **Projekt erstellen**. Das Dialogfenster Neues Projekt wird angezeigt.
 - c. Geben Sie einen Namen ein und wählen Sie **Ja** aus, um der Lizenzvereinbarung zuzustimmen. Klicken Sie dann auf **Erstellen**.
 - d. Verwenden Sie das Suchfeld auf der Registerkarte **Übersicht**, um nach „gmail“ zu suchen. Klicken Sie in den Suchergebnissen auf **GMAIL-API**.
 - e. Klicken Sie auf **Aktivieren**.
 - f. Klicken Sie auf die Registerkarte **Anmeldeinformationen**.
 - g. Klicken Sie auf **OAuth-Zustimmung**.
 - h. Geben Sie im Feld **Benutzern angezeigter Produktname** einen Namen ein und klicken Sie auf **Speichern**.
 - i. Klicken Sie auf **Anmeldeinformationen erstellen** → **OAuth-Client-ID**.
 - j. Wählen Sie **Sonstige** aus und geben einen Namen ein.
 - k. Klicken Sie auf **Erstellen**. Im Dialogfenster OAuth-Client werden Ihre Client-ID und der geheime Clientschlüssel angezeigt.
 - l. Notieren Sie die Client-ID und den geheimen Clientschlüssel für die spätere Verwendung.

- m. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.
- 2. Verwenden Sie das Python-Script [oauth2.py](#), um ein Sicherheitstoken zu generieren und zu autorisieren. Geben Sie zu diesem Zweck die bei der Projekterstellung generierte Client-ID und den geheimen Clientschlüssel ein.

Anmerkung: Dieser Schritt kann nur mit Python 2.7 abgeschlossen werden. Sie können Python 2.7 von der [Python-Website](#) herunterladen und installieren.

- a. Öffnen Sie in einem Webbrowser die [Website zu „gmail-oauth2-tools“](#).
- b. Klicken Sie auf **Raw** und speichern Sie den Inhalt unter dem Dateinamen `oauth2.py` auf Ihrem lokalen System.
- c. Führen Sie den folgenden Befehl auf einem Terminal (Linux) oder über eine Befehlszeile (Windows) aus.

```
py oauth2.py --user={your_email} --client_id={client_id}
--client_secret={client_secret} --generate_oauth2_token
```

Beispiel:

```
py oauth2.py --user=jon@gmail.com
--client_id=884243132302-458elfqjbiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
--client_secret=3tnyXgEiBIbT2m00zqnlTszk --generate_oauth2_token
```

Über diesen Befehl wird eine URL zurückgegeben, die Sie verwenden müssen, um das Token zu autorisieren und einen Überprüfungscode von der Google-Website abzurufen. Beispiel:

To authorize token, visit this url and follow the directions:

```
https://accounts.google.com/o/oauth2/auth?client_id=884243132302
-458elfqjbiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&redirect_uri=
urn%3Aietf%3Awww%3Aoauth%3A2.0%3Aaob&response_type=code&scope=https%3A%2F%2Fmail.
google.com%2F
```

Enter verification code:

- d. Öffnen Sie in einem Webbrowser die URL, die im vorherigen Schritt zurückgegeben wurde.
- e. Klicken Sie auf **Zulassen**, um diesem Service zuzustimmen. Es wird ein Überprüfungscode zurückgegeben.
- f. Geben Sie den Überprüfungscode im `oauth2.py`-Befehl ein. Der Befehl gibt das Sicherheitstoken zurück und aktualisiert es. Beispiel:

```
Refresh Token: 1/K8LPGx6UQQajj7tQGYKq8mVG8LVvGIVzHqzxFIMEYEQMEudVrK5jSpoR30zcRFq6
Access Token: ya29.CjHXAsyoH96uCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Wichtig: Das Sicherheitstoken läuft nach einer bestimmten Zeit ab. Sie können das Python-Script [oauth2.py](#) und das Aktualisierungstoken verwenden, um ein neues Sicherheitstoken zu generieren. Sie sind dafür verantwortlich, das neue Sicherheitstoken zu generieren und die Ereignisweiterleitung in Lenovo XClarity Orchestrator mit dem neuen Token zu aktualisieren.

- 3. Richten Sie über die Webschnittstelle von Lenovo XClarity Orchestrator die Ereignisweiterleitung für E-Mail mithilfe der folgenden Attribute ein.

Parameter	Wert
Host	smtp.gmail.com
Port	587
SSL	Löschen
STARTTLS	Auswählen
Authentifizierung	OAUTH2

Parameter	Wert
Benutzer	Gültige E-Mail-Adresse für Gmail
Token	Sicherheitstoken
Absenderadresse	(optional)

Bestand und Ereignisse an Splunk weiterleiten

Sie können Lenovo XClarity Orchestrator so konfigurieren, dass Bestand und Ereignisse in einem vordefinierten Format an eine Splunk-Anwendung weitergeleitet werden. Sie können dann Splunk verwenden, um Diagramme und Tabellen zu erstellen, die auf diesen Daten basieren, um Bedingungen zu analysieren und Fehler in Ihrer Umgebung vorherzusagen.

Vorbereitende Schritte

Achtung: Bei der Weiterleitung von Daten an diesen Service wird keine sichere Verbindung hergestellt. Die Daten werden über ein Klartextprotokoll gesendet.

Zu dieser Aufgabe

Splunk ist ein Tool, mit dem Bediener von Rechenzentren Ereignisprotokolle und andere Daten nachverfolgen und analysieren können. Lenovo bietet eine XClarity Orchestrator-App für Splunk, die von XClarity Orchestrator weitergeleitete Ereignisse analysiert und die Analyse in mehreren Dashboards darstellt. Sie können die Dashboards in dieser App überwachen, um potenzielle Probleme in Ihrer Umgebung zu ermitteln, damit Sie reagieren können, bevor schwerwiegende Probleme auftreten. Weitere Informationen finden Sie im [XClarity Orchestrator-App für Splunk – Benutzerhandbuch](#) in der Onlinedokumentation zu XClarity Orchestrator.

Sie können mehrere Splunk-Konfigurationen definieren. XClarity Orchestrator kann Ereignisse allerdings nur an eine Splunk-Instanz weiterleiten. Daher kann jeweils nur eine Splunk-Konfiguration aktiviert sein.

Wenn die ressourcenbasierte Zugriffssteuerung aktiviert ist, werden nur für die Ressourcen Daten weitergeleitet, auf die Sie über Zugriffssteuerungslisten zugreifen können. Wenn Sie keiner Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, müssen Sie den von Ihnen erstellten Weiterleitungen eine oder mehrere Zugriffssteuerungslisten zuweisen. Wenn Sie Daten für alle Ressourcen senden möchten, auf die Sie zugreifen können, wählen Sie alle Zugriffssteuerungslisten aus, die Ihnen zur Verfügung stehen. Wenn Sie einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können Sie Daten für alle Ressourcen senden oder Zugriffssteuerungslisten zuweisen, um die Ressourcen einzuschränken.

Daten, die an Splunk-Anwendungen weitergeleitet werden, können nicht gefiltert werden.

Vorgehensweise

Gehen Sie wie folgt vor, um Bestands- und Ereignisdaten an eine Splunk-Anwendung weiterzuleiten.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung**  → **Weiterleitung** und dann im linken Navigationsbereich auf **Datenweiterleiter**, um die Übersicht Datenweiterleiter anzuzeigen.

Schritt 2. Klicken Sie auf das Symbol **Erstellen** , um das Dialogfenster Datenweiterleiter erstellen anzuzeigen.

Schritt 3. Geben Sie den Weiterleiternamen und optional eine Beschreibung ein.

Schritt 4. Aktivieren oder deaktivieren Sie den Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten auswählen.

Schritt 5. Wählen Sie **Splunk** als Weiterleitertyp aus.

Schritt 6. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.

- Geben Sie den Hostnamen oder die IP-Adresse der Splunk-Anwendung ein.
- Geben Sie den Benutzeraccount und das Kennwort an, die für die Anmeldung beim Splunk-Service verwendet werden sollen.
- Geben Sie die REST-API und die Datenportnummern an, die für die Verbindung mit dem Splunk-Service verwendet werden sollen.
- Geben Sie einen oder mehrere HTTP-Ereignissammlerindizes an. Der Standardwert lautet **lxco**.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.

Schritt 7. Klicken Sie auf **Zugriffssteuerungslisten** und wählen Sie eine oder mehrere Zugriffssteuerungslisten aus, die diesem Weiterleiter zugeordnet werden sollen.

Wenn der ressourcenbasierte Zugriff aktiviert ist, müssen Sie mindestens eine Zugriffssteuerungsliste auswählen.

Tipp: Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können optional **Alles abgleichen** auswählen, anstatt eine Zugriffssteuerungsliste auszuwählen, sodass weitergeleitete Daten nicht eingeschränkt sind.

Schritt 8. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

In der Übersicht Datenweiterleiter können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie einen ausgewählten Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten wählen.
- Ändern Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Löschen** (🗑️) klicken.

Ereignisse an ein Syslog weiterleiten

Sie können Lenovo XClarity Orchestrator für die Weiterleitung bestimmter Ereignisse an ein Syslog konfigurieren.

Vorbereitende Schritte

Achtung: Bei der Weiterleitung von Daten an diesen Service wird keine sichere Verbindung hergestellt. Die Daten werden über ein Klartextprotokoll gesendet.

Zu dieser Aufgabe

Wenn die ressourcenbasierte Zugriffssteuerung aktiviert ist, werden nur für die Ressourcen Daten weitergeleitet, auf die Sie über Zugriffssteuerungslisten zugreifen können. Wenn Sie keiner Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, müssen Sie den von Ihnen erstellten Weiterleitungen eine oder mehrere Zugriffssteuerungslisten zuweisen. Wenn Sie Daten für alle Ressourcen senden möchten, auf die Sie zugreifen können, wählen Sie alle Zugriffssteuerungslisten aus, die Ihnen zur Verfügung stehen. Wenn Sie einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können Sie Daten für alle Ressourcen senden oder Zugriffssteuerungslisten zuweisen, um die Ressourcen einzuschränken.

Gängige *Filter für die Datenweiterleitung* werden verwendet, um den Umfang der weiterzuleitenden Ereignisse anhand von Ereigniscodes, Ereignisklassen, Ereignisschweregraden, Servicetypen und Ressourcen zu definieren, die das Ereignis generiert haben. Stellen Sie sicher, dass die Ereignis- und Ressourcenfilter, die Sie für diesen Weiterleiter verwenden möchten, bereits erstellt wurden (siehe [Filter für die Datenweiterleitung erstellen](#)).

Im folgenden Beispiel wird das Standardformat für Daten dargestellt, die an ein Syslog weitergeleitet werden. Worte in doppelten eckigen Klammern sind Attribute, die bei der Weiterleitung von Daten durch tatsächliche Werte ersetzt werden.

```
{
  "appl": "LXCO",
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXMEM0216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
        forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
                 being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
                based on the eventID. At the moment the orchestrator server can not offer more
                information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
  "managerID": "23C87F0A2CB6491097489193447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
  "msgID": null,
  "timeStamp": "2021-03-12T18:32:14.000Z",
  "eventDate": "2021-03-12T18:32:14Z",
  "commonEventID": "FQXMEM0216I",
  "sequenceNumber": "17934247",
  "details": null,
  "device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
    "serialNumber": null
  },
  "resourceType": "XClarity Administrator",
  "componentType": "XClarity Administrator",
  "sourceType": "Management",
  "resourceName": "xhmc194.labs.lenovo.com",
  "fruType": "other",
  "ipAddress": "10.243.2.107",
  "_id": 252349
}
```

Vorgehensweise

Gehen Sie wie folgt vor, um Daten an ein Syslog weiterzuleiten.

- Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Weiterleitung** und dann im linken Navigationsbereich auf **Datenweiterleiter**, um die Übersicht Datenweiterleiter anzuzeigen.
- Schritt 2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Datenweiterleiter erstellen anzuzeigen.
- Schritt 3. Geben Sie den Weiterleiternamen und optional eine Beschreibung ein.
- Schritt 4. Aktivieren oder deaktivieren Sie den Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten auswählen.
- Schritt 5. Wählen Sie **Syslog** als Weiterleitertyp aus.
- Schritt 6. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.
- Geben Sie den Hostnamen oder die IP-Adresse des Syslog ein.
 - Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 514.
 - Wählen Sie das Protokoll aus, das für die Ereignisweiterleitung verwendet werden soll. Es kann einen der folgenden Werte aufweisen.
 - **UDP**
 - **TCP**
 - Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
 - **Optional:** Wählen Sie das Format des Zeitstempels im Syslog aus. Es kann einen der folgenden Werte aufweisen.
 - **Ortszeit.** Das Standardformat, zum Beispiel Fri Mar 31 05:57:18 EDT 2017.
 - **GMT-Uhrzeit.** Internationaler Standard (ISO8601) für Datum und Uhrzeit, zum Beispiel 2017-03-31T05:58:20-04:00.
- Schritt 7. Klicken Sie auf **Filter** und wählen Sie optional die Filter aus, die für diesen Weiterleiter verwendet werden sollen.

Sie können höchstens einen Ereignisfilter und einen Ressourcenfilter auswählen.

Wenn Sie keinen Filter auswählen, werden die Daten für alle Ereignisse weitergeleitet, die von allen Ressourcen generiert werden (Einheiten, Ressourcenmanager und XClarity Orchestrator).

Auf dieser Registerkarte können Sie auch ausgeschlossene Ereignisse weiterleiten, indem Sie die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse** auf **Ja** setzen.

- Schritt 8. Klicken Sie auf **Zugriffssteuerungslisten** und wählen Sie eine oder mehrere Zugriffssteuerungslisten aus, die diesem Weiterleiter zugeordnet werden sollen.

Wenn der ressourcenbasierte Zugriff aktiviert ist, müssen Sie mindestens eine Zugriffssteuerungsliste auswählen.

Tipp: Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können optional **Alles abgleichen** auswählen, anstatt eine Zugriffssteuerungsliste auszuwählen, sodass weitergeleitete Daten nicht eingeschränkt sind.

- Schritt 9. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

In der Übersicht Datenweiterleiter können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie einen ausgewählten Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten wählen.
- Ändern Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Löschen** (🗑) klicken.

Metrikdaten an ein Lenovo TruScale Infrastructure Services weiterleiten

Sie können Lenovo XClarity Orchestrator so konfigurieren, dass Metrikdaten (Telemetriedaten) an ein Lenovo TruScale Infrastructure Services weitergeleitet werden.

Vorbereitende Schritte

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

Achtung: Diese Konfigurationsschritte sind nur für Lenovo Service-Mitarbeiter vorgesehen.

Bei der Weiterleitung von Daten an TruScale Infrastructure Services wird eine sichere Verbindung hergestellt.

Stellen Sie sicher, dass XClarity Orchestrator v1.2.0 oder höher ausführt.

Stellen Sie sicher, dass die Lenovo XClarity Administrator-Ressourcenmanager, die die Einheiten verwalten, für die Sie Metrikdaten weiterleiten möchten, v3.0.0 und das Fixpack oder höher ausführen.

Stellen Sie sicher, dass die entsprechenden XClarity Administrator-Ressourcenmanager mit XClarity Orchestrator verbunden sind (siehe [Ressourcenmanager verbinden](#)).

Stellen Sie sicher, dass auf den Einheiten, für die Sie Metrikdaten weiterleiten möchten, die neueste Lenovo XClarity Controller-Firmware ausgeführt wird (siehe [Aktualisierungen für Ressourcenmanager anwenden und aktivieren](#)).

Stellen Sie sicher, dass die Daten- und Uhrzeiteinstellungen in den folgenden Ressourcen ordnungsgemäß konfiguriert sind.

- XClarity Orchestrator (siehe [Datum und Uhrzeit konfigurieren](#))
- XClarity Administrator-Ressourcenmanager (siehe [Datum und Uhrzeit einstellen](#) in der Onlinedokumentation von XClarity Administrator)
- Baseboard Management Controller in jeder Einheit (siehe [Datum und Uhrzeit für XClarity Controller einstellen](#) in der Onlinedokumentation von Lenovo XClarity Controller)

Stellen Sie sicher, dass die Netzwerkeinstellungen in XClarity Orchestrator korrekt konfiguriert sind.

Stellen Sie sicher, dass Metrikdaten für die verwalteten Einheiten erfasst werden, indem Sie die Auslastungsdiagramme in der Einheitenübersicht anzeigen (siehe [Einheitendetails anzeigen](#)). Wenn keine Metrikdaten angezeigt werden, finden Sie weitere Informationen unter [Fehlerbehebung bei Problemen mit der Datenweiterleitung](#).

Weitere Informationen zu Lenovo TruScale Infrastructure Services finden Sie auf der [Website für TruScale Infrastructure Services](#).

Zu dieser Aufgabe

Sie können mehrere Lenovo TruScale Infrastructure Services-Konfigurationen definieren. XClarity Orchestrator kann Ereignisse allerdings nur an eine Lenovo TruScale Infrastructure Services-Instanz weiterleiten. Daher kann jeweils nur eine Lenovo TruScale Infrastructure Services-Konfiguration aktiviert sein.

Wenn die ressourcenbasierte Zugriffssteuerung aktiviert ist, werden nur für die Ressourcen Daten weitergeleitet, auf die Sie über Zugriffssteuerungslisten zugreifen können. Wenn Sie keiner Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, müssen Sie den von Ihnen erstellten Weiterleitungen eine oder mehrere Zugriffssteuerungslisten zuweisen. Wenn Sie Daten für alle Ressourcen senden möchten, auf die Sie zugreifen können, wählen Sie alle Zugriffssteuerungslisten aus, die Ihnen zur Verfügung stehen. Wenn Sie einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können Sie Daten für alle Ressourcen senden oder Zugriffssteuerungslisten zuweisen, um die Ressourcen einzuschränken.

Daten, die an ein Lenovo TruScale Infrastructure Services weitergeleitet werden, können nicht gefiltert werden.

Im folgenden Beispiel wird das Standardformat für Daten dargestellt, die an ein Lenovo TruScale Infrastructure Services weitergeleitet werden. Worte in doppelten eckigen Klammern sind Attribute, die bei der Weiterleitung von Daten durch tatsächliche Werte ersetzt werden.

```
{\ "msg\":"[[EventMessage]]"\,"eventID\":"[[EventID]]"\,"serialnum\":"
[[EventSerialNumber]]"\,"senderUUID\":"[[EventSenderUUID]]"\,"flags\":"
[[EventFlags]]"\,"userid\":"[[EventUserName]]"\,"localLogID\":"
[[EventLocalLogID]]"\,"systemName\":"[[DeviceFullPathName]]"\,"action\":"
[[EventActionNumber]]"\,"failFRUNumbers\":"[[EventFailFRUs]]"\,"severity\":"
[[EventSeverityNumber]]"\,"sourceID\":"[[EventSourceUUID]]"\,"
sourceLogSequence\":"[[EventSourceLogSequenceNumber]]"\,"failFRUSNs\":"
[[EventFailSerialNumbers]]"\,"failFRUUUIDs\":"[[EventFailFRUUUIDs]]"\,"
eventClass\":"[[EventClassNumber]]"\,"componentID\":"[[EventComponentUUID]]"\,"
mtm\":"[[EventMachineTypeModel]]"\,"msgID\":"[[EventMessageID]]"\,"
sequenceNumber\":"[[EventSequenceID]]"\,"timestamp\":"[[EventTimeStamp]]"\,"
args\":"[[EventMessageArguments]]"\,"service\":"[[EventServiceNumber]]",
commonEventID\":"[[CommonEventID]]"\,"eventDate\":"[[EventDate]]"\}"
```

Vorgehensweise

Gehen Sie wie folgt vor, um Daten an ein Lenovo TruScale Infrastructure Services weiterzuleiten.

Schritt 1. Fügen Sie die vertrauenswürdigen SSL-Zertifikate hinzu, die vom Lenovo TruScale Infrastructure Services bereitgestellt werden.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf die Menüleiste XClarity Orchestrator und **Verwaltung** (🔑) → **Sicherheit** und dann im linken Navigationsbereich auf **Vertrauenswürdige Zertifikate**, um die Übersicht „Vertrauenswürdige Zertifikate“ aufzurufen.
2. Klicken Sie auf das Symbol für **Hinzufügen** (+), um ein Zertifikat hinzuzufügen. Das Dialogfenster Zertifikat hinzufügen wird angezeigt.
3. Kopieren Sie die Zertifikatsdaten und fügen Sie sie im PEM-Format ein.
4. Klicken Sie auf **Hinzufügen**.

Schritt 2. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📧) → **Weiterleitung** und dann im linken Navigationsbereich auf **Datenweiterleiter**, um die Übersicht Datenweiterleiter anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Datenweiterleiter erstellen anzuzeigen.

Schritt 4. Geben Sie den Weiterleiternamen und optional eine Beschreibung ein.

Schritt 5. Aktivieren oder deaktivieren Sie den Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten auswählen.

Schritt 6. Wählen Sie **TruScale Infrastructure Services** als Weiterleitertyp aus.

Schritt 7. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.

- Geben Sie den Hostnamen oder die IP-Adresse des TruScale Infrastructure Service ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 9092.
- Geben Sie optional ein Intervall in Minuten ein, in dem Daten übermittelt werden. Die Standardeinstellung ist 60 Minuten.
- Geben Sie den Themennamen ein.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 300 Sekunden.

Schritt 8. Klicken Sie auf **Verbindung überprüfen**, um sicherzustellen, dass basierend auf der Konfiguration eine Verbindung hergestellt werden kann.

Achtung: Das Überprüfen der Verbindung kann mehrere Minuten in Anspruch nehmen. Sie können die Popup-Nachricht schließen und mit dem Erstellen des Weiterleiters fortfahren. Der Überprüfungsvorgang wird dadurch nicht unterbrochen. Wenn die Überprüfung abgeschlossen ist, werden Sie durch eine weitere Popup-Nachricht darüber informiert, ob die Verbindung erfolgreich hergestellt wurde.

Schritt 9. Klicken Sie auf **Zugriffssteuerungslisten** und wählen Sie eine oder mehrere Zugriffssteuerungslisten aus, die diesem Weiterleiter zugeordnet werden sollen.

Wenn der ressourcenbasierte Zugriff aktiviert ist, müssen Sie mindestens eine Zugriffssteuerungsliste auswählen.

Tipp: Benutzer, die einer Gruppe angehören, der die vordefinierte Rolle **Supervisor** zugewiesen ist, können optional **Alles abgleichen** auswählen, anstatt eine Zugriffssteuerungsliste auszuwählen, sodass weitergeleitete Daten nicht eingeschränkt sind.

Schritt 10. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

In der Übersicht Datenweiterleiter können Sie die folgenden Aktionen ausführen.

- Aktivieren oder deaktivieren Sie einen ausgewählten Weiterleiter, indem Sie in der Spalte **Status** die Option zum Umschalten wählen.
- Ändern Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie einen ausgewählten Weiterleiter, indem Sie auf das Symbol **Löschen** (🗑️) klicken.

Berichte weiterleiten

Sie können Berichte mithilfe eines SMTP-Webservice regelmäßig an eine oder mehrere E-Mail-Adressen weiterleiten.

Zu dieser Aufgabe

Ein *Bericht* sind alle Daten, die in der Benutzerschnittstelle in tabellarischer Form dargestellt werden. Die folgenden Berichte werden derzeit unterstützt.

- Aktive Alerts
- Ressourcen- und Prüfereignisse
- Verwaltete Einheiten (Server, Speicher, Switches und Gehäuse)
- Konformität der Firmware auf der Einheit
- Serverkonfigurationskonformität
- Garantiestatus für Server
- Aktive Service-Tickets

Zielonfigurationen für Weiterleiter erstellen

Sie können gemeinsame Zielkonfigurationen definieren, die von mehreren Berichtsweiterleitern verwendet werden können. Das Ziel gibt an, wohin die Berichte gesendet werden sollen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Zielkonfiguration für Berichtsweiterleiter zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (🔍) → **Weiterleitung** und dann im linken Navigationsbereich auf **Weiterleiterziele**, um die Karte Weiterleiterziele aufzurufen.

Schritt 2. Wählen Sie das Symbol **Erstellen** (+) aus, um das Dialogfeld Weiterleiterziele erstellen aufzurufen.

Schritt 3. Geben Sie den Namen des Berichtsweiterleiters und optional eine Beschreibung ein.

Schritt 4. Wählen Sie **SMTP** als Weiterleitertyp aus.

Schritt 5. Klicken Sie auf **Konfiguration** und geben Sie die protokollspezifischen Informationen ein.

- Geben Sie den Hostnamen oder die IP-Adresse des SMTP-(E-Mail-)Servers ein.
- Geben Sie den Port ein, der für das Ziel verwendet werden soll. Der Standardwert ist 25.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- Geben Sie die E-Mail-Adresse für die einzelnen Empfänger ein. Trennen Sie mehrere E-Mail-Adressen, indem Sie ein Komma verwenden.
- **Optional:** Geben Sie die E-Mail-Adresse des Absenders der E-Mail (z. B. john@company.com) und die Domäne des Absenders ein. Wenn Sie keine E-Mail-Adresse angeben, wird standardmäßig `LXCO.{source_identifizier}@{smtp_host}` als Absenderadresse verwendet.

Wenn Sie nur die Absenderdomäne angeben, wird `{LXCO_host_name}@{sender_domain}` (zum Beispiel XClarity1@company.com) als das Format der Absenderadresse verwendet.

Anmerkungen:

- Wenn Sie festgelegt haben, dass Ihr SMTP-Server für das Weiterleiten von E-Mails einen Hostnamen benötigt und Sie keinen Hostnamen für XClarity Orchestrator definiert haben, lehnt der SMTP-Server die E-Mail unter Umständen ab. Wenn XClarity Orchestrator nicht über einen Hostnamen verfügt, wird die E-Mail zusammen mit der IP-Adresse weitergeleitet. Wenn die IP-Adresse nicht abgerufen werden kann, wird stattdessen „localhost“ gesendet. Dies könnte dazu führen, dass der SMTP-Server die E-Mail ablehnt.
- Wenn Sie die Absenderdomäne angeben, wird die Quelle in der Absenderadresse nicht identifiziert. Stattdessen werden Informationen über die Datenquelle in den Text der E-Mail geschrieben, darunter Systemname, IP-Adresse, Maschinentyp/Modell und Seriennummer.
- Wenn der SMTP-Server nur E-Mails akzeptiert, die von einem registrierten Benutzer gesendet werden, wird die Standardabsenderadresse (`LXCO.<source_identifizier>@{smtp_host}>`) abgelehnt. In diesem Fall müssen Sie im Feld **Von Benutzer** mindestens einen Domännennamen angeben.
- Um eine sichere Verbindung zum SMTP-Server herzustellen, wählen Sie einen der folgenden Verbindungstypen aus.
 - **SSL.** Verwendet das SSL-Protokoll, um eine sichere Kommunikation herzustellen.
 - **STARTTLS.** Verwendet das TLS-Protokoll, um eine sichere Kommunikation über einen unsicheren Kanal herzustellen.

Wenn einer dieser Verbindungstypen ausgewählt ist, versucht XClarity Orchestrator, das Zertifikat des SMTP-Servers herunterzuladen und in den XClarity Orchestrator-Truststore zu importieren. Sie werden aufgefordert, dieses Zertifikat zu akzeptieren.

- Wenn eine Authentifizierung erforderlich ist, wählen Sie einen der folgenden Authentifizierungstypen aus.
 - **Regulär.** Authentifiziert den angegebenen SMTP-Server mithilfe der angegebenen Benutzer-ID und des Kennworts.
 - **OAUTH2.** Verwendet das Protokoll „Simple Authentication and Security Layer (SASL)“, um sich mithilfe des angegebenen Benutzernamens und Sicherheitstokens am angegebenen SMTP-Server zu authentifizieren. Gewöhnlich entspricht der Benutzername Ihrer E-Mail-Adresse.

Achtung: Das Sicherheitstoken läuft nach einer kurzen Zeit ab. Sie sind selber dafür verantwortlich, das Sicherheitstoken zu aktualisieren.
 - **Keine Angabe.** Es wird keine Authentifizierung verwendet.

Schritt 6. Klicken Sie auf **Erstellen**, um die Zielkonfiguration zu erstellen.

Nach dieser Aufgabe

Auf der Karte Weiterleiterziele können Sie die folgenden Aktionen ausführen:

- Ändern Sie ein ausgewähltes Ziel, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie ein ausgewähltes Ziel, indem Sie auf das Symbol **Löschen** (🗑️) klicken. Sie können kein Ziel löschen, das einem Weiterleiter zugewiesen ist.

Berichte per E-Mail weiterleiten

Sie können Berichte mithilfe eines SMTP-Webservice regelmäßig an eine oder mehrere E-Mail-Adressen weiterleiten.

Zu dieser Aufgabe

Ein *Bericht* sind alle Daten, die in der Benutzerschnittstelle in tabellarischer Form dargestellt werden. Die folgenden Berichte werden derzeit unterstützt.

- Aktive Alerts
- Ressourcen- und Prüfereignisse
- Verwaltungseinheiten (Server, Speicher, Switches und Gehäuse)
- Konformität der Firmware auf der Einheit
- Serverkonfigurationskonformität
- Garantiestatus für Server
- Aktive Service-Tickets

Jeder Berichtsweiterleiter kann nur einen Bericht jedes Typs enthalten.

Der Bericht wird als Archivdatei erstellt und auf dem Orchestrator-Serverhost gespeichert. Bei einer Dateigröße von bis zu 10 MB wird die Datei als E-Mail-Anhang weitergeleitet. Bei einer Dateigröße von über 10 MB enthält die E-Mail den Speicherort der Dateien. Sie können die Archivdatei auch herunterladen, indem Sie auf **Berichtsverlauf** klicken und anschließend in der Zeile für den Bericht auf **Herunterladen** klicken.

Lenovo XClarity Orchestrator speichert maximal 100 Berichte. Wenn die maximale Anzahl an Berichten erreicht ist, löscht XClarity Orchestrator den ältesten Bericht, bevor ein neuer generiert wird.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Bericht per E-Mail weiterzuleiten.

- **Ungefilterte Daten senden**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Weiterleitung** und dann im linken Navigationsbereich auf **Berichtsweiterleiter**, um die Karte Berichte anzuzeigen.
2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Bericht erstellen aufzurufen.
3. Geben Sie den Namen des Berichtsweiterleiters und optional eine Beschreibung ein.
4. Aktivieren oder deaktivieren Sie den Berichtsweiterleiter, indem Sie in der Spalte **Status** auf die Umschalt-Schaltfläche klicken.
5. Klicken Sie auf **Inhaltsliste** und wählen Sie einen oder mehrere Berichte aus, die weitergeleitet werden sollen.
6. Klicken Sie auf **Weiterleiterziel** und wählen Sie das Ziel aus (siehe [Zielonfigurationen für Weiterleiter erstellen](#)).
7. Klicken Sie auf **Zeitpläne** und geben Sie den Tag, die Uhrzeit, die Dauer (Start- und Enddatum) an, an dem Berichte gesendet werden sollen. Der Bericht wird jede Woche am gleichen Tag und zur gleichen Uhrzeit während des angegebenen Zeitraums versandt.
8. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

- **Gefilterte Daten senden**

1. Öffnen Sie in der Menüleiste XClarity Orchestrator die Karte, die den Bericht enthält, den Sie senden möchten. Die folgenden Berichte werden unterstützt:
 - Einheitendaten (klicken Sie auf **Ressourcen** (🔗) → *{device_type}*)
 - Daten zu aktiven Alerts (klicken Sie auf **Überwachung** (📊) → **Alerts**)
 - Daten zu Ressourcen- und Prüfereignissen (klicken Sie auf **Überwachung** (📊) → **Ereignisse**)
 - Firmwarekonformität (klicken Sie auf **Bereitstellung** (🔗) → **Aktualisierungen** → **Übernehmen und aktivieren** → **Einheiten**)
 - Konformität der Serverkonfiguration (klicken Sie auf **Bereitstellung** (🔗) → **Serverkonfiguration** → **Zuordnen und bereitstellen**)
 - Garantiedaten der Einheiten (klicken Sie auf **Administration** (⚙️) → **Service und Support** → **Garantie**)
 - Aktive Service-Tickets (klicken Sie auf **Administration** (⚙️) → **Service und Support** → **Service-Tickets**)
2. Optional können Sie den Datensatz auf die Informationen beschränken, die Sie interessieren, indem Sie den Umfang der Daten auf die Ressourcen einschränken, die sich in bestimmten Ressourcenmanagern und -gruppen befinden, und Filter und Suchfunktionen verwenden, um Daten einzuschließen, die bestimmten Kriterien entsprechen (siehe [Tipps und Verfahren für die Benutzerschnittstelle](#)).
3. Klicken Sie auf **Alle Aktionen** → **Berichtsweiterleiter erstellen**, um das Dialogfenster „Berichtsweiterleiter erstellen“ aufzurufen.
4. Geben Sie den Namen des Berichtsweiterleiters und optional eine Beschreibung ein.
5. Aktivieren oder deaktivieren Sie den Berichtsweiterleiter, indem Sie in der Spalte **Status** auf die Umschalt-Schaltfläche klicken.
6. Klicken Sie auf **Weiterleiterziel** und wählen Sie das Ziel aus (siehe [Zielonfigurationen für Weiterleiter erstellen](#)).
7. Klicken Sie auf **Zeitpläne** und geben Sie den Tag, die Uhrzeit, die Dauer (Start- und Enddatum) an, an dem Berichte gesendet werden sollen. Der Bericht wird jede Woche am gleichen Tag und zur gleichen Uhrzeit während des angegebenen Zeitraums versandt.
8. Klicken Sie auf **Erstellen**, um den Weiterleiter zu erstellen.

Nach dieser Aufgabe

Auf der Karte Berichtsweiterleiter können Sie die folgenden Aktionen ausführen:

- Aktivieren oder deaktivieren Sie einen ausgewählten Berichtsweiterleiter, indem Sie in der Spalte **Status** auf die Umschalt-Schaltfläche klicken.
- Ändern Sie einen ausgewählten Berichtsweiterleiter, indem Sie auf das Symbol **Bearbeiten** (✎) klicken.
- Entfernen Sie einen ausgewählten Berichtsweiterleiter, indem Sie auf das Symbol **Löschen** (🗑️) klicken.
- Speichern Sie Berichte auf Ihrem lokalen System, indem Sie auf die Registerkarte **Berichtsverlauf** und dann in der Zeile des jeweiligen Berichts auf **Herunterladen** klicken.

Sie können von jeder unterstützten Berichtskarte aus einen Bericht zu einem bestehenden Berichtsweiterleiter hinzufügen, indem Sie von der jeweiligen Karte aus auf **Alle Aktionen → Inhalt zu vorhandenem Berichtsweiterleiter hinzufügen** klicken und dabei die Datenfilter verwenden, die derzeit auf die Tabelle angewendet werden. Wenn der Berichtsweiterleiter bereits einen Bericht dieses Typs enthält, wird der Bericht so aktualisiert, dass die aktuellen Datenfilter angewendet werden.

Kapitel 4. Ressourcen verwalten

Sie können Lenovo XClarity Orchestrator verwenden, um Ressourcen zu verwalten, einschließlich der Anzeige von Details zu Offline-Einheiten.

Ressourcengruppen erstellen

Als *Ressourcengruppe* wird eine Gruppe von Ressourcen bezeichnet, die Sie in Lenovo XClarity Orchestrator anzeigen und verwenden können. Es werden mehrere Typen von Ressourcengruppen unterstützt.

Weitere Informationen:  [Ressourcengruppe erstellen](#)

Zu dieser Aufgabe

Es werden mehrere Typen von Ressourcengruppen unterstützt.

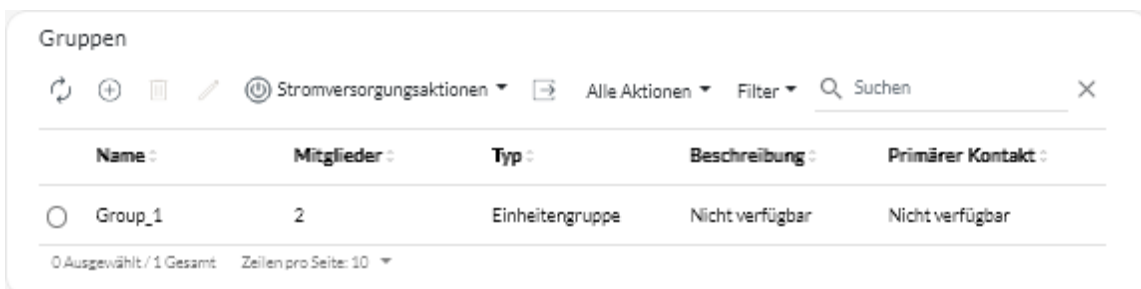
- *Dynamische Einheitengruppen* enthalten einen dynamischen Satz von Einheiten basierend auf bestimmten Kriterien.
- Eine *Einheitengruppe* enthält einen statischen Satz von bestimmten Einheiten.
- Eine *Managergruppe* enthält einen statischen Satz bestimmter Ressourcenmanager sowie XClarity Orchestrator selbst.
- *Infrastrukturgruppen* enthalten eine Gruppe von Netzwerkeinheiten. Wenn Sie einen Schneider Electric EcoStruxure IT Expert Ressourcenmanager verwalten, kloniert XClarity Orchestrator automatisch „Gruppen“-Sammlungen, die in einem verwalteten EcoStruxure IT Expert definiert sind. Die geklonte Gruppe hat im lokalen Repository den Namen $\{domain\}\{groupName\}$. Beachten Sie, dass ortsbezogene Sammlungen (Standort, Gebäude, Raum, Reihe oder Rack) nicht geklont werden.

Anmerkung: Sie können keine Ressourcengruppe mit einer Kombination aus Einheiten, Ressourcenmanagern und Infrastrukturr Ressourcen erstellen.

Vorgehensweise

So erstellen Sie eine dynamische Ressourcengruppe und verwalten die Mitgliedschaft.

- **Erstellen Sie eine dynamische Einheitengruppe und fügen Sie Einheiten hinzu.**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) → **Gruppen**, um die Übersicht Gruppen anzuzeigen.



Name :	Mitglieder :	Typ :	Beschreibung :	Primärer Kontakt :
Group_1	2	Einheitengruppe	Nicht verfügbar	Nicht verfügbar

0 Ausgewählt / 1 Gesamt Zeilen pro Seite: 10

2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster „Gruppe erstellen“ anzuzeigen.
3. Wählen Sie die **Dynamische Einheitengruppe** als Gruppentyp aus.
4. Geben Sie den Namen und optional eine Beschreibung für die Gruppe ein.

5. Klicken Sie auf **Gruppenkriterien** und wählen Sie die Regeln für die Gruppenmitgliedschaft aus.

The screenshot shows a dialog box titled "Gruppe erstellen" with a close button (X) in the top right corner. Below the title bar are three tabs: "Eigenschaften", "Verfügbare Einheiten", and "Kontaktinformationen". The "Eigenschaften" tab is active and contains three input fields: "Gruppentyp *" with a dropdown menu showing "Einheitengruppe", "Gruppenname *" (empty text input), and "Beschreibung" (empty text area with a small icon). At the bottom of the dialog, there are two buttons: "Verfügbare Einheiten >" and "Erstellen".

- Wählen Sie aus, ob die ausgewählte Einheit mit einer oder mehreren **beliebigen** oder **allen** Regeln aus der Dropdownliste **Kriterien** übereinstimmen muss.
 - Geben Sie Attribut, Operator und Wert für jede Regel an. Klicken Sie auf **Kriterien hinzufügen**, um eine weitere Regel hinzuzufügen.
6. Klicken Sie auf **Kontaktinformationen** und wählen Sie optional einen primären Support-Kontakt (in der Spalte **Primäre Kontakte**) und mindestens einen sekundären Kontakt (in der Spalte **Sekundäre Kontakte**) aus, um diesen allen Einheiten in der Gruppe zuzuordnen.
 7. Klicken Sie auf **Erstellen**. Die Gruppe wird zur Tabelle hinzugefügt.
- **Erstellen Sie eine statische Ressourcengruppe und fügen Sie Ressourcen hinzu.**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) → **Gruppen**, um die Übersicht Gruppen anzuzeigen.
 2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster „Gruppe erstellen“ anzuzeigen.
 3. Wählen Sie **Einheitengruppe** oder **Managergruppe** als Gruppentyp aus.
 4. Geben Sie den Namen und optional eine Beschreibung für die Gruppe ein.
 5. Klicken Sie auf **Verfügbare Einheiten** oder **Verfügbare Ressourcenmanager** und wählen Sie je nach Gruppentyp die Ressourcen aus, die in die Gruppe aufgenommen werden sollen.
 6. Klicken Sie auf **Kontaktinformationen** und wählen Sie optional einen primären Support-Kontakt (in der Spalte **Primäre Kontakte**) und mindestens einen sekundären Kontakt (in der Spalte **Sekundäre Kontakte**) aus, um diesen allen Einheiten in der Gruppe zuzuordnen.
 7. Klicken Sie auf **Erstellen**. Die Gruppe wird zur Tabelle hinzugefügt.
 - **Fügen Sie Einheiten zu einer statischen Einheitengruppe hinzu.**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔍) und dann auf den Einheitentyp (z. B. Server oder Switches), um eine Übersicht mit allen Einheiten dieses Typs anzuzeigen.

Server

Suchen

Fernsteuerung starten
 Stromversorgungsaktionen

 Alle Aktionen Filter

<input type="checkbox"/>	Server	Status	Konnekti	Energie	IP-Adres	Produkt	Typ/Mod	Systemfi	Empfehl	Gruppen
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Nich...	Nicht
<input type="checkbox"/>	ite-b...				10.24	Leno...	716...	CGE1f	Nich...	Nicht
<input type="checkbox"/>	Blac...				10.24	Leno...	716...	A3EGf	Nich...	Nicht
<input type="checkbox"/>	nod...				10.24	IBM ...	791...	Nicht	Nich...	Nicht
<input type="checkbox"/>	Cara...				10.24	Eagl...	791...	Nicht	Nich...	Nicht
<input type="checkbox"/>	blad...				10.24	IBM ...	790...	Nicht	Nich...	Nicht
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Nich...	Nicht
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Nich...	Nicht
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Nich...	Nicht
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	Nich...	Nicht

0 ausgewählt / 60 gesamt Zeilen pro Seite: 10

2. Wählen Sie mindestens eine Einheit aus, die zu einer Gruppe hinzugefügt werden soll.

3. Klicken Sie auf das Symbol **Element zur Gruppe hinzufügen** ().

4. Wählen Sie die Gruppe aus oder geben Sie einen Namen und optional eine Beschreibung zum Erstellen einer neuen Gruppe ein und klicken Sie auf **Übernehmen**.

• **Fügen Sie Ressourcenmanager zu einer statischen Managergruppe hinzu.**

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

2. Wählen Sie mindestens einen Ressourcenmanager aus, der zu einer Gruppe hinzugefügt werden soll.

3. Klicken Sie auf das Symbol **Element zur Gruppe hinzufügen** ().

4. Wählen Sie die Gruppe aus oder geben Sie einen Namen und optional eine Beschreibung zum Erstellen einer neuen Gruppe ein und klicken Sie auf **Übernehmen**.

Nach dieser Aufgabe

In der Übersicht Gruppen können Sie die folgenden Aktionen ausführen.

- Bearbeiten Sie die Eigenschaften und Mitgliedschaft einer ausgewählten Gruppe, indem Sie auf das Symbol **Bearbeiten** klicken ().

Anmerkung: Verwenden Sie bei Infrastrukturgruppen, die von Schneider Electric EcoStruxure IT Expert geklont wurden, Schneider Electric EcoStruxure IT Expert zum Ändern von Gruppenname, -beschreibung und -mitgliedschaft.

- Löschen Sie eine ausgewählte Gruppe über das Symbol **Löschen** ().

- Sie können die Mitglieder einer Ressourcengruppe anzeigen, indem Sie auf den Gruppennamen klicken, um das Dialogfenster Gruppe anzeigen zu öffnen, und dann auf die Registerkarte **Mitgliedsübersicht** klicken.

Einheiten offline verwalten

Wenn eine Einheit aktuell nicht von einem Ressourcenmanager verwaltet wird, können Sie Lenovo XClarity Orchestrator verwenden, um die Einheiten im *Offlinemodus* zu verwalten. Dazu importieren Sie ein Servicedatenarchiv, das dieser Einheit zugeordnet ist.

Zu dieser Aufgabe

Nur Server mit IMM2 oder XCC Baseboard Management Controllern können offline verwaltet werden. Diese Einheiten sind in der Webschnittstelle anhand des Konnektivitätsstatus „Offline verwaltet“ erkennbar.

Sie können für offline verwaltete Einheiten die folgenden Aktionen ausführen. Alle anderen Aktionen sind deaktiviert.

- Einheitenbestand anzeigen
- Ereignisse und Alerts ausschließen
- Servicedaten verwalten
- Service-Tickets im Lenovo Support-Center mit der Call-Home-Funktion eröffnen und diese Service-Tickets verwalten
- Informationen zur Garantie abrufen
- Analysefunktionen zur Vorhersage und Analyse von Problemen mit diesen Einheiten verwenden

Wichtig: XClarity Orchestrator kommuniziert nicht mit Offline-Einheiten, um aktuelle Daten abzurufen.

Vorgehensweise

Gehen Sie wie folgt vor, um Einheiten offline zu verwalten.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Orchestrator auf **Ressourcen** (☰) → **Server**. Die Seite „Server“ wird angezeigt.

Schritt 2. Klicken Sie auf das Symbol **Importieren** (📁), um Servicedatenarchive zu importieren.

Schritt 3. Ziehen Sie ein oder mehrere Servicedatenarchive (im GZ-, TZZ- oder TGZ-Format) in das Dialogfeld „Importieren“ oder klicken Sie auf **Durchsuchen**, um das Archiv zu suchen.

Schritt 4. Aktivieren Sie optional **Server in den Servicedaten nur zur Anzeige zum Bestand hinzufügen**, um den entsprechenden Server im Offlineverwaltungsmodus zu verwalten (siehe [Einheiten offline verwalten](#)).

Schritt 5. Klicken Sie auf **Importieren**, um das Archiv zu importieren und zu analysieren. Wenn die Analyse abgeschlossen ist, ändert sich der **Analysestatus** für das importierte Archiv in „Analysiert“.

Sie können den Status des Import- und Analysevorgangs im Auftragsprotokoll überwachen ([Jobs überwachen](#)).

Nach dieser Aufgabe

Sie können die Verwaltung einer ausgewählten offline verwalteten Einheit aufheben, indem Sie auf das Symbol **Verwaltung aufheben** (🗑️) klicken.

Stromversorgungsaktionen auf verwalteten Servern ausführen

Sie können Lenovo XClarity Orchestrator verwenden, um verwaltete Server einzuschalten, auszuschalten und neu zu starten.

Vorbereitende Schritte








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

ThinkSystem Server erfordern ein Betriebssystem, um Stromversorgungsvorgänge durchzuführen.


Stellen Sie sicher, dass das Betriebssystem auf dem Server ACPI-konform (Advanced Configuration and Power Interface) ist und so konfiguriert ist, dass es Vorgänge zum Herunterfahren zulässt.

Zu dieser Aufgabe

XClarity Orchestrator unterstützt die folgenden Stromversorgungsaktionen.

-  **Einschalten**. Ausgewählte Server, die derzeit ausgeschaltet sind, werden eingeschaltet.
-  **Normal ausschalten**. Das Betriebssystem wird heruntergefahren und ausgewählte Server, die derzeit eingeschaltet sind, werden ausgeschaltet.
-  **Sofort ausschalten**. Ausgewählte Server, die derzeit eingeschaltet sind, werden ausgeschaltet.
-  **Normal neu starten**. Das Betriebssystem wird heruntergefahren und ausgewählte Server, die derzeit eingeschaltet sind, werden neu gestartet.
-  **Sofort neu starten**. Ausgewählte Server, die derzeit eingeschaltet sind, werden neu gestartet.
-  **Zur Systemkonfiguration neu starten**. Ausgewählte Server werden zur BIOS-/UEFI-Konfiguration (F1) neu gestartet.
-  **Management-Controller neu starten**. Führt einen Neustart des Baseboard Management Controllers für ausgewählte Server durch.

Anmerkungen:


- Bei ThinkEdge Client-Einheiten wird nur  **Normal neu starten** unterstützt.
- Der Verbindungsstatus des Servers muss „Online“ sein. Sie können keine Stromversorgungsaktionen für Einheiten ausführen, die offline sind, einschließlich der offline verwalteten Einheiten.

Sie können Stromversorgungsaktionen für maximal 25 Einheiten gleichzeitig ausführen.


• Vorgehensweise

Gehen Sie wie folgt vor, um Server einzuschalten, auszuschalten oder neu zu starten.

Für einen einzelnen Server

- a. Klicken Sie im XClarity Orchestrator-Menü auf **Ressourcen**  → **Server**. Die Übersicht „Server“ wird angezeigt, die eine Tabellenansicht aller verwalteten Server enthält.
- b. Klicken Sie auf die Zeile mit dem Server, um die Übersichten für diesen Server anzuzeigen.
- c. Klicken Sie in der Übersicht „Schnelle Aktionen“ auf **Stromversorgungsaktionen** und dann auf die gewünschte Stromversorgungsaktion.
- d. Klicken Sie auf **Bestätigen**.

Für mehrere Server

- a. Klicken Sie im XClarity Orchestrator-Menü auf **Ressourcen**  → **Server**. Die Übersicht „Server“ wird angezeigt, die eine Tabellenansicht aller verwalteten Server enthält.
- b. Wählen Sie einen oder mehrere Server aus. Sie können maximal 25 Server auswählen.
- c. Klicken Sie auf **Stromversorgungsaktionen** und dann auf die gewünschte Stromversorgungsaktion.

Ein Dialogfenster mit einer Liste der ausgewählten Einheiten wird angezeigt. Beachten Sie, dass nicht verfügbare Einheiten (die keine Stromversorgungsaktionen unterstützen) ausgegraut sind.

- d. Klicken Sie auf **Bestätigen**.

Für alle Server in einer Gruppe

- a. Klicken Sie im XClarity Orchestrator-Menü auf **Ressourcen** (🔍) → **Gruppen**. Die Übersicht „Gruppen“ wird angezeigt, die eine Tabellenansicht aller Gruppen enthält.
- b. Wählen Sie eine Servergruppe aus.
- c. Klicken Sie in der Übersicht „Schnelle Aktionen“ auf **Stromversorgungsaktionen** und dann auf die gewünschte Stromversorgungsaktion.

Ein Dialogfenster mit einer Liste der ausgewählten Einheiten wird angezeigt. Beachten Sie, dass nicht verfügbare Einheiten (die keine Stromversorgungsaktionen unterstützen) ausgegraut sind.

- d. Wählen Sie die gewünschten Server in der Gruppe aus, für die Sie eine Aktion ausführen möchten. Sie können maximal 25 Server auswählen.
- e. Klicken Sie auf **Bestätigen**.

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).

Fernsteuerungssitzung für verwaltete Server öffnen

Sie können eine Fernsteuerungssitzung für einen verwalteten Server öffnen, als würden Sie sich an der lokalen Konsole befinden. Sie können die Fernsteuerungssitzung dann verwenden, um den Server ein- und auszuschalten und ein lokales oder Remote-Laufwerk logisch anzuhängen.

Fernsteuerungssitzung für ThinkSystem oder ThinkAgile Server öffnen

Sie können eine Fernsteuerungssitzung für einen verwalteten ThinkSystem oder ThinkAgile Server öffnen, als würden Sie sich an der lokalen Konsole befinden. Sie können die Fernsteuerungssitzung dann für Verwaltungsvorgänge verwenden.

Vorbereitende Schritte

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

Der verwaltete Server muss den Integritätsstatus „Normal“ und den Verbindungsstatus „Online“ haben. Weitere Informationen zum Anzeigen des Serverstatus finden Sie unter [Einheitendetails anzeigen](#).

Lesen Sie die folgenden Hinweise für ThinkSystem SR635 und SR655 Server.

- Baseboard Management Controller-Firmware v2.94 oder höher ist erforderlich.
- Es wird nur der Mehrbenutzermodus unterstützt. Der Einzelbenutzermodus wird nicht unterstützt.
- Internet Explorer 11 wird nicht unterstützt.
- Ein Server kann nicht über eine Fernsteuerungssitzung ein- oder ausgeschaltet werden.

Zu dieser Aufgabe

Sie können eine Fernsteuerungssitzung zu einem einzelnen ThinkSystem oder ThinkAgile Server starten.

Weitere Informationen zur Verwendung der Fernsteuerung und der Medien-Features finden Sie in der ThinkSystem- oder ThinkAgile-Serverdokumentation.

Anmerkung: Für die ThinkSystem- und ThinkAgileserver-Server ist keine Java Runtime Environment (JRE) mit Java WebStart-Unterstützung erforderlich.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Fernsteuerungssitzung für einen ThinkSystem oder ThinkAgile Server zu öffnen.

Schritt 1. Klicken Sie im XClarity Orchestrator-Menü auf **Ressourcen** (🔍) → **Server**. Die Übersicht „Server“ wird angezeigt, die eine Tabellenansicht aller verwalteten Server enthält.

Schritt 2. Wählen Sie den Server für die Fernsteuerung aus.

Schritt 3. Klicken Sie auf das Symbol **Fernsteuerung starten** (🔗).

Schritt 4. Akzeptieren Sie die Sicherheitswarnungen Ihres Webbrowsers.

Nach dieser Aufgabe

Weitere Informationen zur Situation, wenn sich die Fernsteuerungssitzung nicht erfolgreich öffnet, finden Sie unter [Fernsteuerungsprobleme](#) in der Onlinedokumentation zu XClarity Orchestrator.

Fernsteuerungssitzung für ThinkServer Server öffnen

Sie können eine Fernsteuerungssitzung für verwaltete ThinkServer Server öffnen, als würden Sie sich an der lokalen Konsole befinden. Sie können dann die Fernsteuerungssitzung verwenden, um den Server ein- und auszuschalten, Rücksetzungen durchzuführen, ein lokales Laufwerk oder ein Netzwerklaufwerk auf dem Server anzuhängen und Screenshots und Videos aufzunehmen.

Vorbereitende Schritte

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

Der verwaltete Server muss den Integritätsstatus „Normal“ und den Verbindungsstatus „Online“ haben. Weitere Informationen zum Anzeigen des Serverstatus finden Sie unter [Einheitendetails anzeigen](#).

Der FoD-Schlüssel (Feature on Demand) für das ThinkServer System Manager Premium Upgrade muss auf dem verwalteten Server installiert sein. Weitere Informationen zu den auf Ihren Servern installierten FoD-Schlüsseln finden Sie unter [FoD-Schlüssel \(Feature on Demand\) anzeigen](#) in der Onlinedokumentation von Lenovo XClarity Administrator.

Auf dem lokalen Server muss eine Java Runtime Environment (JRE) mit Java WebStart-Unterstützung (z. B. Adopt OpenJDK 8 mit IcedTea-Web v1.8-Plug-In) installiert sein.

Zu dieser Aufgabe

Sie können eine Fernsteuerungssitzung nur zu einem einzelnen ThinkServer Server starten.

Weitere Informationen zur Verwendung der ThinkServer-Fernsteuerung und der Medien-Features finden Sie in der ThinkServer-Serverdokumentation.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Fernsteuerungssitzung für einen ThinkSystem oder ThinkAgile Server zu öffnen.

Schritt 1. Klicken Sie im XClarity Orchestrator-Menü auf **Ressourcen** (🔍) → **Server**. Die Übersicht „Server“ wird angezeigt, die eine Tabellenansicht aller verwalteten Server enthält.

Schritt 2. Wählen Sie den Server für die Fernsteuerung aus.

Schritt 3. Klicken Sie auf das Symbol **Fernsteuerung starten** (🔧).

Schritt 4. Akzeptieren Sie die Sicherheitswarnungen Ihres Webbrowsers.

Nach dieser Aufgabe

Weitere Informationen zur Situation, wenn sich die Fernsteuerungssitzung nicht erfolgreich öffnet, finden Sie unter [Fernsteuerungsprobleme](#) in der Onlinedokumentation zu XClarity Orchestrator.

Fernsteuerungssitzung für System x-Server öffnen

Sie können eine Fernsteuerungssitzung für verwaltete System x-Server öffnen, als würden Sie sich an der lokalen Konsole befinden. Sie können dann die Fernsteuerungssitzung verwenden, um den Server ein- und auszuschalten, Rücksetzungen durchzuführen, ein lokales Laufwerk oder ein Netzwerklaufwerk auf dem Server anzuhängen und Screenshots und Videos aufzunehmen.

Vorbereitende Schritte

Berücksichtigen Sie die Aspekte zur Sicherheit, Leistung und Tastatureingabe, bevor Sie eine Fernsteuerungssitzung öffnen. Weitere Informationen zu diesen Aspekten finden Sie unter [Fernsteuerungshinweise](#).

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

Der verwaltete Server muss den Integritätsstatus „Normal“ und den Verbindungsstatus „Online“ haben. Weitere Informationen zum Anzeigen des Serverstatus finden Sie unter [Einheitendetails anzeigen](#).

Melden Sie sich mit Ihrem Lenovo XClarity Orchestrator Benutzeraccount bei der Fernsteuerungssitzung an. Der Benutzeraccount muss über hinreichende Benutzerberechtigungen für den Zugriff auf einen Server und seine Verwaltung verfügen.

Auf dem lokalen Server muss eine Java Runtime Environment (JRE) mit Java WebStart-Unterstützung (z. B. Adopt OpenJDK 8 mit IcedTea-Web v1.8-Plug-In) installiert sein.

Der FoD-Schlüssel (Feature on Demand) für Fernpräsenz muss auf dem verwalteten Server installiert und aktiviert sein. Auf der Seite „Server“ können Sie feststellen, ob die Fernpräsenz-Funktion aktiviert oder deaktiviert ist, indem Sie auf **Filter** → **Fernpräsenz** klicken. Wenn sie deaktiviert ist:

- Stellen Sie sicher, dass der Server den Integritätsstatus „Normal“ und den Verbindungsstatus „Online“ hat.
- Stellen Sie sicher, dass XClarity Controller Enterprise Level oder MM Advanced Upgrade für Server aktiviert ist, bei denen diese Funktionen nicht bereits standardmäßig aktiviert sind.

Die Fernsteuerungssitzung verwendet die Ländereinstellungs- und Anzeigenspracheneinstellungen, die für das Betriebssystem auf Ihrem lokalen System definiert wurden.

Zu dieser Aufgabe

Sie können mehrere Fernsteuerungssitzungen starten. Jede Sitzung kann mehrere Server verwalten.

Anmerkung: Bei Flex System x280, x480 und x880 Servern können Sie eine Fernsteuerungssitzung nur zum primären Knoten starten. Wenn Sie versuchen, eine Fernsteuerungssitzung zu einem nicht-primären Knoten in einem System mit mehreren Knoten zu starten, startet zwar der Fernsteuerungsdialog, doch es wird kein Video angezeigt.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Fernsteuerungssitzung für einen System x-Server zu öffnen.

Schritt 1. Klicken Sie im XClarity Orchestrator-Menü auf **Ressourcen** (🔍) → **Server**. Die Übersicht „Server“ wird angezeigt, die eine Tabellenansicht aller verwalteten Server enthält.

Schritt 2. Wählen Sie den Server für die Fernsteuerung aus.

Wenn Sie keinen Server auswählen, wird eine nicht zielgerichtete Fernsteuerungssitzung geöffnet.

Schritt 3. Klicken Sie auf das Symbol **Fernsteuerung starten** (🔗).

Schritt 4. Akzeptieren Sie die Sicherheitswarnungen Ihres Webbrowsers.

Schritt 5. Wenn Sie dazu aufgefordert werden, wählen Sie einen der folgenden Verbindungsmodi aus:

- **Einzelbenutzermodus.** Aufbau einer exklusiven Fernsteuerungssitzung mit dem Server. Alle anderen Fernsteuerungssitzungen mit dem Server werden dann blockiert, bis Sie die Verbindung zum Server trennen. Diese Option ist nur verfügbar, wenn keine anderen Fernsteuerungssitzungen zu diesem Server aktiv sind.
- **Mehrbenutzermodus.** Ermöglicht mehrere Fernsteuerungssitzungen zu demselben Server. XClarity Orchestrator unterstützt bis zu sechs gleichzeitige Fernsteuerungssitzungen zu einem Server.

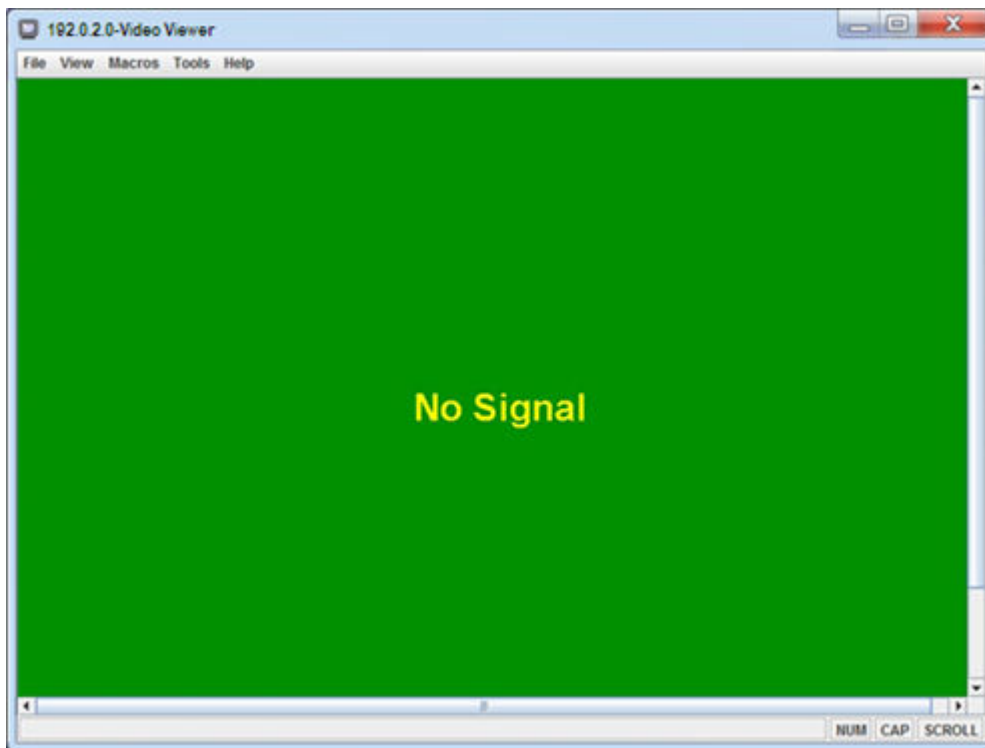
Schritt 6. Klicken Sie auf **Fernsteuerung starten**.

Schritt 7. Wenn Sie dazu aufgefordert werden, wählen Sie aus, ob eine Verknüpfung für die Fernsteuerungssitzung auf Ihrem lokalen System gespeichert werden soll. Über diese Verknüpfung können Sie eine Fernsteuerungssitzung starten, ohne sich an der XClarity Orchestrator-Webschnittstelle anzumelden. Die Verknüpfung enthält einen Link, der eine leere Fernsteuerungssitzung öffnet. Über diese können Sie die Rechenknoten manuell hinzufügen.

Anmerkung: Ihr lokales System muss Zugriff auf XClarity Orchestrator haben, um das Benutzeraccount über den XClarity Orchestrator Authentifizierungsserver zu überprüfen.







Nach dieser Aufgabe

Die Fernsteuerungssitzung enthält eine Miniaturansicht (Symbol) für jeden Server, der derzeit über die Sitzung verwaltet wird.









Weitere Informationen zur Situation, wenn sich die Fernsteuerungssitzung nicht erfolgreich öffnet, finden Sie unter [Fernsteuerungsprobleme](#) in der Onlinedokumentation zu XClarity Orchestrator.

In der Fernsteuerungssitzung können Sie die folgenden Aktionen ausführen.

- Anzeigen mehrerer Serverkonsolen und Wechseln zwischen Serverkonsolen, indem Sie auf eine Miniaturansicht klicken. Die Serverkonsole wird im Videositzungsbereich angezeigt. Wenn Sie auf mehrere Server zugreifen, als im Symbolbereich angezeigt werden können, klicken Sie auf das Symbol **Nach rechts blättern** () und **Nach links blättern** (), um zu den zusätzlichen Servern zu blättern. Klicken Sie auf das Symbol **Alle Sitzungen** (), um eine Liste aller offenen Serversitzungen anzuzeigen.
- Hinzufügen einer Serverkonsole zur aktuellen Fernsteuerungssitzung über das Symbol **Server hinzufügen** ()
- Ausblenden oder Anzeigen eines Miniaturansichtsbereiches über das Symbol **Miniaturansicht ein-/ausschalten** ()
- Anzeigen der Fernsteuerungssitzung als Fenster oder als Vollbild über das Symbol **Bildschirm** () und die Option **Vollbild einschalten** oder **Vollbild ausschalten**.
- Verwenden der Tasten für Einrastfunktion Strg, Alt und Umschalt zum Senden von Tastatureingaben direkt an den Server. Wenn Sie auf eine Taste für Einrastfunktion klicken, bleibt die Taste aktiv, bis Sie auf eine andere Taste auf der Tastatur drücken oder erneut auf die Schaltfläche klicken. Klicken Sie zum Senden von Kombinationen mit den Tasten STRG oder ALT auf die Schaltfläche Strg oder Alt in der Symbolleiste, bewegen Sie den Cursor in den Videositzungsbereich und drücken Sie eine Taste auf der Tastatur.

Anmerkung: Wenn der Mauserfassungsmodus aktiviert ist, drücken Sie die linke Alt-Taste, um den Cursor aus dem Videositzungsbereich zu bewegen. Der Mauserfassungsmodus ist standardmäßig deaktiviert. Sie können ihn über die Seite „Symbolleiste“ aktivieren (siehe [Fernbedienungseinstellungen festlegen](#)).

- Definieren von benutzerdefinierten Tastenkombinationen (auch „Programmierungssymbole“ genannt) über das Symbol **Tastatur** . Die Definitionen von Programmierungssymbolen werden auf dem System gespeichert, auf dem die Fernsteuerungssitzung gestartet wurde. Wenn Sie eine Fernsteuerungssitzung von einem anderen System aus ausführen, müssen Sie daher die Programmierungssymbole erneut definieren. Sie können Benutzereinstellungen einschließlich Programmierungssymbolen exportieren, indem Sie auf das Symbol **Einstellungen** , dann auf die Registerkarte **Benutzereinstellungen** und zuletzt auf **Importieren** klicken.
- Erstellen eines Screenshots der aktuell ausgewählten Serversitzung und Speichern des Screenshots in verschiedenen Formaten über das Symbol **Bildschirm**  und die Option **Screenshot**.
- Anhängen ferner Medien (wie CD-, DVD- oder USB-Einheit, Festplattenimage oder CD-Image (ISO)) für den ausgewählten Server oder Verschieben einer angehängten Einheit auf einen anderen Server über das Symbol **Ferne Medien** .
- Hochladen von Images auf einen Server von fernen Medien über das Symbol **Ferne Medien** , die Option **Ferne Medien anhängen** und dann **Image auf IMM hochladen**.
- Ein- und Ausschalten des Servers von einer fernen Konsole über das Symbol **Strom** .
- Ändern von Fernsteuerungseinstellungen, einschließlich Aktualisierungsrate des Serversymbols (siehe [Fernbedienungseinstellungen festlegen](#)).

Fernsteuerungshinweise

Beachten Sie beim Zugriff auf verwaltete Server über eine Fernsteuerungssitzung die folgenden Aspekte in Bezug auf Sicherheit, Leistung und Tastatur.

Sicherheitsaspekte

Der Benutzeraccount, der zum Starten der Fernsteuerungssitzung verwendet wird, muss gültig und auf dem Lenovo XClarity Orchestrator-Authentifizierungsserver definiert sein. Außerdem muss der Benutzeraccount über hinreichende Benutzerberechtigungen für den Zugriff auf einen Server und seine Verwaltung verfügen.

Standardmäßig können mehrere Fernsteuerungssitzungen mit einem Server eingerichtet werden. Sie haben jedoch beim Starten einer Fernsteuerungssitzung die Möglichkeit, die Sitzung im Einzelbenutzermodus zu starten, wodurch eine exklusive Sitzung mit dem Server eingerichtet wird. Alle anderen Fernsteuerungssitzungen mit dem Server werden dann blockiert, bis Sie die Verbindung zum Server trennen.

Anmerkung: Diese Option ist nur verfügbar, wenn zu diesem Zeitpunkt keine anderen Fernsteuerungssitzungen mit diesem Server aktiv sind.

Zur Verwendung des Federal Information Processing Standard (FIPS) 140 müssen Sie diesen manuell aktivieren, indem Sie die folgenden Schritte auf Ihrem lokalen System ausführen:

1. Suchen Sie nach dem Provider-Namen des nach FIPS 140 zertifizierten Kryptografieanbieters, der auf Ihrem lokalen System installiert ist.
2. Bearbeiten Sie die Datei `$(java.home)/lib/security/java.security`.
3. Hängen Sie an die Zeile, die `com.sun.net.ssl.internal.ssl.Provider` enthält, den Provider-Namen Ihres nach FIPS 140 zertifizierten Kryptografieanbieters an. Ändern Sie beispielsweise folgenden Dateiverweis:
`security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
in folgenden Wert:
`security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Leistungsaspekte

Wenn eine Fernsteuerungssitzung langsam wird oder nicht mehr reagiert, schließen Sie alle Video- und Remote-Mediensitzungen mit dem ausgewählten Server, um die Anzahl offener Serververbindungen zu

reduzieren. Sie können außerdem die Leistung steigern, indem Sie die folgenden Einstellungen ändern: Siehe [Fernbedienungseinstellungen festlegen](#) für weitere Informationen.

- **KVM**

- Verringern Sie den Prozentsatz der Videobandbreite, die von der Anwendung verwendet wird. Die Bildqualität der Fernsteuerungssitzung wird reduziert.
- Verringern Sie den Prozentsatz der Frames, die durch die Anwendung aktualisiert werden. Die Aktualisierungsrate der Fernsteuerungssitzung wird reduziert.

- **Miniaturansichten**

- Erhöhen Sie die Aktualisierungsintervallrate der Miniaturansichten. Die Anwendung aktualisiert Miniaturansichten seltener.
- Deaktivieren Sie die Anzeige der Miniaturansichten vollständig.

Die Größe des Fernsteuerungssitzungs-Fensters und die Anzahl aktiver Sitzungen wirken sich möglicherweise auf Workstation-Ressourcen wie Hauptspeicherkapazität und Netzwerkbandbreite aus, wodurch die Leistung beeinträchtigt werden kann. Für Fernsteuerungssitzungen gilt eine flexible Obergrenze von 32 offenen Sitzungen. Wenn mehr als 32 Sitzungen geöffnet sind, wird die Leistung erheblich herabgesetzt, bis die Fernsteuerungssitzung überhaupt nicht mehr reagiert. Auch bei weniger als 32 offenen Sitzungen kann es zu Leistungseinbußen kommen, wenn Ressourcen wie Netzwerkbandbreite und lokaler Arbeitsspeicher nicht ausreichen.

Tastaturmerkmale

Bei Fernsteuerungssitzungen werden folgende Tastaturtypen unterstützt:

- Belgisch: 105 Tasten
- Brasilianisches Portugiesisch
- Chinesisch
- Französisch: 105 Tasten
- Deutsch: 105 Tasten
- Italienisch: 105 Tasten
- Japanisch: 109 Tasten
- Koreanisch
- Portugiesisch
- Russisch
- Spanisch: 105 Tasten
- Schweiz: 105 Tasten
- Englisch (UK): 105 Tasten
- Englisch (US): 104 Tasten


Informationen zu Tastatureinstellungen finden Sie unter [Fernbedienungseinstellungen festlegen](#).

Fernbedienungseinstellungen festlegen

Sie können die Einstellungen für die aktuelle Fernsteuerungssitzung ändern.

Vorgehensweise

Gehen Sie wie folgt vor, um Fernsteuerungseinstellungen zu ändern.

Schritt 1. Zum Ändern von Fernsteuerungseinstellungen klicken Sie auf das Symbol **Einstellungen** ()**.** Alle Änderungen werden sofort wirksam.

- **KVM**

- **Prozentsatz der Videobandbreite.** Wenn Sie die Bandbreite erhöhen, wird die Fernsteuerungssitzung in besserer Qualität dargestellt. Allerdings kann dadurch die Leistung der Fernsteuerungssitzung beeinträchtigt werden.
- **Prozentsatz der aktualisierten Frames.** Bei einer höheren Frame-Aktualisierungsrate wird die Fernsteuerungssitzung häufiger aktualisiert. Allerdings kann dadurch die Leistung der Fernsteuerungssitzung beeinträchtigt werden.
- **Tastaturtyp.** Wählen Sie den Tastaturtyp aus, den Sie für die Fernsteuerungssitzung verwenden. Der ausgewählte Tastaturtyp muss sowohl den Tastatureinstellungen im lokalen System als auch den Tastatureinstellungen auf dem fernen Host entsprechen.

Anmerkung: Wenn Sie eine internationale Tastatur auswählen und Tastenkombinationen eingeben müssen, die die AltGr-Taste erfordern, stellen Sie sicher, dass die Workstation, auf der Sie die Fernsteuerungssitzung aufrufen, denselben Betriebssystemtyp nutzt wie der Server, auf den Sie per Fernsteuerung zugreifen möchten. Wenn der Server z. B. unter Linux läuft, muss die Fernsteuerungsanwendung auf einer Workstation aufgerufen werden, die ebenfalls unter Linux ausgeführt wird.

- **Bild an Fenster anpassen.** Wählen Sie diese Option aus, um das vom Server empfangene Videobild auf die Größe des Videositzungsbereichs zu skalieren.

- **Sicherheit**

- **Verbindungen im Einzelbenutzermodus bevorzugen.** Geben Sie an, ob Verbindungen im Einzelbenutzermodus die Standardeinstellung sein sollen, wenn eine Verbindung mit einem Server hergestellt wird. Wenn eine Verbindung im Einzelbenutzermodus hergestellt wird, kann immer nur ein Benutzer mit einem Server verbunden sein. Wenn dieses Feld nicht ausgewählt ist, wird die Verbindung zum Server standardmäßig im Mehrbenutzermodus hergestellt.
- **(Sichere) Tunnelverbindungen erforderlich.** Wählen Sie diese Option aus, um über den Verwaltungsknoten auf einen Server zuzugreifen. Mit dieser Option können Sie auf einen Server von einem Client aus zugreifen, der sich nicht im selben Netzwerk wie der Server befindet.

Anmerkung: Die Fernsteuerungsanwendung versucht immer, die Serververbindung direkt von dem lokalen System aus herzustellen, auf dem die Fernsteuerungssitzung gestartet wurde. Wenn Sie diese Option auswählen, greift die Fernsteuerungsanwendung über Lenovo XClarity Orchestrator auf den Server zu, wenn die Client-Workstation den Server nicht direkt erreichen kann.

- **Symbolleiste**

Anmerkung: Klicken Sie auf **Standardwerte wiederherstellen**, um alle Einstellungen auf dieser Seite wieder auf die Standardeinstellungen zurückzusetzen.

- **Symbolleiste am Fenster anheften.** Standardmäßig wird die Symbolleiste über dem Fenster der Fernsteuerungssitzung ausgeblendet und nur angezeigt, wenn Sie den Mauszeiger darüber bewegen. Wenn Sie diese Option auswählen, wird die Symbolleiste am Fenster angeheftet und immer zwischen dem Miniaturansichtsbereich und dem Fenster der Fernsteuerungssitzung angezeigt.
- **Tastaturschaltflächen anzeigen.** Geben Sie an, ob die Tastaturschaltflächensymbole (Feststelltaste, Num- und Rollen-Taste) in der Symbolleiste angezeigt werden sollen.
- **Stromverbrauchssteuerung anzeigen.** Geben Sie an, ob die Stromversorgungsoptionen in der Symbolleiste angezeigt werden sollen.
- **Tasten für Einrastfunktion anzeigen.** Geben Sie an, ob die Tasten für Einrastfunktion (Strg, Alt und Entf) in der Symbolleiste angezeigt werden sollen.

- **Lokalen Mauszeiger ausblenden.** Geben Sie an, ob der lokale Mauszeiger angezeigt werden soll, wenn der Cursor in der aktuell im Videositzungsbereich angezeigten Serversitzung platziert wird.
- **Mauserfassungsmodus aktivieren.** Standardmäßig ist der Mauserfassungsmodus deaktiviert. Dies bedeutet, dass Sie den Cursor frei innerhalb des Videositzungsbereichs und aus dem Bereich heraus bewegen können. Wenn Sie den Mauserfassungsmodus aktivieren, müssen Sie die linke Alt-Taste drücken, bevor Sie den Cursor aus dem Videositzungsbereich bewegen können. Wenn der Mauserfassungsmodus aktiviert ist, können Sie angeben, ob Sie die Tastenkombination Strg+Alt zum Beenden des Mauserfassungsmodus verwenden möchten. Standardmäßig wird hierfür die linke Alt-Taste verwendet.
- **Deckkraft des Symbolleistenhintergrundes.** Wenn Sie den Opazitätsprozentsatz verringern, wird durch den Symbolleistenhintergrund hindurch mehr vom Videositzungsbereich sichtbar.

Anmerkung: Diese Option ist nur verfügbar, wenn nicht die Symbolleiste am Fenster angeheftet ist.

- **Miniaturansichten**

- **Miniaturansicht anzeigen.** Wählen Sie diese Option aus, um den Miniaturansichtsbereich in der Fernsteuerungssitzung anzuzeigen.
- **Aktualisierungsintervall der Miniaturansicht angeben.** Wenn Sie das Intervall für die Aktualisierung der Miniaturansichten verringern, werden die Miniaturansichten der Server häufiger aktualisiert.

- **Allgemein**

- **Debugmodus.** Geben Sie an, ob der Debugmodus für die Fernsteuerungsanwendung festgelegt werden soll. Die Einstellungen bestimmen die Granularität der Ereignisse, die in die Protokolldateien geschrieben werden. Standardmäßig werden nur schwerwiegende Ereignisse protokolliert.
- **Systemdarstellungseinstellungen übernehmen.** Mit dieser Einstellung wird die Darstellung an die Farbschemata angepasst, die für den lokalen Server (unter Windows) konfiguriert sind. Die Fernsteuerungsanwendung muss erneut gestartet werden, damit diese Einstellungen wirksam werden.
- **Desktopsymbol erstellen.** Mit dieser Einstellung wird ein Desktopsymbol auf Ihrem lokalen System erstellt, mit dem Sie die Fernsteuerungsanwendung direkt von Ihrem System starten können. Sie benötigen trotzdem die entsprechenden Berechtigungen, um von Ihrem System aus auf die Verwaltungssoftware zugreifen zu können.
- **Mit Verwaltungsserver synchronisieren.** Diese Einstellung gewährleistet, dass die in der Fernsteuerungsanwendung angezeigten Serverdaten mit den Serverdaten übereinstimmen, die von der Verwaltungssoftware angezeigt werden.

Kapitel 5. Ressourcen bereitstellen

Sie können Lenovo XClarity Orchestrator verwenden, um verwaltete Ressourcen bereitzustellen, z. B. für die Bereitstellung von Aktualisierungen für Lenovo XClarity Administrator Ressourcenmanager und verwaltete Server und für die Konfiguration von verwalteten Servern.

Serverkonfigurationen bereitstellen

Serverkonfigurationsmuster werden verwendet, um mehrere Server schnell über einen einzigen Satz von definierten Konfigurationseinstellungen zu konfigurieren. Jedes Muster definiert die Konfigurationseigenschaften für einen bestimmten Servertyp. Sie können ein Servermuster durch die Übernahme der Einstellungen von einem vorhandenen Server erstellen.

Vorbereitende Schritte

Vergewissern Sie sich, dass die Firmware auf den Servern, die Sie konfigurieren möchten, auf dem neuesten Stand ist.

Zu dieser Aufgabe

Die Konfiguration von Servern mithilfe von Mustern wird nur für ThinkSystem Server (ausgenommen SR635 und SR655) unterstützt.

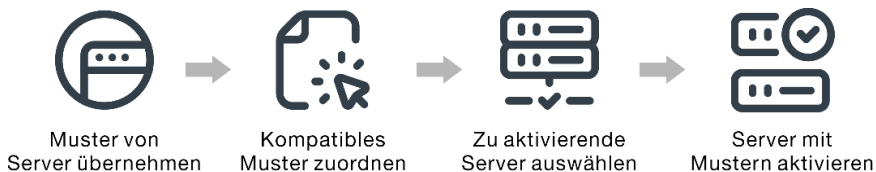
Sie können Serverkonfigurationsmuster verwenden, um die Baseboard Management Controller- und UEFI-Einstellungen und -Definitionen (Unified Extensible Firmware Interface) auf verwalteten Servern zu konfigurieren. Muster integrieren eine Unterstützung für das Virtualisieren von E/A-Adressen, sodass Sie Server-Fabric-Verbindungen virtualisieren oder Server ohne Unterbrechung für den Fabric anderweitig nutzen können.

Die folgenden Einstellungen können Sie nicht konfigurieren.

- Bootreihenfolge
- Lokaler Speicher und SAN-Zoning
- E/A-Adapter
- Lokale Benutzeraccounts
- LDAP-Server

Vorgehensweise

In der folgenden Abbildung wird der Ablauf der Konfiguration von verwalteten Servern dargestellt.



Schritt 1. Servermuster erstellen

Sie können Muster erstellen, die verschiedene in Ihrem Rechenzentrum verwendete Konfigurationen abbilden, indem die Konfigurationseinstellungen und -definitionen von vorhandenen Servern übernommen werden.

Wichtig: Erstellen Sie ggf. ein Servermuster für jeden Servertyp in Ihrem Rechenzentrum. Beispielsweise können Sie ein Servermuster für alle ThinkSystem SR650 Server und ein weiteres Servermuster für alle ThinkSystem SR850 Server erstellen. Implementieren Sie kein Serverkonfigurationsmuster, das für einen bestimmten Servertyp erstellt wurde, für einen anderen Servertyp.

Weitere Informationen zum Erstellen von Servermustern finden Sie unter [Serverkonfigurationsmuster von einem vorhandenen Server übernehmen](#).

Schritt 2. **Muster einem oder mehreren Servern zuordnen**

Sie können mehreren Servern ein Muster zuordnen, aber jedem Server kann nur ein Muster XClarity Orchestrator zugeordnet sein.

Erstellen Sie ggf. ein Servermuster für jeden Servertyp in Ihrem Rechenzentrum. Beispielsweise können Sie ein Servermuster für alle ThinkSystem SR650 Server und ein weiteres Servermuster für alle ThinkSystem SR850 Server erstellen.

Sie sollten ein Servermuster, das für einen bestimmten Servertyp erstellt wurde, keinem anderen Servertyp zuordnen oder darauf implementieren.

Nachdem Sie einem oder mehreren Zielservers ein zutreffendes Muster zugeordnet haben, führt XClarity Orchestrator eine Konformitätsprüfung auf den Servern durch, um festzustellen, ob die Serverkonfiguration mit dem Muster übereinstimmt. Server, die nicht mit dem zugeordneten Muster übereinstimmen, werden gekennzeichnet.

Weitere Informationen zum Erstellen von Servermustern finden Sie unter [Aktualisierungen für Ressourcenmanager anwenden und aktivieren](#).

Schritt 3. **Zugeordnetes Muster auf Zielservers implementieren**

Sie können Muster implementieren, die einem oder mehreren bestimmten Servern oder Servergruppen zugeordnet sind. Wenn Sie ein Muster implementieren, werden die Konfigurationseinstellungen und -definitionen aus diesem Muster in den gemeinsam genutzten Speicher geschrieben und anschließend aktiviert. Einige Einstellungen erfordern einen Systemneustart, bevor sie aktiviert werden.

Server müssen neu gestartet werden, damit bestimmte Konfigurationsänderungen, wie Baseboard Management Controller- und UEFI-Konfigurationseinstellungen (Unified Extensible Firmware Interface) aktiviert werden. Sie können wählen, wann die Änderungen aktiviert werden sollen:

- Bei **Verzögerte Aktivierung** werden alle Konfigurationsänderungen nach dem nächsten Neustart des Servers aktiviert. Der Zielservers muss manuell neu gestartet werden, damit der Implementierungsprozess fortgesetzt wird.

Wichtig: Verwenden Sie **Normal neu starten**, um den Server neu zu starten und den Aktualisierungsprozess fortzuführen. Sie dürfen *nicht* **Sofort neu starten** verwenden.

Anmerkung: Die Einstellungen auf einem Server sind ggf. nicht mehr konform mit dem jeweiligen Muster, wenn Einstellungen nicht in den zugeordneten Mustern, sondern direkt auf dem Server geändert werden, oder wenn während der Implementierung des zugeordneten Musters ein Fehler aufgetreten ist, beispielsweise ein Fehler bei der Firmware oder eine ungültige Einstellung. Sie können den Konformitätsstatus jedes Servers über die Registerkarte **Zuordnen und bereitstellen** ermitteln.

Achtung: XClarity Orchestrator weist bei der Bereitstellung von Servermustern den einzelnen Servern keine IP- und E/A-Adressen zu.

Weitere Informationen zu Aktualisierungskonformitätsrichtlinien finden Sie unter [Serverkonfigurationsmuster zuordnen und implementieren](#).

Schritt 4. **Muster ändern und erneut implementieren** Sie können die folgenden Konfigurationsänderungen an einem vorhandenen Muster vornehmen. Wenn Sie das Muster speichern, führt XClarity Orchestrator eine Konformitätsprüfung auf den Servern aus, denen dieses Muster zugeordnet ist, um festzustellen, ob die Serverkonfiguration mit dem Muster übereinstimmt. Anschließend können Sie das geänderte Muster erneut auf allen oder einigen Servern implementieren, denen dieses Muster zugeordnet ist.

Hinweise zur Serverkonfiguration

Bevor Sie mit der Konfiguration von Servern mit Lenovo XClarity Orchestrator beginnen, sollten Sie die folgenden Aspekte berücksichtigen.

Hinweise zum Server

- Die Konfiguration von Servern mithilfe von Mustern wird nur für ThinkSystem Server (ausgenommen SR635 und SR655) unterstützt.
- Vergewissern Sie sich, dass die Firmware auf den Servern, die Sie konfigurieren möchten, auf dem neuesten Stand ist.

Hinweise zu Konfigurationsmustern

- Sie können mehreren Servern ein Muster zuordnen, aber jedem Server kann nur ein Muster XClarity Orchestrator zugeordnet sein.

Anmerkung: XClarity Orchestrator hindert Sie nicht daran, ein Serverkonfigurationsmuster einem Server zuzuordnen oder es darauf zu implementieren, dem ein Muster oder Serverprofil in Lenovo XClarity Administrator zugeordnet ist. Die Implementierung eines Musters mit XClarity Orchestrator kann die Musterkonformität in XClarity Administrator beeinflussen.

- Sie können Serverkonfigurationsmuster verwenden, um die Baseboard Management Controller- und UEFI-Einstellungen und -Definitionen (Unified Extensible Firmware Interface) auf verwalteten Servern zu konfigurieren. Muster integrieren eine Unterstützung für das Virtualisieren von E/A-Adressen, sodass Sie Server-Fabric-Verbindungen virtualisieren oder Server ohne Unterbrechung für den Fabric anderweitig nutzen können.

Die folgenden Einstellungen können Sie nicht konfigurieren.

- Bootreihenfolge
 - Lokaler Speicher und SAN-Zoning
 - E/A-Adapter
 - Lokale Benutzeraccounts
 - LDAP-Server
- Erstellen Sie ggf. ein Servermuster für jeden Servertyp in Ihrem Rechenzentrum. Beispielsweise können Sie ein Servermuster für alle ThinkSystem SR650 Server und ein weiteres Servermuster für alle ThinkSystem SR850 Server erstellen.
 - Sie sollten ein Servermuster, das für einen bestimmten Servertyp erstellt wurde, keinem anderen Servertyp zuordnen oder darauf implementieren.
 - In den folgenden Situationen sind die Einstellungen auf einem Server ggf. nicht mehr konform mit dem ihnen zugeordneten Muster. Sie können den Konformitätsstatus jedes Servers über die Registerkarte **Zuordnen und bereitstellen** ermitteln.
 - Konfigurationseinstellungen wurden direkt auf dem Server und nicht in den zugeordneten Mustern geändert.
 - Bei der Musterimplementierung ist ein Problem aufgetreten, z. B. ein Fehler bei der Firmware oder eine ungültige Einstellung.

- Firmware wurde aktualisiert, wodurch die Konfigurationseinstellungen und -definitionen geändert wurden.

Anmerkung: Die Implementierung kann fehlschlagen, wenn das zugeordnete Muster auf früheren Firmwareversionen basiert. In diesem Fall wird empfohlen, ein neues Muster basierend auf der aktuell installierten Firmware zu übernehmen oder ein bestehendes Muster zu verändern, um die Konfiguration bestimmter Elemente vor dem Implementieren des Musters auszuschließen.

Hinweise zum Konfigurationsprozess

- Während die Konfiguration läuft, ist der Zielservers gesperrt. Sie können keine anderen Verwaltungsaufgaben auf dem Zielservers starten, bis der Konfigurationsprozess abgeschlossen ist.
- Nachdem ein Konfigurationsmuster auf einem Server implementiert wurde, sind möglicherweise ein oder mehrere Neustarts erforderlich, damit die Änderungen vollständig übernommen werden. Sie können alle Änderungen aktivieren, indem Sie den Server sofort neu starten. Wenn Sie den sofortigen Serverneustart wählen, minimiert XClarity Orchestrator die Anzahl der erforderlichen Neustarts. Wenn Sie die verzögerte Aktivierung wählen, werden alle Änderungen beim nächsten Neustart des Servers aktiviert. Wenn Sie die teilweise Aktivierung auswählen, werden die Änderungen sofort aktiviert, die keinen Neustart des Servers erfordern. Alle anderen Änderungen werden beim nächsten Neustart des Servers aktiviert.
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielservers ausgeführt werden. Wenn gerade Jobs ausgeführt werden, wird der Konfigurationsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt.
- Einige erweiterte Serverfunktionen werden mithilfe von FoD-Schlüsseln (Feature on Demand) aktiviert. Wenn Funktionen konfigurierbare Einstellungen haben, auf die während der UEFI-Konfiguration zugegriffen werden kann, können Sie die Einstellungen mit Konfigurationsmustern festlegen. Die daraus resultierende Konfiguration wird jedoch erst durch die Installation des entsprechenden FoD-Schlüssels aktiviert.

Serverkonfigurationsmuster von einem vorhandenen Server übernehmen

Serverkonfigurationsmuster definieren die Konfigurationseigenschaften für einen bestimmten Servertyp. Sie können ein Servermuster durch die Übernahme der Einstellungen von einem vorhandenen Server erstellen.

Vorbereitende Schritte

- Stellen Sie sicher, dass Sie die Hinweise zur Serverkonfiguration gelesen haben, bevor Sie ein Serverkonfigurationsmuster erstellen (siehe [Bereitstellungshinweise aktualisieren](#)).
- Stellen Sie sicher, dass der Server online ist, mit dem Sie ein Muster erstellen möchten.
- Ermitteln Sie Servergruppen mit den gleichen Hardwareoptionen, die identisch konfiguriert werden sollen. Sie können ein Servermuster verwenden, um dieselben Konfigurationseinstellungen auf mehreren Servern zu implementieren und so über einen zentralen Ort eine gemeinsame Konfiguration umsetzen.

Gehen Sie wie folgt vor, um ein Muster zu erstellen, indem Sie die Konfiguration eines vorhandenen Servers übernehmen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Serverkonfiguration** und dann auf die Registerkarte **Muster**, um die Übersicht Serverkonfigurationsmuster anzuzeigen.

Serverkonfigurationsmuster

Verwenden Sie Serverkonfigurationsmuster, um die Konfigurationseinstellungen für mehrere Server von einem einzigen Muster aus zu ändern.

Alle Aktionen ▾
 Filter ▾

<input type="checkbox"/>	Name :	Beschreibung :	Letzte Aktualisierung :
<input type="checkbox"/>	SD650_pattern	[Learned pattern from server: 10.2...	10.10.22, 08:50
<input type="checkbox"/>	ST650_pattern	[Learned pattern from server: 10.2...	10.10.22, 08:49

0 Ausgewählt / 2 Gesamt Zeilen pro Seite: 10 ▾

Schritt 2. Klicken Sie auf das Symbol **Erstellen** (⊕), um das Dialogfenster Serverkonfigurationsmuster erstellen anzuzeigen.

Serverkonfigurationsmuster erstellen

Mustername und Beschreibung angeben

Name

Beschreibung

Server für die Übernahme der Einstellungen als Basiskonfiguration auswählen ⓘ

Alle Aktionen ▾
 Filter ▾

<input type="checkbox"/>	Einheiten :	IP-Adressen :	Produktname :
<input type="checkbox"/>	Colossus-ST650V2-1	10.240.211.65, 2002:97b:c2bt	ThinkSystem ST650V2
<input type="checkbox"/>	Mehlow-ST250-1	10.240.211.39, 169.254.95.11	ThinkSystem ST250
<input type="checkbox"/>	OceanCat-SDV-6	10.240.211.221, 2002:97b:c2t	Lenovo ThinkSystem SD650

0 Ausgewählt / 3 Gesamt Zeilen pro Seite: 10 ▾

Schritt 3. Geben Sie den Namen und optional eine Beschreibung für das Muster ein.

Schritt 4. Wählen Sie den Server aus, den Sie als Grundlage für dieses Muster verwenden möchten.

Anmerkung: Nicht unterstützte Einheitenmodelle werden mit grauem Text angezeigt und können nicht ausgewählt werden.

Schritt 5. Klicken Sie auf **Übernehmen**.

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

Nach dieser Aufgabe

In der Übersicht Muster können Sie die folgenden Aktionen ausführen.

- Anzeigen von Musterdetails, indem Sie auf die Zeile für das Muster klicken.
- Kopieren eines ausgewählten Musters über einen Klick auf das Symbol **Kopieren** (📄).
- Ändern der Konfigurationseinstellungen in einem Muster, indem Sie die Musterdetails durch Klicken auf die Zeile des Musters aufrufen, die erforderlichen Änderungen vornehmen und dann auf **Speichern** klicken. Standardmäßig werden alle ermittelten Einstellungen in das Muster aufgenommen. Sie können Einstellungen aus dem Muster ausschließen, indem Sie **Einstellungen für das Muster ausschließen/einschließen** auswählen und dann die Einstellungen löschen, die Sie nicht im Muster haben wollen. Gelöschte (zum Ausschluss markierte) Einstellungen sind gelb hervorgehoben. Wenn Sie auf **Speichern** klicken, werden nur die Einstellungen aufgeführt, die im Muster enthalten sind. Wenn Sie Einstellungen ausgeschlossen haben, können Sie sie wieder einbeziehen, indem Sie auf **Einstellungen für das Muster ausschließen/einschließen** und auf **Ausgeschlossene Einstellungen anzeigen** klicken und dann die Einstellungen auswählen, die Sie einschließen möchten. Ausgewählte (zum Einbeziehen markierte) Einstellungen sind grün hervorgehoben.

Anmerkung: Die Konformitätsprüfung basiert nur auf den einbezogenen Einstellungen. Ausgeschlossene Einstellungen werden nicht überprüft.

Wenn Sie das geänderte Muster speichern, führt XClarity Orchestrator eine Konformitätsprüfung auf den Servern aus, denen dieses Muster zugeordnet ist, um festzustellen, ob die Serverkonfiguration mit dem Muster übereinstimmt. Anschließend können Sie das geänderte Muster auf nicht konformen Servern implementieren (siehe [Serverkonfigurationsmuster zuordnen und implementieren](#)).

The screenshot displays the BMC configuration interface. On the left, a sidebar shows a navigation menu with 'Musterkonfiguration' selected, and sub-items 'Erweitertes BMC' and 'Erweiterte UEFI'. Below the menu are two toggle switches: 'Einstellungen für dieses Muster ausschließen/einschließen' (disabled) and 'Ausgeschlossene Einstellungen anzeigen' (disabled). At the bottom of the sidebar, there are two color-coded buttons: 'Ausgeschlossen' (red) and 'Eingeschlossen' (green).

The main content area is titled 'Musterkonfiguration'. It contains a 'Name*' field with the value 'SD650_pattern' and a 'Beschreibung' field with the text '[Learned pattern from server: 10.240.211.221 on 2022-10-10]'. Below this, there is a list of configuration categories, each with a checkbox and a dropdown arrow:

- Integrated Management Module**
 - > Login Profile
 - > General Settings
 - > Network Settings Interface
- UEFI**
 - System Recovery**
 - POST Watchdog Timer: Disable
 - POST Watchdog Timer Value: 5
 - Reboot System on NMI: Disable
 - Post Load Setup Default: Disable
 - <F1> Start Control: Auto
 - > Devices and I/O Ports
 - > Processors
 - > Physical Presence Policy Configuration

- Kopieren Sie ein Konfigurationsmuster, indem Sie die Musterdetails durch Klicken auf die Zeile des Musters aufrufen und dann auf **Speichern unter** klicken.
- Löschen eines ausgewählten Musters über das Symbol **Löschen** (🗑️). Wenn das Muster einem oder mehreren Servern zugeordnet ist, wird ein Dialogfenster mit einer Liste der verfügbaren Server angezeigt. Wenn Sie die Löschanforderung bestätigen, wird die Zuordnung des Musters von diesen Servern aufgehoben.

Anmerkung: Sie können kein Muster löschen, das aktiv Servern zugeordnet wird.

- Zuordnen und Implementieren eines Musters zu bzw. auf einem oder mehreren Zielservers (siehe [Serverkonfigurationsmuster zuordnen und implementieren](#)).

Serverkonfigurationsmuster zuordnen und implementieren

Sie können ein Serverkonfigurationsmuster für einen oder mehrere verwaltete Server zuordnen und implementieren.

Vorbereitende Schritte

- Stellen Sie sicher, dass Sie die Hinweise zur Serverkonfiguration gelesen haben, bevor Sie einem Server ein Muster zuordnen oder es darauf implementieren (siehe [Bereitlungshinweise aktualisieren](#)).

- Vergewissern Sie sich, dass die Firmware auf den Servern, die Sie konfigurieren möchten, auf dem neuesten Stand ist.
- Sie sollten ein Servermuster, das für einen bestimmten Servertyp erstellt wurde, keinem anderen Servertyp zuordnen oder darauf implementieren.
- XClarity Orchestrator hindert Sie nicht daran, ein Serverkonfigurationsmuster einem Server zuzuordnen oder es darauf zu implementieren, dem ein Muster oder Serverprofil in Lenovo XClarity Administrator zugeordnet ist. Die Implementierung eines Musters mit XClarity Orchestrator kann die Musterkonformität in XClarity Administrator beeinflussen.
- XClarity Orchestrator weist bei der Bereitstellung von Servermustern den einzelnen Servern keine IP- und E/A-Adressen zu.

Zu dieser Aufgabe

Wenn einem Server ein Muster zugeordnet wird, führt XClarity Orchestrator eine Konformitätsprüfung durch, um die aktuellen Konfigurationseinstellungen auf dem Server mit den Einstellungen im Konfigurationsmuster zu vergleichen, und aktualisiert die Spalte **Konformitätsstatus** basierend auf den Ergebnissen. Der Konformitätsstatus kann einer der folgenden Werte sein.

- **Konform.** Alle Konfigurationseinstellungen im zugeordneten Muster entsprechen den Einstellungen auf dem Server.
- **Nicht konform.** Mindestens eine Konfigurationseinstellung im zugeordneten Muster entspricht *nicht* den Einstellungen auf dem Server. Bewegen Sie die Maus über die Tabellenzelle und es wird ein Popup angezeigt, das die nicht übereinstimmenden Einstellungen und Werte enthält.
- **Ausstehend.** Es wird eine Musterimplementierung oder eine Konformitätsprüfung ausgeführt.
- **Ausstehender Neustart.** Der Server muss neu gestartet werden, damit die Konfigurationsänderungen nach der Musterimplementierung aktiviert werden.
- **Nicht verfügbar.** Dem Server ist kein Muster zugeordnet.

Wenn Sie ein Muster auf einem Server implementieren, passt XClarity Orchestrator die Einstellungen des Servers so an, dass sie dem zugeordneten Serverkonfigurationsmuster entsprechen. Wenn die Implementierung abgeschlossen ist, führt XClarity Orchestrator die Konformitätsprüfung aus, um zu überprüfen, ob die Einstellungen im zugeordneten Muster mit der Einstellung auf dem Server übereinstimmen. Anschließend wird der Konformitätsstatus für den Server aktualisiert.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Serverkonfigurationsmuster einem oder mehreren Servern zuzuordnen und es zu implementieren.

- Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Serverkonfiguration** und dann auf die Registerkarte **Zuordnen und bereitstellen**, um die Übersicht Serverkonfigurationsmuster zuzuordnen und implementieren anzuzeigen.

Zuordnen und bereitstellen


Sie können die Konfigurationseinstellungen auf mehreren Servern ändern, indem Sie ein entsprechendes Muster zuordnen und dieses Muster anschließend auf den Servern bereitstellen. ⓘ

Alle Aktionen ▾
Filter ▾
Suchen ✕

<input type="checkbox"/> Einheiten :	Status :	Zugeordnetes Muster	Konformitätsstatus :	Gruppen :
<input type="checkbox"/> Colossus-ST650V2-	⊗ Kritisch	Keine Zuordn... ▾	i Kein Muster zu	Nicht verfügbar
<input type="checkbox"/> Mehlow-ST250-1	⊗ Kritisch	Keine Zuordn... ▾	i Kein Muster zu	Nicht verfügbar
<input type="checkbox"/> OceanCat-SDV-6	⊙ Normal	Keine Zuordn... ▾	i Kein Muster zu	Nicht verfügbar

0 Ausgewählt / 3 Gesamt Zeilen pro Seite: 10 ▾

Schritt 2. Ordnen Sie einem oder mehreren Servern ein Muster zu.

1. Wählen Sie einen oder mehrere Server aus.
2. Klicken Sie auf das Symbol **Zuordnen** () , um das Dialogfenster Serverkonfigurationsmuster zuordnen zu öffnen.

Serverkonfigurationsmuster zuordnen ✕

Wählen Sie ein Muster aus, das ausgewählten Servern zugeordnet werden soll. Das Muster wird nur den entsprechenden Servern zugeordnet.

Zuzuordnendes Muster: ⓘ

Bei bestimmten Ressourcengruppen anwenden:

Muster zuordnen zu:

- Allen geeigneten Einheiten (zugeordnete Muster werden überschrieben)
- Geeigneten Einheiten ohne aktuelle Musterzuordnung
- Nur ausgewählten Einheiten (zugeordnete Muster werden überschrieben)
- Nur ausgewählten, geeigneten Einheiten ohne Musterzuordnung

3. Wählen Sie das Muster aus, das sie zuordnen möchten.

Anmerkungen:

- In dieser Liste werden alle entsprechenden Muster für die jeweiligen Server angezeigt. Die Liste ist möglicherweise unvollständig, wenn der Orchestrator-Server die entsprechenden Muster weiterhin berechnet. Schließen Sie in diesem Fall das Dialogfeld, warten Sie einige Zeit und öffnen Sie das Dialogfeld erneut.

- Wählen Sie das Muster **Keine Zuordnung** aus, um die Zuordnung eines Musters aus der ausgewählten Liste der Einheiten zu entfernen.
4. Wählen Sie die Zuordnungsregel aus. Es kann einen der folgenden Werte aufweisen.
 - **Allen geeigneten Einheiten (zugeordnete Muster werden überschrieben)**
 - **Geeigneten Einheiten ohne aktuelle Musterzuordnung**
 - **Nur ausgewählten Einheiten (zugeordnete Muster werden überschrieben)**
 - **Nur ausgewählten, geeigneten Einheiten ohne Musterzuordnung**
 5. Klicken Sie auf **Zuordnen**.

Schritt 3. Implementieren Sie das zugeordnete Muster auf bestimmten Servern.

1. Wählen Sie einen oder mehrere Server aus.

Anmerkung: Nicht unterstützte Einheitenmodelle werden mit grauem Text angezeigt und können nicht ausgewählt werden.

2. Klicken Sie auf das Symbol **Implementieren** (☑), um das Dialogfenster Serverkonfigurationsmuster implementieren zu öffnen.

3. Bestimmen Sie, wann die Aktualisierungen aktiviert werden sollen.
 - Bei **Verzögerte Aktivierung** werden alle Konfigurationsänderungen nach dem nächsten Neustart des Servers aktiviert. Der Zielservers muss manuell neu gestartet werden, damit der Implementierungsprozess fortgesetzt wird.

Wichtig: Verwenden Sie **Normal neu starten**, um den Server neu zu starten und den Aktualisierungsprozess fortzuführen. Sie dürfen *nicht* **Sofort neu starten** verwenden.
4. Klicken Sie auf **Implementieren**. 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).

Nach dieser Aufgabe

In der Übersicht Muster können Sie die folgenden Aktionen ausführen.

- Führen Sie manuell eine Prüfung der Konfigurationskonformität auf ausgewählten Servern durch, indem Sie auf **Alle Aktionen** → **Konformitätsprüfung** klicken.

- Aufheben der Musterzuordnung von einem oder mehreren Zielserversn, indem Sie das Muster **Keine Zuordnung** zuordnen.
- Leiten Sie Berichte über die Konfigurationskonformität regelmäßig an eine oder mehrere E-Mail-Adressen weiter, indem Sie auf das Symbol **Berichtsweiterleiter erstellen** (+) klicken. Der Bericht wird mithilfe der Datenfilter gesendet, die derzeit auf die Tabelle angewendet werden. Alle ein- und ausgeblendeten Tabellenspalten werden in den Bericht einbezogen. Siehe [Berichte weiterleiten](#) für weitere Informationen.
- Fügen Sie einem bestimmten Berichtsweiterleiter einen Bericht über die Konfigurationskonformität hinzu, indem Sie die Datenfilter verwenden, die derzeit auf die Tabelle angewendet werden. Klicken Sie dazu auf das Symbol **Zu Berichtsweiterleiter hinzufügen** (↗). Wenn der Berichtsweiterleiter bereits einen Bericht über die Konfigurationskonformität enthält, wird der Bericht so aktualisiert, dass die aktuellen Datenfilter angewendet werden.

Serverkonfigurationskonformität pflegen

Die Einstellungen auf einem Server können nicht mehr konform sein, wenn Einstellungen ohne den Einsatz von Konfigurationsmustern geändert werden, ein Problem beim Anwenden eines Konfigurationsmusters aufgetreten ist (z. B. wenn das Muster anhand einer früheren Firmwareversion als der erstellt wurde, die auf dem Server installiert ist) oder wenn eine Firmwareaktualisierung angewendet wird, die die Serverkonfiguration geändert hat (z. B. können Einstellungen hinzugefügt oder gelöscht werden, Einstellungsverhalten ändern sich, neue Auswahlmöglichkeiten werden hinzugefügt oder Wertbereiche ändern sich).

Zu dieser Aufgabe

Sie können den Konformitätsstatus jedes Servers auf der Seite Serverkonfiguration: Zuordnen und bereitstellen in der Spalte **Konformitätsstatus** ermitteln. Wenn ein Server nicht konform ist, bewegen Sie den Cursor über den Status, um den Grund zu ermitteln.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um Konformitätsprobleme bei der Konfiguration zu beheben.

- Übernehmen Sie ein neues Konfigurationsmuster basierend auf der aktuellen Firmwareversion (siehe [Serverkonfigurationsmuster von einem vorhandenen Server übernehmen](#)). Weisen Sie dieses Muster anschließend dem Server zu und übernehmen Sie es (siehe [Serverkonfigurationsmuster zuordnen und implementieren](#)).
- Ändern Sie das entsprechende Konfigurationsmuster, sodass die nicht konformen Einstellungen korrigiert werden, indem Sie die Musterdetails durch Klicken auf die Zeile des Musters aufrufen, die erforderlichen Änderungen vornehmen und dann auf **Speichern** klicken. Standardmäßig werden alle ermittelten Einstellungen in das Muster aufgenommen. Sie können Einstellungen aus dem Muster ausschließen, indem Sie **Einstellungen für das Muster ausschließen/einschließen** auswählen und dann die Einstellungen löschen, die Sie nicht im Muster haben wollen. Gelöschte (zum Ausschluss markierte) Einstellungen sind gelb hervorgehoben. Wenn Sie auf **Speichern** klicken, werden nur die Einstellungen aufgeführt, die im Muster enthalten sind. Wenn Sie Einstellungen ausgeschlossen haben, können Sie sie wieder einbeziehen, indem Sie auf **Einstellungen für das Muster ausschließen/einschließen** und auf **Ausgeschlossene Einstellungen anzeigen** klicken und dann die Einstellungen auswählen, die Sie einschließen möchten. Ausgewählte (zum Einbeziehen markierte) Einstellungen sind grün hervorgehoben.

Anmerkung: Die Konformitätsprüfung basiert nur auf den einbezogenen Einstellungen. Ausgeschlossene Einstellungen werden nicht überprüft.

Wenn Sie das geänderte Muster speichern, führt XClarity Orchestrator eine Konformitätsprüfung auf den Servern aus, denen dieses Muster zugeordnet ist, um festzustellen, ob die Serverkonfiguration mit dem Muster übereinstimmt. Anschließend können Sie das geänderte Muster auf nicht konformen Servern implementieren (siehe [Serverkonfigurationsmuster zuordnen und implementieren](#)).

- Erstellen Sie eine modifizierte Kopie des Konfigurationsmusters, indem Sie die Musterdetails durch Klicken auf die Zeile des Musters aufrufen, die erforderlichen Änderungen vornehmen und dann auf **Speichern unter** klicken. Weisen Sie dieses Muster anschließend dem nicht konformen Server zu und übernehmen Sie es (siehe [Serverkonfigurationsmuster zuordnen und implementieren](#)).

Betriebssysteme bereitstellen

Sie können Lenovo XClarity Orchestrator verwenden, um das BS-Images-Repository zu verwalten und Betriebssystem-Images zu implementieren.

Vorbereitende Schritte

XClarity Orchestrator dient nicht dazu, Betriebssysteme direkt auf Einheiten zu implementieren. Stattdessen sendet es Anforderungen an den entsprechenden Ressourcenmanager, um die Implementierung durchzuführen. Stellen Sie sicher, dass der Ressourcenmanager über die erforderlichen Lizenzen für die BS-Implementierungsfunktionen verfügt.

Lesen Sie sich die Implementierungshinweise durch, bevor Sie versuchen, Betriebssysteme auf Ihren verwalteten Einheiten bereitzustellen (siehe [Hinweise zur Betriebssystembereitstellung](#)).

Stellen Sie sicher, dass die Firmware auf dem verwalteten Server auf dem neuesten Stand ist (siehe [Aktualisierungen für verwaltete Ressourcen bereitstellen](#)).

Stellen Sie sicher, dass die Konfiguration auf dem verwalteten Server auf dem neuesten Stand ist (siehe [Serverkonfigurationen bereitstellen](#)).

Achtung: Es wird empfohlen, XClarity Orchestrator *nicht* für eine Bare-Metal-Implementierung des Betriebssystems auf Converged- und ThinkAgile-Einheiten zu verwenden.

Anmerkung: Stellen Sie sicher, dass Server mit XClarity Administrator v4.0 oder höher verwaltet werden.

Zu dieser Aufgabe

XClarity Orchestrator bietet eine einfache Methode, um Betriebssystem-Images auf *Bare-Metal*-Servern zu implementieren, auf denen normalerweise kein Betriebssystem installiert ist. Wenn Sie ein Betriebssystem auf einem Server implementieren, auf dem bereits ein Betriebssystem installiert ist, führt XClarity Orchestrator eine Neuinstallation durch, die die Partitionen auf den Ziellaufwerken überschreibt.

Es wird durch mehrere Faktoren bestimmt, wie viel Zeit erforderlich ist, um ein Betriebssystem auf einem Server zu implementieren.

- Die Größe des auf dem Server installierten Arbeitsspeichers hat Einfluss auf die Zeit, die der Server für den Start benötigt.
- Die Anzahl und die Typen von E/A-Adaptoren, die auf dem Server installiert sind, die sich auf die Zeit auswirken, die für die Erfassung von Bestandsdaten benötigt wird. Sie beeinflussen auch, wie lange der Start der UEFI-Firmware dauert, wenn der Server gestartet wird. Während einer Betriebssystembereitstellung wird der Server mehrmals neu gestartet.
- Die Menge an Netzwerkverkehr. Das Betriebssystem-Image wird über das Datennetzwerk oder das Betriebssystem-Implementierungsnetzwerk auf den Server heruntergeladen.
- Die Menge von RAM, Prozessoren und Festplattenspeicher, die für den Orchestrator-Server und die Ressourcenmanager verfügbar sind.

Vorgehensweise

In der folgenden Abbildung wird der Workflow für die Implementierung eines BS-Images auf einem Server dargestellt.



Schritt 1. BS-Images importieren.

Bevor Sie ein Betriebssystem auf einem Server implementieren können, müssen Sie das Betriebssystem-Image in das BS-Images-Repository im XClarity Orchestrator-Ressourcenmanager importieren. Wenn Sie ein BS-Image importieren:

- Stellt vor dem Importieren des Betriebssystems sicher, dass genügend Speicherplatz im BS-Images-Repository vorhanden ist. Wenn der Speicherplatz zum Importieren nicht ausreicht, löschen Sie ein bestehendes Image aus dem BS-Images-Repository und versuchen Sie erneut, das neue Image zu importieren.
- Erstellt ein oder mehrere Profile von diesem Image und speichert das Profil im BS-Images-Repository. Jedes *Profil* enthält das BS-Image und Installationsoptionen. Weitere Informationen zu vordefinierten BS-Image-Profilen finden Sie unter [Betriebssystem-Image-Profile](#).

Ein *Basisbetriebssystem* ist das vollständige BS-Image, das in das BS-Images-Repository importiert wurde. Das importierte Basis-Image enthält vordefinierte Profile, die die Installationskonfigurationen für dieses Image beschreiben. Sie können beim Basisbetriebssystem-Image angepasste Profile erstellen, die auf vordefinierten Profilen basieren, und für bestimmte Konfigurationen implementiert werden können.

Eine Liste der unterstützten Basis- und angepassten Betriebssysteme finden Sie unter [Unterstützte Betriebssysteme](#).

Schritt 2. **BS-Profil anpassen und zuordnen**

Betriebssystemprofile werden automatisch erstellt, wenn Sie ein Betriebssystem importieren. Die erstellten Profile basieren auf Betriebssystemtyp und -version. Sie können das Profil ändern, einschließlich BS-Anmeldeinformationen, Hostname, Netzwerk- und Speichereinstellungen, Lizenzschlüsseln und Speicherposition.

Schritt 3. **BS-Profil zuordnen und implementieren**

Sie können einem oder mehreren Zielsevern ein BS-Profil zuordnen und dieses dann auf diesen Servern implementieren. Berücksichtigen Sie dabei, dass der Server den Implementierungsstatus **Bereitstellung** aufweisen muss, damit ein Betriebssystem implementiert werden kann.

XClarity Orchestrator dient nicht dazu, Betriebssysteme direkt auf Einheiten zu implementieren. Stattdessen wird eine Anforderung zur Durchführung der Implementierung an den entsprechenden Ressourcenmanager gesendet und anschließend wird der Fortschritt der Anforderung verfolgt. XClarity Orchestrator übergibt die entsprechenden Images an den Ressourcenmanager und erstellt eine Anforderung zum Starten eines Auftrags im Ressourcenmanager, damit die Implementierung durchgeführt wird.

Lesen Sie [Hinweise zur Betriebssystembereitstellung](#), bevor Sie versuchen, ein Betriebssystem-Image zu implementieren.

Weitere Informationen zum Zuordnen und Implementieren eines BS-Profiles finden Sie unter [Ein Betriebssystem-Image implementieren](#).

Hinweise zur Betriebssystembereitstellung

Lesen Sie die folgenden Hinweise, bevor Sie versuchen, ein Betriebssystem-Image bereitzustellen.

Hinweise zum Ressourcenmanager

- Stellen Sie für durch Lenovo XClarity Administrator verwaltete Einheiten sicher, dass die XClarity Administrator-Instanz über die erforderlichen Lizenzen oder den Testzeitraum verfügt, um BS-Implementierungsfunktionen auszuführen.
- BS-Implementierung wird nicht auf Einheiten unterstützt, die von Lenovo XClarity Management Hub verwaltet werden.

Hinweise zu verwalteten Einheiten

- Stellen Sie sicher, dass die BS-Implementierungsfunktion für die Zieleinheiten unterstützt wird..
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielsever ausgeführt werden. Klicken Sie auf **Überwachung** → **Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.
- Stellen Sie sicher, dass die Firmware auf dem verwalteten Server auf dem neuesten Stand ist (siehe [Aktualisierungen für verwaltete Ressourcen bereitstellen](#)).
- Stellen Sie sicher, dass die Konfiguration auf dem verwalteten Server auf dem neuesten Stand ist (siehe [Serverkonfigurationen bereitstellen](#)). Stellen Sie außerdem sicher, dass auf der Zieleinheit kein verzögertes

oder teilweise aktiviertes Servermuster vorhanden ist. Wenn ein Servermuster auf dem verwalteten Server verzögert oder teilweise aktiviert wurde, müssen Sie den Server neu starten, damit alle Konfigurationseinstellungen übernommen werden. Versuchen Sie nicht, ein Betriebssystem auf einem Server mit einem teilweise aktivierten Servermuster zu implementieren.

Den Konfigurationsstatus des Servers ermitteln Sie über das Feld **Konfigurationsstatus** auf der Übersichtsseite für verwaltete Server (siehe [Einheitendetails anzeigen](#)).

- Stellen Sie sicher, dass ein Kennwort für das Rootkonto definiert ist, das für die Implementierung des Betriebssystems verwendet werden soll. Weitere Informationen zum Festlegen des Kennworts finden Sie unter [Betriebssystemprofile konfigurieren](#).
- Stellen Sie sicher, dass keine angehängten Medien (z. B. ISOs) auf dem Zielsystem vorhanden sind. Sorgen Sie außerdem dafür, dass keine aktiven ferneren Mediensitzungen auf dem Management-Controller geöffnet sind.
- Stellen Sie sicher, dass der Zeitstempel im BIOS auf das aktuelle Datum und die Uhrzeit eingestellt ist.
- Für ThinkSystem Server:
 - Stellen Sie sicher, dass die Option „Legacy BIOS“ deaktiviert ist. Wählen Sie im BIOS/UEFI (F1) Setup Utility **UEFI-Konfiguration** → **Systemeinstellungen** aus und stellen Sie sicher, dass die Option „Legacy BIOS“ deaktiviert ist.
 - Die XClarity Controller Enterprise-Funktion ist für die Betriebssystemimplementierung erforderlich.
- Für System x Server:
 - Stellen Sie sicher, dass die Option „Legacy BIOS“ deaktiviert ist. Wählen Sie im BIOS/UEFI (F1) Setup Utility **UEFI-Konfiguration** → **Systemeinstellungen** aus und stellen Sie sicher, dass die Option „Legacy BIOS“ deaktiviert ist.
 - Stellen Sie sicher, dass ein FoD-Schlüssel (Feature on Demand) für die Fernpräsenz installiert ist. Auf der Seite „Server“ sehen Sie, ob die Fernpräsenz-Funktion auf einem Server aktiviert, deaktiviert oder nicht installiert ist (siehe [Einheitendetails anzeigen](#)).
- Stellen Sie bei Flex System-Servern sicher, dass das Gehäuse eingeschaltet ist.
- Stellen Sie bei NeXtScale Servern sicher, dass ein FoD-Schlüssel (Feature on Demand) für die Fernpräsenz installiert ist. Auf der Seite „Server“ sehen Sie, ob die Fernpräsenz-Funktion auf einem Server aktiviert, deaktiviert oder nicht installiert ist (siehe [Einheitendetails anzeigen](#)).
- Für Converged- und ThinkAgile-Einheiten wird empfohlen, XClarity Orchestrator *nicht* für eine Bare-Metal-Implementierung des Betriebssystems zu verwenden.

Hinweise zum Betriebssystem

- Stellen Sie sicher, dass Sie über alle erforderlichen Betriebssystemlizenzen verfügen, um die installierten Betriebssysteme zu aktivieren. Sie müssen Lizenzen direkt beim Hersteller des Betriebssystems anfordern.
- Stellen Sie sicher, dass das Betriebssystem, das Sie implementieren möchten, bereits im BS-Images-Repository geladen ist. Informationen zum Importieren von Images finden Sie unter [Betriebssystem-Images importieren](#).
- Betriebssystem-Images im BS-Images-Repository werden auf bestimmten Hardwareplattformen möglicherweise nicht unterstützt. Sie können in [Lenovo OS Interoperability Guide-Website](#) bestimmen, ob ein Betriebssystem mit einem bestimmten Server kompatibel ist.
- Installieren Sie immer ein aktuelles Betriebssystem, um sicherzustellen, dass die neuesten erforderlichen In-Box-Einheitentreiber für E/A-Adapter vorhanden sind. Verwenden Sie für VMware das aktuelle für Lenovo angepasste Image für ESXi. Dieses Image unterstützt die aktuellen Adapter. Informationen zum Anfordern dieses Image finden Sie auf der [VMware-Support – Downloads-Website](#).

Weitere Informationen zu Begrenzungen für bestimmte Betriebssysteme finden Sie unter [Unterstützte Betriebssysteme](#).

Hinweise zum Netzwerkbetrieb

- Stellen Sie sicher, dass alle erforderlichen Ports geöffnet sind (siehe [Portverfügbarkeit für implementierte Betriebssysteme](#)).
- Stellen Sie sicher, dass der Ressourcenmanager für die Verwendung von Verwaltungs- und Datennetzwerken konfiguriert ist.
- Stellen Sie sicher, dass der Ressourcenmanager über die Verwaltungs- und Datennetzwerkschnittstellen mit dem Zielsystem (sowohl mit dem Baseboard Management Controller als auch mit dem Datennetzwerk der Server) kommunizieren kann. Informationen zur Angabe einer Schnittstelle, die für die Betriebssystemimplementierung verwendet wird, finden Sie unter [Netzwerkzugriff konfigurieren](#) in der Onlinedokumentation zu XClarity Administrator.

Weitere Informationen zum Bereitstellungsnetzwerk und Schnittstellen für das Betriebssystem finden Sie unter [Hinweise zum Netzwerkbetrieb](#) in der Onlinedokumentation zu XClarity Administrator.

- Wenn die Netzwerkverbindung langsam oder instabil ist, kann die Implementierung von Betriebssystemen unvorhersehbare Ergebnisse zur Folge haben.
- Sie müssen dynamisch zugewiesene IP-Adressen über DHCP verwenden. Statische IP-Adressen werden nicht unterstützt.

Weitere Informationen zum Bereitstellungsnetzwerk und Schnittstellen für das Betriebssystem finden Sie unter [Netzwerkzugriff konfigurieren](#) und [Hinweise zum Netzwerkbetrieb](#) in der Onlinedokumentation zu XClarity Administrator.

Hinweise zu Speicher- und Bootoptionen

- Sie können das Betriebssystem nur auf einem lokalen Festplattenlaufwerk installieren. Embedded Hypervisor, M.2 Treiber und SAN-Speicher werden nicht unterstützt.
- Auf jedem Server muss ein Hardware-RAID-Adapter oder SAS/SATA-HBA installiert und konfiguriert sein. Das Software-RAID, das in der Regel auf dem integrierten Intel SATA-Speicheradapter oder Speicher vorhanden ist und als JBOD eingerichtet wurde, wird nicht unterstützt; falls jedoch ein Hardware-RAID-Adapter nicht vorhanden ist, ist das Festlegen des AHCI SATA-Modus für den SATA-Adapter für die Betriebssystemimplementierung oder das Festlegen unkonfigurierter funktionierender Festplatten auf JBOD in einigen Fällen möglich. Siehe [BS-Installationsprogramm kann das Plattenlaufwerk nicht finden, auf dem Sie installieren möchten](#) in der Onlinedokumentation zu XClarity Orchestrator für weitere Informationen.
- Vergewissern Sie sich vor dem Implementieren eines Betriebssystems, dass als UEFI-Bootoption auf dem Zielsystem „Nur UEFI-Boot“ festgelegt ist. Die Bootoptionen „Nur Legacy“ und „UEFI zuerst, dann Legacy“ werden bei der Betriebssystemimplementierung nicht unterstützt.
- Auf jedem Server muss ein Hardware-RAID-Adapter installiert und konfiguriert sein.

Achtung:

- Nur Speicher, der mit Hardware-RAID eingerichtet wurde, wird unterstützt.
- Das Software-RAID, das in der Regel auf dem integrierten Intel SATA-Speicheradapter oder Speicher vorhanden ist und als JBOD eingerichtet wurde, wird nicht unterstützt; falls jedoch ein Hardware-RAID-Adapter nicht vorhanden ist, ist das Festlegen des **AHCI SATA-Modus** für den SATA-Adapter für die Betriebssystemimplementierung oder das Festlegen unkonfigurierter funktionierender Festplatten auf JBOD in einigen Fällen möglich.
- Falls ein SATA-Adapter aktiviert ist, darf der SATA-Modus *nicht auf* „IDE“ festgelegt sein.

- Ein NVMe-Speicher, der mit einem Server-Motherboard oder HBA Controller verbunden ist, wird nicht unterstützt und darf nicht in der Einheit installiert werden. Andernfalls schlägt die BS-Implementierung für den Nicht-NVMe-Speicher fehl.
- Stellen Sie sicher, dass der Secure Boot-Modus für den Server deaktiviert ist. Wenn Sie ein Betriebssystem implementieren, für das der Secure Boot-Modus aktiviert ist (z. B. Windows), müssen Sie den Secure Boot-Modus deaktivieren, das Betriebssystem implementieren und dann den Secure Boot-Modus wieder aktivieren.
- Stellen Sie bei ThinkServer Servern sicher, dass die folgenden Anforderungen erfüllt sind.
 - Die Booteinstellungen auf dem Server müssen eine Speicher-OpROM-Richtlinie mit der Einstellung `UEFI only` enthalten.
 - Wenn Sie ESXi implementieren und PXE-bootfähige Netzwerkadapter vorhanden sind, deaktivieren Sie die PXE-Unterstützung auf den Netzwerkadaptern, bevor Sie das Betriebssystem implementieren. Die Implementierung ist abgeschlossen. Falls gewünscht, können Sie die PXE-Unterstützung nun wieder aktivieren.
 - Wenn Sie ESXi implementieren und sich abgesehen vom Laufwerk, auf dem das Betriebssystem installiert werden soll, weitere bootfähige Einheiten in der Bootreihenfolge befinden, entfernen Sie die bootfähigen Einheiten aus der Bootreihenfolge, bevor Sie das Betriebssystem implementieren. Wenn die Implementierung abgeschlossen ist, können Sie die bootfähigen Einheiten wieder zur Liste hinzufügen. Stellen Sie sicher, dass das installierte Laufwerk ganz oben in der Liste steht.

Weitere Informationen zu den Einstellungen für Speicherpositionen finden Sie unter [Betriebssystemprofile konfigurieren](#).

Unterstützte Betriebssysteme

Lenovo XClarity Orchestrator unterstützt die Implementierung verschiedener Betriebssysteme. In das BS-Images-Repository von XClarity Orchestrator können nur unterstützte Versionen der Betriebssysteme geladen werden.

Wichtig:

- Weitere Informationen zu Einschränkungen bei der Betriebssystemimplementierung für bestimmte Einheiten finden Sie unter [Unterstützte Hardware und Software](#) in der Onlinedokumentation zu XClarity Orchestrator.
- Die Funktion zur Verschlüsselungsverwaltung von XClarity Orchestrator ermöglicht auch das Einschränken der Kommunikation mit bestimmten Mindest-SSL/TLS-Modi. Beachten Sie, dass bei Auswahl von TLS 1.2 nur Betriebssysteme mit einem Installationsprozess, der TLS 1.2 und starke Verschlüsselungsalgorithmen unterstützt, über den XClarity Orchestrator bereitgestellt werden können.
- Betriebssystem-Images im BS-Images-Repository werden auf bestimmten Hardwareplattformen möglicherweise nicht unterstützt. Sie können in [Lenovo OS Interoperability Guide-Website](#) bestimmen, ob ein Betriebssystem mit einem bestimmten Server kompatibel ist.
- Betriebssystem- und Hypervisor-bezogene Kompatibilitäts- und Supportinformationen sowie Ressourcen für Server und Lösungen von Lenovo finden Sie unter [Support-Center-Website für Server-BS](#).

In der folgenden Tabelle sind die 64-Bit-Betriebssysteme aufgelistet, die von XClarity Orchestrator bereitgestellt werden können.

Betriebssystem	Versionen	Hinweise
Red Hat® Enterprise Linux (RHEL) Server	7.2 and later 8.x	Enthält KVM Anmerkungen: <ul style="list-style-type: none"> • Alle vorhandenen und zukünftigen Nebenversionen werden unterstützt, es sei denn, wenn nicht anders vermerkt. • Wenn Sie die DVD-Version des BS-Images importieren, wird nur DVD1 unterstützt. • Bei der Installation von RHEL auf ThinkSystem-Servern wird RHEL v7.4 oder höher empfohlen.
SUSE® Linux Enterprise Server (SLES)	12.3 and later 15.2 and later	Einschließlich KVM- und Xen-Hypervisoren Anmerkungen: <ul style="list-style-type: none"> • Alle vorhandenen und zukünftigen Service Packs werden unterstützt, wenn nicht anders vermerkt. • Wenn Sie die DVD-Version des BS-Images importieren, wird nur DVD1 unterstützt.
VMware vSphere® Hypervisor (ESXi)	6.0.x 6.5.x 6.7.x 7.0.x	VMware vSphere Hypervisor (ESXi)-Basis-Images und angepasste Lenovo VMware ESXi-Images werden unterstützt. Die Lenovo VMware ESXi-Images werden an bestimmte Hardware angepasst und ermöglichen eine Onlineplattformverwaltung, z. B. das Aktualisieren und Konfigurieren von Firmware, Plattformdiagnosen und erweiterte Hardware-Alerts. Die Lenovo Verwaltungstools unterstützen außerdem eine einfachere Verwaltung von ESXi mit ausgewählten System x Servern. Dieses Image steht unter VMware-Support – Downloads-Website zum Herunterladen zur Verfügung. Bei der für das Image bereitgestellten Lizenz handelt es sich um eine kostenlose 60-Tage-Testversion. Sie sind dafür verantwortlich, dass alle Lizenzbestimmungen für VMware eingehalten werden. Wichtig: <ul style="list-style-type: none"> • Alle vorhandenen und zukünftigen Aktualisierungspakete werden unterstützt, wenn nicht anders vermerkt. • ESXi-Basis-Images (ohne Lenovo Anpassung) enthalten nur die grundlegenden Inbox-Einheitentreiber für Netzwerk und Speicher. Das Basis-Image umfasst keine Out-of-Box-Einheitentreiber (die in angepassten Lenovo VMware ESXi-Images vorhanden sind). • Für einige Versionen der angepassten Lenovo VMware ESXi-Images sind möglicherweise separate Images für ThinkSystem, System x und ThinkServer verfügbar. Im BS-Images-Repository kann jeweils nur ein Image für eine bestimmte Version vorhanden sein. • Die ESXi-Implementierung wird nicht für bestimmte ältere Server unterstützt. Weitere Informationen zu unterstützten Servern finden Sie auf der Lenovo OS Interoperability Guide-Website.

Betriebssystem-Image-Profil

Durch den Import eines BS-Images werden vordefinierte BS-Profile generiert. Jedes vordefinierte Profil enthält das BS-Image und die Installationsoptionen für dieses Image.

Sie können die Profile ändern, um Anmeldeinformationen, Netzwerk- und Speichereinstellungen zu konfigurieren. Sie können auch neue Profile basierend auf den vordefinierten BS-Richtlinien erstellen. Siehe [Betriebssystemprofile konfigurieren](#) für weitere Informationen.

Der folgenden Tabelle sind die vordefinierten BS-Profile aufgeführt, die erstellt werden, wenn Sie ein Betriebssystem-Image importieren. Diese Tabelle enthält außerdem die Pakete, die in den einzelnen Profilen enthalten sind.

Betriebssystem	Profil	Pakete im Profil	
Red Hat Enterprise Linux (RHEL) Anmerkung: Enthält KVM	Basic	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimal	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualisierung	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libcups lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 12.3 und höher	Basic	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>	
	Minimal	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>	

Betriebssystem	Profil	Pakete im Profil
	Virtualisierung – KVM	<pre> <pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> </pre>
	Virtualisierung – Xen	<pre> <pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> </pre>
SUSE Linux Enterprise Server (SLES) 15.2 und höher	Basic	<pre> <pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package> </pre>
	Minimal	<pre> <pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package> </pre>
	Virtualisierung – KVM	<pre> <pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package> </pre>

Betriebssystem	Profil	Pakete im Profil
	Virtualisierung – Xen	<pre> <pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package> </pre>
VMware vSphere® Hypervisor (ESXi)	Virtualisierung	VMware vSphere Hypervisor (ESXi)-Basis-Images und angepasste Lenovo VMware ESXi-Images werden unterstützt.

Portverfügbarkeit für implementierte Betriebssysteme

Einige Ports werden von bestimmten Betriebssystemprofilen blockiert. In den folgenden Tabellen sind die offenen (nicht blockierten) Ports aufgeführt.

Stellen Sie sicher, dass der Hypervisor, auf dem die Lenovo XClarity Orchestrator-Einheit ausgeführt wird, Netzwerkverkehr (TCP/UDP) an den Ports 139, 445, 3001, 3900 und 8443 ermöglicht. Diese sind für die Betriebssystembereitstellung erforderlich.

RHEL-Virtualisierungsprofil

Standardmäßig blockiert das Red Hat Enterprise Linux (RHEL)-Virtualisierungsprofil alle bis auf die in der folgenden Tabelle aufgeführten Ports.

Tabelle 1. Portverfügbarkeit bei RHEL-Virtualisierungsprofilen

Port	TCP oder UDP	Richtung	Beschreibung der Kommunikation
22	TCP	Eingehend	SSH-Kommunikation
53	TCP, UDP	Ausgehend/Eingehend	Kommunikation mit RHEL KVM-Netzwerkeinheiten
67	TCP, UDP	Ausgehend/Eingehend	Kommunikation mit RHEL KVM-Netzwerkeinheiten
161	UDP	Ausgehend	Kommunikation mit SNMP-Agenten
162	UDP	Eingehend	Kommunikation mit SNMP-Agenten
427	TCP, UDP	Ausgehend/Eingehend	Kommunikation mit SLP-Serviceagent, SLP-Verzeichnisagent
3001	TCP	Ausgehend/Eingehend	Kommunikation mit dem Image-Implementierungsservice der Verwaltungssoftware
15988	TCP	Ausgehend	CIM-XML über HTTP-Kommunikation

Tabelle 1. Portverfügbarkeit bei RHEL-Virtualisierungsprofilen (Forts.)

Port	TCP oder UDP	Richtung	Beschreibung der Kommunikation
15989	TCP	Ausgehend	CIM-XML über HTTP-Kommunikation
49152 - 49215	TCP	Ausgehend/Eingehend	Kommunikation für virtuelle KVM-Server

RHEL-Basis- und Minimalprofile

Standardmäßig blockieren die RHEL-Basis- und Minimalprofile alle bis auf die in der folgenden Tabelle aufgeführten Ports.

Tabelle 2. Portverfügbarkeit bei RHEL-Basis- und Minimalprofilen

Port	TCP oder UDP	Richtung	Beschreibung der Kommunikation
22	TCP	Eingehend	SSH-Kommunikation
3001	TCP	Ausgehend/Eingehend	Kommunikation mit dem Image-Implementierungsservice der Verwaltungssoftware

SLES-Virtualisierungs-, Basis- und Minimalprofile

Bei SUSE Linux Enterprise Server (SLES) werden einige offene Ports dynamisch auf Grundlage von Betriebssystemversion und Profilen zugewiesen. Eine vollständige Liste aller offenen Ports finden Sie in der Dokumentation für SUSE Linux Enterprise Server.

VMware ESXi Virtualisierungsprofil

Eine komplette Liste aller nicht belegten Ports für VMware vSphere Hypervisor (ESXi) mit Lenovo Anpassung finden Sie in der VMware-Dokumentation für ESXi auf der [VMware Knowledge Base-Website](#).

Betriebssystem-Images importieren

Bevor Sie ein lizenziertes Betriebssystem auf verwalteten Server implementieren können, müssen Sie zunächst das Image in das BS-Images-Repository importieren.

Zu dieser Aufgabe

Informationen zu Betriebssystem-Images, die Sie importieren und implementieren können, einschließlich unterstützter Basis- und angepasster Betriebssysteme, finden Sie unter [Unterstützte Betriebssysteme](#).

Nur bei ESXi können Sie mehrere ESXi-Images mit derselben Haupt-/Nebenversion in das BS-Images-Repository importieren.

Nur bei ESXi können Sie mehrere angepasste ESXi-Images mit derselben Haupt-/Nebenversion und Buildnummer in das BS-Images-Repository importieren.

Wenn Sie ein Betriebssystem-Image importieren, XClarity Orchestrator:

- Stellt vor dem Importieren des Betriebssystems sicher, dass genügend Speicherplatz im BS-Images-Repository vorhanden ist. Wenn der Speicherplatz zum Importieren nicht ausreicht, löschen Sie ein bestehendes Image aus dem Repository und versuchen Sie erneut, das neue Image zu importieren.

- Erstellt ein oder mehrere Profile von diesem Image und speichert das Profil im BS-Images-Repository. Jedes *Profil* enthält das BS-Image und Installationsoptionen. Weitere Informationen zu vordefinierten BS-Image-Profilen finden Sie unter [Betriebssystem-Image-Profile](#).

Anmerkung: Für Internet Explorer sowie Microsoft Edge-Webbrowser besteht ein Upload-Limit von 4 GB. Wenn die importierte Datei größer als 4 GB ist, sollten Sie einen anderen Webbrowser verwenden, z. B. Chrome oder Firefox.

Vorgehensweise

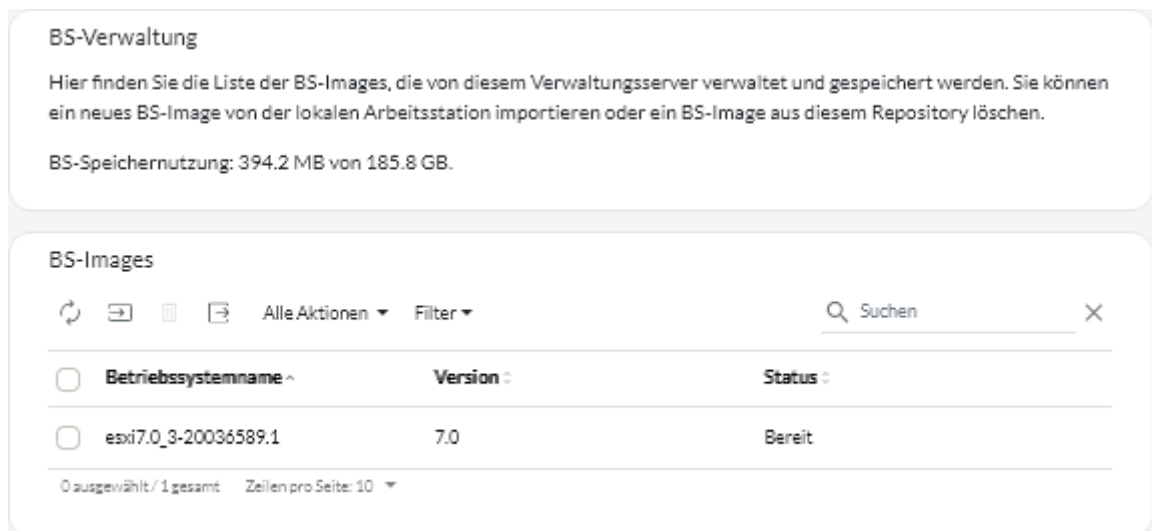
Gehen Sie wie folgt vor, um ein Betriebssystem-Image in das BS-Images-Repository zu importieren.

Schritt 1. Rufen Sie ein lizenziertes ISO-Image des Betriebssystems ab.

Anmerkung: Sie müssen zugehörige Lizenzen für das Betriebssystem selbst anfordern.

Schritt 2. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔑) → **BS-Implementierung** und dann auf die Registerkarte **BS-Verwaltung**, um die Seite BS-Verwaltung anzuzeigen.

Schritt 3. Klicken Sie im linken Navigationsbereich auf **BS-Images**, um die Übersicht BS-Images zu öffnen.



Schritt 4. Klicken Sie auf das Symbol **Dateien importieren** (📁), um das Dialogfeld BS-Images importieren anzuzeigen.

Schritt 5. Ziehen und legen Sie das ISO-Image ab, das Sie importieren möchten, oder klicken Sie auf **Durchsuchen**, um das gewünschte ISO-Image zu finden.

Schritt 6. **Optional:** Wählen Sie einen Prüfsummentyp aus, kopieren Sie die Prüfsumme und fügen Sie diese in das Textfeld ein.

Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit das hochgeladene BS-Image auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn das hochgeladene Image dem Prüfsummenwert entspricht, können Sie mit der Bereitstellung fortfahren. Andernfalls müssen Sie das Image erneut hochladen oder den Prüfsummenwert überprüfen.

Die folgenden Prüfsummentypen werden unterstützt: MD5, SHA1 und SHA256.

Schritt 7. Klicken Sie auf **Importieren**.

XClarity Orchestrator lädt das BS-Image in das BS-Images-Repository hoch und fügt die vordefinierten BS-Profilen zur Registerkarte **BS-Profil** hinzu.

Tipp: Das ISO-Image wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und die Leistung des Netzwerks, wie lange das Importieren des Images dauert.

Nach dieser Aufgabe

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Löschen eines ausgewählten BS-Images über das Symbol **Löschen** (🗑️).
- Anzeigen und Bearbeiten von BS-Profilen. Klicken Sie dazu auf die XClarity Orchestrator-Menüleiste, anschließend auf **Bereitstellung** (🔧) → **BS-Implementierung** und auf die Registerkarte **BS-Profil**. Wählen Sie das Profil aus und klicken Sie auf das Symbol **Bearbeiten** (✎) (siehe „Betriebssystemprofile konfigurieren“).
- Löschen von BS-Profilen. Klicken Sie dazu auf die XClarity Orchestrator-Menüleiste, anschließend auf **Bereitstellung** (🔧) → **BS-Implementierung** und auf die Registerkarte **BS-Profil**. Wählen Sie die Profile aus und klicken Sie auf das Symbol **Löschen** (🗑️).

Anmerkung: Wenn Sie das letzte verbleibende vordefinierte Profil für ein Betriebssystem löschen, wird auch das Betriebssystem gelöscht.

Betriebssystemprofile konfigurieren

Betriebssystemprofile werden automatisch erstellt, wenn Sie ein Betriebssystem importieren. Die erstellten Profile basieren auf Betriebssystemtyp und -version. Sie können das Profil ändern, einschließlich BS-Anmeldeinformationen, Hostname, Netzwerk- und Speichereinstellungen, Lizenzschlüsseln und Speicherposition.

Vorbereitende Schritte

Lesen Sie die Hinweise, bevor Sie ein Betriebssystem auf einer verwalteten Servereinheit implementieren. Informationen hierzu finden Sie unter [Hinweise zur Betriebssystembereitstellung](#).

Vorgehensweise

Gehen Sie wie folgt vor, um ein BS-Profil für die Implementierung zu konfigurieren.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **BS-Implementierung** und dann auf die Registerkarte **BS-Profil**, um die Seite BS-Profil anzuzeigen.

Schritt 2. Wählen Sie das BS-Profil aus.

Schritt 3. Klicken Sie auf das Symbol **Bearbeiten** (✎), um die Übersicht BS-Profildetails anzuzeigen.

Schritt 4. Konfigurieren Sie die Profilattribute.

- **Name.** Durch Ändern des Profilnamens wird ein neues BS-Profil erstellt.
- **Beschreibung.** Ändern Sie die Beschreibung für dieses BS-Profil.
- **BS-Anmeldeinformationen.** Geben Sie die BS-Anmeldeinformationen ein, die für die Anmeldung des Administratoraccounts am Betriebssystem verwendet werden sollen.
- **Hostname.** Wählen Sie aus, welcher Hostname verwendet werden soll. Sie können einen der folgenden Werte auswählen.
 - **Standard-Hostname verwenden.** (Standard) Der Hostname ist „Knoten“, gefolgt von den ersten 11 Zeichen der Einheiten-ID (z. B. nodeABC31213310).
- **Netzwerkeinstellungen.** Wählen Sie die IP-Einstellungen für dieses Profil aus. Sie können einen der folgenden Werte auswählen.
 - **DHCP.** (Standard) Verwenden Sie die vorhandene DHCP-Infrastruktur, um den Servern IPv4-Adressen zuzuordnen.
- **MAC-Adresseinstellung.** Wählen Sie die MAC-Adresse des Anschlusses am Host aus, über den das Betriebssystem installiert wird. Sie können einen der folgenden Werte auswählen.

Anmerkung: Virtuelle Netzwerkanschlüsse werden nicht unterstützt. Verwenden Sie keinen physischen Netzwerkanschluss, um mehrere virtuelle Netzwerkanschlüsse zu simulieren.

- **AUTO verwenden.** (Standard) Erkennt automatisch die Ethernet-Anschlüsse, die konfiguriert und zur Bereitstellung verwendet werden können. Standardmäßig wird die erste erkannte MAC-Adresse (Anschluss) verwendet. Wenn eine Konnektivität über eine andere MAC-Adresse erkannt wird, wird der Server automatisch neu gestartet, um die erkannte MAC-Adresse für die Bereitstellung zu verwenden. Der XClarity Administrator Ressourcenmanager kann die Netzwerkanschlüsse in den Steckplätzen 1–16 automatisch erkennen. Mindestens

ein Anschluss an den Steckplätzen 1–16 muss eine Verbindung zum zuständigen Ressourcenmanager haben.

Wenn Sie für die MAC-Adresse einen Netzwerkanschluss in Steckplatz 17 oder höher verwenden möchten, können Sie das Programm „AUTO“ nicht verwenden.

- **Storage.** Wählen Sie die Speicherposition aus, an der Sie das Betriebssystem-Image implementieren möchten.
 - **Plattenlaufwerk verwenden.** Installieren Sie das Betriebssystem-Image auf der zuerst aufgelisteten lokalen RAID-Festplatte auf dem verwalteten Server. Nur mit einem RAID-Controller oder einem SAS/SATA-HBA verbundene Festplatten werden unterstützt.

Wenn die RAID-Konfiguration auf dem Server nicht ordnungsgemäß konfiguriert wurde oder inaktiv ist, kann der Orchestrator-Server die lokale Festplatte möglicherweise nicht erkennen. Um das Problem zu beheben, aktivieren Sie die RAID-Konfiguration mithilfe von Konfigurationenmustern (siehe [Serverkonfigurationsmuster von einem vorhandenen Server übernehmen](#)) oder über die RAID-Verwaltungssoftware auf dem Server.




Anmerkungen:

- Falls auch ein M.2-Laufwerk vorhanden ist, muss das Festplattenlaufwerk für die Hardware-RAID konfiguriert werden.
- Wenn ein SATA-Adapter aktiviert ist, darf der SATA-Modus *nicht* auf **IDE** festgelegt sein.
- Bei ThinkServer-Servern ist die Konfiguration nur über die RAID-Verwaltungssoftware auf dem Server verfügbar.

Schritt 5. Klicken Sie auf **Speichern**.

Nach dieser Aufgabe

Sie können die folgenden Aktionen durchführen.

- Einem oder mehreren Servern ein BS-Profil auf der Registerkarte **Zuordnen und bereitstellen** zuordnen. Wählen Sie dazu Server aus und klicken Sie dann auf das Symbol **Zuordnen** () oder klicken Sie auf das Symbol **Zuordnen** () und wählen Sie dann eine Gruppe von Servern aus. Nachdem Sie das BS-Profil ausgewählt haben, können Sie das BS-Profil zuordnen.
 - **Allen geeigneten Einheiten (zugeordnete Profile werden überschrieben)**
 - **Geeigneten Einheiten ohne aktuelle Profilzuordnung**
 - **Nur ausgewählten Einheiten (zugeordnete Profile werden überschrieben)**
 - **Nur ausgewählten, geeigneten Einheiten ohne Profilzuordnung**
- Ausgewählte BS-Images über das Symbol **Löschen** () löschen.

Anmerkung: Wenn Sie das letzte verbleibende vordefinierte Profil für ein Betriebssystem löschen, wird auch das Betriebssystem gelöscht.

Ein Betriebssystem-Image implementieren

Sie können Lenovo XClarity Orchestrator verwenden, um ein Betriebssystem auf Ihren verwalteten Servern zu implementieren.

Vorbereitende Schritte

Lesen Sie sich die Überlegungen zur Betriebssystemimplementierung durch, bevor Sie versuchen, Betriebssysteme auf Ihren verwalteten Servern bereitzustellen (siehe [Hinweise zur Betriebssystembereitstellung](#)).

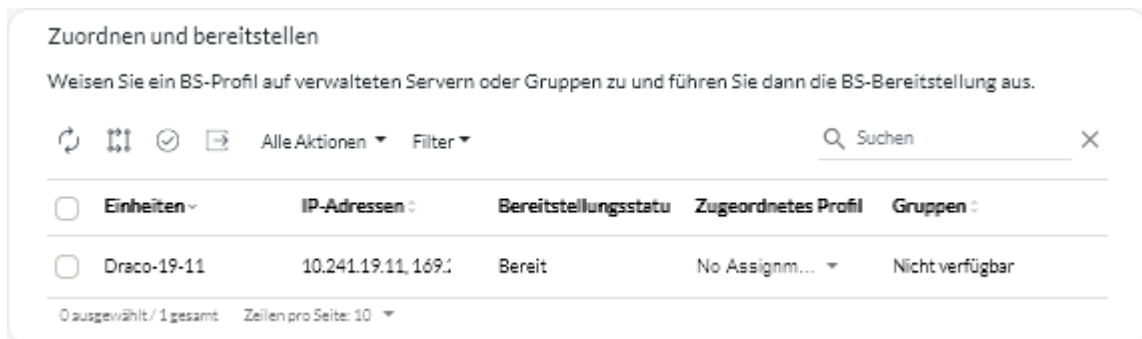
Achtung: Wenn auf dem Server bereits ein Betriebssystem installiert ist, wird das aktuelle Betriebssystem durch die Implementierung eines BS-Image-Profiles überschrieben.

Vorgehensweise

Verwenden Sie eine der folgenden Vorgehensweisen, um ein Betriebssystem-Image auf einem oder mehreren verwalteten Servern zu implementieren.

- **Auf bestimmten Einheiten**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **BS-Implementierung** und dann auf die Registerkarte **Zuordnen und bereitstellen**, um die Übersicht Zuordnen und bereitstellen anzuzeigen.



2. Wählen Sie mindestens einen Server aus, auf dem Sie ein Betriebssystem implementieren möchten.
3. Wählen Sie für jeden Zielsever das zu implementierende BS-Profil aus der Dropdown-Liste in der Spalte **BS-Profil** aus. Stellen Sie sicher, dass Sie ein BS-Profil auswählen, das mit dem Zielsever kompatibel ist.
4. Überprüfen Sie, ob der Implementierungsstatus in der Spalte **Status** für alle ausgewählten Server „Bereitstellung“ ist.
5. Klicken Sie auf das Symbol **Implementieren** (☑), um das Dialogfenster Profil bereitstellen anzuzeigen.
6. Klicken Sie auf das Symbol **Implementieren**, um die Betriebssystemimplementierung einzuleiten. 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).

- **Auf allen Einheiten in einer bestimmten Gruppe**

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **BS-Implementierung** und dann auf die Registerkarte **Zuordnen und bereitstellen**, um die Übersicht Zuordnen und bereitstellen anzuzeigen.
2. Ordnen Sie der Servergruppe ein BS-Profil zu.
 - a. Klicken Sie auf das Symbol **Zuordnen** (↔), um das Dialogfenster Profil zuordnen zu öffnen.

Profil zuordnen
✕

Wählen Sie ein Profil aus, das mehreren Ressourcen zugeordnet wird. Das Profil wird nur geeigneten Ressourcen zugeordnet.

Zuzuordnendes Profil Profil auswählen*

Bei bestimmten Ressourcengruppen anwenden: Einheitengruppen

Profil zuordnen zu:

- Allen geeigneten Einheiten (zugeordnete Profile werden überschrieben)
- Geeigneten Einheiten ohne aktuelle Profilzuordnung
- Nur ausgewählten Einheiten (zugeordnete Profile werden überschrieben)
- Nur ausgewählten, geeigneten Einheiten ohne Profilzuordnung

Übernehmen

- b. Wählen Sie das Profil aus, was zugeordnet werden soll.
 - c. Wählen Sie die Gruppe der Einheiten aus, die zugeordnet werden sollen.
 - d. Wählen Sie aus, welche Einheiten in der Gruppe zugeordnet werden sollen.
 - **Allen geeigneten Einheiten (zugeordnete Profile werden überschrieben)**
 - **Geeigneten Einheiten ohne aktuelle Profilzuordnung**
 - **Nur ausgewählten Einheiten (zugeordnete Profile werden überschrieben)**
 - **Nur ausgewählten, geeigneten Einheiten ohne Profilzuordnung**
 - e. Klicken Sie auf **Implementieren**.
3. Klicken Sie auf das Symbol **Implementieren** (☑), um das Dialogfenster Profil bereitstellen anzuzeigen.

Profil bereitstellen
✕

Klicken Sie auf "Bereitstellen", um das Profil auf den ausgewählten Servern bereitzustellen und zu aktivieren.

HINWEIS: Der Prozess wird als Job im Hintergrund ausgeführt wird und kann einige Minuten dauern. Sie können zur Seite Jobs wechseln, um den Fortschritt des Jobstatus anzuzeigen.

Bei bestimmten Ressourcengruppen anwenden: Einheitengruppen

Bereitstellen

4. Wählen Sie die Gruppe der Einheiten aus, auf denen das zugeordnete BS-Profil implementiert werden soll.
5. Klicken Sie auf das Symbol **Implementieren**, um die Betriebssystemimplementierung einzuleiten. 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).

Aktualisierungen für verwaltete Ressourcen bereitstellen

Sie können Lenovo XClarity Orchestrator verwenden, um aktuelle Softwareversionen auf Lenovo XClarity Administrator-Ressourcenmanagern und verwalteten Servern zu verwalten. Mithilfe des Aktualisierungskatalogs können Sie herausfinden, welche Softwareversionen verfügbar sind. Verwenden Sie Aktualisierungskonformitätsrichtlinien, um zu ermitteln, welche Ressourcen basierend auf benutzerdefinierten Kriterien aktualisiert werden müssen, und implementieren Sie dann die gewünschten Aktualisierungen für diese Ressourcen.

Vorgehensweise

In der folgenden Abbildung wird der Ablauf der Aktualisierung von verwalteten Servern dargestellt.



Schritt 1. Katalog aktualisieren

Das *Repository für Aktualisierungen* enthält einen Katalog und die Aktualisierungspakete, die auf verwaltete Ressourcen angewendet werden können.

Der *Katalog* enthält Informationen zu aktuell verfügbaren Aktualisierungen. Der Katalog organisiert die Aktualisierungen nach Ressourcentypen (Plattformen) und Komponenten. Wenn Sie den Katalog aktualisieren, ruft XClarity Orchestrator Informationen zu den neuesten verfügbaren Aktualisierungen von der Lenovo Support-Website ab und speichert die Informationen im Repository für Aktualisierungen.

Wichtig: XClarity Orchestrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und herunterzuladen.

Wenn neue Aktualisierungspakete verfügbar werden, müssen Sie die jeweiligen Aktualisierungspakete importieren, bevor Sie eine Aktualisierung anwenden können. Beim Aktualisieren des Katalogs werden die Aktualisierungspakete nicht automatisch importiert.

Bei der Erstinstallation von XClarity Orchestrator ist das Repository für Aktualisierungen leer.

Schritt 2. Aktualisierungspakete in das Repository herunterladen oder importieren

Wenn XClarity Orchestrator mit dem Internet verbunden ist, können Sie im Aktualisierungskatalog aufgeführte Aktualisierungspakete direkt über die Lenovo Support-Website herunterladen. Wenn XClarity Orchestrator nicht mit dem Internet verbunden ist, können Sie Aktualisierungspakete, die

Sie zuvor von der [Lenovo Website zu Support für Rechenzentrum](#) heruntergeladen haben, manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Orchestrator-Host importieren.

Wenn Sie nur eine Nebenversion herunterladen, werden erforderlichen Aktualisierungspakete trotzdem heruntergeladen.

Wenn Sie manuell Repository-Pakete importieren, müssen Sie die Nutzlastdatei (.tgz), Metadatenfile (.xml), Änderungsprotokoll (.chg) und Readme (.txt) importieren.

Wenn Sie Aktualisierungen manuell importieren, müssen Sie die erforderlichen Dateien auf Basis des Ressourcentyps importieren.

- Importieren Sie für ThinkSystem V3 Server das einzelne Aktualisierungspaket (*.zip). Diese ZIP-Datei enthält die Nutzlastdatei, Metadatenfiles (mehrere *.json), die Änderungsprotokollfile (*.chg) und die Readme-Datei (*.txt).
- Importieren Sie für ThinkEdge Client-Einheiten die Nutzlastdatei (Windows.exe). Die Readme-Datei (.txt) ist optional. Beachten Sie, dass derzeit nur die Aktualisierung **BIOS-Flash-Dienstprogramm für Windows** unterstützt wird.
- Importieren Sie für XClarity Management Hub und XClarity Management Hub 2.0 die einzelne Aktualisierungspaketdatei (.tgz). Diese Datei enthält die Nutzlast-, Metadaten-, Änderungsprotokoll- und Readme-Dateien.
- Importieren Sie für alle anderen Ressourcen (einschließlich XClarity Administrator, ThinkEdge Server, ThinkSystem V1 und V2 und ältere Einheiten) die Nutzlastdatei (.zip, .uxz, .tar.gz, .tar, .bin), die Metadatenfile (.xml), das Änderungsprotokoll (.chg) und die Readme-Datei (.txt).

Weitere Informationen zum Importieren von Aktualisierungen finden Sie im Abschnitt [Aktualisierungen herunterladen und importieren](#).

Schritt 3. **Aktualisierungskonformitätsrichtlinien erstellen und zuordnen**

Aktualisierungskonformitätsrichtlinien stellen sicher, dass die Software oder Firmware auf bestimmten verwalteten Ressourcen auf dem neuesten oder einem bestimmten Stand ist. Dazu werden Ressourcen markiert, die Ihre Aufmerksamkeit erfordern. Eine Aktualisierungskonformitätsrichtlinie legt fest, welche Ressourcen überwacht werden und welche Software- oder Firmwareversion zur Erhaltung der Konformität installiert sein muss. XClarity Orchestrator verwendet die Richtlinien dann, um den Status von verwalteten Ressourcen zu überprüfen und nicht konforme Ressourcen zu erkennen.

Bei der Erstellung einer Aktualisierungskonformitätsrichtlinie können Sie festlegen, dass XClarity Orchestrator eine Ressource kennzeichnet, wenn deren Software oder Firmware veraltet ist.

Nachdem eine Aktualisierungskonformitätsrichtlinie einer Ressource zugeordnet wurde, überprüft XClarity Orchestrator den Konformitätsstatus der Ressource, wenn das Repository für Aktualisierungen geändert wird. Wenn die Software oder Firmware auf der Ressource nicht mit der zugewiesenen Richtlinie übereinstimmt, markiert XClarity Orchestrator die Ressource entsprechend den mit der Seite *Übernehmen / Aktivieren* in der Aktualisierungskonformitätsrichtlinie festgelegten Regeln als nicht konform.

Sie können beispielsweise eine Aktualisierungskonformitätsrichtlinie erstellen, die die Basis-Softwareversion für XClarity Administrator definiert, und diese Richtlinie dann allen XClarity Administrator-Ressourcenmanagern zuordnen. Wenn der Aktualisierungskatalog aktualisiert und eine neue Aktualisierung heruntergeladen oder importiert wird, sind die XClarity Administrator-Instanzen möglicherweise nicht mehr konform. Wenn dies der Fall ist, aktualisiert XClarity Orchestrator die Seite *Übernehmen/Aktivieren*, um zu zeigen, welche XClarity Administrator-Instances nicht konform sind, und generiert einen Alert.

Weitere Informationen zu Aktualisierungskonformitätsrichtlinien finden Sie unter [Aktualisierungskonformitätsrichtlinien erstellen und zuordnen](#).

Schritt 4. Aktualisierungen übernehmen und aktivieren

XClarity Orchestrator wendet Aktualisierungen nicht automatisch an. Um Softwareressourcen zu aktualisieren, müssen Sie die Aktualisierung für ausgewählte Ressourcen, die nicht mit der zugewiesenen Aktualisierungskonformitätsrichtlinie konform sind, manuell anwenden und aktivieren.

XClarity Orchestrator aktualisiert Ressourcen nicht direkt. Stattdessen wird eine Anforderung zur Durchführung der Aktualisierung an den entsprechenden Ressourcenmanager gesendet und anschließend wird der Fortschritt der Anforderung verfolgt. XClarity Orchestrator identifiziert die für die Aktualisierung erforderlichen Abhängigkeiten, stellt sicher, dass die Zielressourcen in der richtigen Reihenfolge aktualisiert werden, übergibt die entsprechenden Aktualisierungspakete an den Ressourcenmanager und erstellt eine Anforderung zum Starten eines Jobs im Ressourcenmanager, damit die Aktualisierung durchgeführt wird.

Weitere Informationen zum Anwenden von Aktualisierungen finden Sie unter [Aktualisierungen für Ressourcenmanager anwenden und aktivieren](#) und [Aktualisierungen für verwaltete Server anwenden und aktivieren](#).

Bereitstellungshinweise aktualisieren

Lesen Sie die folgenden wichtigen Hinweise, bevor Sie Aktualisierungen mit Lenovo XClarity Orchestrator durchführen.

- Um optimale Leistung zu erzielen, stellen Sie sicher, dass auf den Lenovo XClarity Administrator-Ressourcenmanagern v3.2.1 oder höher ausgeführt wird.
- Achten Sie darauf, dass das Repository für Aktualisierungen die Aktualisierungspakete enthält, die Sie übernehmen möchten. Ist dies nicht der Fall, dann aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Aktualisierungen herunter (siehe [Aktualisierungen herunterladen und importieren](#)).
- Stellen Sie sicher, dass derzeit keine Jobs auf der Zielressource ausgeführt werden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt.
- Wenn der Ressource eine Aktualisierungskonformitätsrichtlinie zugeordnet ist, die zu einer Konformitätsverletzung führt, müssen Sie diese durch die Anpassung der Konformitätsrichtlinie oder durch die Zuordnung einer anderen Richtlinie beheben.
- Wenn Sie ein Aktualisierungspaket mit Aktualisierungen für verschiedene Komponenten installieren, werden alle Komponenten aktualisiert, für die das Aktualisierungspaket übernommen wird.

Hinweise zu Ressourcen

- Die Aktualisierungsfunktion unterstützt die Aktualisierung nur von Servern und Ressourcenmanagern. Für ThinkSystem SR635 und SR655 werden nur BMC- und UEFI-Firmwareaktualisierungen unterstützt.

Bei ThinkSystem und ThinkAgile Einheiten werden Firmwareaktualisierungen für Baseboard Management Controller und UEFI-Sicherungsgruppen nicht unterstützt. Aktualisieren Sie stattdessen die primäre Gruppe und aktivieren Sie dann die automatisierte Hochstufung.

- Bevor Sie verwaltete Einheiten aktualisieren, lesen Sie die wichtigen Hinweise zur Aktualisierung (siehe [Hinweise zur Firmwareaktualisierung](#) in der Onlinedokumentation zu XClarity Administrator).
- Bevor Sie die XClarity Administrator Ressourcenmanager aktualisieren, lesen Sie die Hinweise zur Aktualisierung für XClarity Administrator (siehe [XClarity Administrator-Verwaltungsserver aktualisieren](#) in der Onlinedokumentation zu XClarity Administrator).

- Bevor Sie die XClarity Administrator Ressourcenmanager aktualisieren, sichern Sie die virtuelle Einheit, indem Sie einen Klon erstellen (siehe [XClarity Administrator sichern](#) in der Onlinedokumentation zu XClarity Administrator).
- Achten Sie darauf, dass den Ressourcen, die Sie aktualisieren möchten, eine Aktualisierungskonformitätsrichtlinie zugeordnet ist.
- XClarity Orchestrator überträgt die entsprechenden Aktualisierungen während des Aktualisierungsprozesses an den Ressourcenmanager. Stellen Sie sicher, dass auf dem Verwaltungsserver genügend Speicherplatz für die Aktualisierungen verfügbar ist.
- Bei ThinkEdge Client-Einheiten werden nur BIOS-Aktualisierungen auf Servern unterstützt, auf denen Windows 10 Version 1809 oder ein höheres 64-Bit-Betriebssystem ausgeführt wird. Sondereditionen (z. B. 10 S oder 10x) werden derzeit nicht unterstützt.
- Sie können keine Firmwareaktualisierungen für die folgenden Server über die Webschnittstelle herunterladen. Laden Sie Aktualisierungen stattdessen manuell von [ibm.com](#) herunter und importieren Sie sie anschließend.
 - IBM System x iDataPlex dx360 M4
 - IBM System Serie M4
 - IBM System x3100 M5 und x3250 M
 - IBM System x3850 X5 und x3950 X5
 - IBM System x3850 X6 und x3950 X6
 - IBM Flex System

Hinweise zu Repositorys

- Achten Sie darauf, dass das Repository für Aktualisierungen die Aktualisierungspakete enthält, die Sie übernehmen möchten. Ist dies nicht der Fall, dann aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Aktualisierungen herunter (siehe [Aktualisierungen herunterladen und importieren](#)). Sie können angeben, dass bei einer Zielaktualisierung auch erforderliche Aktualisierungen installiert werden. Die erforderlichen Aktualisierungen müssen erst in das Repository heruntergeladen werden, bevor sie übernommen werden können.

In einigen Fällen können mehrere Versionen für die Übernahme einer Aktualisierung erforderlich sein. Dann müssen alle Versionen in das Repository heruntergeladen werden.

Hinweise zum Aktualisierungsprozess

- Wenn Sie ein Aktualisierungspaket mit Aktualisierungen für verschiedene Komponenten installieren, werden alle Komponenten aktualisiert, für die das Aktualisierungspaket übernommen wird.
- Wenn eine Aktualisierungsanforderung für einen Ressourcenmanager und eine oder mehrere von diesem Ressourcenmanager verwaltete Einheiten erfolgt, werden die Aktualisierungen zuerst vom Ressourcenmanager übernommen.
- Während die Aktualisierung läuft, ist die Zielressource gesperrt. Sie können keine anderen Verwaltungsaufgaben auf der Zielressource starten, bis der Aktualisierungsprozess abgeschlossen ist.
- Nachdem eine Aktualisierung von einer Ressource übernommen wurde, sind möglicherweise ein oder mehrere Neustarts erforderlich, um die sie vollständig zu aktivieren. Sie können auswählen, ob die Ressource zur Aktivierung sofort oder verzögert neu gestartet werden soll. Sie können die Aktivierung auch priorisieren. Wenn Sie den sofortigen Neustart wählen, minimiert XClarity Orchestrator die Anzahl der erforderlichen Neustarts. Wenn Sie die verzögerte Aktivierung wählen, werden die Aktualisierungen beim nächsten Neustart der Ressource aktiviert. Wenn Sie die priorisierte Aktivierung auswählen, werden die Aktualisierungen auf dem Baseboard Management Controller sofort aktiviert. Alle anderen Aktualisierungen werden beim nächsten Neustart der Einheit aktiviert.
- Wenn Sie die Ressource während des Aktualisierungsprozesses neu starten (*sofortige Aktivierung*), müssen Sie sicherstellen, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf eine andere Ressource verschoben wurden.

- Bei einigen Firmwareaktualisierungen muss ein Bildschirm mit der Zieleinheit verbunden sein. Der Aktualisierungsprozess kann fehlschlagen, wenn kein Bildschirm verbunden ist.

Aktualisierungen herunterladen und importieren

Aktualisierungspakete müssen im Repository für Aktualisierungen verfügbar sein, bevor sie auf verwaltete Ressourcen angewendet werden können.

Vorbereitende Schritte

Wenn Sie die neuesten Informationen zu Aktualisierungspaketen abrufen möchten, wählen Sie den Ressourcentyp aus und klicken Sie auf **Nach Aktualisierungen suchen → Ausgewählte aktualisieren**, um Informationen zu allen verfügbaren Aktualisierungspaketen zu erhalten, oder klicken Sie auf **Nach Aktualisierungen suchen → Ausgewählte aktualisieren – Nur aktuelle Version**, um nur zum neuesten Aktualisierungspaket für diese Ressource Informationen abzurufen. Sortieren Sie anschließend die Tabelle mithilfe der Spalte **Name**, um die Aktualisierungen nach Version zu ordnen.

XClarity Orchestrator verwendet ein separates Laufwerk für das Aktualisierungs-Repository. Die erforderliche Mindestgröße für dieses Laufwerk ist 100 GB.

Zu dieser Aufgabe

Sie können ein einzelnes XClarity Administrator-Repository-Paket oder ein oder mehrere Aktualisierungspakete gleichzeitig herunterladen oder importieren.

- **XClarity Administrator-Repository-Pakete** Lenovo XClarity Administrator-Repository-Pakete enthalten die neuesten zu einem bestimmten Zeitpunkt verfügbaren Firmwareaktualisierungen für die meisten unterstützten Einheiten sowie eine aktualisierte Standard-Firmwarekonformitätsrichtlinie. Wenn Sie ein Repository-Paket von der [Website zum Herunterladen von XClarity Administrator](#) herunterladen, wird jedes Aktualisierungspaket im Repository-Paket extrahiert und in das Aktualisierungs-Repository importiert. Danach wird die Repository-Nutzdatendatei gelöscht. Die aktualisierte Standard-Firmwarekonformitätsrichtlinie wird auch als vordefinierte Richtlinie importiert. Diese vordefinierte Richtlinie kann nicht geändert werden.







Die folgenden Repositorypakete sind verfügbar.

- **Invgy_sw_lxca_cmmswitchrepo***x-x.x.x_anyos_noarch*. Enthält Firmwareaktualisierungen für alle CMMs und Flex System-Switches.
- **Invgy_sw_lxca_storagerackswitchrepo***x-x.x.x_anyos_noarch*. Enthält Firmwareaktualisierungen für alle RackSwitch-Switches und Lenovo Storage-Einheiten.
- **Invgy_sw_lxca_systemxrepo***x-x.x.x_anyos_noarch*. Enthält Firmwareaktualisierungen für alle Converged HX Series-, Flex System- und System x-Server.
- **Invgy_sw_thinksystemrepo***x-x.x.x_anyos_noarch*. Enthält Firmwareaktualisierungen für alle ThinkSystem-Server.
- **Invgy_sw_lxca_thinksystemv2repo***x-x.x.x_anyos_noarch*. Enthält Firmwareaktualisierungen für alle ThinkSystem V2 Server.
- **Invgy_sw_lxca_thinksystemv3repo***x-x.x.x_anyos_noarc*. Enthält Firmwareaktualisierungen für alle ThinkAgile und ThinkSystem V3 Server.

Wenn Sie manuell Repository-Pakete importieren, müssen Sie die Nutzlastdatei (.tgz), Metadatendatei (.xml), Änderungsprotokoll (.chg) und Readme (.txt) importieren.

Sie können den Status eines Repository-Pakets der Spalte **Status** auf der Seite „Repository-Verwaltung“ entnehmen. Die Spalte enthält die folgenden Werte.

-  **Nicht heruntergeladen**. Das Repository-Paket ist über das Web verfügbar, wird aber nicht heruntergeladen und in das Aktualisierungs-Repository extrahiert.

-  **Ausstehender Download.** Das Repository-Paket befindet sich in der Warteschlange, um vom Internet heruntergeladen zu werden.
 -  **Wird heruntergeladen.** Das Repository-Paket wird gerade vom Internet heruntergeladen.
 -  **Ausstehende Anwendung.** Das Repository-Paket befindet sich in der Warteschlange, um Aktualisierungspakete im Repository-Paket in das Aktualisierungs-Repository zu extrahieren.
 -  **Wird angewendet.** Die Aktualisierungspakete im Repository-Paket werden in das Aktualisierungs-Repository extrahiert.
 -  **x von y heruntergeladen.** Einige, aber nicht alle Repository-Pakete werden heruntergeladen und in das Aktualisierungs-Repository extrahiert. Die Zahlen in Klammern geben die Anzahl der heruntergeladenen Aktualisierungen und die Anzahl der verfügbaren Aktualisierungen an.
 -  **Heruntergeladen.** Alle Aktualisierungspakete im Repository-Paket werden im Aktualisierungs-Repository gespeichert. Die Nutzdatendatei des Repository-Pakets wird gelöscht.
- **Aktualisierungspakete** Wenn XClarity Orchestrator mit dem Internet verbunden ist, können Sie im Aktualisierungskatalog aufgeführte Aktualisierungspakete direkt über die Lenovo Support-Website herunterladen. Wenn XClarity Orchestrator nicht mit dem Internet verbunden ist, können Sie Aktualisierungspakete, die Sie zuvor von der [Lenovo Website zu Support für Rechenzentrum](#) heruntergeladen haben, manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Orchestrator-Host importieren.






Wenn Sie nur eine Nebenversion herunterladen, werden erforderlichen Aktualisierungspakete trotzdem heruntergeladen.

Wenn Sie Aktualisierungen manuell importieren, müssen Sie die erforderlichen Dateien auf Basis des Ressourcentyps importieren.

- Importieren Sie für ThinkSystem V3 Server das einzelne Aktualisierungspaket (*.zip). Diese ZIP-Datei enthält die Nutzlastdatei, Metadatendateien (mehrere *.json), die Änderungsprotokolldatei (*.chg) und die Readme-Datei (*.txt).
- Importieren Sie für ThinkEdge Client-Einheiten die Nutzlastdatei (Windows.exe). Die Readme-Datei (.txt) ist optional. Beachten Sie, dass derzeit nur die Aktualisierung **BIOS-Flash-Dienstprogramm für Windows** unterstützt wird.
- Importieren Sie für XClarity Management Hub und XClarity Management Hub 2.0 die einzelne Aktualisierungspaketdatei (.tgz). Diese Datei enthält die Nutzlast-, Metadaten-, Änderungsprotokoll- und Readme-Dateien.
- Importieren Sie für alle anderen Ressourcen (einschließlich XClarity Administrator, ThinkEdge Server, ThinkSystem V1 und V2 und ältere Einheiten) die Nutzlastdatei (.zip, .uxz, .tar.gz, .tar, .bin), die Metadatendatei (.xml), das Änderungsprotokoll (.chg) und die Readme-Datei (.txt).

Wichtig: Die maximale Größe aller gleichzeitig zu importierenden Dateien beträgt 8 GB.

Über die Spalte **Status** auf der Seite Repository-Verwaltung können Sie ermitteln, ob bestimmte Aktualisierungsdateien im Repository für Aktualisierungen gespeichert sind. Die Spalte enthält die folgenden Werte.

-  **Nicht heruntergeladen.** Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist über das Web verfügbar, aber derzeit nicht im Repository gespeichert.
-  **Ausstehender Download.** Das Aktualisierungspaket befindet sich in der Warteschlange, um vom Internet heruntergeladen zu werden.
-  **Wird heruntergeladen.** Das Aktualisierungspaket wird gerade vom Internet heruntergeladen.
-  **x von y heruntergeladen.** Es sind nur einige Aktualisierungen des Aktualisierungspakets im Repository gespeichert. Die Zahlen in Klammern geben die Anzahl der gespeicherten Aktualisierungen und die Anzahl der verfügbaren Aktualisierungen an.
-  **Heruntergeladen.** Das gesamte Aktualisierungspaket oder die einzelne Aktualisierung ist im Repository gespeichert.

Anmerkung: Einige Aktualisierungspakete werden von mehreren Plattformen verwendet. Wenn Sie ein Aktualisierungspaket in der Tabelle auswählen, wird es für jede Plattform ausgewählt, die es verwendet.

Vorgehensweise

Führen Sie zum Herunterladen oder manuellen Importieren von Aktualisierungspaketen und Repository-Paketen einen der folgenden Schritte aus.

- Wenn XClarity Orchestrator mit dem Internet verbunden ist, laden Sie die im Katalog aufgeführten Aktualisierungspakete herunter.
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Aktualisierungen** und dann auf die Registerkarte **Repository-Verwaltung**, um die Übersicht Repository-Verwaltung aufzurufen. Die Übersicht Repository-Verwaltung enthält Informationen zu Aktualisierungspaketen in einer Baumstruktur, die nach Ressourcentypen, Komponenten und Aktualisierungspaketen organisiert ist. Standardmäßig werden Ressourcentypen nur für *verwaltete* Ressourcen in der Tabelle aufgeführt. Klicken Sie auf **Verfügbare Ressourcentypen anzeigen**, um *alle unterstützten* Ressourcentypen aufzulisten, die im Katalog verfügbar sind.

Repositoryverwaltung

Verwalten Sie das Aktualisierungsrepository, einschließlich den Import von Aktualisierungspaketen aus dem lokalen System und das Herunterladen von Kataloginformationen und Aktualisierungspaketen aus dem Internet. Aktualisieren Sie den Katalog, um die neuesten Informationen abzurufen, bevor Sie Aktualisierungspakete herunterladen.

Repository-Nutzung: 18.2 GB von 93.2 GB.

Wenn das ausgewählte Paket eine kleinere Aktualisierung ist, werden die als Voraussetzung erforderlichen Aktualisierungspakete ebenfalls heruntergeladen.

Nur verwaltete Ressourcentypen anzeigen 🔍 Suchen ✕

🔄 ☰ ⬇️ 📄 📁 Katalog aktualisieren 🔍 Alle Aktionen ⌵ Filter ⌵

<input type="checkbox"/>	Name :	Ressou	Versior	Veröffi	Status	Paketg	Versior
<input type="checkbox"/>	> IBM Flex System x220 Compute Node	79...			📦..	77...	
<input type="checkbox"/>	> IBM Flex System x222 Compute Node	79...			📦..	65...	
<input type="checkbox"/>	> IBM Flex System x240 Compute Node	87...			📦..	1...	
<input type="checkbox"/>	> IBM Flex System x280/x480/x880 X6 Compute Node	79...			📦..	1...	
<input type="checkbox"/>	> IBM Flex System x440 Compute Node	79...			📦..	85...	
<input type="checkbox"/>	> Lenovo Converged HX5510/HX5510-C/HX3510-G/HX7	86...			📦..	5...	
<input type="checkbox"/>	> Lenovo Devices Repository Pack	Re...			📦..	27...	
<input type="checkbox"/>	> Lenovo Flex System x240 Compute Node	71...			📦..	6...	
<input type="checkbox"/>	> Lenovo Flex System x240 M5 Compute Node	95...			📦..	6...	
<input type="checkbox"/>	> Lenovo Flex System x280/x480/x880 X6 Compute Node	71...			📦..	6...	

0 Ausgewählt / 14 Gesamt Zeilen pro Seite: 10 ⌵

⏪ < 1 2 > ⏩

2. (Optional) Laden Sie Information zu den neuesten verfügbaren Aktualisierungen für bestimmte Ressourcen herunter, indem Sie in der Tabelle mindestens einen Ressourcentypen auswählen, auf **Nach Aktualisierungen suchen** klicken und dann eine der folgenden Optionen wählen.
 - **Ausgewählte aktualisieren**. Ruft Informationen zu allen Aktualisierungsversionen ab, die für die ausgewählte Ressource verfügbar sind.
 - **Ausgewählte aktualisieren – Nur aktuelle Version**. Ruft Informationen zur aktuellsten Aktualisierungsversion ab, die für die ausgewählte Ressource verfügbar ist. Bei ThinkEdge Client-Einheiten wird nur **Ausgewählte aktualisieren – Nur aktuelle Version** unterstützt.

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).
3. Wählen Sie ein(e) oder mehrere Repository-Pakete, Ressourcen, Komponenten und Aktualisierungsversionen aus, die heruntergeladen werden sollen. Sie können die Ressourcentypen und Komponenten erweitern, um die Liste der Aktualisierungsversionen anzuzeigen, die im Katalog für jeden Ressourcentyp und jede Komponente verfügbar sind.
4. Klicken Sie auf das Symbol **Aktualisierungen herunterladen** (⬇️), um die ausgewählten Aktualisierungen herunterzuladen. 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).

Wenn der Download abgeschlossen ist, ändert sich der **Downloadstatus** für die ausgewählten Aktualisierungen in „Heruntergeladen“.

- Wenn XClarity Orchestrator nicht mit dem Internet verbunden ist, importieren Sie die Aktualisierungspakete und Repository-Pakete manuell.
 1. Laden Sie die Dateien für jedes Repository-Paket und Aktualisierungspaket über einen Webbrowser auf eine Arbeitsstation herunter, die über eine Netzwerkverbindung zum XClarity Orchestrator-Host verfügt. Verwenden Sie diese Links, um die entsprechenden Aktualisierungen herunterzuladen.
 - Gehen Sie für Lenovo XClarity Administrator-Aktualisierungen zur [Website zum Herunterladen von XClarity Administrator](#). Sie können XClarity Administrator-Aktualisierungen auch mithilfe von Lenovo XClarity Essentials OneCLI-Befehlen herunterladen. Im folgenden Beispiel wird die neueste Aktualisierung (einschließlich der Nutzlast) in das Aktualisierungsverzeichnis /lxca heruntergeladen und die Protokolldateien werden im Aktualisierungsverzeichnis /logs/lxca gespeichert. Weitere Informationen über OneCLI finden Sie [Befehl „acquire“](#) in der Lenovo XClarity Essentials OneCLI-Onlinedokumentation.


```
Onecli.exe update acquire --lxca --ostype none --mt lxca --scope latest --superseded --xml --dir ./lxca-updates --output ./logs/lxca-updates
```
 - Gehen Sie für Firmwareaktualisierungs-Repository-Pakete zur [Website zum Herunterladen von XClarity Administrator](#).
 - Gehen Sie für Firmwareaktualisierungen zur [Lenovo Website zu Support für Rechenzentrum](#).
 2. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Aktualisierungen** und dann auf die Registerkarte **Repository-Verwaltung**, um die Übersicht Repository-Verwaltung aufzurufen.
 3. Klicken Sie auf das Symbol **Importieren** (📁), um das Dialogfenster Aktualisierungen importieren anzuzeigen.
 4. Ziehen Sie die heruntergeladenen Dateien in das Dialogfeld Importieren oder klicken Sie auf **Durchsuchen**, um die Dateien zu suchen.

Achtung:

- Bei ThinkEdge Client-Einheiten müssen Sie die Nutzlastdatei für jedes Aktualisierungspaket importieren. Die Readme-Datei ist optional.

- Für alle anderen Einheiten müssen Sie die Metadatendatei sowie das Image oder die Nutzlastdatei, die Änderungsprotokolldatei und die README-Datei für jedes Repository-Paket und Aktualisierungspaket importieren. Alle ausgewählten und nicht in der Metadatendatei angegebenen Dateien werden gelöscht. Wenn Sie keine Metadatendatei auswählen, wird die Aktualisierung nicht importiert.
 - Importieren Sie keine anderen Dateien, die sich möglicherweise auf den Lenovo-Websites mit Downloads befinden.
 - Wenn Sie keine Metadatendatei (.xml oder .json) für das Repository-Paket oder Aktualisierungspaket hinzufügen, wird das Repository-Paket bzw. das Aktualisierungspaket nicht importiert.
5. Klicken Sie auf **Importieren**. 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).

Wenn die Dateien importiert und im Repository gespeichert werden, wird die Spalte **Downloadstatus** in „Heruntergeladen“ geändert.

Nach dieser Aufgabe

Auf der Übersicht Repository-Verwaltung können Sie die folgenden Aktionen ausführen.

- Lesen Sie die README- und Änderungsverlaufsdatei sowie die Liste der behobenen Common Vulnerabilities and Exposures (CVEs) für eine bestimmte Aktualisierung, indem Sie auf das Info-Symbol (ℹ️) in der Spalte **Versionshinweise** klicken. Sie finden auch eine Liste der behobenen CVEs, indem Sie den Mauszeiger über die Spalte **Behobene CVEs** bewegen. Klicken Sie auf die CVE-ID, um detaillierte Informationen über die CVE auf der Website „National Vulnerability Data“ anzuzeigen.

Die Spalten **Versionshinweise** und **Behobene CVEs** sind standardmäßig ausgeblendet. Sie können diese Spalten einblenden, indem Sie auf **Alle Aktionen** → **Spalten ein-/ausschalten** klicken.

- Löschen Sie nur die Imagedatei (Nutzlastdatei) der ausgewählten Aktualisierungen mithilfe des Symbols **Nur Nutzlastdateien löschen** (🗑️). Informationen zur Aktualisierung (die XML-Metadatendatei) verbleiben im Repository und der Downloadstatus ändert sich zu „Nicht heruntergeladen“.

Wichtig:

- Die Nutzlast für Repository-Pakete wird automatisch gelöscht, nachdem die Aktualisierungspakete während des Download- oder Importvorgangs extrahiert wurden.
- Sie können keine Nutzlasten aus Aktualisierungspaketen löschen, die gerade in Aktualisierungskonformitätsrichtlinien verwendet werden. Sie müssen zuerst das Aktualisierungspaket aus den Richtlinien entfernen (siehe [Aktualisierungskonformitätsrichtlinien erstellen und zuordnen](#)).
- Einige Aktualisierungspakete gelten für mehrere Plattformen und Komponenten. Das Löschen eines gemeinsamen Aktualisierungspakets wirkt sich auf alle Plattformen und Komponenten aus, die es verwenden.

Aktualisierungskonformitätsrichtlinien erstellen und zuordnen

Sie können eine Aktualisierungskonformitätsrichtlinie erstellen, die auf den im Repository für Aktualisierungen bezogenen Aktualisierungen basiert. Sie können die Richtlinie dann einem oder mehreren Ressourcenmanagern oder verwalteten Servern zuordnen.

Vorbereitende Schritte

Wenn Sie eine Aktualisierungskonformitätsrichtlinie erstellen, wählen Sie die Zielaktualisierungsversion zur Anwendung auf die Ressourcen aus, die der Richtlinie zugeordnet werden sollen. Achten Sie darauf, dass sich die Aktualisierungsdateien für die Zielversion im Repository für Aktualisierungen befinden, bevor Sie die Richtlinie erstellen.

Wenn Sie ein Firmwareupdate-Repository-Paket herunterladen oder importieren, werden die vordefinierten Firmwarekonformitätsrichtlinien im Repository-Paket zum Aktualisierungs-Repository hinzugefügt. Dies ist dann eine *vordefinierte Richtlinie*, die nicht geändert oder gelöscht werden kann.

Zu dieser Aufgabe

Aktualisierungskonformitätsrichtlinien stellen sicher, dass die Software oder Firmware auf bestimmten verwalteten Ressourcen auf dem neuesten oder einem bestimmten Stand ist. Dazu werden Ressourcen markiert, die Ihre Aufmerksamkeit erfordern. Eine Aktualisierungskonformitätsrichtlinie legt fest, welche Ressourcen überwacht werden und welche Software- oder Firmwareversion zur Erhaltung der Konformität installiert sein muss. XClarity Orchestrator verwendet die Richtlinien dann, um den Status von verwalteten Ressourcen zu überprüfen und nicht konforme Ressourcen zu erkennen.

Bei der Erstellung einer Aktualisierungskonformitätsrichtlinie können Sie festlegen, dass XClarity Orchestrator eine Ressource kennzeichnet, wenn deren Software oder Firmware veraltet ist.

Nachdem eine Aktualisierungskonformitätsrichtlinie einer Ressource zugeordnet wurde, überprüft XClarity Orchestrator den Konformitätsstatus der Ressource, wenn das Repository für Aktualisierungen geändert wird. Wenn die Software oder Firmware auf der Ressource nicht mit der zugewiesenen Richtlinie übereinstimmt, markiert XClarity Orchestrator die Ressource entsprechend den mit der Seite *Übernehmen / Aktivieren* in der Aktualisierungskonformitätsrichtlinie festgelegten Regeln als nicht konform.

Sie können beispielsweise eine Aktualisierungskonformitätsrichtlinie erstellen, die die Basis-Softwareversion für XClarity Administrator definiert, und diese Richtlinie dann allen XClarity Administrator-Ressourcenmanagern zuordnen. Wenn der Aktualisierungskatalog aktualisiert und eine neue Aktualisierung heruntergeladen oder importiert wird, sind die XClarity Administrator-Instanzen möglicherweise nicht mehr konform. Wenn dies der Fall ist, aktualisiert XClarity Orchestrator die Seite *Übernehmen/Aktivieren*, um zu zeigen, welche XClarity Administrator-Instances nicht konform sind, und generiert einen Alert.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Aktualisierungskonformitätsrichtlinie zu erstellen und zuzuordnen.

Schritt 1. Erstellen Sie eine Aktualisierungskonformitätsrichtlinie.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔑) → **Aktualisierungen** und dann auf **Richtlinienverwaltung**, um die Übersicht Richtlinienverwaltung aufzurufen.

Richtlinienverwaltung

Über die Richtlinienverwaltung können Sie basierend auf erfassten Aktualisierungen im Firmwarerepository eine Richtlinie erstellen oder ändern.

ⓘ Eine zugeordnete Konformitätsrichtlinie kann nicht bearbeitet oder gelöscht werden. ✕

🔄 + 🗑️ ✎ 📄 📄 Alle Aktionen ▾ Filter ▾ 🔍 Suchen ✕



<input type="checkbox"/>	Name der Konformit	Verwendungsstatus	Ursprung der Konfor	Letzte Änderung	Beschreibung
<input type="checkbox"/>	ThinkAgile_VX_0...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 18:08	ThinkAgile VX M...
<input type="checkbox"/>	v2.6.0-2020-01-...	→ Zugeordnet	👤 Benutzerdef...	04.10.22, 18:23	Production firmw...
<input type="checkbox"/>	v3.2.0-2021-07-...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 18:34	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 18:42	Production firmw...
<input type="checkbox"/>	ThinkAgile-VX-Se...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 18:54	System and Com...
<input type="checkbox"/>	ThinkAgile-VX-Se...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 19:07	System and Com...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 19:25	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 19:33	Production firmw...
<input type="checkbox"/>	v2.6.0-2019-12-...	← Nicht zugeor...	👤 Benutzerdef...	04.10.22, 19:41	Production firmw...

0 Ausgewählt / 9 Gesamt Zeilen pro Seite: 10 ▾

2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Konformitätsrichtlinie erstellen zu öffnen.
3. Geben Sie den Namen und optional eine Beschreibung für die Richtlinie ein.
4. Geben Sie den Auslöser für die Richtlinie an. Es kann einen der folgenden Werte aufweisen.
 - **Bei nicht exakter Übereinstimmung markieren.** Wenn die auf der Ressource installierte Software- oder Firmwareversion *älter oder jünger* als die Firmwareversion des Ziels in der Aktualisierungskonformitätsrichtlinie ist, wird die Ressource als nicht konform markiert. Wenn Sie beispielsweise einen Netzwerkadapter in einem Server ersetzen und die Firmware auf diesem Netzwerkadapter in der zugewiesenen Aktualisierungskonformitätsrichtlinie von der Firmwareversion des Ziels abweicht, wird der Server als nicht konform gekennzeichnet.
 - **Nicht markieren.** Ressourcen, die nicht konform sind, werden nicht markiert.
5. Klicken Sie auf die Registerkarte **Regeln**, um Konformitätsregeln für diese Richtlinie hinzuzufügen.
 - a. Wählen Sie den Ressourcentyp für diese Richtlinie aus.
 - b. Geben Sie das Konformitätsziel für die betreffenden Ressourcen und Komponenten an. Bei Ressourcen mit Komponenten können Sie einen der folgenden Werte auswählen.
 - **Angepasst.** Das Konformitätsziel für jede Ressourcenkomponente ist standardmäßig auf die aktuelle neueste Version im Repository für diese Komponente festgelegt.
 - **Nicht aktualisieren.** Das Konformitätsziel für jede Ressourcenkomponente lautet standardmäßig **Nicht aktualisieren**. Wenn Sie den Standardwert für eine Komponente ändern, ändert sich das Konformitätsziel für die gesamte Ressource in **Angepasst**. Bei

Ressourcen ohne Komponenten sowie für jede Komponente können Sie einen der folgenden Werte auswählen.

- *{firmware_level}*. Gibt an, dass die Firmware auf der Komponente der ausgewählten Basis-Firmwareversion entsprechen muss.
- **Nicht aktualisieren**. Gibt an, dass die Firmware auf der Komponente nicht aktualisiert werden soll. Beachten Sie, dass die Firmware auf dem (sekundären) Sicherungs-Management-Controller nicht standardmäßig aktualisiert wird.

c. Klicken Sie auf das Symbol **Hinzufügen** () , um weitere Regeln hinzuzufügen, und dann auf das Symbol **Löschen** () , um Regeln zu löschen.

6. Klicken Sie auf **Erstellen**.

Schritt 2. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** () → **Aktualisierungen** und dann auf **Übernehmen und Aktivieren**, um die Übersicht Übernehmen und aktivieren aufzurufen.


Schritt 3. Weisen Sie die Aktualisierungskonformitätsrichtlinie den Ressourcen zu.

- **Einer einzelnen Ressource** Wählen Sie im Dropdown-Menü in der Spalte **Zugeordnete Konformitätsrichtlinie** für jede Ressource eine Richtlinie aus.

Sie können aus einer Liste von Konformitätsrichtlinien auswählen, die für die Ressource anwendbar sind. Wenn der Ressource aktuell keine Richtlinie zugeordnet ist, wird die zugeordnete Richtlinie auf **Keine Zuordnung** festgelegt. Wenn keine Richtlinien für die Ressource anwendbar sind, wird die zugeordnete Richtlinie auf **Keine anwendbaren Richtlinien** festgelegt.

- **Mehreren Ressourcen**

1. Wählen Sie eine oder mehrere Ressourcen aus, denen die Richtlinie zugewiesen werden soll.

2. Klicken Sie auf das Symbol **Zuordnen** () , um das Dialogfenster Richtlinie zuordnen zu öffnen.

3. Wählen Sie die Richtlinie aus, die Sie zuordnen möchten. Sie können aus einer Liste von Konformitätsrichtlinien auswählen, die für die ausgewählten Ressourcen anwendbar sind. Wenn der Ressource aktuell keine Richtlinie zugeordnet ist, wird die zugeordnete Richtlinie auf **Keine Zuordnung** festgelegt. Wenn keine Richtlinien für die Ressource anwendbar sind, wird die zugeordnete Richtlinie auf **Keine anwendbaren Richtlinien** festgelegt. Wenn vor dem Öffnen des Dialogs keine Ressourcen ausgewählt wurden, werden alle Richtlinien aufgelistet.

Anmerkung: Wählen Sie **Keine Zuordnung** aus, um die Richtlinienzuordnung von der ausgewählten Ressource zu entfernen.

4. Wählen Sie einen der folgenden Bereiche für die Richtlinienzuordnung aus.


- **Allen geeigneten Einheiten, die ...**
- **Nur ausgewählte geeignete Einheiten, die ...**

5. Wählen Sie mindestens ein Richtlinienkriterium aus.

- **Ohne zugewiesene Richtlinie**
- **Nicht-konform (die aktuell zugeordnete Richtlinie wird überschrieben)**
- **Konform (die aktuell zugeordnete Richtlinie wird überschrieben)**

6. Klicken Sie auf **Übernehmen**. Die in der Spalte Zugeordnete Richtlinie auf der Seite „Repository für Firmwareaktualisierungen“ aufgeführte Richtlinie ändert sich in den Namen der ausgewählten Firmwarekonformitätsrichtlinie.


- **Für Ressourcengruppen**

1. Klicken Sie auf das Symbol **Zuordnen** () , um das Dialogfenster Richtlinie zuordnen zu öffnen.
2. Wählen Sie die Richtlinie aus, die Sie zuordnen möchten. Sie können aus einer Liste von Konformitätsrichtlinien auswählen, die für alle Ressourcen in der Gruppe anwendbar sind. Wenn der Ressource aktuell keine Richtlinie zugeordnet ist, wird die zugeordnete Richtlinie auf **Keine Zuordnung** festgelegt. Wenn keine Richtlinien für die Ressource anwendbar sind, wird die zugeordnete Richtlinie auf **Keine anwendbaren Richtlinien** festgelegt.



Anmerkung: Wählen Sie **Keine Zuordnung** aus, um die Richtlinienzuordnung von den Ressourcen in der Gruppe zu entfernen.
3. Wählen Sie eine oder mehrere Gruppen von Ressourcen aus, denen die Richtlinie zugewiesen werden soll.
4. Wählen Sie einen der folgenden Bereiche für die Richtlinienzuordnung aus.
 - **Allen geeigneten Einheiten, die ...**
 - **Nur ausgewählte geeignete Einheiten, die ...**
5. Wählen Sie mindestens ein Richtlinienkriterium aus.
 - **Ohne zugewiesene Richtlinie**
 - **Nicht-konform (die aktuell zugeordnete Richtlinie wird überschrieben)**
 - **Konform (die aktuell zugeordnete Richtlinie wird überschrieben)**
6. Klicken Sie auf **Übernehmen**. Die in der Spalte Zugeordnete Richtlinie auf der Seite „Repository für Firmwareaktualisierungen“ aufgeführte Richtlinie ändert sich in den Namen der ausgewählten Firmwarekonformitätsrichtlinie.

Nach dieser Aufgabe


Auf der Übersicht Richtlinienverwaltung können Sie die folgenden Aktionen ausführen.

- Richtliniendetails anzeigen, indem Sie auf die Zeile in der Tabelle klicken.
- Eine Richtlinie ändern, indem Sie auf das Symbol **Bearbeiten** () klicken.

Anmerkung: Sie können keine Richtlinie ändern, die einer oder mehreren Ressourcen zugewiesen ist. Sie müssen die Zuweisung der Richtlinie zunächst aufheben.

- Eine ausgewählte Vorlage kopieren und ändern, indem Sie auf das Symbol **Kopieren** () klicken.
- Eine *benutzerdefinierte* Richtlinie löschen, indem Sie auf das Symbol **Löschen** () klicken.

Anmerkung: Sie können keine Richtlinie löschen, die einer oder mehreren Ressourcen zugewiesen ist. Sie müssen die Zuweisung der Richtlinie zunächst aufheben.

In der Übersicht Übernehmen und aktivieren können Sie die Zuordnung einer Richtlinie für eine ausgewählte Ressource aufheben, indem Sie auf das Symbol **Zuordnen** () klicken, die Richtlinie **Keine Zuordnung** auswählen und dann angeben, ob die Änderung auf alle Ressourcen mit Richtlinienzuordnung oder nur auf die ausgewählten Ressourcen angewendet werden soll.

Aktualisierungen für Ressourcenmanager anwenden und aktivieren

XClarity Orchestrator wendet Aktualisierungen nicht automatisch an. Um Software zu aktualisieren, müssen Sie die Aktualisierung für ausgewählte Lenovo XClarity Administrator-Ressourcenmanager, die nicht mit der zugewiesenen Aktualisierungskonformitätsrichtlinie konform sind, manuell anwenden und aktivieren.

Vorbereitende Schritte

Bevor Sie versuchen, Aktualisierungen auf eine Ressource zu anzuwenden und zu aktivieren, lesen Sie die Hinweise zur Aktualisierung (siehe [Bereitstellungshinweise aktualisieren](#)).

Stellen Sie sicher, dass der Zielressource eine Aktualisierungskonformitätsrichtlinie zugeordnet ist (siehe [Aktualisierungskonformitätsrichtlinien erstellen und zuordnen](#)).

Eine Aktualisierung kann nicht für dieselbe oder eine frühere als die derzeit installierte Softwareversion durchgeführt werden.

Zu dieser Aufgabe

Sie können Firmwareaktualisierungen auf XClarity Administrator Ressourcenmanagern anwenden, denen eine Firmwarekonformitätsrichtlinie zugewiesen ist und die diese nicht erfüllen. Sie können die Software auf folgende Arten aktualisieren:

- Für bestimmte nicht konforme Manager
- Für alle nicht konformen Manager in bestimmten Gruppen
- Für alle nicht konformen Manager, denen eine bestimmte Aktualisierungskonformitätsrichtlinie zugeordnet ist
- Für alle nicht konformen Manager in bestimmten Gruppen, denen eine bestimmte Aktualisierungskonformitätsrichtlinie zugeordnet ist
- Für alle nicht konformen Manager, die einer Richtlinie zugeordnet sind und diese nicht erfüllen

XClarity Orchestrator aktualisiert Ressourcen nicht direkt. Stattdessen wird eine Anforderung zur Durchführung der Aktualisierung an den entsprechenden Ressourcenmanager gesendet und anschließend wird der Fortschritt der Anforderung verfolgt. XClarity Orchestrator identifiziert die für die Aktualisierung erforderlichen Abhängigkeiten, stellt sicher, dass die Zielressourcen in der richtigen Reihenfolge aktualisiert werden, übergibt die entsprechenden Aktualisierungspakete an den Ressourcenmanager und erstellt eine Anforderung zum Starten eines Jobs im Ressourcenmanager, damit die Aktualisierung durchgeführt wird.

Während des Aktualisierungsprozesses wird die Zielressource möglicherweise mehrmals automatisch neu gestartet, bis der gesamte Prozess abgeschlossen ist. Legen Sie alle Anwendungen auf der Zielressource still, bevor Sie fortfahren.

Wenn beim Aktualisieren der Komponenten in einer Zielressource ein Fehler auftritt, wird diese Komponente nicht aktualisiert. Die Aktualisierung aller anderen Komponenten in der Ressource und aller anderen Zielressourcen im laufenden Aktualisierungsjob wird jedoch fortgesetzt.

Erforderliche Aktualisierungen werden nicht automatisch angewendet.

Tipps:

- In der Tabelle sind nur die Ressourcenmanager aufgeführt, die aktualisiert werden können.
- Die Spalten **Buildnummer** und **Buildnummer Konformitätsziel** sind standardmäßig ausgeblendet. Sie können diese Spalten einblenden, indem Sie auf **Alle Aktionen** → **Spalten ein-/ausschalten** klicken.

Vorgehensweise

Um Aktualisierungen auf XClarity Orchestrator Ressourcenmanager anzuwenden, wählen Sie eine der folgenden Vorgehensweisen.





- **Für bestimmte nicht konforme Ressourcenmanager**



1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Aktualisierungen** und dann auf **Übernehmen und aktivieren**, um die Übersicht Übernehmen und aktivieren aufzurufen.

Übernehmen und aktivieren






Um Aktualisierungen für Ressourcen durchzuführen, ordnen Sie ihnen eine Konformitätsrichtlinie zu und wählen zunächst die Ressource und dann die Aktion "Aktualisierungen durchführen" aus.

Ressourcenmanager Einheiten





 Alle Aktionen ▾ Filter ▾

<input type="checkbox"/>	Name	Status	Konformitäts:	Installierte Ve	Zugeordnete	Konformitäts:	Gruppen:
<input type="checkbox"/>	10.243.2.10	Normal	 Calcula	4.0.0	No Ass... ▾	Nicht verfüg	Nicht verfüg
<input type="checkbox"/>	lxca-0.node-	Normal	 No Poli	2.99.99	No Ass... ▾	Nicht verfüg	Nicht verfüg

0 Ausgewählt / 2 Gesamt Zeilen pro Seite: 10 ▾

2. Klicken Sie auf die Registerkarte **Ressourcenmanager**.
 3. Wählen Sie einen oder mehrere Ressourcenmanager aus, auf die Aktualisierungen angewendet werden sollen.
 4. Klicken Sie auf das Symbol **Aktualisierung übernehmen** () , um das Dialogfenster Aktualisierungszusammenfassung anzuzeigen.
 5. Klicken Sie auf **Aktualisierungen durchführen**, um die Aktualisierungen anzuwenden. 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).
- **Für alle nicht konformen Ressourcenmanager in bestimmten Gruppen oder denen eine bestimmte Aktualisierungskonformitätsrichtlinie zugeordnet ist**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** () → **Aktualisierungen** und dann auf **Übernehmen und Aktivieren**, um die Übersicht Übernehmen und aktivieren aufzurufen.
 2. Klicken Sie auf die Registerkarte **Ressourcenmanager**.
 3. Klicken Sie auf das Symbol **Aktualisierung übernehmen** () , um das Dialogfenster Aktualisierungszusammenfassung anzuzeigen.
 4. Wählen Sie die Gruppen und die Aktualisierungskonformitätsrichtlinie aus.
 - Wenn Sie keine Richtlinie oder Gruppe auswählen, werden alle Manager aktualisiert, denen eine Richtlinie zugeordnet ist und die diese nicht erfüllen.
 - Wenn Sie eine Richtlinie aber keine Gruppe auswählen, werden alle Manager aktualisiert, denen diese Richtlinie zugeordnet ist und die diese nicht erfüllen.
 - Wenn Sie eine oder mehrere Gruppen aber keine Richtlinie auswählen, werden alle Manager in der Gruppe aktualisiert, die nicht mit der zugewiesenen Richtlinie konform sind.
 - Wenn Sie eine Richtlinie und eine oder mehrere Gruppen auswählen, werden alle Manager in der Gruppe aktualisiert, die dieser Richtlinie zugewiesen sind, mit dieser aber nicht konform sind.
 5. Klicken Sie auf **Aktualisierungen durchführen**, um die Aktualisierungen anzuwenden. 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).

Aktualisierungen für verwaltete Server anwenden und aktivieren

Lenovo XClarity Orchestrator wendet Aktualisierungen nicht automatisch an. Um Firmware zu aktualisieren, müssen Sie die Aktualisierung für ausgewählte Einheiten, die nicht mit der zugewiesenen Aktualisierungskonformitätsrichtlinie konform sind, manuell anwenden und aktivieren.

Vorbereitende Schritte

Bevor Sie versuchen, Aktualisierungen auf eine Einheit zu anzuwenden und zu aktivieren, lesen Sie die Hinweise zur Aktualisierung (siehe [Bereitstellungshinweise aktualisieren](#)).

Stellen Sie sicher, dass der Zieleinheit eine Aktualisierungskonformitätsrichtlinie zugeordnet ist (siehe [Aktualisierungskonformitätsrichtlinien erstellen und zuordnen](#)).

Sie können Firmwareaktualisierungen nur auf verwaltete Server anwenden.

Wenn Sie Firmware auf vielen Einheiten gleichzeitig aktualisieren, verwenden Sie XClarity Orchestrator v1.3.1 oder höher und Lenovo XClarity Administrator v3.2.1 oder höher, um eine bessere Leistung zu erzielen.

Zu dieser Aufgabe

Sie können Firmwareaktualisierungen auf Einheiten anwenden, denen eine Firmwarekonformitätsrichtlinie zugewiesen ist und die diese nicht erfüllen. Sie können die Firmware auf folgende Arten aktualisieren:

- Für bestimmte nicht konforme Einheiten
- Für alle nicht konformen Einheiten in bestimmten Gruppen
- Für alle nicht konformen Einheiten, denen eine bestimmte Aktualisierungskonformitätsrichtlinie zugeordnet ist
- Für alle nicht konformen Einheiten in bestimmten Gruppen, denen eine bestimmte Aktualisierungskonformitätsrichtlinie zugeordnet ist
- Für alle nicht konformen Geräte, die einer Richtlinie zugeordnet sind und diese nicht erfüllen

Wenn die installierte Firmwareversion einer oder mehrerer Komponenten *älter oder jünger* als die Firmwareversion des Ziels in der Aktualisierungskonformitätsrichtlinie ist, wird der Server als nicht konform markiert. Wenn die installierte Firmwareversion *älter* ist als die Firmwareversion des Ziels, müssen Sie die Option **Aktualisierung erzwingen** wählen, wenn Sie mithilfe der Aktualisierung ein Downgrade der Firmware auf den Komponenten durchführen möchten. Wenn die Option **Aktualisierung erzwingen** nicht ausgewählt ist, werden nur Firmwareversionen des Ziels angewendet, die neuer sind als die installierten Versionen.

Anmerkung: Ein Downgrade wird nur für bestimmte Einheitenoptionen, Adapter und Laufwerke unterstützt. In der Hardwareokumentation erfahren Sie, ob Downgrades unterstützt werden.

XClarity Orchestrator aktualisiert Ressourcen nicht direkt. Stattdessen wird eine Anforderung zur Durchführung der Aktualisierung an den entsprechenden Ressourcenmanager gesendet und anschließend wird der Fortschritt der Anforderung verfolgt. XClarity Orchestrator identifiziert die für die Aktualisierung erforderlichen Abhängigkeiten, stellt sicher, dass die Zielressourcen in der richtigen Reihenfolge aktualisiert werden, übergibt die entsprechenden Aktualisierungspakete an den Ressourcenmanager und erstellt eine Anforderung zum Starten eines Jobs im Ressourcenmanager, damit die Aktualisierung durchgeführt wird.

Während des Aktualisierungsprozesses wird die Zieleinheit möglicherweise mehrmals automatisch neu gestartet, bis der gesamte Prozess abgeschlossen ist. Legen Sie alle Anwendungen auf der Zieleinheit still, bevor Sie fortfahren.

Wenn beim Aktualisieren der Komponenten in einer Zieleinheit ein Fehler auftritt, wird diese Komponente nicht aktualisiert. Die Aktualisierung aller anderen Komponenten in der Einheit und aller anderen Zieleinheiten im laufenden Aktualisierungsjob wird jedoch fortgesetzt.

Erforderliche Aktualisierungen werden nicht automatisch angewendet.

Tipps:

- In der Tabelle sind nur die Einheiten aufgeführt, die aktualisiert werden können.
- Die Spalten **Buildnummer**, **Buildnummer Konformitätsziel** und **Produktname** sind standardmäßig ausgeblendet. Sie können diese Spalten einblenden, indem Sie auf **Alle Aktionen** → **Spalten ein-/ausschalten** klicken.
- Um bei ThinkSystem SR635, SR645, SR655 und SR665 Servern sowohl In-Band- als auch Out-of-Band-Firmware anzuwenden, wenden Sie zuerst Aktualisierungen bei den Baseboard Management Controllern und anschließend Firmwareaktualisierungen auf den verbleibenden Optionen an.

Vorgehensweise

Um Aktualisierungen auf verwaltete Einheiten anzuwenden, wählen Sie eine der folgenden Vorgehensweisen.

• Für bestimmte nicht konforme Einheiten

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Aktualisierungen** und dann auf **Übernehmen und Aktivieren**, um die Übersicht Übernehmen und aktivieren aufzurufen.
2. Klicken Sie auf die Registerkarte **Einheiten**.
3. Wählen Sie eine oder mehrere Einheiten aus, auf die Aktualisierungen angewendet werden sollen.
4. Klicken Sie auf das Symbol **Aktualisierung übernehmen** (☑), um das Dialogfenster „Aktualisierungszusammenfassung“ anzuzeigen.
5. Wählen Sie aus, wann die Aktualisierungen aktiviert werden sollen.
 - **Priorisierte Aktivierung:** Firmwareaktualisierungen auf dem Baseboard Management Controller werden sofort aktiviert. Alle anderen Firmwareaktualisierungen werden das nächste Mal aktiviert, wenn die Einheit neu gestartet wird. Anschließend werden weitere Neustarts ausgeführt, bis der Aktualisierungsvorgang abgeschlossen ist. Es wird ein Ereignis ausgelöst, wenn der Status zum Firmware-Wartungsmodus „Ausstehend“ wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.
 - **Verzögerte Aktivierung.** Es werden einige, aber nicht alle Aktualisierungsvorgänge ausgeführt. Zieleinheiten müssen manuell neu gestartet werden, damit der Aktualisierungsprozess fortgesetzt wird. Anschließend werden weitere Neustarts ausgeführt, bis der Aktualisierungsvorgang abgeschlossen ist. Es wird ein Ereignis ausgelöst, wenn der Status zum Firmware-Wartungsmodus „Ausstehend“ wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.

Wenn die Zieleinheit aus irgendeinem Grund neu startet, wird der verzögerte Aktualisierungsprozess abgeschlossen.

Wichtig:

- Verwenden Sie **Normal neu starten**, um den Server neu zu starten und den Aktualisierungsprozess fortzuführen. Sie dürfen *nicht* **Sofort neu starten** verwenden.
- Sie dürfen die Option „Verzögerte Aktivierung“ für maximal 50 Einheiten gleichzeitig auswählen. XClarity Orchestrator überwacht Einheiten mit verzögerter Aktivierung aktiv. So wird dafür gesorgt, dass die verzögerte Aktivierung beim Neustart einer Einheit durchgeführt wird. Wenn Sie Aktualisierungen mit verzögerter Aktivierung für mehr als 50 Einheiten nutzen möchten, teilen Sie diese in Gruppen mit jeweils 50 Einheiten auf.
- **Sofortige Aktivierung.** Während des Aktualisierungsprozesses wird die Zieleinheit möglicherweise mehrmals automatisch neu gestartet, bis der gesamte Prozess abgeschlossen ist. Legen Sie alle Anwendungen auf der Zieleinheit still, bevor Sie fortfahren.

Anmerkungen:

- Bei Servern, die von XClarity Management Hub 2.0 und für ThinkEdge Client-Einheiten verwaltet werden, wird unabhängig von der ausgewählten Aktivierungsregel nur die sofortige Aktivierung unterstützt.
 - Wenn die Wake-On-LAN-Booption aktiviert ist, kann sie beim Ausschalten des Servers zu Konflikten mit Lenovo XClarity Administrator führen. Dies gilt auch für Firmwareaktualisierungen, bei denen ein Wake-On-LAN-Client im Netzwerk „Aktivierung durch Magic Packet“-Befehle sendet.
6. **Optional:** Wählen Sie **Aktualisierung erzwingen** aus, um die Firmware auch dann auf den ausgewählten Komponenten zu aktualisieren, wenn die Firmwareversion aktuell ist oder eine Firmwareaktualisierung auf eine frühere Version als die aktuelle Version vorzunehmen, die derzeit auf den ausgewählten Komponenten installiert ist.
 7. **Optional:** Wählen Sie **Aktualisierung planen** aus, um das Datum und die Uhrzeit für die Ausführung der Firmwareaktualisierung auszuwählen. Wenn diese Option nicht ausgewählt ist, wird die Firmware sofort aktualisiert.
 8. Klicken Sie auf **Aktualisierungen durchführen**, um die Aktualisierungen anzuwenden. 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).
- **Für alle nicht konformen Einheiten in bestimmten Gruppen, denen eine bestimmte Aktualisierungskonformitätsrichtlinie zugeordnet ist**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Bereitstellung** (🔧) → **Aktualisierungen** und dann auf **Übernehmen und Aktivieren**, um die Übersicht Übernehmen und aktivieren aufzurufen.
 2. Klicken Sie auf die Registerkarte **Einheiten**.
 3. Wählen Sie eine oder mehrere Einheitengruppen aus, auf die Aktualisierungen angewendet werden sollen.
 4. Klicken Sie auf das Symbol **Aktualisierung übernehmen** (📧), um das Dialogfenster „Aktualisierungszusammenfassung“ anzuzeigen.
 5. Wählen Sie die Gruppen und die Aktualisierungskonformitätsrichtlinie aus.
 - Wenn Sie keine Richtlinie oder Gruppe auswählen, werden alle Einheiten aktualisiert, denen eine Richtlinie zugeordnet ist und die diese nicht erfüllen.
 - Wenn Sie eine Richtlinie aber keine Gruppe auswählen, werden alle Einheiten aktualisiert, denen diese Richtlinie zugeordnet ist und die diese nicht erfüllen.
 - Wenn Sie eine oder mehrere Gruppen aber keine Richtlinie auswählen, werden alle Einheiten in der Gruppe aktualisiert, die nicht mit der zugewiesenen Richtlinie konform sind.
 - Wenn Sie eine Richtlinie und eine oder mehrere Gruppen auswählen, werden alle Einheiten in der Gruppe aktualisiert, die dieser Richtlinie zugewiesen sind, mit dieser aber nicht konform sind.
 6. Wählen Sie aus, wann die Aktualisierungen aktiviert werden sollen.
 - **Priorisierte Aktivierung:** Firmwareaktualisierungen auf dem Baseboard Management Controller werden sofort aktiviert. Alle anderen Firmwareaktualisierungen werden das nächste Mal aktiviert, wenn die Einheit neu gestartet wird. Anschließend werden weitere Neustarts ausgeführt, bis der Aktualisierungsvorgang abgeschlossen ist. Es wird ein Ereignis ausgelöst, wenn der Status zum Firmware-Wartungsmodus „Ausstehend“ wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.
 - **Verzögerte Aktivierung.** Es werden einige, aber nicht alle Aktualisierungsvorgänge ausgeführt. Zieleinheiten müssen manuell neu gestartet werden, damit der Aktualisierungsprozess fortgesetzt wird. Anschließend werden weitere Neustarts ausgeführt, bis der Aktualisierungsvorgang

abgeschlossen ist. Es wird ein Ereignis ausgelöst, wenn der Status zum Firmware-Wartungsmodus „Ausstehend“ wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.

Wenn die Zieleinheit aus irgendeinem Grund neu startet, wird der verzögerte Aktualisierungsprozess abgeschlossen.

Wichtig:

- Verwenden Sie **Normal neu starten**, um den Server neu zu starten und den Aktualisierungsprozess fortzuführen. Sie dürfen *nicht* **Sofort neu starten** verwenden.
- Sie dürfen die Option „Verzögerte Aktivierung“ für maximal 50 Einheiten gleichzeitig auswählen. XClarity Orchestrator überwacht Einheiten mit verzögerter Aktivierung aktiv. So wird dafür gesorgt, dass die verzögerte Aktivierung beim Neustart einer Einheit durchgeführt wird. Wenn Sie Aktualisierungen mit verzögerter Aktivierung für mehr als 50 Einheiten nutzen möchten, teilen Sie diese in Gruppen mit jeweils 50 Einheiten auf.
- **Sofortige Aktivierung**. Während des Aktualisierungsprozesses wird die Zieleinheit möglicherweise mehrmals automatisch neu gestartet, bis der gesamte Prozess abgeschlossen ist. Legen Sie alle Anwendungen auf der Zieleinheit still, bevor Sie fortfahren.

Anmerkungen:

- Bei Servern, die von XClarity Management Hub 2.0 und für ThinkEdge Client-Einheiten verwaltet werden, wird unabhängig von der ausgewählten Aktivierungsregel nur die sofortige Aktivierung unterstützt.
 - Wenn die Wake-On-LAN-Bootoption aktiviert ist, kann sie beim Ausschalten des Servers zu Konflikten mit Lenovo XClarity Administrator führen. Dies gilt auch für Firmwareaktualisierungen, bei denen ein Wake-On-LAN-Client im Netzwerk „Aktivierung durch Magic Packet“-Befehle sendet.
7. **Optional:** Wählen Sie **Aktualisierung erzwingen** aus, um die Firmware auch dann auf den ausgewählten Komponenten zu aktualisieren, wenn die Firmwareversion aktuell ist oder eine Firmwareaktualisierung auf eine frühere Version als die aktuelle Version vorzunehmen, die derzeit auf den ausgewählten Komponenten installiert ist.
 8. **Optional:** Wählen Sie **Aktualisierung planen** aus, um das Datum und die Uhrzeit für die Ausführung der Firmwareaktualisierung auszuwählen. Wenn diese Option nicht ausgewählt ist, wird die Firmware sofort aktualisiert.
 9. Klicken Sie auf **Aktualisierungen durchführen**, um die Aktualisierungen anzuwenden. 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).

Nach dieser Aufgabe

In der Übersicht Muster können Sie die folgenden Aktionen ausführen.

- Leiten Sie Berichte über die Firmwarekonformität regelmäßig an eine oder mehrere E-Mail-Adressen weiter, indem Sie auf das Symbol **Berichtsweiterleiter erstellen** (⊕) klicken. Der Bericht wird mithilfe der Datenfilter gesendet, die derzeit auf die Tabelle angewendet werden. Alle ein- und ausgeblendeten Tabellenspalten werden in den Bericht einbezogen. Siehe [Berichte weiterleiten](#) für weitere Informationen.
- Fügen Sie einem bestimmten Berichtsweiterleiter einen Bericht über die Firmwarekonformität hinzu, indem Sie die Datenfilter verwenden, die derzeit auf die Tabelle angewendet werden. Klicken Sie dazu auf das Symbol **Zu Berichtsweiterleiter hinzufügen** (↗). Wenn der Berichtsweiterleiter bereits einen Bericht über die Firmwarekonformität enthält, wird der Bericht so aktualisiert, dass die aktuellen Datenfilter angewendet werden.

Sie können einen geplanten Firmwareaktualisierungsjob, der noch nicht ausgeführt wurde, abbrechen, indem Sie in der Menüleiste von XClarity Orchestrator zu **Überwachung** (📊) → **Jobs** navigieren und die Registerkarte **Zeitpläne** öffnen, um die Übersicht Geplante Jobs anzuzeigen. Wählen Sie den geplanten Job aus und klicken Sie auf das Symbol **Abgebrochen** (🛑).

Kapitel 6. Trends analysieren und Probleme vorhersagen

Lenovo XClarity Orchestrator generiert Analyse-Alerts auf Basis bekannter Hardware- und Firmwareprobleme, überwacht Trends, um Anomalien in den verwalteten Ressourcen zu erkennen, und erstellt Heuristiken, die die Wahrscheinlichkeit von bevorstehenden Problemen oder Ausfällen berechnen können. Die Trends werden als Abfragen, Grafiken und Diagramme dargestellt, die den Konformitätsstatus, den Problemverlauf und die Aufschlüsselung der Ressourcen mit den meisten Problemen angeben. Anschließend können Sie diese Trends analysieren, um Einblicke in die Ursache von Problemen zu erhalten und diese schnell zu beheben.

Wichtig:

- Die Analysefunktionen werden für ThinkAgile, ThinkSystem und ThinkEdge Server unterstützt, auf denen XCC-Firmware v1.4 oder höher ausgeführt wird.
- Zur Verwendung der Analysefunktionen wird eine Lenovo XClarity Orchestrator Analytics-Lizenz für jede verwaltete Einheit benötigt, die die Analysefunktionen unterstützt. Eine Lizenz ist *nicht* an bestimmte Einheiten gebunden. Siehe [Lizenzen von XClarity Orchestrator anwenden](#) in der Onlinedokumentation zu XClarity Orchestrator für weitere Informationen.

Angepasste Analyseberichte erstellen

Analyseberichte werden kontinuierlich im Hintergrund ausgeführt, um einen Echtzeit-Einblick darüber zu geben, wie gut Ihr Rechenzentrum arbeitet.

Zu dieser Aufgabe

Lenovo XClarity Orchestrator enthält mehrere vordefinierte Analyseberichte, die auf Ereignis-, Bestands- oder Metrikdaten basieren, die von den verwalteten Ressourcen erfasst werden. Diese werden dann als Statistiken (in tabellarischer Form) oder grafisch als Balkendiagramme, Kreisdiagramme angezeigt. Beispiele für diese Berichte finden Sie auf den Seiten **Analysen** (🔍) → **Vordefinierte Analysen**.

Sie können auch eigene angepasste Berichte erstellen, um für Sie besonders relevante Daten darzustellen.

Vorgehensweise

Gehen Sie wie folgt vor, um angepasste Analyseberichte zu erstellen.

Schritt 1. Erstellen Sie angepasste Alerts.

XClarity Orchestrator generiert Analyse-Alerts auf Basis bekannter Hardware- und Firmwareprobleme. Sie können auch angepasste Alerts erstellen, die in Ihren angepassten Berichten verwendet werden sollen.

Schritt 2. Erstellen Sie angepasste Berichte (Abfragen).

Sie können XClarity Orchestrator angepasste grafische Berichte hinzufügen, indem Sie auf den Daten basierende Abfragen definieren, die Sie am meisten interessieren.

Regeln für angepasste Analyse-Alerts erstellen

Lenovo XClarity Orchestrator generiert Alerts auf der Grundlage bekannter Hardware- und Firmwareprobleme. Sie können benutzerdefinierte *Alert-Regeln* festlegen, um Analyse-Alerts auszulösen, wenn ein bestimmtes Ereignis eintritt oder wenn eine bestimmte Metrik überschritten wird. Anschließend können Sie diese Alerts verwenden, um benutzerdefinierte Analyseberichte (Abfragen) zu generieren.

Zu dieser Aufgabe

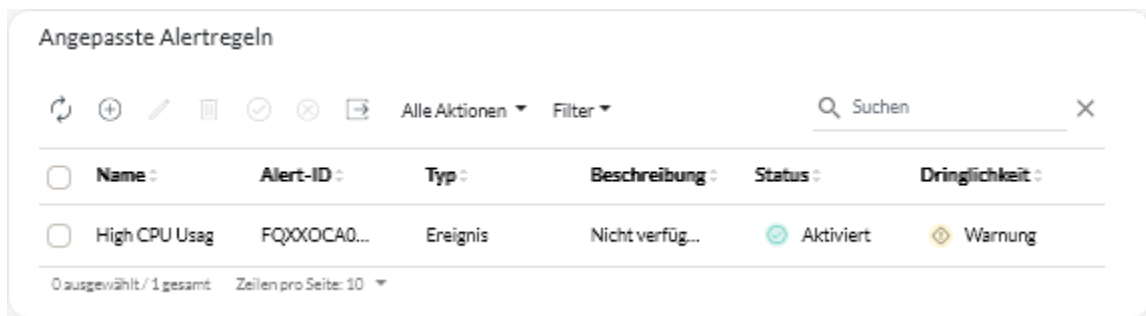
Ereignisse werden für alle Alerts ausgelöst, einschließlich angepasster Analyse-Alerts. Für den aktiven Alert und das Ereignis wird derselbe Ereigniscode im Format FQXX0CAxxxxc verwendet, wobei xxxx der eindeutige Bezeichner und c der Schweregrad ist.

Angepasste Alerts sind in der Liste der aktiven Alerts für den Integritätsstatus enthalten. Alle aktiven Alerts, einschließlich angepasster Alerts, werden in einer einzigen, einheitlichen Ansicht angezeigt (siehe [Aktive Alerts überwachen](#)).

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Regeln für angepasste Alerts zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Analysen** (🔍) → **Angepasste Alerts**, um die Übersicht Angepasste Alertregeln aufzurufen.



Schritt 2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Regel für angepasste Alerts erstellen aufzurufen.

Schritt 3. Geben Sie einen eindeutigen Namen und eine optionale Beschreibung für den angepassten Alert an.

Schritt 4. Wählen Sie den Quelltyp für diese Regel aus.

- **Ereignis:** Löst auf der Grundlage der Regelkriterien einen Alert aus, wenn ein bestimmtes Ereignis eintritt.
- **Metrik:** Löst auf der Grundlage der Regelkriterien einen Alert aus, wenn eine bestimmte Metrik überschritten wird.

Schritt 5. Klicken Sie auf **Details für Regelauslöser** und geben Sie die Kriterien für diese Regel an. Die Kriterien variieren je nach Quelltyp.

- **Ereignisbasierte Alert-Regeln**

- Geben Sie den Zieltyp für diesen Alert an.
 - **Einheit:** Löst einen Alert aus, wenn das Ereignis auf einer beliebigen Einheit eintritt. Der Gerätenamenname ist in diesem Alert enthalten.
 - **Einheitengruppe:** Löst einen Alert aus, wenn das Ereignis auf einer Einheit in einer beliebigen Einheitengruppe eintritt. Der Gruppenname ist im Alert enthalten.
- Geben Sie die ID des Ereignisses an, das einen Alert auslöst. Eine Liste von Ereignis-IDs finden Sie unter [Ereignis- und Altermeldungen](#) in der Onlinedokumentation zu XClarity Orchestrator.
- Geben Sie an, wie oft (Anzahl) das Ereignis im angegebenen Intervall auftreten muss, bevor ein Alert ausgelöst wird.
- Wählen Sie den Zeitraum (Intervall) in Minuten aus, in dem das Ereignis eintritt, bevor ein Alert ausgelöst wird.

- **Metrikbasierte Alert-Regeln**

- Wählen Sie den Kriterienmodus aus.
 - **Durchschnitt:** Löst einen Alert aus, wenn der Durchschnittswert der Metrik während eines bestimmten Intervalls den Schwellenwert (basierend auf dem Vergleichswert) überschreitet.

Sie können z. B. eine Regel erstellen, um einen Alert auszulösen, wenn die durchschnittliche CPU-Temperatur (**metric**) während eines 24-Stunden-Zeitraums (**interval**) größer als (**operator**) 40 °C (**threshold**) ist.
 - **Anzahl:** Löst einen Alert aus, wenn die Metrik während eines bestimmten Intervalls den Schwellenwert (basierend auf dem Vergleichswert) eine gewisse Anzahl Male überschreitet.

Sie können z. B. eine Regel erstellen, um einen Alert auszulösen, wenn die CPU-Temperatur (**metric**) während eines 24-Stunden-Zeitraums (**interval**) fünfmal (**count**) größer als (**operator**) 40 °C (**threshold**) ist.
 - **Einfach:** Löst einen Alert aus, wenn die Metrik den Schwellenwert (basierend auf dem Vergleichswert) überschreitet.

Sie können z. B. eine Regel erstellen, um einen Alert auszulösen, wenn die CPU-Temperatur (**metric**) größer als (**operator**) 40 °C (**threshold**) ist.
- Wählen Sie die Kennzahl (Metrik) für diesen Alert aus einer Liste von Metriken aus, die für die verwalteten Ressourcen unterstützt werden.
- Wenn der Kriterienmodus „Anzahl“ lautet, geben Sie an, wie oft der Wert im angegebenen Intervall überschritten werden muss, bevor ein Alert ausgelöst wird.
- Wählen Sie die Vergleichsfunktion aus.
 - **>=.** Größer als oder gleich
 - **<=.** Kleiner als oder gleich
 - **>.** Größer als
 - **<.** Kleiner als
 - **=.** Gleich
 - **!=.** Nicht gleich
- Geben Sie den Schwellenwert an, der mit dem metrischen Wert verglichen werden soll.
- Wenn der Kriterienmodus „Durchschnitt“ oder „Anzahl“ lautet, wählen Sie den Zeitraum (Intervall) in Minuten aus, in dem die Metrik ausgewertet wird.

Schritt 6. Klicken Sie auf **Alert- und Ereignisdetails** und geben Sie die Informationen an, die für den Alert und das Ereignis angezeigt werden sollen.

1. Geben Sie die Nachricht, Beschreibung und Benutzeraktion an, die für den Alert und das Ereignis angezeigt werden sollen. Sie können Variablen einschließen, indem Sie den Feldnamen (Variable) in doppelte Klammern setzen, z. B. `[[DeviceName]]`. Eine Liste der verfügbaren Felder (basierend auf der ausgewählten Metrik) wird in der Tabelle rechts neben den Eingabefeldern angezeigt.
2. Wählen Sie den Schweregrad für diese Alert-Regel aus.
 - **Warnung.** Der Benutzer kann entscheiden, ob eine Maßnahme erforderlich ist.
 - **Kritisch.** Eine Maßnahme ist sofort erforderlich. Die Auswirkungen sind weitreichend (möglicherweise steht der Ausfall einer kritischen Ressource unmittelbar bevor).
3. Geben Sie eine eindeutige 4-stellige Nummer an, die für den Ereigniscode dieses Alerts verwendet werden soll. Sie können eine Zahl von 0001 bis 9999 angeben, die noch nicht verwendet wird.

Schritt 7. Ändern Sie optional den Status in **Aktiviert**, damit XClarity Orchestrator einen Analyse-Alert auslöst, wenn die Kriterien für den angepassten Alert erfüllt sind.

Schritt 8. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

Sie können die Liste der Analyse-Alerts anzeigen, die aufgrund der aktivierten Regeln für angepasste Alerts ausgelöst wurden. Klicken Sie dazu auf **Überwachung** (🔍) → **Alerts**.

In der Übersicht Regeln für angepasste Alerts können Sie die folgenden Aktionen ausführen:

- Bearbeiten Sie die Eigenschaften einer ausgewählten Regel für angepasste Alerts, indem Sie auf das Symbol **Bearbeiten** klicken (✎).
- Sie können eine ausgewählte Regel für angepasste Alerts löschen, indem Sie auf das Symbol **Löschen** klicken (🗑️).
- Aktivieren oder deaktivieren Sie eine oder mehrere ausgewählte Regeln für angepasste Alerts durch Klicken auf das Symbol **Aktivieren** (✅) oder **Deaktivieren** (❌).

Angepasste Berichte erstellen (Abfragen)

Sie können angepasste tabellarische und grafische Berichte zu Lenovo XClarity Orchestrator hinzufügen, indem Sie Abfragen auf Grundlage von erfassten Daten definieren, z. B. Alerts, Ereignisse, Bestand, Einheitenmetriken oder Ihre benutzerdefinierten Metriken (Aggregationen).

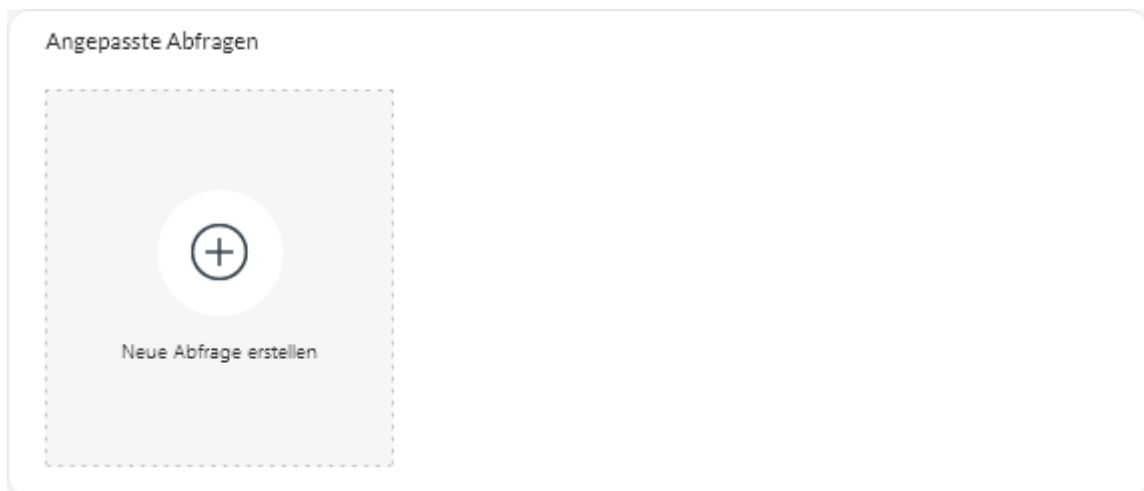
Vorbereitende Schritte

Wichtig: Für die Erstellung von angepassten und Analyseberichten in XClarity Orchestrator ist ein grundlegendes Verständnis von Datenbanken und Datenbankabfragen erforderlich.

Zu dieser Aufgabe

Führen Sie die folgenden Schritte aus, um einen angepassten Bericht zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Analysen** (🔍) → **Angepasste Abfragen**, um die Übersicht Angepasste Abfragen aufzurufen.



Schritt 2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfenster Angepasste Abfragen erstellen aufzurufen.

Schritt 3. Geben Sie einen eindeutigen Namen für die angepasste Abfrage an.

Schritt 4. Wählen Sie den Datentyp aus, den Sie als Quelle für diese Abfrage verwenden möchten.

Sie können einen der folgenden Datenquellentypen auswählen.

- **Alerts.** Hardware- oder Verwaltungsbedingungen, die untersucht werden müssen und eine Benutzeraktion erfordern
- **Ereignisse.** Ressourcen- und Prüfereignisse
- **Ereignisressource.** Hardware- oder Orchestrator-Bedingung, die auf einer verwalteten Einheit, einem Ressourcenmanager oder XClarity Orchestrator aufgetreten ist
- **Ereignisprüfung.** Benutzeraktivitäten, die über einen Ressourcenmanager oder XClarity Orchestrator durchgeführt wurden
- **Bestandsmanager.** Bestandsdaten für Ressourcenmanager
- **Bestandseinheit.** Bestandsdaten für alle Typen von verwalteten Einheiten
- **Bestandseinheitenserver.** Bestandsdaten für verwaltete Server
- **Bestandseinheiten-Switch.** Bestandsdaten für verwaltete Switches
- **Bestandseinheitenspeicher.** Bestandsdaten für verwalteten Speichereinheiten
- **Bestandseinheitengehäuse.** Bestandsdaten für verwaltete Gehäuse
- **CPUTemp.** Metrikdaten für die Temperatur in Celsius von jedem Prozessor in einer verwalteten Einheit. Die Metrikdaten werden jede Minute erfasst.
- **CPUUtilizationStats.** Metrikdaten für die Prozessorauslastung als Prozentsatz für eine verwaltete Einheit. Die Metrikdaten werden jede Minute erfasst.
- **InletAirTemp.** Metrikdaten für die Einlasslufttemperatur in Celsius für jeden Prozessor in einer verwalteten Einheit. Die Temperatur wird jede Minute erfasst.
- **MemoryUtilizationStats.** Metrikdaten für die Hauptspeicherauslastung als Prozentsatz für eine verwaltete Einheit. Die Metrikdaten werden jede Minute erfasst.
- **PowerMetrics.** Metrikdaten für den Stromverbrauch in Watt, für alle Prozessoren, Speichermodule oder das gesamte System für eine verwaltete Einheit. Diese Metriken werden alle 30 Sekunden erfasst.
- **PowerSupplyStats.** Metrikdaten für Netzteileingang und -ausgang in Watt für eine verwaltete Einheit. Diese Metriken werden alle 30 Sekunden erfasst.

Die aufgelisteten Typen von Datenquellen (Alerts, Ereignisse, Bestände und Metriken) variieren je nach den in XClarity Orchestrator verfügbaren Daten. Wenn z. B. Alerts-Daten verfügbar sind, ist der **Alerts**-Typ aufgelistet. Wenn Ereignisdaten verfügbar sind, werden **Ereignis***-Typen aufgelistet.

Die ausgewählte Datenquelle wirkt sich auf die Daten aus, die auf der Registerkarte **Abfragebedingungen** verfügbar sind. Wenn Sie einen generischen Typ, z. B. **Bestandseinheiten** auswählen, werden nur die Attribute aufgelistet, die allen Einheiten gemeinsam sind. Wenn Sie **Bestandseinheitenserver** auswählen, werden die Attribute aufgelistet, die allen Servern gemeinsam sind.

Schritt 5. Klicken Sie auf **Abfragebedingungen**, um die Abfragebedingungen für den Bericht zu definieren.

1. Grenzen Sie die Daten ein, die für diese Abfrage verwendet werden sollen.
 - a. Wählen Sie mindestens ein Feld aus der Dropdown-Liste **Gefilterte Felder** aus. Die Felder sind basierend auf dem Datenquellentyp gelistet, den Sie in [Schritt 4](#) ausgewählt haben.
 - b. Wenn Sie mehrere Filterfelder ausgewählt haben, wählen Sie den Operator aus, der zum Erstellen der Abfrage verwendet werden soll. Es kann einen der folgenden Werte aufweisen.
 - **AND.** Alle Werte müssen übereinstimmen.
 - **OR.** Mindestens ein Wert muss übereinstimmen.
 - **AND (negiert).** Kann Wert darf mit einem anderen übereinstimmen.
 - **OR (negiert).** Ein oder mehrere Werte dürfen nicht übereinstimmen.
 - c. Wählen Sie für jedes ausgewählte gefilterte Feld den Operator aus der Dropdown-Liste **Vergleich** und den Wert des Felds aus. Die verfügbaren Vergleichsoperatoren unterscheiden sich je nach dem Datentyp des Attributs.
 - **>=.** Entspricht Werten, die *größer oder gleich* einem angegebenen Wert sind.

- **<=**. Entspricht Werten, die *kleiner oder gleich* einem angegebenen Wert sind.
- **>**. Entspricht Werten, die *größer* als ein angegebener Wert sind.
- **<**. Entspricht Werten, die *kleiner* als ein angegebener Wert sind.
- **=**. Entspricht Werten, die *gleich* einem angegebenen Wert sind.
- **! =**. Entspricht Werten, die *ungleich* einem angegebenen Wert sind.
- **Enthält**. (Nur Bestands- und Ereignisabfragen) Entspricht allen in einem Array angegebenen partiellen Werten.
- **In**. (Nur Bestands- und Ereignisabfragen) Entspricht allen in einem Array angegebenen Werten.
- **NotIn**. (Nur Bestands- und Ereignisabfragen) Entspricht keinem der in einem Array angegebenen partiellen Werten.

Tipp: Erstellen Sie zum Suchen der aktuellen Werte für ein beliebiges Feld eine neue Abfrage mit demselben Datenquellentyp und wählen Sie in der Dropdown-Liste **Gruppierte Felder** den Feldnamen aus. Geben Sie 0 für den **Grenzwert** an und klicken Sie auf **Speichern**. Die Registerkarte **Diagrammoptionen** wird mit einer Liste aller aktuellen Werte angezeigt.

2. Wählen Sie optional im Abschnitt **Ergebniszusammenlegung** eine Zusammenlegungsfunktion aus, um ein neues Feld basierend auf den gefilterten Daten zu erstellen und einen Namen (Alias) für das neue Feld anzugeben. Bei einigen Zusammenlegungsfunktionen wie „Durchschnitt“ und „Maximum“ müssen Sie auch das Feld angeben, auf das die Funktion angewendet werden soll.

Bei Ereignis- und Bestandsabfragen können Sie eine der folgenden Funktionen auswählen:

- **Durchschnitt**. Statistisches Mittel aller Werte
- **Summe**. Summe aller Werte
- **Anzahl**. Anzahl der Werte
- **Maximum**. Höchster Wert
- **Minimum**. Niedrigster Wert
- **Erster**. Wert mit dem ältesten Zeitstempel
- **Letzter**. Wert mit dem neuesten Zeitstempel

Bei metrischen Abfragen können Sie eine der folgenden Funktionen auswählen.

- **Anzahl**. Anzahl der Werte, die nicht null sind
- **Eindeutig**. Liste der eindeutigen Werte
- **Integral**. Durchschnittlicher Feldwert
- **Mittel**. Arithmetisches Mittel (Durchschnitt) der Werte
- **Median**. Zentralwert
- **Modus**. Häufigster Wert
- **Streuung**. Unterschied zwischen den Minimal- und Maximalwerten
- **Stddev**. Standardabweichung
- **Summe**. Summe aller Werte

3. Wählen Sie optional die Felder aus, die Sie verwenden möchten, um die Abfrageergebnisse mit der Dropdown-Liste **Gruppierte Felder** zu gruppieren. Wenn Sie ein gruppiertes Feld auswählen, dekonstruiert XClarity Orchestrator die Daten, sodass für jeden Wert in den ausgewählten Feldern ein Datenpunkt vorhanden ist.
4. Wählen Sie optional aus, wie die Abfrageergebnisse sortiert werden sollen, indem Sie ein Feld in der Dropdown-Liste **Sortierung nach Feld** und die Sortierreihenfolge in der Dropdown-Liste **Sortierreihenfolge** auswählen. Bei Metrikabfragen können Sie nur nach Zeit sortieren.
5. Geben Sie optional die Anzahl der in den Abfrageergebnissen zurückzugebenden Datenpunkte im Feld **Grenzwert** an. Der Standardgrenzwert ist 10. Wenn Sie 0 angeben oder das Feld leer lassen, werden alle Datenpunkte zurückgegeben.

Optional können Sie auch die Anzahl der Datenpunkte angeben, die im Feld **Abweichung** in den Abfrageergebnissen übersprungen werden sollen.

6. (Nur Metrikabfragen) Wenn Sie gruppierte Felder auswählen, können Sie optional die Anzahl der Datensätze angeben, die in den Abfrageergebnissen im Feld **Seriengrenzwert** zurückgegeben werden sollen. Der Standardgrenzwert ist ein leeres Feld (0). Wenn Sie 0 angeben oder das Feld leer lassen, werden alle Datensätze zurückgegeben.

Optional können Sie auch die Anzahl der Datensätze angeben, die im Feld **Serienabweichung** in den Abfrageergebnissen übersprungen werden sollen.

7. Klicken Sie auf **Speichern**, um die Abfrage zu speichern und den Bericht zu generieren.


Schritt 6. Klicken Sie auf **Diagrammoptionen**, um das Aussehen des Berichts auszuwählen. Die folgenden Diagrammtypen stehen zur Verfügung:

- **Tabelle.** Darstellung der Daten in tabellarischer Form.
- **Balken.** Darstellung der Daten als grafisches Balkendiagramm. Wählen Sie die Felder aus, die für die X- und Y-Achse verwendet werden sollen.
- **Kreis.** Darstellung der Daten als Kreisdiagramm. Wählen Sie die Felder aus, die für die X- und Y-Achse verwendet werden sollen. Sie können nur dann ein Kreisdiagramm wählen, wenn die Daten nicht gruppiert sind.



Schritt 7. Klicken Sie auf **Erstellen**, um eine neue Übersicht hinzuzufügen, die einen Bericht mit den aktuellen Abfrageergebnissen enthält.

Nach dieser Aufgabe

Auf der Übersicht Angepasste Abfragen können Sie die folgenden Aktionen ausführen.


- Vergrößern Sie einen angepassten Bericht, indem Sie auf der Übersicht mit den angepassten Berichten auf das Symbol **Vergrößern** () klicken. Bei Tabellenberichten werden mit dem Berichtssymbol auf der Übersicht „Angepasste Abfragen“ nur die ersten vier Spalten der Tabelle angezeigt. Sie können den Bericht vergrößern, um alle Spalten der Tabelle zu sehen.

Der Link **Details ansehen** in einer Tabellenspalte weist darauf hin, dass die Spalte mehrere Datenfelder enthält. Klicken Sie auf den Link **Details ansehen**, um eine Popup-Tabelle anzuzeigen, in der die zusätzlichen Daten aufgelistet sind.

- Bearbeiten Sie die Eigenschaften in einem angepassten Bericht, indem Sie in der Übersicht auf das Symbol **Bearbeiten** () klicken.
- Sie können einen angepassten Bericht löschen, indem Sie in der Übersicht auf das Symbol **Löschen** () klicken.

Bootzeiten der Einheit analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, in denen die Bootzeiten für verwaltete Einheiten zusammengefasst sind. Die *Bootzeit* ist die Zeitdauer (in Sekunden) bis zum Abschluss des Systemstarts vor Übergabe an das Betriebssystem.

Klicken Sie zum Anzeigen der Berichte zu Bootzeiten auf **Analysen** () → **Vordefinierte Analysen** und dann auf **Bootzeiten**, um die zugehörigen Analyseübersichten zu öffnen.

Anmerkung: Boot-Statistiken stehen nur für ThinkSystem und ThinkAgile Einheiten zur Verfügung, auf denen XCC-Firmware v1.40 oder höher ausgeführt wird.

Bootzeiten

Diese Berichtskarte enthält ein Balkendiagramm, in dem die Dauer der Ausführung von Bootvorgängen für Einheiten mit der längsten der aktuellen Bootzeiten angezeigt wird.

Verbindungsprobleme analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, in denen Statistiken zu Verbindungsproblemen aufgeführt sind.

Verbindungsverluste werden mit dem folgenden Ereignis gemeldet.

- **FQXHMDM0163J**: Die Verbindung zwischen Ressourcenmanager und Baseboard Management Controller in der Einheit ist offline.

Klicken Sie zum Anzeigen der Berichte zu Verbindungsverlusten auf **Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Verbindungsprobleme**, um die zugehörigen Analyseübersichten zu öffnen.

Verbindungsprobleme nach Zeit

Diese Berichtskarte enthält ein Balkendiagramm, in dem die Anzahl der Verbindungsprobleme angezeigt werden, die für jede Ressource im Laufe des aktuellen Tages oder Monats aufgetreten sind.

Sie können Daten für einen bestimmten Zeitbereich anzeigen, indem Sie in der rechten oberen Ecke der Karte das Symbol **Einstellungen** (⚙️) auswählen.

Top-10-Einheiten nach Anzahl der Verbindungsprobleme

Diese Berichtskarte enthält ein Balkendiagramm, in dem die ersten zehn Einheiten angezeigt werden, die insgesamt die meisten Verbindungsprobleme gemeldet haben. Sie können auf ein Element in der Legende klicken, um weitere Informationen zu einer bestimmten Ressource zu erhalten.

Sicherheitskorrekturen analysieren

Die Anzeige Analysen enthält Berichtsübersichten, die Analysen zu Sicherheitskorrekturen für allgemeine Sicherheitsrisiken und -lücken (CVEs) zeigen.

Klicken Sie zum Anzeigen der CVE-Berichte auf **Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Sicherheitskorrekturen**, um die zugehörigen Analyseübersichten zu öffnen.

Sicherheitskorrekturen

Diese Berichtskarte enthält die folgenden Statistiken und Diagramme.

- Ein Kreisdiagramm, das die Anzahl der verwalteten Einheiten mit allgemeinen Sicherheitsrisiken und -lücken (CVEs) zeigt, für die eine Sicherheitskorrektur verfügbar ist, sortiert nach dem höchsten CVE-Schweregrad
 - **Kritisch**. Anzahl der Einheiten, die mindestens eine kritische CVE aufweisen
 - **Nicht kritisch**. Anzahl der Einheiten, die mindestens eine hohe, mittlere oder niedrige CVE, aber keine kritischen CVEs aufweisen
 - **Geschützt**. Anzahl der Einheiten, die keine bekannten CVEs aufweisen und geschützt sind
- Ein Kreisdiagramm, das die Anzahl eindeutiger CVEs nach Schweregrad (kritisch, hoch, mittel oder niedrig) zeigt, für die Sicherheitskorrekturen verfügbar sind

Sie können den Mauszeiger über die einzelnen farbigen Balken im Kreisdiagramm bewegen, um weitere Informationen zum Status zu erhalten. Sie können auch auf die Zahl neben jedem Status klicken, um eine Liste aller Geräte anzuzeigen, die den Kriterien entsprechen.

Einheiten

Die Übersicht Einheiten zeigt die Gesamtzahl der CVEs, für die eine Sicherheitskorrektur verfügbar ist, und den höchsten CVE-Schweregrad für jede Einheit. Sie können die Einheit erweitern, um eine Liste der

Komponenten in dieser Einheit anzuzeigen, für die Sicherheitskorrekturen verfügbar sind, sowie die Anzahl der Sicherheitskorrekturen, die in Firmwareaktualisierungen verfügbar sind, die im Firmwareaktualisierungs-Repository heruntergeladen sind.

Wenn Sie auf die Anzahl der Sicherheitskorrekturen klicken, wird ein Dialogfenster mit einer gefilterten Liste der für diese Komponente anwendbaren CVEs geöffnet. In diesem Dialogfenster können Sie auf den CVE-Link klicken, um ausführliche Informationen zu diesem CVE im Internet zu erhalten.

Die Übersicht Einheiten kann mit der Umschalt-Schaltfläche **Einheiten ein-/ausblenden** ein- oder ausgeblendet werden. Die Umschalt-Schaltfläche ändert sich automatisch zu **Einheiten anzeigen**, wenn Sie auf eine Zahl in den Diagrammen klicken.

Integrität des Laufwerks analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, die Analysen zum Zustand und zur Fehlervoraussage von Festplattenlaufwerken und Solid-State-Laufwerken in verwalteten ThinkAgile und ThinkSystem Servern anzeigen.

Klicken Sie zum Anzeigen von Firmwareberichten auf **Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Vorausschauende Laufwerkanalyse**, um die zugehörigen Analyseübersichten zu öffnen.

Für die folgenden Laufwerkmodelltypen werden Analysen unterstützt.

Festplattenlaufwerke

- ST2000NX0253
- ST8000NM0055
- ST10000NM0086
- ST12000NM0008

Solid-State-Laufwerke

- Intel SSDSC2BB800G4

Wichtig: Laufwerke mit älterer Firmware können nicht analysiert werden. Installieren Sie die neueste Firmwareversion für die Laufwerke, um eine vorausschauende Analyse zu ermöglichen.

Gefährdete Laufwerke

Diese Berichtskarte enthält ein Kreisdiagramm, das die Anzahl der Laufwerke in jedem Integritätsstatus (normal oder gefährdet) zeigt.

Verlauf der gefährdeten Laufwerke

Diese Berichtskarte enthält ein Balkendiagramm, das die Anzahl der ausgefallenen Laufwerke in der letzten Woche oder im letzten Jahr anzeigt. Bewegen Sie den Mauszeiger über jeden Balken im Diagramm, um eine gefilterte Liste der ausgefallenen Laufwerke nach Gerät am betreffenden Tag anzuzeigen.

Datenträger mit Fehlervoraussage

Diese Berichtskarte enthält eine Tabelle, in der die Geräte mit ausgefallenen Laufwerken aufgeführt sind. Sie können auf ein Gerät klicken, um die Details zu jedem gefährdeten Laufwerk in diesem Gerät anzuzeigen.

Firmware analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, die Analysen zur Firmware zeigen.

Klicken Sie zum Anzeigen von Firmwareberichten auf **Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Firmwareanalyse**, um die zugehörigen Analyseübersichten zu öffnen.

Firmwareanalyse

Diese Berichtskarte enthält ein Balkendiagramm, das die Anzahl der auf allen Einheiten installierten Firmware basierend auf Firmwarekategorie und Alter zeigt.

Firmware wird in die folgenden Kategorien unterteilt:

- Management-Controller
- Systemtools
- UEFI

Das Alter der Firmware wird in folgende Intervalle unterteilt:

- < 6 Monate
- 6 bis 12 Monate
- 1 bis 2 Jahre
- > 2 Jahre

Sie können die im Bericht enthaltenen Einheiten über die **Filter**-Eingabefelder filtern. Sie können auch Filterabfragen speichern, die regelmäßig verwendet werden sollen.

Die Übersicht Einheiten kann mit der Umschalt-Schaltfläche **Einheiten ein-/ausblenden** ein- oder ausgeblendet werden. Auf der Übersicht „Einheiten“ werden die Firmwaretypen und Altersgruppen für alle im Diagramm enthaltenen Einheiten aufgelistet.

Verlorene Ereignisse analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, in denen Statistiken zu verlorenen Ereignissen aufgeführt sind. Verlorene Ereignisse werden durch eine Lücke in den Sequenznummern ermittelt.

Ereignisse haben eine Sequenznummer, die die Reihenfolge angibt, in der jedes Ereignis auf einer bestimmten Einheit aufgetreten ist. Die Ereignissequenznummern von einzelnen Einheiten sollte immer fortlaufend sein. Wenn Sequenznummern fehlen, kann diese Lücke darauf hinweisen, dass ein oder mehrere Ereignisse verloren gegangen sind.

Klicken Sie zum Anzeigen der Berichte zu Ereignisverlusten auf **Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Verlorene Ereignisse**, um die zugehörigen Analysekarten zu öffnen.

Verlorene Ereignisse nach Zeit

Diese Berichtskarte enthält ein Balkendiagramm, in dem die Anzahl der Ereignisse angezeigt werden, die bei jeder Ressource im Laufe des aktuellen Tages oder Monats verloren wurden.

Sie können Daten für einen bestimmten Zeitbereich anzeigen, indem Sie in der rechten oberen Ecke der Karte das Symbol **Einstellungen** (⚙️) auswählen.

Top-10-Einheiten nach Anzahl der verlorenen Ereignisse

Diese Berichtskarte enthält ein Balkendiagramm, in dem die ersten zehn Einheiten angezeigt werden, die insgesamt die meisten verlorenen Ereignisse gemeldet haben.

Kapazität des Ressourcenmanagers analysieren und vorhersagen

Die Anzeige „Analysen“ enthält Berichtskarten, in denen prognostiziert wird, wann Ressourcenmanager die maximal zulässige Anzahl verwalteter Einheiten überschreiten. Für Lenovo XClarity Administrator-Ressourcenmanager werden bis zu 1.000 verwaltete Einheiten unterstützt.

Klicken Sie zum Anzeigen der Berichte zur Kapazität von Ressourcenmanagern auf **Erweiterte Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Vorhersage für Manager-Kapazität**, um die zugehörigen Analyseübersichten zu öffnen.

Managerkapazität

Dieser Bericht zeigt die Einheitenkapazität für jeden Ressourcenmanager, darunter Anzahl verwalteter Einheiten und Kapazitätsstatus, der angibt, ob die Kapazität überlastet ist. Die folgenden Kapazitätsstatus werden verwendet.

- (🟢) **Normal**. Die Anzahl der verwalteten Einheiten ist geringer als die maximale Anzahl unterstützter Einheiten.
- (🟡) **Warnung**. Die Anzahl der verwalteten Einheiten liegt nahe an der maximalen Anzahl unterstützter Einheiten.
- (🔴) **Kritisch**. Die Anzahl der verwalteten Einheiten übersteigt die maximale Anzahl unterstützter Einheiten.

Kapazitätstrend verwalten

Diese Berichtskarte enthält ein Liniendiagramm, in dem die Anzahl der verwalteten Einheiten im Laufe der Zeit für einen bestimmten Ressourcenmanager und ein Trend angezeigt werden, der angibt, wann die Anzahl der verwalteten Einheiten die maximal unterstützte Kapazität für diesen Ressourcenmanager erreicht.

Klicken Sie in der Tabelle „Managerkapazität“ auf eine Zeile, um die Kapazitätstrends für diesen Ressourcenmanager anzuzeigen.

Sie können den angezeigten Zeitraum ändern, indem Sie auf das Dropdown-Menü klicken. Sie können angeben, ob die Daten nach Jahr, Quartal, Monat oder Tag angezeigt werden sollen. Sie können die Anzahl der im Diagramm angezeigten Zeiträume auch mit dem Zoomfeld unter dem Diagramm ändern.

Auslastungstrends analysieren und vorhersagen

Die Anzeige Analysen enthält Berichtskarten, die historische und prognostizierte Prozessor-, Speicher- sowie Hauptspeichernutzung in Einheiten und virtuellen Ressourcen (wie Hosts, Clustern und virtuellen Maschinen) anzeigen.

Wichtig: Diese Funktion erfordert eine Verbindung mit dem VMware vRealize Operations Manager Ressourcenmanager (siehe [Ressourcenmanager verbinden](#)).

Navigieren Sie zum Anzeigen der Auslastungstrendberichte zu **Erweiterte Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Arbeitslastauslastungstrend**, um die zugehörigen Analyseübersichten zu öffnen.

Ressourcenauswahl

In diesem Bericht werden die vom Orchestrator-Server verwalteten Einheiten und virtuellen Ressourcen aufgeführt.

Klicken Sie in der Tabelle auf eine Zeile, um die Auslastungstrends für diese Ressource anzuzeigen.

CPU-Auslastungstrend

Diese Berichtskarte enthält ein Liniendiagramm, in dem die Prozessorauslastung im Laufe der Zeit für eine bestimmte virtuelle Ressource angezeigt wird. Ebenfalls wird ein Trend angezeigt, der angibt, wann die Prozessorauslastung die maximal unterstützte Kapazität für diese virtuelle Ressource erreicht.

Sie können den Zeitraum, der für historische und prognostizierte Daten angezeigt wird, über die Dropdown-Menüs **Protokoll** und **Projektion** ändern. Sie können die Anzahl der im Diagramm angezeigten Zeiträume auch mit dem Zoomfeld unter dem Diagramm ändern.

Hauptspeicherauslastungstrend

Diese Berichtskarte enthält ein Liniendiagramm, in dem die Hauptspeicherauslastung im Laufe der Zeit für eine bestimmte virtuelle Ressource angezeigt wird. Ebenfalls wird ein Trend angezeigt, der angibt, wann die Hauptspeicherauslastung die maximal unterstützte Kapazität für diese virtuelle Ressource erreicht.

Sie können den Zeitraum, der für historische und prognostizierte Daten angezeigt wird, über die Dropdown-Menüs **Protokoll** und **Projektion** ändern. Sie können die Anzahl der im Diagramm angezeigten Zeiträume auch mit dem Zoomfeld unter dem Diagramm ändern.

Speicherauslastungstrend

Diese Berichtskarte enthält ein Liniendiagramm, in dem die Speicherauslastung im Laufe der Zeit für eine bestimmte virtuelle Ressource angezeigt wird. Ebenfalls wird ein Trend angezeigt, der angibt, wann die Speicherauslastung die maximal unterstützte Kapazität für diese virtuelle Ressource erreicht.

Sie können den Zeitraum, der für historische und prognostizierte Daten angezeigt wird, über die Dropdown-Menüs **Protokoll** und **Projektion** ändern. Sie können die Anzahl der im Diagramm angezeigten Zeiträume auch mit dem Zoomfeld unter dem Diagramm ändern.

Leistungs- und Nutzungsmetriken analysieren

Die Anzeige „Analysen“ enthält Berichtsübersichten, die Heatmaps basierend auf bestimmten Metriken und Ressourcen der letzten 24 Stunden anzeigen.

Klicken Sie zum Anzeigen von Leistungs-Heatmaps auf **Erweiterte Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Leistungs-Heatmap**, um die zugehörigen Analyseübersichten zu öffnen.

Leistungs-Heatmap

Diese Berichtskarte enthält eine Heatmap mit der Anzahl der Einheiten, die metrische Werte innerhalb von bestimmten Bereichen in einem bestimmten Zeitraum haben.

Sie können auf eine beliebige Zelle in der Heatmap klicken, um eine Popup-Liste der in dieser Zelle enthaltenen Einheiten aufzurufen. Außerdem werden Informationen über den tatsächlichen metrischen Wert der einzelnen Einheiten angezeigt sowie der Zeitstempel, mit dem die Metrik erfasst wurde.

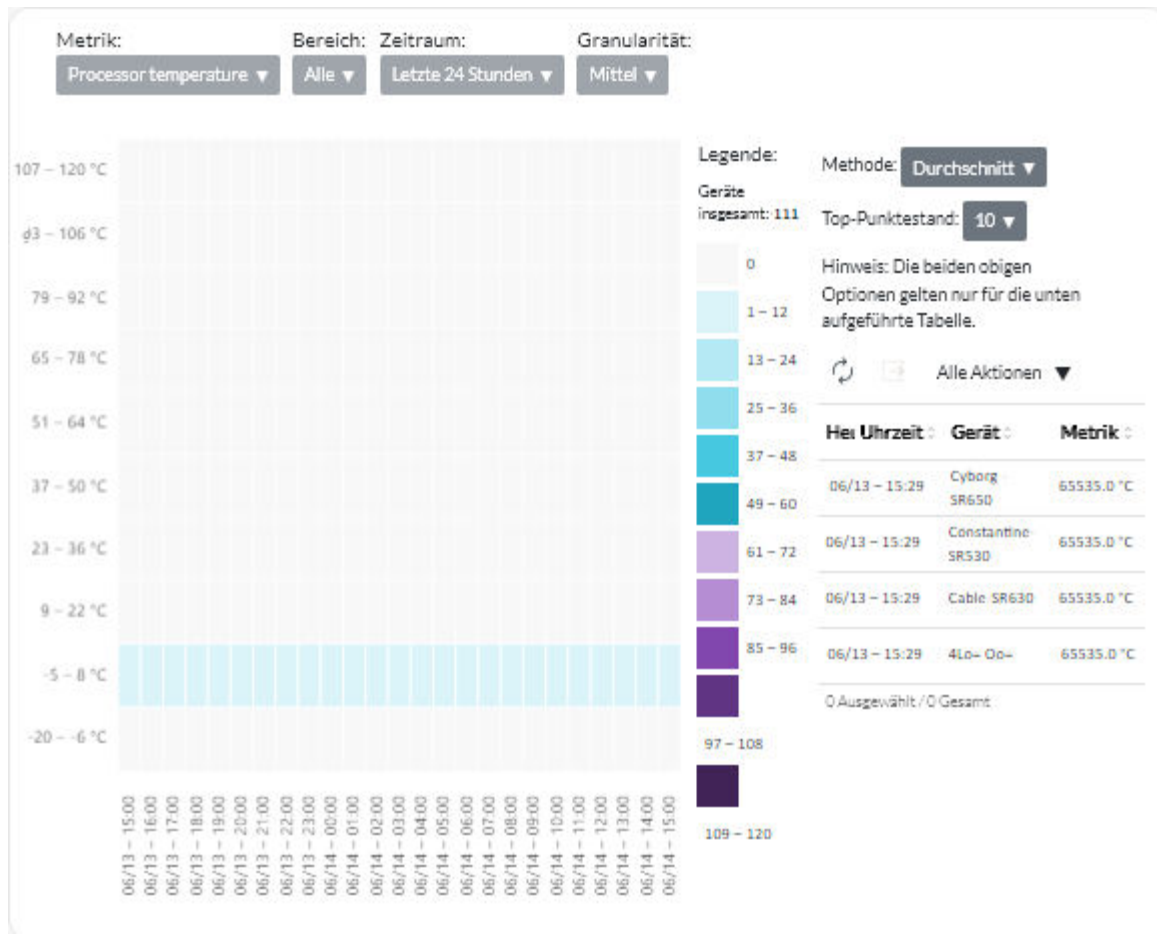
Sie können die Heatmap so konfigurieren, dass nur die Informationen angezeigt werden, die für Sie von Interesse sind.

- Sie können auswählen, die Daten für eine der folgenden Metriken anzuzeigen:
 - Prozessortemperatur
 - Prozessornutzung
 - Hauptspeichernutzung
- Sie können auswählen, ob Metrikdaten auf Basis des Durchschnittswerts oder des Spitzenwerts (Höchstwerts) aggregiert werden.
- Sie können die Heatmap filtern, sodass nur Metrikdaten für Einheiten in einer bestimmten Einheitengruppe enthalten sind.

Anmerkung: Wenn Sie die Benutzerschnittstelle zu einem bestimmten Ressourcenmanager hinzugefügt haben, werden nur Daten für Einheiten in den ausgewählten Gruppen, die ebenfalls vom Ressourcenmanager verwaltet werden, in die Heatmap aufgenommen.

- Sie können auch die Zahlenwertbereiche auswählen, die auf der X-Achse der Heatmap angezeigt werden sollen. Dies ist die Anzahl der Werte zwischen dem Maximum und dem Minimum, die je nach gewählter Zahl in gleiche Teile aufgeteilt wird. Sie können zwischen 10, 15 oder 20 wählen.

- Sie können auch auswählen, dass die obersten 10, 15 oder 20 Einheiten mit den höchsten Werten aufgelistet werden, inklusive des Zeitstempels, mit dem die Metrik erfasst wurde.



Wiederholte Ereignisse analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, in denen die wiederholten Ereignisse für jede Einheit zusammengefasst sind.

Wiederholte Ereignisse werden generiert, wenn die folgenden Bedingungen erfüllt sind:

- **FQXXOIS0002J**. Ein kritisches Ereignis oder ein Warnereignis mit derselben ID wurde mindestens einmal für dieselbe Einheit in mindestens drei aufeinander folgenden 5-Minuten-Zeiträumen generiert.
- **FQXXOIS0003J**. Für dieselbe Einheit wurden pro Stunde mehr als fünf kritische oder Warnereignisse in zwei oder mehr aufeinander folgenden Stunden generiert.

Klicken Sie zum Anzeigen der Berichte zu wiederholten Ereignissen auf **Erweiterte Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Wiederholte Ereignisse**, um die zugehörigen Analyseübersichten zu öffnen.

Wiederholte Ereignisse

Diese Berichtskarte enthält ein Balkendiagramm, in dem die Gesamtzahl der wiederholten Ereignisse für jede Einheit dargestellt wird.

Wiederholte Ereignisse pro Zeitraum

Diese Berichtskarte enthält ein Balkendiagramm, das die Gesamtzahl aller wiederholten Ereignisse am aktuellen Tag für jede Einheit anzeigt.

Nicht autorisierte Anmeldeversuche analysieren

Die Anzeige „Analysen“ enthält Berichtskarten, in denen die nicht autorisierten Zugriffsversuche (fehlgeschlagenen Anmeldeversuche) zusammengefasst sind.

Klicken Sie zum Anzeigen der Berichte zu nicht autorisierten Anmeldeversuchen auf **Analysen** (🔍) → **Vordefinierte Analysen** und dann auf **Nicht autorisierte Anmeldeversuche**, um die Analyseübersichten zu nicht autorisierten Zugriffen zu öffnen.

Anzahl der fehlgeschlagenen Anmeldeversuche pro Benutzer

Diese Berichtskarte enthält ein Diagramm, das die Gesamtzahl aller nicht autorisierten Anmeldeversuche für jeden Benutzer (nach Benutzername) anzeigt. Sie können die Daten als Balkendiagramm (📊) oder Kreisdiagramm (📈) anzeigen, indem Sie in der linken oberen Ecke der Karte auf das entsprechende Symbol klicken.

Sie können den Mauszeiger über die einzelnen Balken oder Sektor des Diagramms bewegen, um weitere Informationen zu erhalten, z. B. das letzte Auftreten.

Anzahl der fehlgeschlagenen Anmeldeversuche pro Benutzer, in jedem Zeitraum

Diese Berichtskarte enthält ein Balkendiagramm, das die Gesamtzahl aller nicht autorisierten Anmeldeversuche am aktuellen Tag für jeden Benutzer (nach Benutzername) anzeigt.

Anzahl der fehlgeschlagenen Anmeldeversuche pro Benutzer-IP-Adresse

Diese Berichtskarte enthält ein Balkendiagramm, das die Gesamtzahl aller nicht autorisierten Anmeldeversuche für jeden Benutzer (nach IP-Adresse) anzeigt. Sie können die Daten als Balkendiagramm (📊) oder Kreisdiagramm (📈) anzeigen, indem Sie in der linken oberen Ecke der Karte auf das entsprechende Symbol klicken.

Sie können den Mauszeiger über die einzelnen Balken oder Sektor des Diagramms bewegen, um weitere Informationen zu erhalten, z. B. das letzte Auftreten.

Anzahl der fehlgeschlagenen Anmeldeversuche pro Benutzer-IP-Adresse, in jedem Zeitraum

Diese Berichtskarte enthält ein Balkendiagramm, das die Gesamtzahl aller nicht autorisierten Anmeldeversuche am aktuellen Tag für jeden Benutzer (nach IP-Adresse) anzeigt.

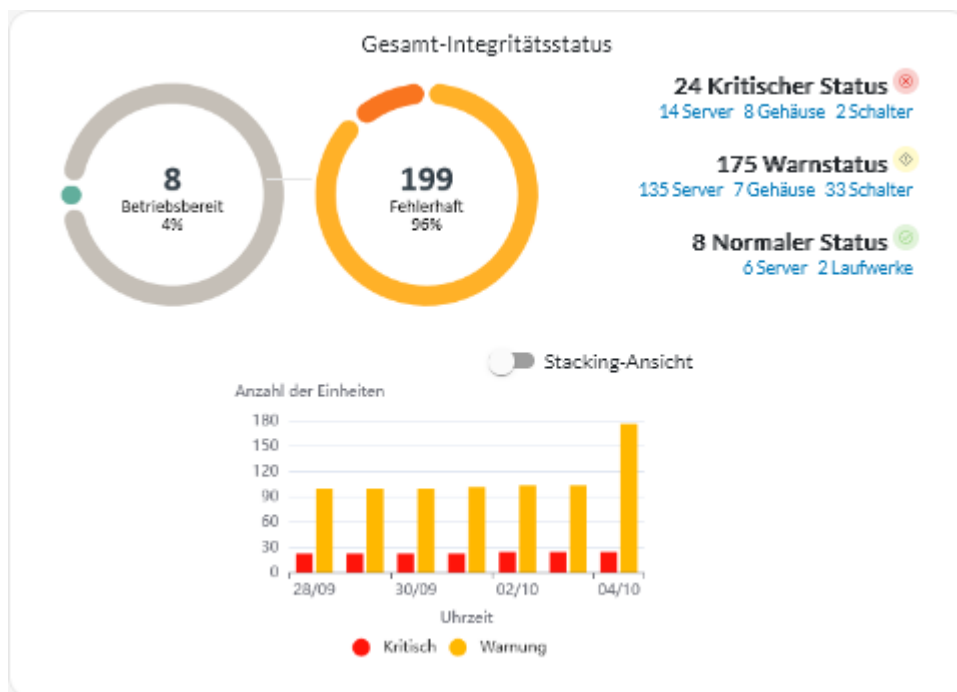
Integrität der Einheit analysieren

Auf der Karte „Gesamt-Integritätsstatus“ im Dashboard und auf der Karte „Einheitenanalyse“ auf den einzelnen Einheitenseiten ist der Gesamtzustand der verwalteten Einheiten zusammengefasst.

Statusübersicht aller Einheiten

Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Dashboard** (🏠), um die Dashboard-Karte mit einer Übersicht und dem Status aller verwalteten Einheiten und anderen Ressourcen anzuzeigen (siehe [Übersicht über Ihre Umgebung anzeigen](#)).

Sie können den Umfang der Zusammenfassung nur auf Einheiten ändern, die von einem bestimmten Ressourcenmanager oder in einer bestimmten Ressourcengruppe verwaltet werden, indem Sie das Dropdown-Menü **Manager auswählen** verwenden.



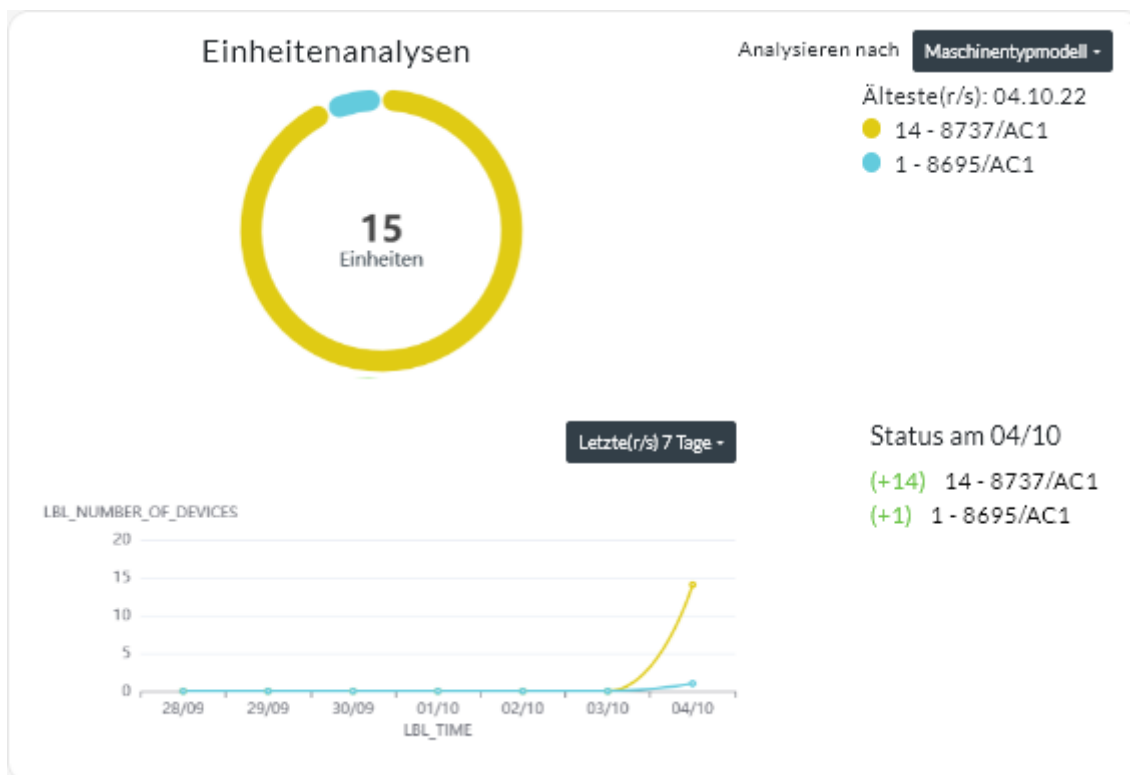
Jeder farbige Balken in den Kreis- und Balkendiagrammen zeigt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten. Sie können auch auf die Anzahl der Einheiten in jedem Status klicken, um eine Liste aller Einheiten anzuzeigen, die den Kriterien entsprechen.

Statusübersicht für alle Einheiten eines bestimmten Typs

Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (⚙️) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen. Wenn Sie beispielsweise **Server** auswählen, wird eine Liste aller Rack-, Tower- und Density-Server sowie aller Flex System- und ThinkSystem-Server in einem Gehäuse angezeigt.

Sie können den Umfang der Zusammenfassung basierend auf der Eigenschaft der Einheit in der Dropdown-Liste **Analysieren nach** ändern.

- **Maschinentypmodell.** (Standardeinstellung) In diesem Bericht wird der Zustand der Einheit nach Maschinentypmodell (MTM) zusammengefasst.
- **Maschinentyp.** In diesem Bericht wird der Zustand der Einheit nach Maschinentyp zusammengefasst.
- **Produktname.** In diesem Bericht wird der Zustand der Einheit nach Produkt zusammengefasst.



XClarity Orchestrator fasst den Zustand der Einheit basierend auf bestimmten Kriterien zusammen. Jede Zusammenfassung enthält die folgenden Informationen:

- Ein Kreisdiagramm, das die Gesamtzahl der fehlerhaften Einheiten sowie den Prozentsatz der Einheiten in jedem fehlerhaften Zustand anzeigt („Kritisch“, „Warnung“ und „Unbekannt“).

Jeder farbige Balken im Kreisdiagramm gibt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten.

- Ein Liniendiagramm, das die Anzahl der Einheiten in jedem Integritätsstatus pro Tag über die angegebene Anzahl an Tagen zeigt.

Jeder farbige Balken im Liniendiagramm gibt die Anzahl der Einheiten in einem bestimmten Status an. Sie können den Mauszeiger über die einzelnen farbigen Balken bewegen, um weitere Informationen zum Status zu erhalten.

- Die Anzahl der Einheiten jedes Typs, die an einem bestimmten Tag fehlerhaft sind. Der aktuelle Tag wird standardmäßig angezeigt. Sie können den Tag ändern, indem Sie den Mauszeiger über jeden Tag im Liniendiagramm bewegen.

Infrastrukturressourcenzustand analysieren

Sie können den allgemeinen Zustand und Sensortrends von Infrastrukturressourcen ermitteln.

Integritätsstatus der Infrastrukturressourcen

Klicken Sie in der Menüleiste von Lenovo XClarity Orchestrator auf **Ressourcen** (⚙️) → **Infrastruktur**, um die Übersicht „Infrastruktur“ anzuzeigen. Sie können den Integritätsstatus jeder Ressource in der Spalte **Status** ermitteln.

Sensortrends

Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) → **Infrastruktur**, um die Übersicht „Infrastruktur“ anzuzeigen. Klicken Sie anschließend in der Tabelle auf eine Infrastrukturrressource, um eine Liste der Sensoren für diese Ressource und ihre aktuellen Messwerte anzuzeigen.

Wählen Sie einen oder mehrere Sensoren aus und klicken Sie auf das Symbol **Diagramm** (📊), um die Liniendiagramme mit den Messwerten im Laufe der Zeit für jeden ausgewählten Sensor anzuzeigen. Standardmäßig werden Sensoren mit derselben Einheit (z. B. Watt oder Ampere) im selben Diagramm dargestellt.

Anmerkung: Schneider Electric EcoStruxure IT Expert erfasst alle 5 Minuten Sensordaten und XClarity Orchestrator synchronisiert diese Daten einmal stündlich. Aktuell speichert XClarity Orchestrator nur die letzten 60 Minuten an Daten.

Aktive Alerts analysieren

Auf der Alerts Analytics-Karte werden die aktiven Alerts zusammengefasst.

Lenovo XClarity Orchestrator fasst aktive Alerts basierend auf bestimmten Kriterien zusammen. Jede Zusammenfassung enthält die folgenden Informationen:

- Ein Kreisdiagramm, in dem die Gesamtanzahl der aktiven Alerts und der Prozentsatz der Alerts dargestellt wird, die den einzelnen Zusammenfassungstypen zugeordnet sind.
- Die Anzahl der aktiven Alerts für jeden Zusammenfassungstyp
- Alter des älteren aktiven Alerts
- Ein Liniendiagramm, das die Anzahl der aktiven Alerts für jede Zusammenfassung pro Tag über die angegebene Anzahl an Tagen zeigt
- Die Anzahl der Alerts, die für jeden Zusammenfassungstyp an einem bestimmten Tag aktiv waren. Der aktuelle Tag wird standardmäßig angezeigt. Sie können den Tag ändern, indem Sie den Mauszeiger über jeden Tag im Liniendiagramm bewegen.

Gesamte aktive Alerts

Gehen Sie wie folgt vor, um die gesamten Zusammenfassungen zu aktiven Alerts anzuzeigen.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Überwachung** (📊) → **Alerts**, um die Übersicht Alerts Analytics anzuzeigen.
2. Wählen Sie in der Dropdown-Liste über dem Liniendiagramm den Zeitraum aus. Der Standardwert sind die letzten sieben Tage.
3. Wählen Sie den Zusammenfassungstyp aus der Dropdown-Liste **Analysieren nach** aus.
 - **Wertigkeit.** (Standard) In diesem Bericht werden aktive Alerts nach Schweregrad zusammengefasst: „kritisch“, „Warnung“ und „Information“.
 - **Qelltyp** In diesem Bericht werden aktive Alerts zusammengefasst, die von den einzelnen Quelltypen generiert wurden, z. B. Einheit, Verwaltung und Analyse.
 - **Ressourcentyp.** In diesem Bericht werden aktive Alerts für jeden Ressourcentyp zusammengefasst, z. B. Einheiten, Ressourcenmanager und XClarity Orchestrator.
 - **Wartbarkeit.** In diesem Bericht werden aktive Alerts zusammengefasst, die jedem Wartungstyp zugeordnet sind: **keine** (kein Service erforderlich), **Benutzer** (Service wird vom Benutzer ausgeführt), **wartbar** (Service wird von Lenovo ausgeführt).

Aktive Alerts für eine bestimmte Einheit

Gehen Sie wie folgt vor, um den aktiven Alert für eine bestimmte Aktivität anzuzeigen.

1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔊) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.
2. Klicken Sie auf die Zeile für die Einheit, um die Übersichten für diese Einheit anzuzeigen.
3. Klicken Sie auf **Alertprotokoll**, um die Liste der aktiven Alerts für die Einheit und die Alerts Analytics-Karte anzuzeigen.
4. Wählen Sie auf der Übersicht Alerts Analytics den Zeitraum aus der Dropdown-Liste oberhalb des Liniendiagramms aus. Der Standardwert sind die letzten sieben Tage.
5. Wählen Sie den Zusammenfassungstyp aus der Dropdown-Liste **Analysieren nach** aus.
 - **Quelltyp** In diesem Bericht werden aktive Alerts zusammengefasst, die von den einzelnen Quelltypen generiert wurden, z. B. Einheit, Verwaltung und Analyse.
 - **Wartbarkeitstyp** In diesem Bericht werden aktive Alerts zusammengefasst, die jedem Wartungstyp zugeordnet sind: „keine“ (kein Service erforderlich), „Benutzer“ (Service wird vom Benutzer ausgeführt), „wartbar“ (Service wird von Lenovo ausgeführt).
 - **Wertigkeit**. In diesem Bericht werden aktive Alerts nach Wertigkeit zusammengefasst: „kritisch“, „Warnung“ und „Information“.

Kapitel 7. Mit Service und Unterstützung arbeiten

Lenovo XClarity Orchestrator bietet eine Reihe von Tools, um Servicedateien zu sammeln und an Lenovo Support zu senden, um automatische Benachrichtigungen an Service Provider im Falle von bestimmten wartungsfähigen Ereignissen auf spezifischen Einheiten einzurichten und um den Status von Service-Tickets und Informationen zur Garantie anzuzeigen. Sie können sich an den Lenovo Support wenden, um bei Problemen Hilfe und technische Unterstützung zu erhalten.

Regelmäßig Daten an Lenovo senden

Sie können optional zulassen, dass Lenovo XClarity Orchestrator Informationen über Ihre Hardwareumgebung sammelt und diese Daten regelmäßig an Lenovo sendet. Lenovo verwendet diese Daten, um Ihre Erfahrungen mit den Lenovo Produkten und dem Lenovo Support zu verbessern.

Vorbereitende Schritte

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

Achtung: Sie müssen die [Lenovo Datenschutzerklärung](#) akzeptieren, bevor Sie Daten an den Lenovo Support übermitteln können.

Zu dieser Aufgabe

Durch die Analyse der Hardwaredaten mehrerer Benutzer kann Lenovo Informationen zu Hardwareänderungen erhalten, die regelmäßig vorgenommen werden. Diese Daten können verwendet werden, um die prädiktiven Analysen sowie Ihre Service- und Unterstützungserfahrung zu verbessern, indem die entsprechenden Teile in den richtigen Regionen aufgestockt werden.

Wenn Sie zustimmen, Hardwaredaten an Lenovo zu senden, werden die folgenden Daten gesammelt und regelmäßig gesendet.

- **Tägliche Hardwaredaten.** Nur Änderungen an Bestandsdaten und Daten der Laufwerkanalyse (wenn die Datenerfassung aktiviert ist) für jede verwaltete Einheit.
- **Wöchentliche Hardwaredaten.** Alle Bestandsdaten für verwaltete Einheiten sowie Informationen zu verbundenen Ressourcenmanagern.

Achtung: Diese Daten sind *nicht anonymisiert*.

- Die gesammelten Daten *enthalten* UUIDs, WWNs, Einheiten-IDs und Seriennummern. XClarity Orchestrator ändert den Bestand, indem die UUIDs, WWNs und Einheiten-IDs mit SHA512 gehasht werden.
- Die gesammelten Daten *enthalten keine* Netzwerkinformationen (IP-Adressen, Domännennamen oder Hostnamen) oder Benutzerinformationen.

Wenn Daten an Lenovo gesendet werden, werden sie über HTTPS von der XClarity Orchestrator-Instanz an die Lenovo Upload-Funktionalität übertragen. REST-APIs werden über diese HTTPS-Verbindung aufgerufen, um die Daten zu senden. Ein bereits vorinstalliertes Zertifikat auf XClarity Orchestrator wird für die Authentifizierung verwendet. Wenn eine XClarity Orchestrator-Instanz keinen direkten Zugriff auf das Internet hat, aber ein Proxy für XClarity Orchestrator konfiguriert ist, werden die Daten über diesen Proxy übertragen.

Anschließend werden die Daten in das Lenovo Customer Care-Repository verschoben, wo sie für bis zu 5 Jahre gespeichert werden. Dieses Repository dient der sicheren Aufbewahrung und wird auch für an

Lenovo gesendete Debugdaten verwendet, die zur Problembehandlung benötigt werden. Es wird von den meisten Lenovo Server-, Speicher- und Switch-Produkten verwendet.

Im Lenovo Customer Care-Repository werden Abfragen für die angegebenen Daten ausgeführt und es werden dem Lenovo Produktteam Diagramme zur Analyse zur Verfügung gestellt.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Orchestrator das Sammeln und Senden von Kundendaten an Lenovo zu ermöglichen.

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

Regelmäßiges Hochladen von Daten

Wir möchten Sie um einen Gefallen bitten. Erlauben Sie uns, Informationen darüber zu sammeln, wie Sie dieses Produkt nutzen, damit wir es verbessern und enger auf Ihre Anforderungen abstimmen können?

[Lenovo Datenschutzerklärung](#)

Ich bin damit einverstanden, regelmäßig Hardwaredaten an Lenovo zu senden ?

Daten von Hardwarebestand und aus Laufwerkanalysen werden regelmäßig an Lenovo gesendet. Lenovo kann diese Daten nutzen, um seinen Support zu verbessern (z. B. die richtigen Teile in Ihrer Nähe zu lagern und schneller zu liefern).

Es werden niemals personenbezogene Daten gesammelt. Sie können uns jederzeit anweisen, die Sammlung dieser Daten zu beenden, indem Sie das regelmäßige Hochladen von Daten unter Verwendung der obenstehenden Schaltfläche deaktivieren.

Sie können das zuletzt gesendete Archiv oder ein Beispielarchiv basierend auf den von Ihnen gesammelten Informationen speichern. ?

Verfügbare Archive

Schritt 2. Hier können Sie sich optional damit einverstanden erklären, Hardwaredaten an Lenovo zu senden.

Schritt 3. Akzeptieren Sie die [Lenovo Datenschutzerklärung](#).

Nach dieser Aufgabe

Wenn Sie zustimmen, Ihre Daten zu senden, können Sie auf dieser Seite die folgenden Aktionen ausführen.

- Sie können die letzten Tages- und Wochen-Datenarchive, die an Lenovo gesendet wurden, auf dem lokalen System speichern. Wählen Sie dazu das Archiv aus, das Sie herunterladen möchten, und klicken Sie dann auf **Datei speichern**.

Service­daten für XClarity Orchestrator erfassen

Sie können Service­daten für Lenovo XClarity Orchestrator manuell erfassen und die Daten dann als Archiv im TAR.GZ-Format auf dem lokalen System speichern. Sie können die Service­dateien an Ihren bevorzugten Service Provider senden, damit dieser Ihnen bei der Behebung auftretender Probleme helfen kann.

Vorbereitende Schritte


Weitere Informationen: [Servicedaten erfassen](#)

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

Stellen Sie sicher, dass Webbrowser keine Popups für die XClarity Orchestrator-Website blockiert, wenn Sie Servicedaten herunterladen.


Vorgehensweise

Gehen Sie wie folgt vor, um Servicedaten für XClarity Orchestrator zu erfassen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung**  → **Service und Support** und klicken Sie dann im linken Navigationsbereich auf **Servicedaten**, um die Übersicht Verwaltungsservicedaten anzuzeigen.





Schritt 2. Klicken Sie auf **Speichern unter**, um Servicedaten zu sammeln und das Archiv auf dem lokalen System zu speichern.


Es wird ein Job zum Sammeln von Servicedaten erstellt. 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).

Nach dieser Aufgabe

Sie können außerdem diese verwandten Aktionen ausführen.

- Öffnen Sie in der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite manuell ein Service-Ticket für eine Einheit, indem Sie auf das Symbol **Service-Ticket öffnen**  klicken (siehe [Service-Ticket im Lenovo Support-Center manuell öffnen](#)).
- In der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite können Sie ein Servicedatenarchiv an ein ausgewähltes aktives Service-Ticket anhängen, indem Sie auf das Symbol **Servicedatei anhängen**  klicken. Sie können eine Datei von XClarity Orchestrator oder dem lokalen System anhängen.

Anmerkungen:

- Sie können eine einzelne Archivdatei anfügen, die nicht mehr als 2 GB groß ist. Der Dateiname darf nicht länger als 200 Zeichen sein. Informationen zum Erstellen von Servicedatenarchiven finden Sie unter (siehe [Servicedaten für Einheiten erfassen](#)).
- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können kein Archiv an ein Service-Ticket anhängen, das sich im geschlossenen oder in einem anderen Status befindet.
- Sie können kein Archiv an ein *Software*-Service-Ticket anhängen, das für einen Ressourcenmanager geöffnet wurde.
- In der Übersicht Verwaltungsservicedaten können Sie ein oder mehrere ausgewählte Servicedatenarchive auf dem lokalen System speichern, indem Sie auf das Symbol **Speichern**  klicken. Wenn mehrere Dateien ausgewählt sind, werden die Dateien vor dem Herunterladen in eine einzelne TAR.GZ-Datei komprimiert.

- In der Übersicht Verwaltungsservicedaten können Sie ein oder mehrere ausgewählte Servicedatenarchive, die nicht mehr benötigt werden, löschen. Klicken Sie dazu auf das Symbol **Löschen** (🗑️). Sie können auch alle Archive löschen, indem Sie auf das Symbol **Alle löschen** (☹️) klicken.

Servicedaten für Einheiten erfassen

Wenn bei einer Einheit ein Problem auftritt, bei dessen Lösung die Hilfe eines Service Providers wie Lenovo Support erforderlich ist, können Sie die Servicedaten (z. B. Protokolle, Serviceinformationen und Bestandsangaben) für diese Einheit manuell als Archivdatei im TAR.GZ-Format erfassen und so die Ermittlung der Problemursache unterstützen. Sie können die Archivdatei auf Ihrem lokalen System speichern und das Archiv anschließend an Ihren bevorzugten Service Provider senden.

Vorbereitende Schritte

Sie müssen erst die [Lenovo Datenschutzerklärung](#) akzeptieren, bevor Sie Servicedaten erfassen können. Klicken Sie zum Akzeptieren der Datenschutzerklärung auf **Verwaltung** (⚙️) → **Service und Support** und dann im linken Navigationsbereich auf **Call-Home-Konfiguration**. Wählen Sie dann **Ich stimme der Lenovo Datenschutzerklärung zu** aus.

Informationen zum Speichern von Servicedaten für XClarity Orchestrator auf Ihrem lokalen System finden Sie unter „[Servicedaten für XClarity Orchestrator erfassen](#)“ auf Seite 206.

Informationen zum manuellen Öffnen eines Service-Tickets und zum Senden der Servicedaten an das Lenovo Support-Center finden Sie unter „[Service-Ticket im Lenovo Support-Center manuell öffnen](#)“ auf Seite 216.

Informationen zum Einrichten der Call-Home-Funktion, um automatisch ein Service-Ticket im Lenovo Support-Center zu öffnen und das Servicedaten-Archiv zu senden, wenn ein wartungsfähiges Ereignis auf einer Einheit eintritt, finden Sie unter „[Service-Tickets mit Call-Home-Funktion automatisch öffnen](#)“ auf Seite 212.

Zu dieser Aufgabe

Wenn Sie Servicedaten über Lenovo XClarity Orchestrator sammeln, sendet der Orchestrator-Server die Anforderung an den Ressourcenmanager (z. B. Lenovo XClarity Administrator). Der Ressourcenmanager erfasst und speichert die Daten als Archivdatei in seinem lokalen Repository und übermittelt die Archivdatei anschließend an XClarity Orchestrator.

Sie können Servicedaten für maximal **50** Einheiten gleichzeitig erfassen.

Vorgehensweise

Gehen Sie wie folgt vor, um Servicedaten für eine bestimmte Einheit zu erfassen.

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

- Öffnen Sie in der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite manuell ein Service-Ticket für eine Einheit, indem Sie auf das Symbol **Service-Ticket öffnen** (🔍) klicken (siehe [Service-Ticket im Lenovo Support-Center manuell öffnen](#)).
- In der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite können Sie ein Servicedatenarchiv an ein ausgewähltes aktives Service-Ticket anhängen, indem Sie auf das Symbol **Servicedatei anhängen** (📎) klicken. Sie können eine Datei von XClarity Orchestrator oder dem lokalen System anhängen.

Anmerkungen:

- Sie können eine einzelne Archivdatei anfügen, die nicht mehr als 2 GB groß ist. Der Dateiname darf nicht länger als 200 Zeichen sein. Informationen zum Erstellen von Servicedatenarchiven finden Sie unter (siehe [Servicedaten für Einheiten erfassen](#)).
- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können kein Archiv an ein Service-Ticket anhängen, das sich im geschlossenen oder in einem anderen Status befindet.
- Sie können kein Archiv an ein *Software*-Service-Ticket anhängen, das für einen Ressourcenmanager geöffnet wurde.
- In der Übersicht Servicedaten können Sie ein oder mehrere ausgewählte Servicedatenarchive auf dem lokalen System speichern, indem Sie auf das Symbol **Speichern** (↓) klicken. Wenn mehrere Dateien ausgewählt sind, werden die Dateien als eine einzige TAR.GZ-Datei gespeichert.

Anmerkung: Sie können maximal **50** Servicedatenarchive gleichzeitig auf dem lokalen System speichern.

- In der Übersicht Servicedaten können Sie ein oder mehrere ausgewählte Servicedatenarchive, die nicht mehr benötigt werden, löschen. Klicken Sie dazu auf das Symbol **Löschen** (🗑️). Sie können auch alle Archive löschen, indem Sie auf das Symbol **Alle löschen** (⊖) klicken.

Anmerkung: Sie müssen Mitglied der Gruppe **SupervisorGroup** sein, um alle Archive löschen zu können.

Servicedaten für Einheiten importieren

Sie können Servicedatenarchive für bestimmte Einheiten importieren. Das Archiv kann von einem Lenovo XClarity Administrator-Ressourcenmanager oder direkt vom Baseboard Management Controller abgerufen werden.

Zu dieser Aufgabe

Sie können bis zu 10 Dateien gleichzeitig mit insgesamt 2 GB oder weniger importieren.

Wenn Sie Servicedaten für die Einheit mehrmals importieren, werden die Bestandsdaten durch die zuletzt importierten Servicedaten überschrieben.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Servicedatenarchiv zu importieren.

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

Schritt 2. Klicken Sie auf das Symbol **Importieren** (➡️), um Servicedatenarchive zu importieren.

Schritt 3. Ziehen Sie ein oder mehrere Servicedatenarchive (im TAR.GZ-, TZZ- oder TGZ-Format) in das Dialogfeld „Importieren“ oder klicken Sie auf **Durchsuchen**, um das Archiv zu suchen.

Schritt 4. Wählen Sie **Server in den Servicedaten nur zur Überprüfung zum Bestand hinzufügen** aus, wenn das Archiv für eine Einheit ist, die derzeit nicht von XClarity Orchestrator.

Schritt 5. Klicken Sie auf **Importieren**, um das Archiv zu importieren und zu analysieren und optional das Offlinegerät zu verwalten.

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).

Kontakte für Service und Support erstellen und zuordnen

Wenn Ressourcen Unterstützung vom Lenovo Support benötigen, muss Lenovo wissen, wer der Ansprechpartner ist. Sie können an zentraler Stelle Kontaktinformationen definieren und diese Kontakte dann als primäre und sekundäre Standardkontakte für bestimmte Ressourcen zuordnen.

Vorbereitende Schritte

Stellen Sie sicher, dass die [Lenovo Datenschutzerklärung](#) akzeptiert wird. Sie können die Datenschutzrichtlinie auf der Seite **Verwaltung** → **Service und Support** → **Call-Home-Konfiguration** prüfen und akzeptieren.

Zu dieser Aufgabe

Sie können primäre und sekundäre Kontakte Ressourcengruppen zuordnen. Wenn Sie Kontakte einer Ressourcengruppe zuordnen, werden die Kontakte allen Ressourcen in dieser Gruppe zugewiesen.

Die Zuordnung von primären und sekundären Kontakten ist optional. Wenn Sie jedoch einen sekundären Kontakt zuordnen möchten, müssen Sie auch einen primären Kontakt 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 (siehe [Service-Ticket im Lenovo Support-Center manuell öffnen](#)).

Wenn eine Einheit keiner Gruppe mit einem zugewiesenen primären Kontakt angehört, wird standardmäßig der Call-Home-Kontakt zugeordnet. Der Call-Home-Kontakt wird verwendet, wenn Service-Tickets automatisch über die Call-Home-Funktion geöffnet werden (siehe [Service-Tickets mit Call-Home-Funktion automatisch öffnen](#)). Die den Ressourcen und Gruppen zugeordneten Kontakte haben Vorrang vor dem standardmäßigen Call-Home-Kontakt.

Wird ein Service-Ticket manuell geöffnet, können Sie angeben, ob die der problematischen Ressource zugeordneten Kontakte verwendet werden sollen, oder einen anderen Kontakt auswählen (siehe [Service-Ticket im Lenovo Support-Center manuell öffnen](#)).

Vorgehensweise

• Einen Kontakt definieren

1. Klicken Sie in der Menüleiste von Lenovo XClarity Orchestrator auf **Verwaltung** (⚙️) → **Service und Support** und klicken Sie dann im linken Navigationsbereich auf **Kontaktinformationen**, um die Übersicht Kontaktinformationen anzuzeigen.
2. Klicken Sie auf das Symbol **Erstellen** (+), um das Dialogfeld Kontakt hinzufügen anzuzeigen.
3. Geben Sie den Kontaktnamen, die E-Mail-Adresse, die Telefonnummer und den Standort ein.
4. Wählen Sie die bevorzugte Kontaktmethode aus.

5. Klicken Sie auf **Speichern**, um den Kontakt zu erstellen.

- **Kontakte Ressourcengruppen zuordnen**

1. Klicken Sie in der Menüleiste von Lenovo XClarity Orchestrator auf **Ressourcen** (🔍) → **Gruppen**, um die Übersicht „Gruppen“ anzuzeigen.
2. Wählen Sie die Gruppe aus und klicken Sie auf das Symbol **Bearbeiten** (✎), um das Dialogfeld „Gruppe bearbeiten“ anzuzeigen.
3. Wählen Sie die Ressourcengruppe aus.
4. Klicken Sie auf die Registerkarte **Kontaktinformationen**.
5. Wählen Sie den primären Support-Kontakt sowie einen oder mehrere sekundäre Support-Kontakte aus, die allen Einheiten in der Gruppe zugeordnet werden sollen.
6. Klicken Sie auf **Speichern**.

Nach dieser Aufgabe

In der Übersicht Kontaktinformationen können Sie die folgenden Aktionen ausführen.

- Einen ausgewählten Kontakt ändern, indem Sie auf das Symbol **Bearbeiten** (✎) klicken
- Einen ausgewählten Kontakt löschen, indem Sie auf das Symbol **Entfernen** (🗑️) klicken

Service-Tickets mit Call-Home-Funktion automatisch öffnen

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

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

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.

Wenn sich Kontakte in den folgenden Ländern befinden, ist für die Call-Home-Unterstützung ein Lenovo Premier Support-Vertrag erforderlich. Weitere Informationen erhalten Sie von Ihrem Lenovo Ansprechpartner oder autorisierten Business Partner.

- Katar
- Saudi-Arabien
- Vereinigte Arabische Emirate

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 .

Weitere Informationen zum Anzeigen von Service-Tickets, die von der Call-Home-Funktion automatisch geöffnet wurden, finden Sie unter .

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

Sie können für Servicedaten die folgenden Aktionen ausführen.

- Sie setzen die Call-Home-Einstellungen auf die Standardwerte zurück, indem Sie auf **Konfiguration zurücksetzen** klicken.
- Sie zeigen Informationen zu *allen* Service-Tickets an, die entweder automatisch oder manuell mittels Call-Home-Funktion an das Lenovo Support-Center übermittelt wurden, indem Sie im linken Navigationsbereich auf **Service-Tickets** klicken. Siehe [Service-Tickets und Status anzeigen](#) für weitere Informationen.
- Sie sammeln die Servicedaten für eine ausgewählte Einheit in der Übersicht Einheitenaktionen. Klicken Sie dazu auf das Symbol **Servicedaten sammeln** (⏴). Siehe [Servicedaten für Einheiten erfassen](#) für weitere Informationen.
- In der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite können Sie ein Servicedatenarchiv an ein ausgewähltes aktives Service-Ticket anhängen, indem Sie auf das Symbol **Servicedatei anhängen** (⏵) klicken. Sie können eine Datei von XClarity Orchestrator oder dem lokalen System anhängen.

Anmerkungen:

- Sie können eine einzelne Archivdatei anfügen, die nicht mehr als 2 GB groß ist. Der Dateiname darf nicht länger als 200 Zeichen sein. Informationen zum Erstellen von Servicedatenarchiven finden Sie unter (siehe [Servicedaten für Einheiten erfassen](#)).
- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können kein Archiv an ein Service-Ticket anhängen, das sich im geschlossenen oder in einem anderen Status befindet.
- Sie können kein Archiv an ein *Software*-Service-Ticket anhängen, das für einen Ressourcenmanager geöffnet wurde.
- Öffnen Sie manuell ein Service-Ticket im Lenovo Support-Center, sammeln Sie Servicedaten für eine bestimmte Einheit und senden Sie diese Dateien an das Lenovo Support-Center über die Übersicht Einheitenaktionen. Wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Service-Ticket**

öffnen (☰). Siehe [Service-Ticket im Lenovo Support-Center manuell öffnen](#) für weitere Informationen. Falls das Lenovo Support-Center weitere Daten benötigt, werden Sie vom Lenovo Support aufgefordert, die Servicedaten für diese oder eine andere Einheit erneut zu sammeln.

Service-Ticket im Lenovo Support-Center manuell öffnen

Wenn die Call-Home-Funktion für einen Service-Weiterleiter aktiviert ist und ein wartungsfähiges Ereignis auf einer verwalteten Einheit eintritt, öffnet Lenovo XClarity Orchestrator automatisch ein Service-Ticket, sammelt die Servicedateien für die verwaltete Einheit und sendet sie an das Lenovo Support-Center. Sie können die Servicedateien für eine verwaltete Einheit auch manuell als Archiv erfassen, das Archiv auf dem lokalen System speichern und jederzeit an das Lenovo Support-Center senden. Durch Öffnen eines Service-Tickets wird der Lösungsfindungsprozess für Ihr Hardwareproblem gestartet, indem die relevanten Informationen dem Lenovo Support schnell und effizient zur Verfügung gestellt werden. Die Lenovo Kundendiensttechniker können beginnen, an einer Lösung für Ihr Problem zu arbeiten, sobald Sie ein Service-Ticket ausgefüllt und geöffnet haben.

Vorbereitende Schritte

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.

- Stellen Sie sicher, dass die Call-Home-Kontaktinformationen konfiguriert und aktiviert sind ([Service-Tickets mit Call-Home-Funktion automatisch öffnen](#)).
- Stellen Sie sicher, dass XClarity Orchestrator mit dem Lenovo Support-Center kommunizieren kann, indem Sie in der Menüleiste von XClarity Orchestrator auf **Verwaltung** (⚙️) → **Service und Support** klicken und im linken Navigationsfenster auf **Call-Home-Konfiguration** klicken, um die Seite „Call-Home-Konfiguration“ anzuzeigen. Klicken Sie anschließend auf **Call-Home-Konfigurationstest**, um ein Testereignis zu generieren und zu überprüfen, ob XClarity Orchestrator mit dem Lenovo Support-Center kommunizieren kann.
- Stellen Sie sicher, dass alle von XClarity Orchestrator benötigten Ports (darunter auch die Ports, die für die Call-Home-Funktion erforderlich sind) zur Verfügung stehen, bevor Sie die Call-Home-Funktion aktivieren. Weitere Informationen über Ports finden Sie unter [Portverfügbarkeit](#) in der Onlinedokumentation von XClarity Orchestrator.
- Stellen Sie sicher, dass eine Verbindung zu den Internetadressen hergestellt werden kann, die von der Call-Home-Funktion benötigt werden. Weitere Informationen zu Firewalls finden Sie unter [Firewalls und Proxy-Server](#) in der Onlinedokumentation von 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 über die Proxy-Einrichtung finden Sie unter [Netzwerkeinstellungen konfigurieren](#).

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.

Zu dieser Aufgabe

Wird ein Service-Ticket manuell geöffnet, können Sie angeben, ob die der problematischen Ressource zugeordneten Kontakte verwendet werden sollen, oder einen anderen Kontakt auswählen.



Wenn primäre und sekundäre Kontakte einer Gruppe zugeordnet sind, werden diese Kontakte den einzelnen Einheiten in dieser Gruppe zugewiesen. Jeder Einheit kann ein primärer Kontakt und ein oder mehrere

sekundäre Kontakte zugeordnet werden. Wenn eine Einheit mehreren Gruppen angehört, werden der Einheit alle sekundären Kontakte zugeordnet, die allen Gruppen zugewiesen sind, deren Mitglied die Einheit ist. 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 (siehe [Service-Tickets mit Call-Home-Funktion automatisch öffnen](#)).

Wenn eine Einheit keiner Gruppe mit einem zugewiesenen primären Kontakt angehört, wird standardmäßig der Call-Home-Kontakt zugeordnet. Der Call-Home-Kontakt wird verwendet, wenn Service-Tickets automatisch über die Call-Home-Funktion geöffnet werden (siehe [Service-Tickets mit Call-Home-Funktion automatisch öffnen](#)). Die den Ressourcen und Gruppen zugeordneten Kontakte haben Vorrang vor dem standardmäßigen Call-Home-Kontakt.


Vorgehensweise

Gehen Sie wie folgt vor, um manuell ein Service-Ticket zu öffnen.


- Wenn die Call-Home-Funktion konfiguriert und aktiviert ist, führen Sie die folgenden Schritte aus, um ein Service-Ticket zu öffnen, Servicedaten zu erfassen und die Dateien dann an das Lenovo Support-Center zu senden.
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen**  und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.
 2. Klicken Sie auf die Zeile für die Einheit, um die Übersichten für diese Einheit anzuzeigen.
 3. Klicken Sie im linken Navigationsbereich auf **Service**, um die Übersicht Service-Tickets zu öffnen.
 4. Klicken Sie auf das Symbol **Service-Ticket öffnen** , um das Dialogfeld „Neues Ticket hinzufügen“ anzuzeigen.
 5. Geben Sie eine Beschreibung des gemeldeten Problems einschließlich aller relevanter Ereigniscodes ein.
 6. Wählen Sie optional den Schweregrad des Problems aus. Es kann einen der folgenden Werte aufweisen.
 - **Dringend**
 - **Hoch**
 - **Mittel** (Standardeinstellung)
 - **Gering**
 7. Klicken Sie auf **Senden**.
- 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.

Nach dieser Aufgabe

Auf der einheitenspezifischen Serviceseite können Sie die folgenden Aktionen ausführen.

- Zeigen Sie Informationen zu *allen* geöffneten Service-Tickets an, indem Sie in der Menüleiste von XClarity Orchestrator zu **Service und Support** → **Service-Tickets** navigieren.
- Fügen Sie eine Notiz zu einem ausgewählten Service-Ticket hinzu, indem Sie auf das Symbol **Notiz zu Service-Ticket hinzufügen**  klicken.

Anmerkungen:

- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können keine Notiz zu einem Service-Ticket hinzufügen, das den Status „Geschlossen“ oder „Andere“ hat.
- Sie können Notizen nur zu Lenovo Service-Tickets hinzufügen. Sie können keine Notizen zu IBM, Service Now oder Cherwill Service-Tickets hinzufügen.
- Sie können keine Notiz zu einem *Software*-Service-Ticket hinzufügen, das für einen Ressourcenmanager geöffnet wurde.
- In der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite können Sie ein Servicedatenarchiv an ein ausgewähltes aktives Service-Ticket anhängen, indem Sie auf das Symbol **Servicedatei anhängen** () klicken. Sie können eine Datei von XClarity Orchestrator oder dem lokalen System anhängen.

Anmerkungen:

- Sie können eine einzelne Archivdatei anfügen, die nicht mehr als 2 GB groß ist. Der Dateiname darf nicht länger als 200 Zeichen sein. Informationen zum Erstellen von Servicedatenarchiven finden Sie unter (siehe [Servicedaten für Einheiten erfassen](#)).
- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können kein Archiv an ein Service-Ticket anhängen, das sich im geschlossenen oder in einem anderen Status befindet.
- Sie können kein Archiv an ein *Software*-Service-Ticket anhängen, das für einen Ressourcenmanager geöffnet wurde.

Service-Tickets und Status anzeigen

Mit der Call-Home-Funktion können Sie Informationen zu Service-Tickets anzeigen, die manuell erstellt oder automatisch an das Lenovo Support-Center übermittelt wurden, sowie Service-Tickets, die von anderen Unterstützungsservices als der Call-Home-Funktion generiert wurden.

Zu dieser Aufgabe

Der Status von Service-Tickets wird alle 24 Stunden mit dem Lenovo Support-Center synchronisiert.

In der Spalte **Status** wird der Status des Service-Tickets angegeben. Ein Service-Ticket kann einen der folgenden Status aufweisen.

- **Aktiv**
- **Beantwortet**
- **Abgebrochen**
- **Abgebrochen**
- **Erstellt**
- **Kunde storniert**
- **Geschlossen**
- **Verweigerte Partei**
- **Duplikat**
- **Fehler**
- **Fehlerstatus**
- **In Bearbeitung**
- **Initialisiert**
- **Gemischt**
- **Überwachung – Lösung implementiert**
- **Neu**
- **In der Warteschleife**
- **Ausstehend**

- Probleminitiierung
- Problem gelöst
- Verarbeitung läuft
- Abgelehnt
- Recherche
- Behoben
- Angebotene Lösung
- Übergeben
- Nicht bekannt
- Wartestatus
- Warten auf Details
- Warten auf internen Lenovo Support.
- Warten auf externen Supporter
- Warten auf Kundenfeedback zur Lösung
- Warten auf die Bereitstellung der Lösung
- Übertragen auf Managed Services
- Warme Übertragung
- Arbeit wird ausgeführt

Die Spalte **Typ** gibt den Typ des Service-Tickets an, der in der Spalte „Service-Ticketnummer“ aufgeführt ist. Der Service-Ticket-Typ kann einer der folgenden Werte sein:

- Cherwill-Ticket
- IBM Call-Home-Ticket
- Lenovo Call-Home-Ticket
- Lenovo Call-Home-Pass-Through-Ticket
- Lenovo Call-Home-Ticket per Software
- ServiceNow

Vorgehensweise

- **Status aller Service-Tickets anzeigen** Klicken Sie auf **Verwaltung** (🔗) → **Service und Support** und dann im linken Navigationsbereich auf **Service-Tickets**, um die Übersicht Service-Tickets anzuzeigen.

Tipp: Klicken Sie auf die Ereignis-ID, um eine Zusammenfassung des Ereignisses anzuzeigen, das das Service-Ticket generiert hat, einschließlich Benutzeraktion (falls vorhanden).

<input type="checkbox"/>	Service-Ticket	Status	Ereignis-ID	Beschreibur	Produktnam	Seriennumm	Erstellungszeitpunkt
<input type="checkbox"/>	100103...	Wird ...	FQXXOSS	test_ticket	Abyss-S...	ABYSSR...	11.09.23...
<input type="checkbox"/>	100103...	Wird ...	806F010C	Uncorre...	Abyss-S...	ABYSSR...	11.09.23...

0 ausgewählt / 2 gesamt Zeilen pro Seite: 15

- **Status von Service-Tickets für eine bestimmte Einheit anzeigen**
 1. Klicken Sie in der Menüleiste von XClarity Orchestrator auf **Ressourcen** (🔗) und dann auf den Einheitentyp, um eine tabellarische Übersicht mit allen verwalteten Einheiten dieses Typs anzuzeigen.
 2. Klicken Sie auf die Zeile für die Einheit, um die Übersichten für diese Einheit anzuzeigen.




3. Klicken Sie im linken Navigationsbereich auf **Service**, um die Übersicht Service-Tickets mit einer Liste aller Service-Tickets für die Einheit anzuzeigen.

Tipp: Klicken Sie auf die Ereignis-ID, um eine Zusammenfassung des Ereignisses anzuzeigen, das das Service-Ticket generiert hat, einschließlich Benutzeraktion (falls vorhanden).


Service-Ticket-ID	Status	Ereignis-ID	Beschreibung	Seriennummer	Erstellungsdatum
1001032647	Wird ...	FQXXOSS00	test_ticket	ABYSSR093	11.09.23, 0...
1001032643	Wird ...	806F010C2C	Uncorrecta...	ABYSSR093	11.09.23, 0...

Nach dieser Aufgabe

Sie können für Service-Tickets die folgenden Aktionen ausführen.

- Konfigurieren Sie XClarity Orchestrator so, dass ein Service-Ticket automatisch geöffnet wird, wenn ein wartungsfähiges Ereignis eintritt (siehe „[Service-Tickets mit Call-Home-Funktion automatisch öffnen](#)“ auf [Seite 212](#)).
- Synchronisieren Sie die Daten mit dem Lenovo Support-Center und aktualisieren Sie den Status aller aktiven Service-Tickets, indem Sie auf das Symbol **Service-Ticketstatus aktualisieren** () klicken.
- Öffnen Sie manuell ein Service-Ticket für eine bestimmte Einheit über die Service-Tickets-Karte auf der einheitsspezifischen Seite „Einheiten“, indem Sie auf das Symbol **Service-Ticket öffnen** () klicken.
- Fügen Sie eine Notiz zu einem ausgewählten Service-Ticket hinzu, indem Sie auf das Symbol **Notiz zu Service-Ticket hinzufügen** () klicken.

Anmerkungen:

- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können keine Notiz zu einem Service-Ticket hinzufügen, das den Status „Geschlossen“ oder „Andere“ hat.
- Sie können Notizen nur zu Lenovo Service-Tickets hinzufügen. Sie können keine Notizen zu IBM, Service Now oder Cherwill Service-Tickets hinzufügen.
- Sie können keine Notiz zu einem *Software*-Service-Ticket hinzufügen, das für einen Ressourcenmanager geöffnet wurde.
- In der Übersicht Service-Tickets auf der einheitenspezifischen Serviceseite können Sie ein Servicedatenarchiv an ein ausgewähltes aktives Service-Ticket anhängen, indem Sie auf das Symbol **Servicedatei anhängen** () klicken. Sie können eine Datei von XClarity Orchestrator oder dem lokalen System anhängen.

Anmerkungen:

- Sie können eine einzelne Archivdatei anfügen, die nicht mehr als 2 GB groß ist. Der Dateiname darf nicht länger als 200 Zeichen sein. Informationen zum Erstellen von Servicedatenarchiven finden Sie unter (siehe [Servicedaten für Einheiten erfassen](#)).

- Das Service-Ticket muss sich im Status „Offen“, „In Bearbeitung“ oder „In der Warteschleife“ befinden. Sie können kein Archiv an ein Service-Ticket anhängen, das sich im geschlossenen oder in einem anderen Status befindet.
- Sie können kein Archiv an ein *Software*-Service-Ticket anhängen, das für einen Ressourcenmanager geöffnet wurde.
- Leiten Sie Berichte über aktive Service-Tickets regelmäßig an eine oder mehrere E-Mail-Adressen weiter, indem Sie auf das Symbol **Berichtsweiterleiter erstellen** (+) klicken. Der Bericht wird mithilfe der Datenfilter gesendet, die derzeit auf die Tabelle angewendet werden. Alle ein- und ausgeblendeten Tabellenspalten werden in den Bericht einbezogen. Siehe für weitere Informationen.
- Fügen Sie einem bestimmten Berichtsweiterleiter einen Bericht über aktive Service-Tickets hinzu, indem Sie die Datenfilter verwenden, die derzeit auf die Tabelle angewendet werden. Klicken Sie dazu auf das Symbol **Zu Berichtsweiterleiter hinzufügen** (↗). Wenn der Berichtsweiterleiter bereits einen Bericht über aktive Service-Tickets enthält, wird der Bericht so aktualisiert, dass die aktuellen Datenfilter angewendet werden.

Informationen zur Garantie anzeigen

Sie können den Garantiestatus (einschließlich erweiterte Garantien) der verwalteten Einheiten bestimmen.

Vorbereitende Schritte

Lenovo XClarity Orchestrator muss Zugriff auf die folgenden URLs haben, um Informationen zur Garantie für die verwalteten Einheiten zu sammeln. Stellen Sie sicher, dass der Zugriff auf die URLs nicht von Firewalls blockiert wird. Siehe [Firewalls und Proxy-Server](#) in der Onlinedokumentation zu XClarity Orchestrator für weitere Informationen.

- Lenovo Warranty Datenbank (weltweit) – <https://ibase.lenovo.com/POIRequest.aspx>
- Lenovo Warranty Webservice – <http://supportapi.lenovo.com/warranty/> oder <https://supportapi.lenovo.com/warranty/>

Anmerkungen:

- Der Garantieservice wird für Benutzer in China derzeit nicht unterstützt.
- Garantien sind für Gehäuse, aber nicht für die entsprechenden Chassis Management Modules (CMM) aufgeführt.





Zu dieser Aufgabe

Einmal wöchentlich werden Garantieinformationen für Einheiten mit Garantien und einmal täglich für Einheiten ohne Garantien abgerufen.

Vorgehensweise

Klicken Sie zum Anzeigen von Informationen zur Garantie auf **Verwaltung** (⚙️) → **Service und Support** und dann im linken Navigationsbereich auf **Garantie**, um die Übersicht Garantie zu öffnen.

Garantie





 Alle Aktionen ▾ Filter ▾ Suchen X

Gerät	Status	Produktname	Typ/Modell	Garantienu	Seriennumr	Startdatum	Ablaufdatu	Gruppen
*node02	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT002	Nicht ver	Nicht ver	Nicht ver
*node02	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT002	Nicht ver	Nicht ver	Nicht ver
*node03	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT003	Nicht ver	Nicht ver	Nicht ver
*node03	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT003	Nicht ver	Nicht ver	Nicht ver
*node06	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT006	Nicht ver	Nicht ver	Nicht ver
*node06	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT006	Nicht ver	Nicht ver	Nicht ver
*node09	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT009	Nicht ver	Nicht ver	Nicht ver
*node09	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT009	Nicht ver	Nicht ver	Nicht ver
*node11	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT011	Nicht ver	Nicht ver	Nicht ver
*node11	Nicht v...	IBM Flex	7916/...	Nicht ver	SLOT011	Nicht ver	Nicht ver	Nicht ver
10.243.1	Nicht v...	Lenovo F	9532/...	Nicht ver	06DGCV	Nicht ver	Nicht ver	Nicht ver
10.243.1	Nicht v...	IBM Flex	8731/...	Nicht ver	23LAR6E	Nicht ver	Nicht ver	Nicht ver
10.243.1	Nicht v...	IBM Flex	7916/...	Nicht ver	CAR206:	Nicht ver	Nicht ver	Nicht ver
10.243.1	Nicht v...	IBM Flex	7917/...	Nicht ver	06EKZB:	Nicht ver	Nicht ver	Nicht ver
10.243.2	Nicht v...	IBM Flex	8737/...	Nicht ver	06PGVA:	Nicht ver	Nicht ver	Nicht ver

211 Gesamt Zeilen pro Seite: 15 ▾ 1 2 3 4 5 >

Nach dieser Aufgabe

Über die Karte Garantie können Sie die folgenden Aktionen ausführen:

- Konfigurieren Sie, wann Sie zum Garantieablauf von verwalteten Einheiten benachrichtigt werden möchten. Klicken Sie dazu auf das Symbol **Garantieeinstellungen konfigurieren** (⚙️). Die folgenden Einstellungen können Sie konfigurieren.
 - Aktivieren Sie die Generierung von Alerts, wenn die Garantie der Einheit bald abläuft.
 - Legen Sie fest, wie viele Tage vor Garantieablauf ein Alert generiert werden soll.
- Prüfen Sie die Informationen zur Garantie (falls verfügbar) für eine bestimmte Einheit auf der Lenovo Support-Website, indem Sie auf den Link in der Spalte **Status** klicken.
- Leiten Sie Berichte über aktive Garantien regelmäßig an eine oder mehrere E-Mail-Adressen weiter, indem Sie auf **Alle Aktionen** → **Berichtsweiterleiter hinzufügen** klicken. Der Bericht wird mithilfe der Datenfilter gesendet, die derzeit auf die Tabelle angewendet werden. Alle ein- und ausgeblendeten Tabellenspalten werden in den Bericht einbezogen.
- Fügen Sie einem bestimmten Berichtsweiterleiter einen Bericht über Garantien hinzu, indem Sie die Datenfilter verwenden, die derzeit auf die Tabelle angewendet werden. Klicken Sie dazu auf das Symbol

Zu Berichtsweiterleiter hinzufügen (↗). Wenn der Berichtsweiterleiter bereits einen Bericht über die Garantie enthält, wird der Bericht so aktualisiert, dass die aktuellen Datenfilter angewendet werden.

Lenovo