Lenovo XClarity Administrator Benutzerhandbuch

Version 4.0.0

Erste Ausgabe (Februar 2023)

Inhaltsverzeichnis

Tabellen

Zusammenfassung der Änderungen

Nachfolgeversionen der Lenovo XClarity Administrator-Verwaltungssoftware unterstützen neue Hardware, 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.

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

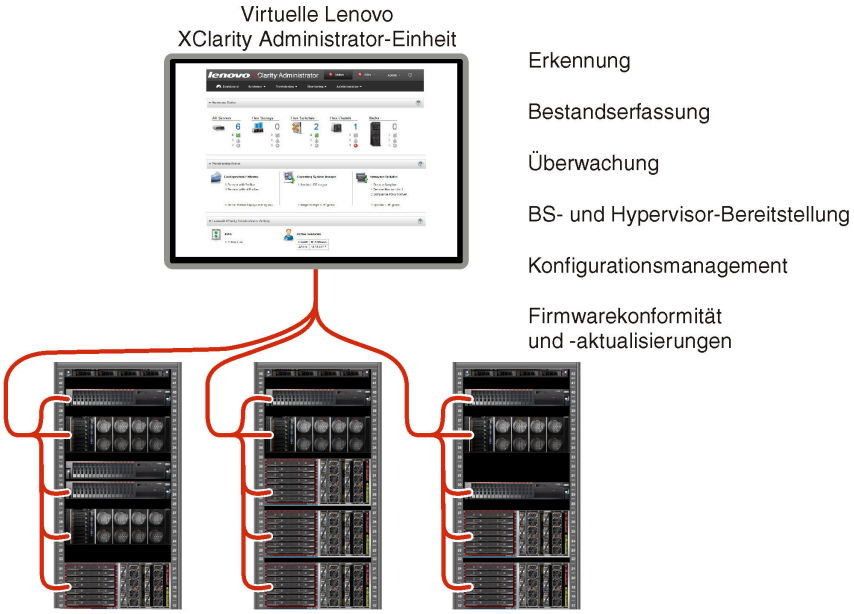
Funktion	Beschreibung
Verwaltung	Sie können den vollständig qualifizierten Domänennamen (FQDN) und DNS-Informationen des XClarity Administrator-Verwaltungsservers an verwaltete Server mit IMM2, XCC und XCC2 weiterleiten, damit die verwalteten Server den Verwaltungsserver mithilfe dieser Informationen finden können (siehe Netzwerkzugriff konfigurieren).
Überwachung	Sie können weitere Bestandsdaten zu PMEM-Komponenten (Persistent Memory) anzeigen (siehe Die Details eines verwalteten Servers anzeigen). Sie können weitere Bestandsdaten für Speichereinheiten anzeigen (siehe Die Details eines verwalteten Servers anzeigen).
Einheitenverwaltung	Sie können den Sicherheitsmodus für bestimmte Server getrennt von XClarity Administrator (Sicherheitseinstellungen für einen verwalteten Server konfigurieren und Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren) anzeigen und konfigurieren. Sekundäre IP-Adressen werden für den Baseboard Management Controller in entsprechenden ThinkSystem Servern unterstützt (siehe Die Details eines verwalteten Servers anzeigen).
Firmwareaktualisierungen	Sie können die Firmware für IBM TS4300 Bandbibliotheken aktualisieren (siehe Firmware auf verwalteten Einheiten aktualisieren).
Betriebssystembereitstellung	Sie können die folgenden Betriebssysteme für verwaltete Server implementieren (siehe Unterstützte Betriebssysteme). • Microsoft Windows Client 10 21H2, 10 22H2 und 11 22H2 • RedHat Enterprise Linux 9.x • Ubuntu Server 22.04.x

Kapitel 1. Lenovo XClarity Administrator – Übersicht

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

Weitere Informationen:

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



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

Hardwareverwaltung

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

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

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

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

Weitere Informationen:

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

Hardwareüberwachung

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

Weitere Informationen über das Verwalten von Hardware finden Sie unter Ereignisse handhaben und Mit Alerts arbeiten.

Weitere Informationen: XClarity Administrator: Überwachung

Konfigurationsmanagement

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

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

Weitere Informationen zum Konfigurieren von Servern finden Sie unter Server mithilfe von Konfigurationsmustern konfigurieren.

Weitere Informationen:

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

Firmwarekonformität und -aktualisierungen

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

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

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

Weitere Informationen zum Aktualisieren von Firmware finden Sie unter Firmware auf verwalteten Einheiten aktualisieren.

Weitere Informationen:

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

Betriebssystemimplementierung

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

Weitere Informationen zum Implementieren von Betriebssystemen finden Sie unter Betriebssysteme auf Bare-Metal-Servern installieren.

Weitere Informationen:

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

Benutzerverwaltung

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

XClarity Administrator unterstützt drei Arten von Authentifizierungsservern:

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

Weitere Informationen zum Authentifizierungstypen finden Sie unter Authentifizierungsserver verwalten.

Wenn Sie einen Benutzeraccount erstellen, weisen Sie diesem eine vordefinierte oder angepasste Rollengruppe zu, um die Zugriffsebene für diesen Benutzer zu steuern. Weitere Informationen zu Rollengruppen finden Sie unter Angepasste Rollengruppe erstellen.

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

Einheitenauthentifizierung

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

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

  Weitere Informationen zu Benutzern finden Sie unter Benutzeraccounts verwalten.

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

  Weitere Informationen zu gespeicherten Anmeldeinformationen finden Sie im Abschnitt Gespeicherte Anmeldeinformationen verwalten.

Sicherheit

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

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

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

Weitere Informationen zur Sicherheit finden Sie unter Eine sichere Umgebung implementieren.

Service und Support

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

Weitere Informationen:  XClarity Administrator: Service und Support

Taskautomatisierung mithilfe von Scripts

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

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

- Bei XClarity Administrator anmelden
- Verwalten und Beenden der Verwaltung von Gehäusen, Servern, Speichereinheiten und Top-of-Rack-Switches (Einheiten)
- Erfassen und Anzeigen von Bestandsdaten für Einheiten und Komponenten
- Implementieren eines Betriebssystemimages in einem oder mehreren Servern
- Konfigurieren von Servern mithilfe von Konfigurationsmustern
- Anwenden von Firmwareaktualisierungen auf Einheiten

Integration in andere verwaltete Software

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

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

Weitere Hinweise finden Sie unter Verwaltungshinweise in der Onlinedokumentation von XClarity Administrator.

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

Dokumentation

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

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

Sie können die Sprache der Onlinedokumentation folgendermaßen ändern:

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

Bei XClarity Administrator anmelden

Melden Sie sich über einen unterstützten Webbrowser bei der Lenovo XClarity Administrator-Webschnittstelle an.

Vorbereitende Schritte

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

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

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

Vorgehensweise

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

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

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

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

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

- **Für virtuelle Einheiten**: Die verwendete IP-Adresse hängt davon ab, wie Ihre Umgebung eingerichtet ist.

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

  Statische IPv4-Adresse verwenden

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

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

  DHCP-Server in derselben Übertragungsdomäne wie XClarity Administrator verwenden

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

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

  DHCP-Server in einer anderen Übertragungsdomäne als XClarity Administrator verwenden

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

```
------------------------------------------
Lenovo XClarity Administrator  Version x.x.x
------------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>
```

```
================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

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

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

– **Firefox:**

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

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

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

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

– **Internet Explorer:**

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

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

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

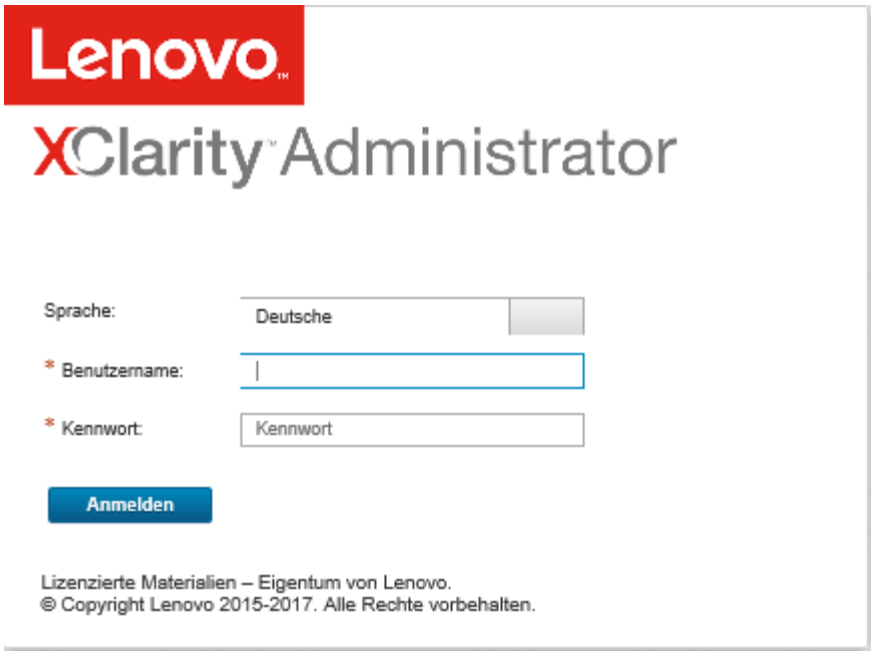
  ```
  PS C:> ipconfig
  Windows IP-Konfiguration

  Ethernet-Adapter vEthernet (teamVirtualSwitch):

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

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

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

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

Die Seite für die erste Anmeldung bei XClarity Administrator wird angezeigt:



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

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

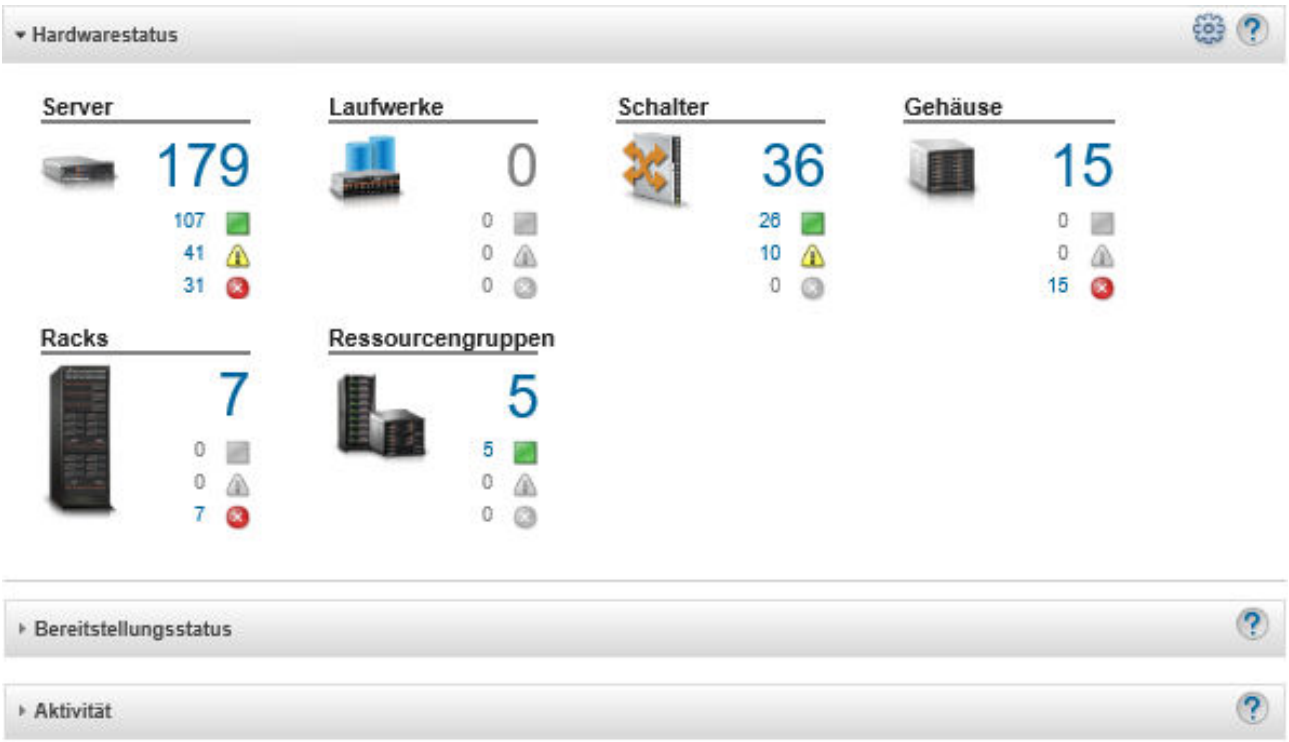
Schritt 3. Geben Sie eine gültige Benutzer-ID und ein gültiges Kennwort ein und klicken Sie auf **Anmelden**.

Wenn Sie sich zum ersten Mal mit einem Benutzeraccount anmelden, müssen Sie das Kennwort ändern. Die Kennwörter müssen die folgenden Kriterien erfüllen:

- (1) Es muss mindestens ein Buchstabe und es dürfen nicht mehr als zwei aufeinanderfolgende Zeichen enthalten sein, einschließlich Abfolgen von Buchstaben, Ziffern und Tasten auf der QWERTZ-Tastatur (z. B. sind „abc“, „123“ und „asd“ nicht zulässig).
- (2) Es muss mindestens eine Zahl (0–9) enthalten sein.
- (3) Sie müssen mindestens *zwei* der folgenden Zeichen enthalten:
  - Großbuchstaben (A – Z)
  - Kleinbuchstaben (a – z)
  - Sonderzeichen ; @ _ ! ' $ & +
- (4) Es darf keine Wiederholung oder Umkehrung des Benutzernamens sein.
- (5) Es dürfen nicht mehr als zwei identische Zeichen hintereinander enthalten sein (z. B. sind „aaa“, „111“ und „...“ nicht zulässig).

Nach dieser Aufgabe

Die Dashboard-Seite von XClarity Administrator wird angezeigt:



Anmerkung: Wenn das Hostbetriebssystem unerwartet heruntergefahren wird, erhalten Sie beim Versuch, sich bei XClarity Administrator anzumelden, möglicherweise einen Authentifizierungsfehler. Beheben Sie dieses Problem, indem Sie XClarity Administrator aus der letzten Sicherung wiederherstellen, um auf den Verwaltungsserver zuzugreifen (siehe Lenovo XClarity Administrator sichern).

Sie können die folgenden Aktionen über das Benutzeraktionen-Menü (ADMIN_USER) in der XClarity Administrator-Titelleiste durchführen.

- Informationen zur Verwendung von XClarity Administrator finden Sie im eingebetteten Hilfesystem durch Klicken auf **Hilfe**.

  Die XClarity Administrator Dokumentation wird regelmäßig online in Englisch aktualisiert. Aktuelle Informationen und Verfahren finden Sie in XClarity Administrator Onlinedokumentation.
- Sie können die XClarity Administrator-Lizenz durch Klicken auf **Lizenz** anzeigen.
- Sie können Informationen zur XClarity Administrator-Version durch Klicken auf **Info** anzeigen.
- Sie können die Sprache der Benutzerschnittstelle durch Klicken auf **Sprache ändern** ändern.
- Sie können sich durch Klicken auf **Abmelden** von der aktuellen Sitzung abmelden.
- Sie können Ideen und Feedback zu XClarity Administrator einreichen, indem Sie auf **Ideen einreichen** oder **Feedback senden** klicken.
- Sie können im Community-Forumswebsite für Lenovo XClarity Fragen stellen und Antworten finden, indem Sie auf **Forum besuchen** klicken.

Tipps und Verfahren für die Benutzerschnittstelle

Beachten Sie diese Tipps und Verfahren, wenn Sie die Lenovo XClarity Administrator-Benutzerschnittstelle verwenden.

Mehr oder weniger Daten pro Seite anzeigen

Sie können die Anzahl der Zeilen ändern, die pro Seite angezeigt werden. Verwenden Sie dazu die Links unten rechts in der Tabelle. Sie können **10**, **25**, **50** oder **Alle** Zeilen anzeigen.

Daten in großen Listen suchen

Die meisten Felder können bis zu 128 Zeichen enthalten.

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.

  Die Änderung der Sortierreihenfolge einer Tabellenspalte ist in den Benutzersitzungen dauerhaft.
- Sie können die Symbole **Filtern nach** und die Dropdown-Liste **Anzeigen** verwenden, die auf einigen Seiten verfügbar sind, um anhand der ausgewählten Kriterien eine Teilmenge der Daten anzuzeigen.
- Sie können die Teilmenge weiter verfeinern, indem Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um nach Daten zu suchen, die in jeder verfügbaren Spalte gefunden werden.

  Sie können die letzten zehn Suchvorgänge wiederverwenden, indem Sie in der Dropdown-Liste neben dem Feld **Filter** die Suchvorgänge auswählen. Die letzte aktive Suche auf einer Seite ist für Benutzersitzungen dauerhaft.

Spaltendaten anzeigen

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 den Text in der Zelle bewegen.

Tabellenspalten konfigurieren

Sie können Tabellen so konfigurieren, dass Informationen angezeigt werden, die für Sie von Bedeutung 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 haben die Möglichkeit, die Sprache der Benutzerschnittstelle bei der ersten Anmeldung festzulegen.

Nachdem Sie sich angemeldet haben, können Sie die Sprache der Benutzerschnittstelle ändern, indem Sie auf das Benutzeraktionen-Menü (

) und dann auf **Sprache ändern**ändern klicken. Wählen Sie die Sprache aus, die angezeigt werden soll.

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

Hilfe anfordern

XClarity Orchestrator bietet Ihnen verschiedene Möglichkeiten, um Hilfe zur Benutzerschnittstelle zu erhalten.

- Einige Seiten bieten anhand von Symbolen für **Hilfe** (
) zusätzliche Details zu einem bestimmten Feld oder einem bestimmten Status. Bewegen Sie den Cursor über das Symbol, um ein Dialogfenster mit nützlichen Informationen anzuzeigen.
- Hilfe zum Ausführen von bestimmten Aktionen über die Benutzerschnittstelle erhalten Sie, wenn Sie auf das Benutzeraktionen-Menü (

) und dann auf **Hilfe** klicken.

Lenovo XClarity Mobile-App verwenden

Lenovo XClarity Administrator bietet eine mobile App für Android- und iOS-Geräte. Sie können die App Lenovo XClarity Mobile verwenden, um physische Systeme auf sichere Weise zu überwachen, um Statuswarnungen und -benachrichtigungen in Echtzeit zu erhalten und Aktionen für allgemeine Systemaufgaben auszuführen. Die App kann sich außerdem direkt über einen aktivierten USB-Anschluss mit einem ThinkSystem-Server verbinden und virtuelle LCD-Funktionalität bereitstellen.

Weitere Informationen:  Übersicht über die Lenovo XClarity-Mobile-App

Mit der XClarity Mobile-App können Sie die folgenden Aktivitäten durchführen:
- Netzwerkeinstellungen und -eigenschaften konfigurieren
- Statusübersicht der einzelnen verbundenen XClarity Administrator-Instanzen anzeigen
- Statusübersicht aller verwalteten Einheiten anzeigen
- Grafische Ansichten (Übersichten) für Gehäuse, Rack-Server und Speichereinheiten anzeigen
- Ressourcengruppen anzeigen, die auf XClarity Administrator definiert werden.
- Zeigen Sie Rack-Switch Portinformationen an und ändern Sie den Status der konfigurierten Ports.
- Bestand und detaillierten Status der einzelnen verwalteten Einheiten überwachen
- Prüfereignisse, Hardware- und Verwaltungsereignisse, Alerts und Jobs überwachen
- Die Positionsanzeige einer verwalteten Einheit ein- oder ausschalten
- Verwaltete Einheiten einschalten, ausschalten, neu starten oder erneut einsetzen
- Die Erfassung von Diagnosedaten starten
- Informationen zur Garantie und Status anzeigen
- Automatische Problembenachrichtigung über Call-Home-Funktion einrichten
- Übersicht über offene Service-Tickets anzeigen und Service-Tickets löschen
- Ereignisbenachrichtigungen per Push an mobile Einheiten übertragen lassen (siehe Ereignisse an mobile Einheiten weiterleiten)
- Übersicht über aktive Benutzer und Verwendung der Systemressourcen anzeigen
- Feedback zu dieser mobilen App an die Lenovo Unterstützung übermitteln
- Schließen Sie Ihr mobiles Gerät direkt an einen ThinkSystem Server an, um den Server mit der XClarity Mobile-App zu verwalten (für Einheiten mit Unterstützung für USB-Tethering).
- Lenovo XClarity Controller-Servicedaten herunterladen, wenn das mobile Gerät mit einem ThinkSystem-Server verbunden ist.

Sie können auch Ihre mobilen Geräte direkt mit ThinkSystem-Servern verbinden und anschließend die XClarity Mobile App starten und sich beim Baseboard Management Controller des Servers mit den gleichen Web- und CLI-Anmeldeinformationen anmelden. Es steht ein Menü mit zusätzlichen Informationen und Aktionen zur Verfügung:

- Service
  - Übersichtsinformationen per E-Mail oder eine andere Option, die vom mobilen Gerät bereitgestellt wird, teilen
  - Ereignis- und Prüfprotokoll löschen
  - Ereignis- und Prüfprotokoll in den lokalen Speicher des mobilen Geräts herunterladen oder das Protokoll über eine andere, vom mobilen Gerät bereitgestellte Option übermitteln
  - BMC FFDC Servicedatei in den lokalen Speicher des mobilen Gerätes herunterladen oder die Datei über eine andere, vom mobilen Gerät bereitgestellte Option übermitteln
  - Historische Diagrammdaten für die Verwendung von Netzstrom, Temperatur und System anzeigen
  - Servicemodus „One-Touch“ aktivieren, der eine sofortige Übersicht über die aktiven Alerts und wichtige Einheitendaten bereitstellt
- Konfiguration und Erstkonfiguration
  - Neue Einheit mit dem ausgewählten XClarity Administrator verwalten
  - Servereigenschaften wie Position und Kontaktinformationen für die Erstkonfiguration konfigurieren
  - Einstellungen der IPv4- und IPv6-BMC-Netzwerkschnittstelle anzeigen und ändern

  - Bootreihenfolge und einmalige Booteinstellungen angeben
  - USB-Anschlussbelegung am Bedienfeld ändern
  - Anzahl der Serverneustarts und Gesamtbetriebsdauer in Stunden anzeigen
- Stromversorgungsaktionen
  - Server ein- oder ausschalten, neu starten oder NMI auslösen
  - BMC zurücksetzen

Tipp: Wenn die Anwendung geöffnet ist, müssen Sie sie aktualisieren, um aktualisierte Informationen zu Status, Bestand, Ereignissen und Jobs anzuzeigen.

Vorbedingungen

- iOS-Tablets werden nur mit der Bildschirmauflösung für iPhones unterstützt. Android-Tablets werden derzeit nicht unterstützt.
- Die folgenden Betriebssysteme für mobile Einheiten werden unterstützt:
  - Android 7-11
  - iOS 10 und höher

    Anmerkungen:

    - Android 5 wird nur für XClarity Mobile 2.3.0 und früher unterstützt.
    - Die auf iPhone X/XR/XS-Geräten verwendete Gesichtserkennung wird nicht unterstützt.
- Stellen Sie sicher, dass eine Netzwerkverbindung von Ihrer mobilen Einheit zu den Instanzen von XClarity Administrator verfügbar ist. Dazu ist möglicherweise der Einsatz einer VPN-Lösung erforderlich. Bitten Sie Ihren Netzwerkadministrator um Unterstützung.
- Importieren Sie das Zertifizierungsstellenzertifikat für jede XClarity Administrator-Instanz.

  Wichtig: Alle Verbindungen zu XClarity Administrator verwenden HTTPS. Allerdings muss es eine gültige Zertifikatskette geben, bevor die Verbindung als vertrauenswürdig eingestuft wird und Daten an die mobile Einheit übertragen werden können. Um eine vertrauenswürdige Zertifikatskette zu erstellen, müssen Sie die selbst signierte Zertifizierungsstelle von XClarity Administrator auf die mobile Einheit importieren.

  Gehen Sie wie folgt vor, um das selbst signierte Zertifizierungsstellenzertifikat für *jede XClarity Administrator-Instanz* auf die mobile Einheit zu importieren.

  1. Laden Sie das Zertifizierungsstellenzertifikat auf ein lokales System herunter:
     a. Stellen Sie über einen Webbrowser auf Ihrem lokalen System eine Verbindung zur Instanz von XClarity Administrator her.
     b. Wählen Sie in der XClarity Administrator-Menüleiste **Verwaltung → Sicherheit** aus, um die Seite „Sicherheit“ anzuzeigen.
     c. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Zertifizierungsstelle**. Die Seite Zertifizierungsstelle wird angezeigt.
     d. Wählen Sie **Stammzertifikat der Zertifizierungsstelle herunterladen** aus.

        Achtung: Normalerweise müssen Sie nicht auf **Stammzertifikat der Zertifizierungsstelle neu generieren** klicken, um diesen Prozess abzuschließen. Wenn nicht das richtige Verfahren angewendet wird, kann dieser Schritt die Kommunikation mit verwalteten Einheiten unterbrechen. Siehe Mit Sicherheitszertifikaten arbeiten für weitere Informationen.
     e. Klicken Sie auf **Als „DER“ speichern** oder auf **Als „PEM“ speichern**, um das Zertifizierungsstellenzertifikat auf dem lokalen System als DER- bzw. PEM-Datei zu speichern. Das PEM-Format funktioniert in den meisten Fällen.
  2. Übertragen Sie das Zertifizierungsstellenzertifikat auf Ihre mobile Einheit (z. B. über ein verfügbares Speicher-Repository wie Dropbox™, per E-Mail oder direkt über ein verbundenes Kabel).

3. Importieren Sie das vertrauenswürdige Zertifizierungsstellenzertifikat:
   - Android: In der Regel wählen Sie dazu im Speicherbereichs des Telefons **Einstellungen → Sicherheit → Installieren** und dann die heruntergeladene Zertifikatsdatei aus.

     Wichtig: Wenn das erfolgreich installierte Zertifizierungsstellenzertifikat nicht von einer unabhängigen Zertifizierungsstelle signiert ist, wird auf Android-Geräten die Nachricht `Das Netzwerk wird möglicherweise von einem unbekannten Drittanbieter überwacht` angezeigt. Da das Zertifizierungsstellenzertifikat in Ihrer vertrauenswürdigen Umgebung generiert wurde, kann diese Nachricht problemlos ignoriert werden. Stellen Sie sicher, dass sich die Nachricht auf das Zertifizierungsstellenzertifikat von XClarity Administrator bezieht, bevor Sie die Nachricht ignorieren.
   - iOS: Öffnen Sie die E-Mail auf Ihrer mobilen Einheit und klicken Sie auf den Dokumentlink in der E-Mail, um das vertrauenswürdige Zertifizierungsstellenzertifikat zu importieren.

   Achtung: Bei iOS 10.3 und höher sind importierte Zertifikate standardmäßig nicht vertrauenswürdig. Um Zertifikate als vertrauenswürdig einzustufen, wählen Sie **Einstellungen → Allgemein → Info → Zertifikats-Vertrauenswürdigkeitseinstellungen** aus, und aktivieren Sie anschließend, dass Zertifikaten vertrauenswürdig sind.

Installieren und konfigurieren

1. Laden Sie die XClarity Mobile-App aus dem iTunes App Store (iOS) oder Google Play Store (Android) herunter.
2. Um die App zu installieren, befolgen Sie die Anweisungen auf der mobilen Einheit.

   Wichtig: Sie benötigen einen Sicherheitscode auf der Betriebssystemebene für mobile Einheiten, um Zugriff auf den Bildschirm zu erhalten und die XClarity Mobile-App verwenden zu können. Wenn noch kein Code eingerichtet wurde, werden Sie aufgefordert, diesen bei der Installation festzulegen.
3. Klicken Sie auf **Einstellungen**, um Verbindungen zu mehreren Instanzen von XClarity Administrator mithilfe der automatischen Erkennung oder durch Angabe von IP-Adresse und Benutzeranmeldeinformationen hinzuzufügen oder zu bearbeiten, einen PIN-Code für die App festzulegen, die Einstellungen für Prüf- und Ereignisprotokolle zu ändern und die bevorzugte Sprache auszuwählen.

Direkte Verbindung mit ThinkSystem-Servern

Lenovo ThinkSystem-Server verfügen über einen Bedienfeld-USB-Anschluss, den Sie verwenden können, um Ihr mobiles Gerät zu verbinden, um ähnliche Funktionen bereitzustellen, die auf der LCD-Systeminformationsanzeige auf anderen Lenovo-Servern verfügbar waren.

Gehen Sie wie folgt vor, um einen ThinkSystem-Server über eine direkte Verbindung zu verwalten.

1. Ändern Sie den Bedienfeld-USB-Anschluss des Servers von Host auf BMC, indem Sie einen der folgenden Schritte ausführen.
   a. In der Management-Controller-Befehlszeilenschnittstelle (CLI), führen Sie den Befehl `usbfp` aus.
   b. Klicken Sie in der Management-Controller-Webschnittstelle auf **BMC-Konfiguration → Netzwerk → Bedienfeld-USB-Anschluss verwalten**.
   c. Halten Sie die blaue ID-Positionsanzeige auf dem Bedienfeld für mindestens 3 Sekunden gedrückt, bis die Anzeige im Abstand von einigen Sekunden blinkt.
2. Verbinden Sie das USB-Kabel Ihres Telefons mit dem Bedienfeld-USB-Anschluss des ThinkSystem-Servers.
3. Aktivieren Sie USB-Tethering auf Ihrem mobilen Gerät.
   a. Auf iOS-Geräten klicken Sie auf **Einstellungen → Mobiltelefon → Persönlicher Hotspot**.

b. Auf Android-Geräten klicken Sie auf **Einstellungen → Mobiler Hotspot und Tethering → USB-Tethering**.

4. Auf Ihrem mobilen Gerät starten Sie die XClarity Mobile App.
5. Wenn die automatische Erkennung deaktiviert ist, klicken Sie auf **Ermitteln** auf der USB-Ermittlungsseite, um eine Verbindung zum Management-Controller des Servers herzustellen und Informationen einschließlich Bestand, Zustand, Firmware, Netzwerkkonfiguration und eine Liste der aktuellen aktiven Ereignisse zu sammeln.

Tipp:

- Stellen Sie sicher, dass Sie ein hochwertiges USB-Kabel verwenden, das den Datenübertragungs- und Auflademodus unterstützt. Beachten Sie, dass einige Kabel, die mit mobilen Geräten mitgeliefert werden, nur für den Auflademodus geeignet sind.

  Anmerkung: Um eine Verbindung zum ThinkSystem SD530 herzustellen, müssen Sie zusätzlich ein hochwertiges Micro-USB-zu-USB-Kabel bzw. einen Adapter verwenden.
- Der über USB verbundene Server muss eingeschaltet sein, um alle Informationen wie Spannung, Temperatur und Nutzungsstatistiken in den Statusübersichtskarten zu melden.
- Wenn der über USB verbundene Server über keine/n externe/n „blaue/n ID“-Anzeige/Schalter auf dem Bedienfeld verfügt, müssen Sie die Management-Controller-Webschnittstelle oder -Befehlszeilenschnittstelle (CLI) verwenden, um bei Bedarf die Auswahl in der Verwaltung des Bedienfeld-USB-Anschlusses zu ändern.
- An der Management-Controller-Netzwerkschnittstelle über die XClarity Mobile App vorgenommene Änderungen werden ohne einen Neustart des Management-Controllers sofort wirksam. Beispielsweise wenn die IPv4-Schnittstelle von einer statischen Adresse auf DHCP geändert wird, erhält die Schnittstelle unverzüglich eine von DHCP zugewiesene Adresse.
- Auf der Registerkarte „Newsfeed“ zeigt der Reiter „Neueste aktive Ereignisse“ zuerst bis zu drei aktive Ereignisse an, die auf der Registerkarte „Aktive Ereignisse“ des Management-Controllers aufgelistet sind. Wenn Sie in der mobilen App auf diese Karte tippen, werden alle aktiven Ereignisse angezeigt. Beachten Sie, dass es sich hierbei um eine Liste der aktiven und behobenen Ereignisse und nicht um eine vollständige Liste aller Ereignisse handelt.

Demomodus verwenden

Sie können auf der Seite „Einstellungen“ den **Demomodus** aktivieren, damit die XClarity Mobile-App Demodaten für zwei Instanzen von XClarity Administrator erhält, einschließlich Racks und Gehäuse. In diesem Modus können Sie die Statusübersicht der XClarity Administrator-Instanzen, den detaillierten Status und den Bestand für Einheiten anzeigen sowie Ereignisse und Alerts überwachen. Verwaltungsaktionen, wie das Ein- und Ausschalten, werden jedoch nicht unterstützt.

Anmerkungen:

- Der Demomodus kann nur aktiviert werden, wenn keine Verbindungen zu tatsächlichen XClarity Administrator-Instanzen aktiv sind.
- Sie können keine Verbindungen zu tatsächlichen XClarity Administrator-Instanzen hinzufügen, wenn der Demomodus aktiviert ist.

Suchen

Sie können das Feld **Suchen** verwenden, um verwaltete Einheiten mit einem bestimmten Namen oder einem bestimmten Status anzuzeigen („Kritisch“, „Warnung“ oder „Normal“). Wenn Sie beispielsweise nach „crit“ suchen, werden nur verwaltete Einheiten angezeigt, die einen kritischen Status haben und deren Name die Zeichenfolge „crit“ enthält.

Probleme behandeln

Installationsprobleme:

- Die mobile Android-App ist mit einem sicheren Schlüssel „signiert“, um die Sicherheit zu erhöhen. Die Größe des sicheren Schlüssels wurde in der neuen Version erhöht. Da die signierte App nicht mit der Signatur früherer Apps übereinstimmt, verhindert der Sicherheitsprozess bei der Android-Installation die automatische Aktualisierung.

  Um die mobile App zu aktualisieren, deinstallieren Sie die aktuelle Version der mobilen App, laden Sie die neueste Version der Android-App vom App-Store herunter und installieren Sie die App neu. Auf den meisten Android-Geräten kann die App unter **Einstellungen → Anwendungen → Anwendungsmanager** deinstalliert werden.

Verbindungsprobleme:

- Die USB-Tethering-Funktion in iOS 14, 14.0.1 und 14.0.2 funktioniert nicht ordnungsgemäß. Daher ist die Tethering Lenovo XClarity Mobile-App-Tethering-Funktion nicht für diese iOS-Versionen verfügbar. Dies betrifft nur die Verwaltung durch per USB verbundene Handgeräte im Rechenzentrum. Die Remoteverwaltung mithilfe mobiler Geräte, die Mobilfunk- und WLAN-Kommunikation unterstützen, ist davon nicht betroffen und kann zum Herstellen von Verbindungen und zum Erfassen von Daten von XClarity Administrator sowie zum Ausführen von Verwaltungsvorgängen auf verwalteten Geräten verwendet werden.

  Wenn die Funktion zur Verwaltung mit per USB verbundenen Handgeräten benötigt wird, aktualisieren Sie nicht auf iOS 14.

  Diese Benachrichtigung wird aktualisiert, wenn Apple das Problem mit iOS 14 behoben hat.
- XClarity Mobile erfordert eine verfügbare Netzwerkverbindung von Ihrer mobilen Einheit zu den Instanzen von XClarity Administrator. Dazu ist möglicherweise der Einsatz einer VPN-Lösung erforderlich. Bitten Sie Ihren Netzwerkadministrator um Unterstützung.
- Verbindungen von Ihrer mobilen Einheit zu den einzelnen XClarity Administrator-Instanzen erfordern eine vertrauenswürdige Zertifikatskette. Anweisungen zum Herunterladen und Installieren der vertrauenswürdigen Zertifizierungsstellenzertifikate auf Ihrer mobilen Einheit finden Sie in der Onlinedokumentation.

  Wenn das erfolgreich installierte Zertifizierungsstellenzertifikat nicht von einer unabhängigen Zertifizierungsstelle signiert ist, wird die Nachricht `Das Netzwerk wird möglicherweise von einem unbekannten Drittanbieter überwacht` angezeigt. Da das Zertifizierungsstellenzertifikat in Ihrer vertrauenswürdigen Umgebung generiert wurde, kann diese Nachricht problemlos ignoriert werden. Stellen Sie sicher, dass sich die Nachricht auf das Zertifizierungsstellenzertifikat von XClarity Administrator bezieht, bevor Sie die Nachricht ignorieren.
- Wenn Ihre mobile Einheit von einem virtuellen privaten Netzwerk (VPN) auf ein lokales Netzwerk umschaltet (oder umgekehrt), wird möglicherweise die folgende Nachricht angezeigt: `Das sichere Gateway hat den Verbindungsversuch abgelehnt. Es ist ein neuer Verbindungsversuch zu demselben oder einem anderen sicheren Gateway und aus diesem Grund eine erneute Authentifizierung erforderlich.` Melden Sie sich bei Lenovo XClarity Mobile an, um die App weiterhin zu verwenden.

Sicherheitsprobleme:

- Wenn Sie Ihren PIN-Code vergessen haben, müssen Sie die XClarity Mobile-App deinstallieren und anschließend wieder neu installieren. Stellen Sie dann alle Verbindungen wieder her.
- Wenn Sie Anmeldeinformationen auf einer Android-Einheit löschen, wird auch der Verschlüsselungsschlüssel gelöscht. Sie müssen dann alle Verbindungen wiederherstellen.

Ereignisbezogene Probleme:

- Standardmäßig werden im Ereignisprotokoll Hardware- und Verwaltungsereignisse angezeigt, die in den vergangenen 24 Stunden empfangen wurden. Das Prüfprotokoll zeigt Prüfereignisse an, die in den vergangenen 2 Stunden empfangen wurden. Wenn in den ausgewählten Zeiträumen keine Ereignisse empfangen wurden, werden das Ereignisprotokoll und das Prüfprotokoll nicht auf der Seite „Überwachung“ in XClarity Mobile angezeigt.
- Wenn Sie die Ereignisweiterleitung in XClarity Administrator so eingerichtet haben, dass Ereignisse an ein E-Mail-Konto gesendet werden, kann es sein, dass die Links in der E-Mail auf Android-Einheiten nicht funktionieren. Stellen Sie sicher, dass Ihre Android-Version und Ihre E-Mail-App Hyperlinks unterstützen. Werden Hyperlinks nicht unterstützt, verwenden Sie eine andere E-Mail-App.

Probleme beim Hilfesystem:

- Bei einigen Einheiten wird das Hilfesystem nicht ordnungsgemäß für die Größe des Bildschirms skaliert. Verwenden Sie die Steuerelemente des Hilfesystems, um die Seite zunächst zu maximieren und danach zu minimieren.

Kapitel 2. Lenovo XClarity Administrator verwalten

Einige Verwaltungsaufgaben, wie das Hinzufügen von Benutzern oder Anzeigen von Jobs, sind in Lenovo XClarity Administrator verfügbar.

Authentifizierung und Berechtigungen verwalten

Lenovo XClarity Administrator bietet Sicherheitsmechanismen, um die Anmeldeinformationen eines Benutzers zu überprüfen und den Zugriff auf Ressourcen und Tasks zu steuern.

Authentifizierungsserver verwalten

Lenovo XClarity Administrator verwendet standardmäßig einen lokalen LDAP(Lightweight Directory Access Protocol)-Server zur Authentifizierung der Berechtigungsnachweise von Benutzern.

Zu dieser Aufgabe

Unterstützte Authentifizierungsserver

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

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

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

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

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

Einheitenauthentifizierung

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

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

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

  Anmerkungen:

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

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

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

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

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

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

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

  Anmerkung: Single Sign-On ist automatisch deaktiviert, wenn das CyberArk Identitätsverwaltungssystem zur Authentifizierung verwendet wird.
- Wenn die verwaltete Authentifizierung für ThinkSystem SR635 und SR655 Server aktiviert ist:
  - Die Baseboard Management Controller-Firmware unterstützt bis zu fünf LDAP-Benutzerrollen. XClarity Administrator fügt diese LDAP-Benutzerrollen während der Verwaltung zu den Servern hinzu: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** und **lxc-os-admin**.

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

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

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

Wiederherstellungsaccount

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

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

- Wenn Sie Änderungen an den deaktivierten lokalen Benutzeraccounts vornehmen (z. B. ein Kennwort ändern), haben diese Änderungen keinerlei Auswirkungen auf den Account `RECOVERY_ID`. Im Modus „Verwaltete Authentifizierung“ ist der Account `RECOVERY_ID` der einzige aktive und betriebsbereite Benutzeraccount.
- Verwenden Sie den Account `RECOVERY_ID` nur in Notfällen, z. B. bei Ausfall des Verwaltungsserver oder wenn ein Netzwerkproblem verhindert, dass die Einheit zur Benutzerauthentifizierung mit XClarity Administrator kommuniziert.
- Das Kennwort `RECOVERY_ID` wird angegeben, wenn Sie das Gerät erkennen. Notieren Sie sich das Kennwort für die spätere Verwendung.

Informationen zum Wiederherstellen einer Einheitenverwaltung erhalten Sie in den Abschnitten „Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen“ auf Seite 236 und „Rack- oder Tower-Serververwaltung nach einem Verwaltungsserverausfall wiederherstellen“ auf Seite 288.

Externen LDAP-Authentifizierungsserver konfigurieren

Sie können auswählen, dass ein externer LDAP-Authentifizierungsserver anstelle des lokalen Lenovo XClarity Administrator-Authentifizierungsservers auf dem Verwaltungsknoten verwendet wird.

Vorbereitende Schritte

Bevor Sie den externen Authentifizierungsserver konfigurieren, muss die Erstkonfiguration von XClarity Administrator abgeschlossen sein.

Die folgenden externen Authentifizierungsserver werden unterstützt:

- OpenLDAP
- Microsoft Active Directory: Dieser Server muss sich auf einem externen Microsoft Windows-Server befinden, der mit dem Verwaltungsnetzwerk, Datennetzwerk oder beidem verbunden ist.

Stellen Sie sicher, dass alle für den externen Authentifizierungsserver erforderlichen Ports im Netzwerk und in den Firewalls geöffnet sind. Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der XClarity Administrator-Onlinedokumentation.

Sie müssen Rollengruppen auf dem lokalen Authentifizierungsserver erstellen oder umbenennen, die den auf dem externen Authentifizierungsserver definierten Gruppen entsprechen.

Stellen Sie sicher, dass mindestens einer der Benutzer über die **lxc-recovery**-Berechtigung auf dem lokalen Authentifizierungsserver verfügt. Sie können diesen lokalen Benutzeraccount verwenden, um die Authentifizierung direkt in XClarity Administrator durchzuführen, wenn ein Kommunikationsfehler mit dem externen LDAP-Server auftritt.

Anmerkung: Wenn XClarity Administrator für die Verwendung eines externen Authentifizierungsservers konfiguriert ist, ist die Seite „Benutzerverwaltung“ der XClarity Administrator-Webschnittstelle deaktiviert.

Achtung: Um die Bindungsmethode für Active Directory so zu konfigurieren, dass Anmeldeinformationen verwendet werden, muss im Baseboard Management Controller für jeden verwalteten Server Firmware ab September 2016 (oder später) ausgeführt werden.

XClarity Administrator führt alle fünf Minuten eine Konnektivitätsprüfung durch, um die Konnektivität für konfigurierte externe LDAP-Server aufrechtzuerhalten. In Umgebungen mit vielen LDAP-Servern kommt es möglicherweise zu einer hohen CPU-Auslastung während dieser Konnektivitätsprüfung. Um die optimale Leistung zu erreichen, stellen Sie sicher, dass die meisten oder alle LDAP-Server in der Domäne erreichbar sind, oder setzen Sie die Authentifizierungserver-Auswahlmethode auf **Vorkonfigurierte Server verwenden** und geben Sie nur bekannte, erreichbare LDAP-Server an.

Vorgehensweise

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

Schritt 1. Richten Sie das Benutzerauthentifizierungsverfahren für Microsoft Active Directory oder OpenLDAP ein.

Wenn Sie keine gesicherte Authentifizierung verwenden, ist keine weitere Konfiguration erforderlich. Standardmäßig verwenden Windows Active Directory- oder OpenLDAP-Domänencontroller die nicht gesicherte LDAP-Authentifizierung.

Wenn Sie die Verwendung der sicheren LDAP-Authentifizierung auswählen, müssen Sie die Domänencontroller so einrichten, dass sie die sichere LDAP-Authentifizierung zulassen. Weitere Informationen zum Konfigurieren der sicheren LDAP-Authentifizierung in Active Directory finden Sie unter Artikel über LDAP-over-SSL(LDAPS)-Zertifikate auf der Microsoft TechNet-Website.

So stellen Sie sicher, dass die Active Directory-Domänencontroller für die Verwendung der sicheren LDAP-Authentifizierung konfiguriert sind:

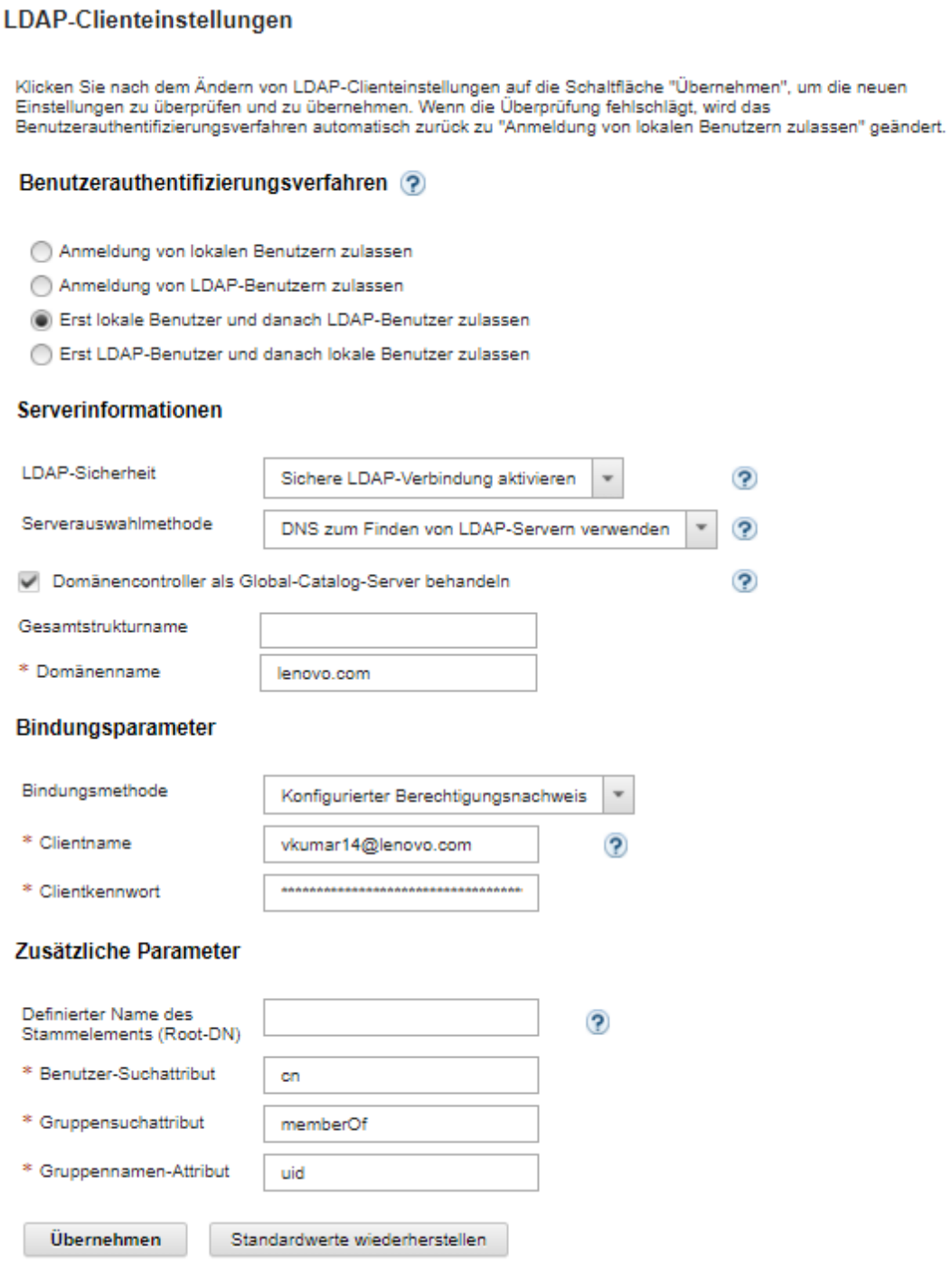
- Suchen Sie im Fenster der Ereignisanzeige der Domänencontroller nach dem Ereignis `LDAP über SSL-Funktionen (Secure Sockets Layer) ist jetzt verfügbar`.
- Verwenden Sie das Windows-Tool `ldp.exe`, um zu testen, dass die LDAP-Verbindung zu den Domänencontrollern sicher ist.

Schritt 2. Importieren Sie das Active Directory- oder OpenLDAP-Serverzertifikat oder das Stammzertifikat der Zertifizierungsstelle, die das Serverzertifikat signiert hat.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
b. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Vertrauenswürdige Zertifikate**.
c. Klicken Sie auf das Symbol für **Erstellen** ( ), um ein Zertifikat hinzuzufügen.
d. Suchen Sie die Datei oder fügen Sie den Zertifikatstext im PEM-Format ein.
e. Klicken Sie auf **Erstellen**.

Schritt 3. Konfigurieren Sie den LDAP-Client für XClarity Administrator:

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
b. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **LDAP-Client**, um das Dialogfenster LDAP-Clienteinstellungen anzuzeigen.



c. Füllen Sie das Dialogfenster anhand der folgenden Kriterien aus.

   1. Wählen Sie eins dieser Benutzerauthentifizierungsverfahren aus:

      - **Anmeldung von lokalen Benutzern zulassen**. Es wird die lokale Authentifizierung verwendet. Wenn diese Option ausgewählt ist, befinden sich alle Benutzeraccounts auf dem lokalen Authentifizierungsserver im Verwaltungsknoten.
      - **Anmeldung von LDAP-Benutzern zulassen**. Die Authentifizierung wird über einen externen LDAP-Server ausgeführt. Diese Methode ermöglicht die Fernverwaltung von Benutzeraccounts. Wenn diese Option ausgewählt ist, liegen alle Benutzeraccounts fern auf einem externen LDAP-Server vor.

- **Erst lokale Benutzer und danach LDAP-Benutzer zulassen**. Der lokale Authentifizierungsserver führt die Authentifizierung zuerst aus. Wenn dieser Schritt nicht erfolgreich ist, führt ein externer LDAP-Server die Authentifizierung aus.
- **Erst LDAP-Benutzer und danach lokale Benutzer zulassen**. Zuerst führt ein externer LDAP-Server die Authentifizierung aus. Wenn dieser Schritt nicht erfolgreich ist, führt der lokale Authentifizierungsserver die Authentifizierung aus.

2. Wählen Sie aus, ob die sichere LDAP-Verbindung aktiviert oder deaktiviert werden soll:
   - **Sichere LDAP-Verbindung aktivieren**. XClarity Administrator verwendet das LDAPS-Protokoll, um eine sichere Verbindung mit dem externen Authentifizierungsserver herzustellen. Wenn diese Option ausgewählt wird, müssen Sie auch vertrauenswürdige Zertifikate konfigurieren, um die sichere LDAP-Unterstützung zu aktivieren.
   - **Sichere LDAP-Verbindung deaktivieren**. XClarity Administrator verwendet ein nicht gesichertes Protokoll, um eine Verbindung mit dem externen Authentifizierungsserver herzustellen. Diese Einstellung macht Ihre Hardware eventuell anfälliger für potenzielle Sicherheitsrisiken.
3. Wählen Sie eins dieser Serverauswahlverfahren aus:
   - **Vorkonfigurierte Server verwenden**. XClarity Administrator verwendet die angegebenen IP-Adressen und Ports, um den externen Authentifizierungsserver zu ermitteln.

     Wenn Sie diese Option auswählen, müssen Sie bis zu vier vorkonfigurierte Server-IP-Adressen und Ports angeben. Der LDAP-Client versucht, die Authentifizierung mithilfe der ersten Serveradresse durchzuführen. Wenn die Authentifizierung fehlschlägt, verwendet der LDAP-Client die nächste Server-IP-Adresse für die Authentifizierung.

     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.

     Wichtig: Es muss mindestens ein Domänencontroller festgelegt werden, selbst wenn der globale Katalog angegeben wird. Wenn nur der globale Katalog angegeben wird, kann dies zu einer scheinbar erfolgreichen Authentifizierung führen, die jedoch keine gültige Konfiguration ist.

     Wenn als Verschlüsselungsmodus NIST-800-131A festgelegt ist, kann sich XClarity Administrator möglicherweise nicht mit einem externen LDAP-Server über einen sicheren Port verbinden (z. B. bei Verwendung von LDAPS über Standardport 636), wenn der LDAP-Server über Transport Layer Security (TLS) Version 1.2 keine Verbindung mit dem LDAP-Client in XClarity Administrator herstellen kann.
   - **DNS zum Finden von LDAP-Servern verwenden**. XClarity Administrator verwendet den angegebenen Domänennamen oder den Gesamtstrukturnamen, um den externen Authentifizierungsserver dynamisch zu ermitteln. Die Verwendung des Domänennamens und des Gesamtstrukturnamens dient dazu, eine Liste von Domänencontrollern abzurufen. Der Gesamtstrukturname wird verwendet, um eine Liste von globalen Katalogservern abzurufen.

Achtung: Wenn Sie DNS zum Suchen von LDAP-Servern verwenden, müssen Sie sicherstellen, dass der für die Authentifizierung auf dem externen Authentifizierungsserver verwendete Benutzeraccount auf den angegebenen Domänencontrollern gehostet wird. Wenn der Benutzeraccount auf einem untergeordneten Domänencontroller gehostet wird, müssen Sie den untergeordneten Controller in die Serviceanforderungsliste aufnehmen.

4. Wählen Sie eine dieser Bindungsmethoden aus:

   - **Konfigurierter Berechtigungsnachweis**. Verwenden Sie diese Bindungsmethode, um den Clientnamen und das Kennwort für die Bindung von XClarity Administrator an den externen Authentifizierungsserver zu verwenden. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden.

     Als Clientname kann ein beliebiger Name dienen, den der LDAP-Server unterstützt. Dazu gehören definierte Namen, AMAccountName, der NetBIOS-Name und UserPrincipalName. Der Clientname muss ein Benutzeraccount innerhalb der Domäne sein, der mindestens über Leserechte verfügt. Beispiele:
     ```
     cn=username,cn=users,dc=example,dc=com
     domain\username
     username@domain.com
     username
     ```

     Achtung: Wenn Sie das Clientkennwort auf dem externen Authentifizierungsserver ändern, müssen Sie das neue Kennwort auch in XClarity Administrator aktualisieren. Weitere Informationen finden Sie unter Anmelden bei XClarity Administrator nicht möglich in der Onlinedokumentation von XClarity Administrator.

   - **Anmeldeinformationen**. Verwenden Sie diese Bindungsmethode, um einen Active Directory- oder OpenLDAP-Benutzernamen und das Kennwort für die Bindung von XClarity Administrator an den externen Authentifizierungsserver zu verwenden.

     Die angegebene Benutzer-ID und das Kennwort werden nur verwendet, um die Verbindung zum Authentifizierungsserver zu testen. Wenn dieser Test erfolgreich ist, werden die LDAP-Clienteinstellungen gespeichert. Allerdings werden die von Ihnen für die Testanmeldung angegebenen Anmeldeinformationen nicht gespeichert. Alle zukünftigen Verbindungen verwenden den Benutzernamen und das Kennwort, die Sie für die Anmeldung bei XClarity Administrator verwendet haben.

     Anmerkungen:

     – Sie müssen bei XClarity Administrator mit einer vollständig qualifizierten Benutzer-ID angemeldet sein (z. B. `administrator@domain.com` oder `DOMAIN\admin`).
     – Sie müssen einen vollständig qualifizierten Testclientnamen für die Bindungsmethode verwenden.

     Achtung: Um die Bindungsmethode so zu konfigurieren, dass Anmeldeinformationen verwendet werden, muss im Management-Controller für jeden verwalteten Server Firmware ab September 2016 (oder später) ausgeführt werden.

5. Es wird empfohlen, im Feld **Definierter Name des Stammelements** keinen definierten Namen des Stammelements anzugeben, insbesondere für Umgebungen mit mehreren Domänen. Wenn dieses Feld leer ist, fragt XClarity Administrator den externen Authentifizierungsserver nach den Namenskontexten. Wenn Sie DNS zum Ermitteln des externen Authentifizierungsservers verwenden oder wenn Sie mehrere Server festlegen (beispielsweise `dc=example,dc=com`), können Sie optional den Eintrag an der ersten Stelle der LDAP-Verzeichnisstruktur angeben. In diesem Fall beginnt eine Suche mit dem angegebenen definierten Namen des Stammelements.

6. Geben Sie das Attribut an, das für die Suche nach dem Benutzernamen verwendet werden soll.

   Wenn als Bindungsmethode **Konfigurierter Berechtigungsnachweis** festgelegt wurde, folgt der einleitenden Verbindung zum LDAP-Server eine Suchanforderung, die bestimmte Informationen über den Benutzer abruft, einschließlich des definierten Namens (DN), der Anmeldeberechtigungen und der Gruppenmitgliedschaft des Benutzers. Diese Suchanforderung muss den Attributnamen angeben, der für die Benutzer-IDs auf diesem Server steht. Dieser Attributname wird in diesem Feld konfiguriert. Wenn in diesem Feld keine Angaben gemacht werden, lautet der Standardwert **cn**.

7. Geben Sie den Attributnamen an, der zum Identifizieren der Gruppen verwendet wird, denen ein Benutzer angehört. Wenn in diesem Feld keine Angaben gemacht werden, wird für den Attributnamen im Filter standardmäßig **memberOf** verwendet.
8. Geben Sie den Attributnamen an, der verwendet werden soll, um den Gruppennamen zu identifizieren, der vom LDAP-Server konfiguriert ist. Wenn in diesem Feld keine Angaben gemacht werden, lautet der Standardwert **uid**.

d. Klicken Sie auf **Übernehmen**.

   XClarity Administrator versucht, die Konfiguration zu testen, um allgemeine Fehler zu erkennen. Wenn der Test fehlschlägt, werden Fehlernachrichten mit der Fehlerquelle angezeigt. Wenn der Test erfolgreich war und Verbindungen zu den angegebenen Servern hergestellt wurden, können in den folgenden Fällen möglicherweise dennoch Fehler bei der Benutzerauthentifizierung auftreten:

   - Es ist kein lokaler Benutzer mit Berechtigungen vom Typ **lxc-recovery** vorhanden.
   - Der definierte Name des Stammelements ist falsch.
   - Der Benutzer ist kein Mitglied einer Gruppe auf dem externen Authentifizierungsserver, die dem Namen einer Rollengruppe auf dem XClarity Administrator-Authentifizierungsserver entspricht. XClarity Administrator kann nicht feststellen, ob der definierte Name des Stammelements richtig ist. Lenovo XClarity Administrator kann jedoch erkennen, ob ein Benutzer Mitglied mindestens einer Gruppe ist. Ist ein Benutzer kein Mitglied mindestens einer Gruppe, wird eine Fehlernachricht angezeigt, wenn der Benutzer versucht, sich bei XClarity Administrator anzumelden. Weitere Informationen zur Fehlerbehebung von Problemen mit externen Authentifizierungsservern finden Sie unter Verbindungsprobleme in der Onlinedokumentation von XClarity Administrator.

Schritt 4. Erstellen Sie einen externen Benutzeraccount, der auf XClarity Administrator zugreifen kann:

a. Erstellen Sie einen Benutzeraccount auf dem externen Authentifizierungsserver. Anleitungen finden Sie in der Active Directory- oder OpenLDAP-Dokumentation.

b. Erstellen Sie eine globale Active Directory- oder OpenLDAP-Gruppe mit dem Namen einer vordefinierten und autorisierten Gruppe. Die Gruppe muss sich im Kontext des definierten Namens des Stammelements befinden, der auf dem LDAP-Client definiert wurde.

c. Fügen Sie den Active Directory- oder OpenLDAP-Benutzer als Mitglied der Sicherheitsgruppe hinzu, die Sie zuvor erstellt haben.

d. Melden Sie sich mit dem Active Directory- oder OpenLDAP-Benutzernamen bei XClarity Administrator an.

e. **Optional:** Definieren und erstellen Sie weitere Gruppen. Sie können diese Gruppen autorisieren und über die Seite „Benutzer und Gruppen“ Rollen zuweisen.

f. Wenn die Verwendung sicherer LDAP-Verbindungen aktiviert ist, importieren Sie vertrauenswürdige Zertifikate auf den externen LDAP-Server (siehe Ein angepasstes, extern signiertes Serverzertifikat installieren).

Ergebnisse

XClarity Administrator überprüft die Verbindung zum LDAP-Server. Wenn die Überprüfung erfolgreich war, wird bei der Anmeldung an XClarity Administrator, CMM und dem Management-Controller eine Benutzerauthentifizierung auf dem externen Authentifizierungsserver durchgeführt.

Wenn die Überprüfung nicht erfolgreich war, wird der Authentifizierungsmodus automatisch zurück auf die Einstellung **Anmeldung von lokalen Benutzern zulassen** geändert. Dann wird eine Nachricht angezeigt, die die Fehlerursache erläutert.

Anmerkung: In XClarity Administrator müssen die richtigen Rollengruppen konfiguriert sein und Benutzeraccounts müssen als Mitglied einer dieser Rollengruppen auf dem Active Directory-Server definiert sein. Andernfalls schlägt die Benutzerauthentifizierung fehl.

Externen SAML-Identity Provider einrichten

Sie können einen SAML 2.0-Identity Provider (Security Assertion Markup Language) zur Authentifizierung und Autorisierung für Lenovo XClarity Administrator nutzen.

Vorbereitende Schritte

Bevor Sie den Identity Provider konfigurieren, muss die Erstkonfiguration von XClarity Administrator abgeschlossen sein.

Beim Identity Provider muss es sich um einen Microsoft Active Directory-Verbundservice (AD FS) handeln. Er kann entweder mit dem Verwaltungsnetzwerk, Datennetzwerk oder beidem verbunden sein. Da die Authentifizierung über den Webbrowser erfolgt, muss der Webbrowser auf XClarity Administrator und den SAML-Server zugreifen können.

Sie können über die folgende URL IDP-Metadaten herunterladen: `https://<ADFS_IP_Adresse>/federationmetadata/2007-06/federationmetadata.xml`, wobei *<ADFS_IP_Address>* die IP-Adresse für AD FS ist (z. B. https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

Sie müssen Rollengruppen auf dem Authentifizierungsserver des Standortes erstellen oder umbenennen, die den auf dem externen Authentifizierungsserver definierten Gruppen entsprechen.

Um einen SAML-Identity Provider einzurichten, müssen Sie als Benutzer angemeldet sein, der Mitglied der Gruppe **lxc_admin** oder **lxc_supervisor** ist.

Zu dieser Aufgabe

XClarity Administrator unterstützt die Verwendung eines SAML 2.0-Identity Providers zur Authentifizierung und Autorisierung von Benutzern. Zusätzlich zur Eingabe eines Benutzernamens und des Kennworts kann der Identity Provider so eingerichtet werden, dass ein weiteres Kriterium zur Identifikation des Benutzers erforderlich ist (beispielsweise die Eingabe eines PIN-Codes, das Lesen einer Smartcard und die Authentifizierung über ein Clientzertifikat).

Wenn XClarity Administrator für die Verwendung eines Identity Providers eingerichtet ist, werden interaktive Anmeldeanforderungen der XClarity Administrator-Webschnittstelle zur Authentifizierung an den Identity Provider umgeleitet. Wenn der Benutzer authentifiziert ist, wird der Webbrowser wieder zu XClarity Administrator umgeleitet.

Anmerkung: Wenn der Identity Provider aktiviert ist, können Sie Identity Provider umgehen und sich über einen lokalen oder externen LDAP-Authentifizierungsserver in XClarity Administrator anmelden, indem Sie die XClarity Administrator-Anmeldeseite in Ihrem Webbrowser öffnen (beispielsweise `https://<ip_address>/ui/login.htm`).

Wenn XClarity Administrator für die Verwendung eines Identity Provider-Profils konfiguriert ist, ist die Seite „Benutzerverwaltung“ der XClarity Administrator-Webschnittstelle nicht deaktiviert. Zur direkten Anmeldung an einem verwalteten Gehäuse oder einem Server (außer wenn Encapsulation auf der Einheit aktiviert ist) und für die PowerShell- und REST-API-Authentifizierung sind lokale Benutzerkonten erforderlich.

Vorgehensweise

Gehen Sie wie folgt vor, um einen externen SAML-Identity Provider (AD FS) einzurichten:

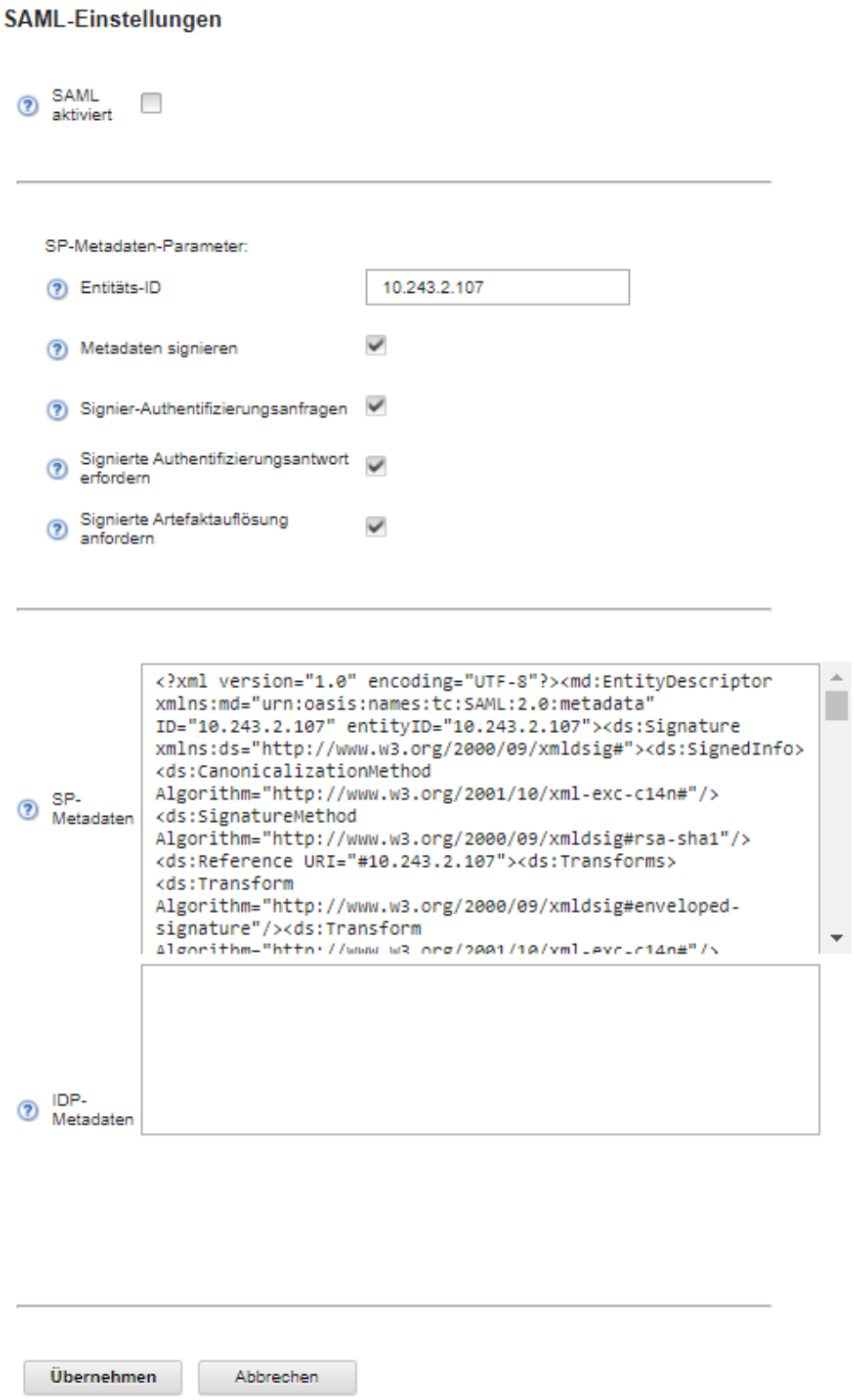
Schritt 1. Erstellen Sie ein Wiederherstellungsbenutzeraccount, das im Fall einer Nichtverfügbarkeit des Identity Provider zur Anmeldung in XClarity Administrator verwendet werden kann (siehe Benutzeraccounts verwalten).

Schritt 2. Rufen Sie die Identity Provider-Metadaten (IDP) vom Identity Provider ab und speichern Sie die Datei auf dem XClarity Administrator-Host.

Schritt 3. Konfigurieren Sie den XClarity Administrator-SAML-Client.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

b. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **SAML-Einstellungen**, um den Dialog SAML-Clienteinstellungen anzuzeigen.



c. Füllen Sie die Felder auf der Seite „SAML-Einstellungen“ aus:

   1. Stellen Sie sicher, dass die Entitäts-ID mit der IP-Adresse des XClarity Administrator Verwaltungsservers übereinstimmt.
   2. Wählen Sie aus, ob die generierten Metadaten digital signiert werden sollen.

3. Wählen Sie aus, ob Authentifizierungsanforderungen signiert werden sollen.
4. Wählen Sie aus, ob Authentifizierungsantworten signiert sein müssen.
5. Wählen Sie aus, ob die an den Remote-Identity Provider gesendeten Artefakt-Auflösungsanforderungen signiert sein müssen.
6. Fügen Sie die SAML-Identity Provider- Metadaten (IDP) in das Feld **IDP-Metadaten** ein, die vom Identity Provider generiert und in Schritt Schritt 2 3 auf Seite 27 abgerufen wurden.

d. Klicken Sie auf **Übernehmen**, um die Änderungen anzuwenden und den Text im Feld „SP-Metadaten“ zu aktualisieren.

Achtung: Zu diesem Zeitpunkt dürfen Sie **SAML aktiviert** *nicht* auswählen. SAML wird in einem späteren Schritt aktiviert, um XClarity Administrator neu zu starten.

e. Kopieren Sie die Daten im Feld **SP-Metadaten** und fügen Sie diese in einer Datei ein. Speichern Sie die Datei mit der Erweiterung .XML (beispielsweise sp_metadata.xml). Kopieren Sie diese Datei auf AD FS-Host.

Schritt 4. Konfigurieren Sie AD FS.

a. Öffnen Sie das AD FS-Verwaltungstool.
b. Klicken Sie auf **ADFS → Vertrauensstellung der vertrauenden Seite**.
c. Klicken Sie mit der rechten Maustaste auf **Vertrauensstellung der vertrauenden Seite** und klicken Sie auf **Vertrauensstellung der vertrauenden Seite hinzufügen**, um den Assistenten anzuzeigen.
d. Klicken Sie auf **Start**.
e. Wählen Sie auf der Seite „Datenquelle auswählen“ die Option **Daten über vertrauende Seite aus einer Datei importieren** und anschließend die SP-Metadatendatei, die Sie in Schritt 3e gespeichert haben.
f. Geben Sie einen Anzeigenamen ein.
g. Klicken Sie auf allen Seiten auf **Weiter** und übernehmen Sie die Standardwerte.
h. Klicken Sie auf **Fertigstellen**, um die Seite Anspruchsregeln anzuzeigen
i. Übernehmen Sie die Standardeinstellung **LDAP-Attribute als Ansprüche senden** und klicken Sie auf **Weiter**.
j. Geben Sie einen Anspruchsregelnamen ein.
k. Wählen Sie für den Attributspeicher **Active Directory** aus.
l. Fügen Sie eine Zuordnung hinzu. Klicken Sie links auf **SAM-Account-Name** und wählen Sie auf der rechten Seite **Namens-ID** für den ausgehenden Anspruchstyp aus.
m. Fügen Sie eine weitere Zuordnung hinzu. Wählen Sie links **Token-Groups-Unqualified Names** und wählen Sie auf der rechten Seite **Gruppe** für den ausgehenden Anspruchstyp aus.
n. Klicken Sie auf **OK**.
o. Suchen Sie in der Liste **Vertrauensstellung der vertrauenden Seite** die Vertrauensstellung, die Sie soeben erstellt haben.
p. Klicken Sie mit rechts auf die Vertrauensstellung und klicken Sie auf **Eigenschaften auswählen**. Der Dialog „Vertrauenseigenschaften“ wird angezeigt.
q. Klicken Sie auf die Registerkarte **Erweitert** und wählen Sie `SHA-1` als sicheren Hashalgorithmus aus.

Schritt 5. Speichern Sie das Serverzertifikat aus AD FS.

a. Klicken Sie auf **AD FS-Konsole → Dienst → Zertifikate**.

b. Wählen Sie unter Tokensignatur **Zertifikat** aus.

c. Klicken Sie mit rechts auf das Zertifikat und auf **Zertifikat anzeigen**.

d. Klicken Sie auf die Registerkarte **Details**.

e. Klicken Sie auf **In Datei kopieren** und speichern Sie das Zertifikat als DER-kodierte X.509-Binardatei (.CER).

f. Kopieren Sie die .CER-Datei des Serverzertifikats auf den XClarity Administrator-Host.

Schritt 6. Importieren Sie das vertrauenswürdige AD FS-Zertifikat in die XClarity Administrator-Webschnittstelle.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

b. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Vertrauenswürdige Zertifikate**.

c. Klicken Sie auf das Symbol für **Erstellen** ( ), um ein Zertifikat hinzuzufügen.

d. Wählen Sie die CER-Datei mit dem Serverzertifikat aus, die Sie im vorherigen Schritt gespeichert haben.

e. Klicken Sie auf **Erstellen**.

Schritt 7. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **SAML-Einstellungen**, um den Dialog SAML-Clienteinstellungen anzuzeigen.

Schritt 8. Wählen Sie **SAML aktiviert** aus, um die Verwaltung der Benutzerkonten über einen externen Identity Provider zu aktivieren. Wenn diese Option ausgewählt ist, befinden sich alle Benutzeraccounts auf einem externen Identity Provider.

Schritt 9. Klicken Sie auf **Übernehmen**, um die Änderungen anzuwenden und den Verwaltungsserver neu zu starten.

Schritt 10. Warten Sie mehrere Minuten, bis der XClarity Administrator gestartet ist.

Achtung: Starten Sie die virtuelle Einheit während des Prozesses nicht manuell neu.

Schritt 11. Schließen Sie den Webbrowser und öffnen Sie ihn erneut.

Schritt 12. Melden Sie sich über den Identity Provider an der XClarity Administrator-Webschnittstelle an.

Ergebnisse

XClarity Administrator versucht, die Konfiguration zu testen, um allgemeine Fehler zu erkennen. Wenn der Test fehlschlägt, werden Fehlernachrichten mit der Fehlerquelle angezeigt.

XClarity Administrator überprüft die Identity Provider-Verbindung. Wenn die Überprüfung erfolgreich ist, findet die Benutzerauthentifizierung bei der Anmeldung an XClarity Administrator auf dem Identity Provider statt.

Externes Identitätsverwaltungssystem einrichten

Ein *Identitätsverwaltungssystem* ist ein externer Kennworttresor, der optional mit Lenovo XClarity Administrator zum Speichern von XClarity Administrator- und XClarity Controller-Anmeldeinformationen verwendet werden kann. Wenn ein Identitätsverwaltungssystem zu XClarity Administrator hinzugefügt wird, ruft XClarity Administrator Kennwörter nicht von Authentifizierungsservern, sondern aus dem Identitätsverwaltungssystem ab.

Zu dieser Aufgabe

XClarity Administrator unterstützt das folgende Identitätsverwaltungssystem.

- CyberArk

CyberArk-Identitätsverwaltungssystem einrichten

CyberArk ist ein externer Kennworttresor, der optional mit Lenovo XClarity Administrator zum Speichern von XClarity Administrator und Lenovo XClarity Controller Anmeldeinformationen verwendet werden kann. Nach dem Speichern eines Accountkennworts in CyberArk wird das Kennwort von CyberArk verwaltet.

Zu dieser Aufgabe

Mit XClarity Administrator können Sie Ihre XCC-Kennwörter in Identitätsverwaltungssystemen von CyberArk speichern, ein Drittanbieterdienst. Lenovo ist nicht für den CyberArk-Dienst verantwortlich und Sie sind für Ihre direkte Beziehung mit CyberArk verantwortlich.

Wenn Benutzeraccounts für einen ThinkSystem oder ThinkAgile Server auf CyberArk integriert werden, können Sie wählen, dass XClarity Administrator die Anmeldeinformationen für die Anmeldung beim Server bei der Ersteinrichtung der Server zur Verwaltung (mit verwalteter oder lokaler Authentifizierung) von CyberArk abruft. Bevor Anmeldeinformationen von CyberArk abgerufen werden können, müssen die CyberArk-Pfade in XClarity Administrator definiert werden und es muss eine gegenseitige Vertrauensstellung zwischen CyberArk Und XClarity Administrator mithilfe von TLS für gegenseitige Authentifizierung über Clientzertifikate hergestellt werden.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Administrator für die Verwendung von CyberArk zu konfigurieren.

Schritt 1. Konfigurieren Sie CyberArk.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
2. Klicken Sie im Abschnitt für die Identitätsverwaltung auf **CyberArk**.
3. Klicken Sie in der Symbolleiste auf **CyberArk-Serverdetails bearbeiten**.
4. Geben Sie den CyberArk-Hostnamen oder die IP-Adresse und die Portnummer ein.
5. Klicken Sie auf **Übernehmen**.

Schritt 2. Importieren Sie das XClarity Administrator Zertifikat für gegenseitige Authentifizierung in CyberArk.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
2. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Serverzertifikat**.
3. Klicken Sie auf die Registerkarte **Client-Zertifikat**.
4. Wählen Sie **CyberArk** als Servertyp aus.
5. Klicken Sie auf **Zertifikat neu generieren**, um ein neues TLS-Zertifikat für gegenseitige Authentifizierung für CyberArk zu generieren.

   Achtung: Wenn Sie das TLS-Zertifikat für gegenseitige Authentifizierung für CyberArk neu generieren, nachdem eine Verbindung zwischen und XClarity Administrator und CyberArk hergestellt wurde, geht die Verbindung verloren, bis Sie das neue Zertifikat in CyberArk importieren.
6. Klicken Sie auf **Zertifikat herunterladen** und anschließend auf **Als „DER“ speichern** oder **Als „PEM“ speichern**, um das Serverzertifikat auf dem lokalen System zu speichern.
7. Importieren Sie das heruntergeladene Zertifikat in CyberArk.

Schritt 3. Importieren Sie das CyberArk-CA-Stammzertifikat in XClarity Administrator.

1. Laden Sie das CA-Stammzertifikat von CyberArk herunter.
2. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
3. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Vertrauenswürdige Zertifikate**.
4. Klicken Sie auf das Symbol für **Erstellen** ( ), um ein Zertifikat hinzuzufügen.

5. Suchen Sie die Datei oder fügen Sie den Zertifikatstext im PEM-Format ein.
6. Klicken Sie auf **Erstellen**.

Schritt 4. Fügen Sie Pfade hinzu, die die Position der integrierten Benutzeraccounts in CyberArk identifizieren.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
2. Klicken Sie im Abschnitt für die Identitätsverwaltung auf **CyberArk**.
3. Klicken Sie auf die Registerkarte **Pfade**.
4. Klicken Sie auf das Symbol **Erstellen** ( ), um das Dialogfenster CyberArk-Pfad erstellen aufzurufen.

5. Optional können Sie die Anwendungs-ID, den Safe und Ordner angeben, in dem die Benutzeraccounts in CyberArk gespeichert sind.

   Wenn Sie die Anwendungs-ID und den Safe und optional den Ordner angeben, versucht XClarity Administrator, den Benutzeraccount am angegebenen Speicherort zu finden.

   Wenn Sie eine Kombination von anderen Feldern als Anwendungs-ID und Safe angeben (z. B. wenn Sie nur die Anwendungs-ID, nur den Safe und Ordner oder nur die Anwendungs-ID und den Ordner angeben), filtert XClarity Administrator der Pfad mithilfe der angegebenen Werte.
6. Klicken Sie auf **Übernehmen**.

Nach dieser Aufgabe

- Ändern Sie einen ausgewählten CyberArk-Pfad, indem Sie auf das Symbol **Bearbeiten** ( ) klicken.
- Sie können einen ausgewählten CyberArk-Pfad über das Symbol **Löschen** ( ) löschen.

Den Typ der Authentifizierungsmethode bestimmen, der von Lenovo XClarity Administrator verwendet wird

Sie können den Typ der Authentifizierungsmethode bestimmen, der derzeit von den Registerkarten **LDAP-Client** und **SAML-Einstellungen** auf der Seite „Sicherheit“ verwendet wird.

Zu dieser Aufgabe

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

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

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

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

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

Vorgehensweise

Anhand der folgenden Schritte bestimmen Sie, welcher Typ von Authentifizierungsserver von der Verwaltungssoftware verwendet wird:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **LDAP-Client**, um das Dialogfenster LDAP-Clienteinstellungen anzuzeigen.

Überprüfen Sie, welches Benutzerauthentifizierungsverfahren ausgewählt wurde:

- **Anmeldung von lokalen Benutzern zulassen**. Es wird die lokale Authentifizierung verwendet. Wenn diese Option ausgewählt ist, befinden sich alle Benutzeraccounts auf dem lokalen Authentifizierungsserver im Verwaltungsknoten.
- **Anmeldung von LDAP-Benutzern zulassen**. Die Authentifizierung wird über einen externen LDAP-Server ausgeführt. Diese Methode ermöglicht die Fernverwaltung von Benutzeraccounts. Wenn diese Option ausgewählt ist, liegen alle Benutzeraccounts fern auf einem externen LDAP-Server vor.
- **Erst lokale Benutzer und danach LDAP-Benutzer zulassen**. Der lokale Authentifizierungsserver führt die Authentifizierung zuerst aus. Wenn dieser Schritt nicht erfolgreich ist, führt ein externer LDAP-Server die Authentifizierung aus.

- **Erst LDAP-Benutzer und danach lokale Benutzer zulassen**. Zuerst führt ein externer LDAP-Server die Authentifizierung aus. Wenn dieser Schritt nicht erfolgreich ist, führt der lokale Authentifizierungsserver die Authentifizierung aus.

Schritt 3. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **SAML-Einstellungen**, um die Seite „SAML-Einstellungen“ anzuzeigen.

Wenn **SAML aktiviert** ausgewählt ist, wird ein Identity Provider verwendet.

Nach einem externen LDAP-Serverfehler auf Lenovo XClarity Administrator zugreifen

Wenn Sie einen externen LDAP-Authentifizierungsserver verwenden und dieser Server fehlerhaft oder nicht verfügbar ist, verwenden Sie das folgende Verfahren, um den Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle mithilfe des lokalen Authentifizierungsservers auf dem Verwaltungsknoten wiederherzustellen.

Vorgehensweise

Gehen Sie wie folgt vor, um die LDAP-Clienteinstellungen zu ändern:

Schritt 1. Melden Sie sich über einen Benutzeraccount mit **lxc-recovery**-Berechtigungen bei der XClarity Administrator-Webschnittstelle an. Weitere Informationen zum Clientdomänennamen finden Sie unter Externen LDAP-Authentifizierungsserver konfigurieren.

Schritt 2. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 3. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **LDAP-Client**, um das Dialogfenster LDAP-Client anzuzeigen.

Schritt 4. Wählen Sie als Benutzerauthentifizierungsverfahren **Anmeldung von lokalen Benutzern zulassen**, um die lokale Verwaltung von Benutzeraccounts zu aktivieren. Wenn diese Option ausgewählt ist, befinden sich alle Benutzeraccounts lokal auf dem Verwaltungsserver.

Schritt 5. Klicken Sie auf **Übernehmen**.

Ergebnisse

Die Benutzeraccounts in der lokalen Benutzerregistry des Verwaltungsknotens können jetzt für den Zugriff auf den XClarity Administrator-Verwaltungsserver verwendet werden. Nachdem Ihr externer Authentifizierungsserver wiederhergestellt wurde und für den Verwaltungsserver verfügbar ist, können Sie die Einstellung für den LDAP-Client wieder auf den externen Authentifizierungsserver zurücksetzen.

Nach einem externen SAML-Identity Provider-Fehler auf Lenovo XClarity Administrator zugreifen

Wenn Sie einen externen SAML-Identity Provider verwenden und dieser Server fehlerhaft oder nicht verfügbar ist, verwenden Sie das folgende Verfahren, um den Zugriff auf die Lenovo XClarity Administrator-Webschnittstelle mithilfe des lokalen Authentifizierungsservers von XClarity Administrator wiederherzustellen.

Vorgehensweise

Gehen Sie wie folgt vor, um SAML-Clienteinstellungen zu ändern:

Schritt 1. Öffnen Sie die XClarity Administrator-Anmeldeseite im Webbrowser (z. B. `https://<ip_address>/ui/login.html`).

Schritt 2. Melden Sie sich mit einem bei der Einrichtung des Identity Provider erstellten lokalen Wiederherstellungsbenutzeraccounts an der XClarity Administrator-Webschnittstelle an.

Schritt 3. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 4. Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **SAML-Einstellungen**, um den Dialog SAML-Clienteinstellungen anzuzeigen.

Schritt 5. Deaktivieren Sie die Option **SAML aktivieren**, um den SAML-Identity Provider zu deaktivieren. Wenn diese Option deaktiviert ist, wird der lokale Authentifizierungsserver der externen LDAP-Server (falls konfiguriert) zur Authentifizierung verwendet.

Schritt 6. Klicken Sie auf **Übernehmen**.

Ergebnisse

Die Benutzeraccounts in der lokalen Benutzerregistry des Verwaltungsknotens können jetzt für den Zugriff auf den XClarity Administrator-Verwaltungsserver verwendet werden. Nachdem Ihr externer Identity Provider wiederhergestellt und für den Verwaltungsserver verfügbar ist, können Sie die Authentifizierungsmethode für den Identity Provider ändern.

Benutzeraccounts verwalten

Benutzeraccounts werden verwendet, um sich anzumelden und Lenovo XClarity Administrator sowie alle Gehäuse und Server, die von XClarity Administrator gesteuert werden, zu verwalten. XClarity Administrator-Benutzeraccounts unterliegen zwei unabhängigen Prozessen: Authentifizierung und Autorisierung.

Zu dieser Aufgabe

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

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

Anmerkung: Die Benutzeraccounts SYSMGR_* und SYSRDR_* (wobei * ein zufällig gewähltes Suffix aus den Zeichen A–Z und 0–9 ist) werden von XClarity Administrator als Service-Benutzeraccounts generiert und verwendet. Sie werden für Funktionen wie verwaltete Authentifizierung, BS-Implementierung und Firmwareaktualisierung verwendet. Die Kennwörter SYSMGR_* und SYSRDR_* werden bei jedem Booten von XClarity Administrator und kurz vor Ablauf der Kennwortablaufdauer geändert.

Benutzer erstellen

Benutzeraccounts werden verwendet, um Berechtigungen und den Zugriff auf Ressourcen zu verwalten.

Zu dieser Aufgabe

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

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

Vorgehensweise

So fügen Sie einen Benutzer zu XClarity Administrator hinzu:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Lokale Benutzer**, um die Seite Benutzerverwaltung anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ), um einen Benutzer zu erstellen. Das Dialogfenster „Neuen Benutzer erstellen“ wird angezeigt.

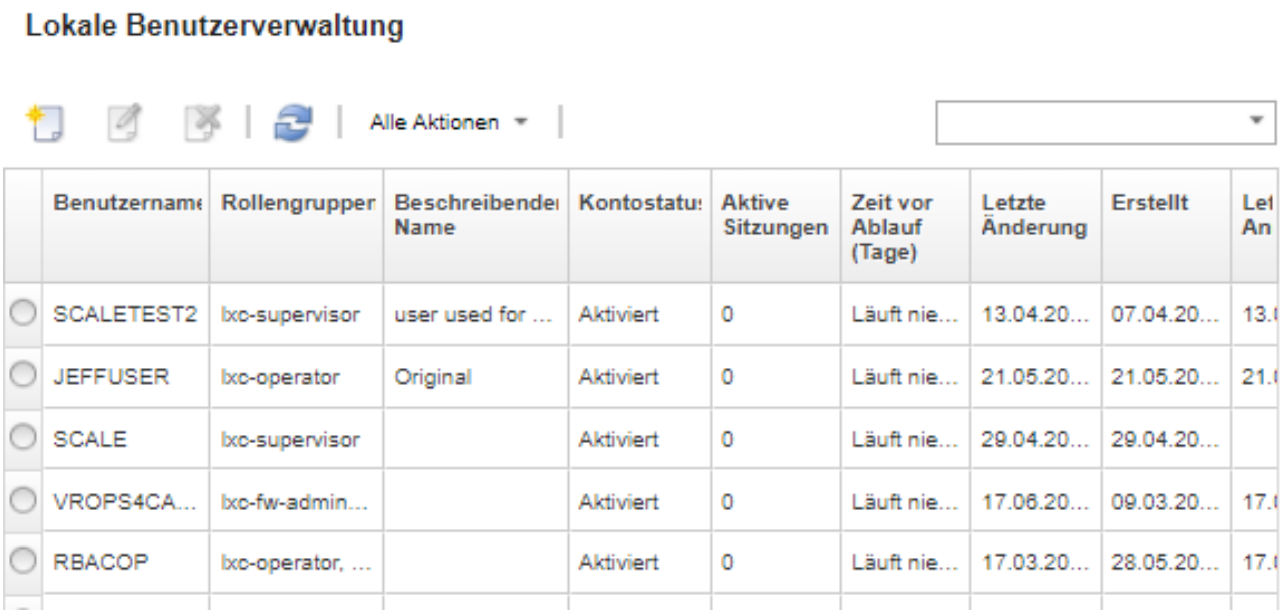
Schritt 4. Tragen Sie die folgenden Informationen ein.

- Geben Sie einen Benutzernamen und eine Beschreibung für den Benutzer ein.
- Geben Sie das neue Kennwort ein und bestätigen Sie es. Die Regeln für Kennwörter basieren auf den aktuellen Accountsicherheitseinstellungen.
- Wählen Sie mindestens eine Rollengruppen aus, um den Benutzer für die Ausführung entsprechender Aufgaben zu autorisieren.Informationen zu Rollengruppen und zur Erstellung angepasster Rollengruppen finden Sie unter Angepasste Rollengruppe erstellen.
- (Optional) Legen Sie die Option **Kennwort beim ersten Zugriff ändern** auf `Yes` fest, wenn Sie den Benutzer bei der ersten Anmeldung an XClarity Administrator zur Kennwortänderung zwingen möchten.

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

Nach dieser Aufgabe

Der Benutzeraccount wird in der Tabelle Benutzerverwaltung angezeigt. In der Tabelle werden die zugeordneten Rollengruppen und der Accountstatus für jeden Benutzeraccount angezeigt.



Nachdem Sie einen Benutzeraccount erstellt haben, können Sie die folgenden Aktionen für einen ausgewählte Benutzeraccount ausführen:

- Ändern Sie den Benutzernamen, die Beschreibung und die Rolle für einen Benutzeraccount, indem Sie auf das Symbol **Bearbeiten** ( ) klicken.
- Löschen Sie den Benutzeraccount, indem Sie auf das Symbol **Löschen** ( ) klicken.
- Setzen Sie das Kennwort für den Benutzeraccount zurück (siehe Das Kennwort für einen Benutzer zurücksetzen).

- Entsperren Sie den Benutzeraccount (siehe Einen Benutzer freigeben).
- Aktivieren oder deaktivieren Sie einen Benutzeraccount (siehe Einen Benutzer aktivieren oder deaktivieren).

Einen Benutzer aktivieren oder deaktivieren

Sie können einen lokalen Benutzeraccount auf dem Authentifizierungsserver ändern, aktivieren oder deaktivieren.

Vorgehensweise

So aktivieren oder deaktivieren Sie einen Benutzeraccount:

- Wenn der lokale Authentifizierungsserver verwendet wird:
  1. Klicken Sie in der Lenovo XClarity Administrator-Titelleiste auf **Verwaltung → Sicherheit**.
  2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Lokale Benutzer**, um die Seite Benutzerverwaltung anzuzeigen.
  3. Wählen Sie ein Benutzerkonto aus.
  4. Wenn der Benutzeraccount aktiviert ist, klicken Sie auf **Alle Aktionen → Ausgewählten Account deaktivieren**, um den Benutzer zu deaktivieren. Der Accountstatus in der Tabelle ändert sich zu `Disabled`.
  5. Wenn der Benutzeraccount deaktiviert ist, klicken Sie auf **Alle Aktionen → Ausgewählten Account aktivieren**, um den Benutzer zu aktivieren. Der Accountstatus in der Tabelle ändert sich zu `Enabled`.
- Wenn ein externer LDAP-Server verwendet wird, aktivieren oder deaktivieren Sie den Benutzeraccount in Microsoft Active Directory.
- Wenn ein externer SAML-Identity Provider verwendet wird, aktivieren oder deaktivieren Sie den Benutzeraccount in Identity Provider.

Aktiven Benutzer abmelden

Sie können einen aktiven Benutzer von Lenovo XClarity Administrator abmelden (Beenden).

Sie müssen mit einen Benutzeraccount an XClarity Administrator angemeldet sein, das über die Rechte **lxc-supervisor** oder **lxc-security-admin** verfügt.

Vorgehensweise

So melden Sie einen aktiven Benutzer ab:

Schritt 1. Klicken Sie in der XClarity Administrator-Titelleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Aktive Sitzungen**, um die Seite Verwaltung aktiver Sitzungen anzuzeigen.

Schritt 3. Wählen Sie mindestens einen Benutzeraccount aus.

Schritt 4. Klicken Sie auf **Benutzer abmelden**.

Das Kennwort für Ihren Benutzeraccount ändern

Sie können das Kennwort für Ihren Benutzeraccount ändern.

Vorgehensweise

So ändern Sie Ihr Kennwort:

- Wenn der lokale Authentifizierungsserver verwendet wird:

1. Klicken Sie in der Lenovo XClarity Administrator -Titelleiste auf das Benutzeraktionen-Menü (ADMIN_USER) und dann auf **Kennwort ändern**. Das Dialogfenster Kennwort ändern wird angezeigt.

2. Geben Sie das aktuelle Kennwort ein.
3. Geben Sie das neue Kennwort ein und bestätigen Sie es. Die Regeln für Kennwörter basieren auf den aktuellen Accountsicherheitseinstellungen.
4. Klicken Sie auf **Ändern**.

- Wenn ein externer Authentifizierungsserver verwendet wird, ändern Sie Ihr Kennwort in Microsoft Active Directory.

  Achtung: Wenn Sie Microsoft Active Directory mit einem neuen Kennwort für den Client-Account aktualisieren, das zur Bindung von XClarity Administrator an den externen Authentifizierungsserver verwendet wird, stellen Sie sicher, dass Sie das neue Kennwort auch in der XClarity Administrator-Webschnittstelle aktualisieren (siehe Externen LDAP-Authentifizierungsserver konfigurieren).
- Wenn ein externes SAML-Identity Provider verwendet wird, ändern Sie Ihr Kennwort in Identity Provider.

Das Kennwort für einen Benutzer zurücksetzen

Sie können das Kennwort für einen Benutzeraccount zurücksetzen.

Vorgehensweise

So setzen Sie ein Kennwort zurück:

- Wenn der lokale Authentifizierungsserver verwendet wird, setzen Sie das Kennwort über die Lenovo XClarity Administrator-Webschnittstelle zurück:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
  2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Lokale Benutzer**, um die Seite Benutzerverwaltung anzuzeigen.
  3. Wählen Sie einen Benutzeraccount aus der Tabelle aus.

4. Wenn der Benutzeraccount aktiviert ist, klicken Sie auf **Alle Aktionen → Kennwort für ausgewählten Benutzer zurücksetzen**. Das Dialogfenster „Kennwort zurücksetzen“ wird angezeigt.
   a. Geben Sie das neue Kennwort ein und bestätigen Sie es. Die Regeln für Kennwörter basieren auf den aktuellen Accountsicherheitseinstellungen.
   b. Legen Sie optional die Option **Beim ersten Zugriff ändern** auf `Yes` fest, wenn Sie den Benutzer bei der ersten Anmeldung an XClarity Administrator zur Kennwortänderung zwingen möchten.
   c. Klicken Sie auf **Zurücksetzen**.

- Wenn ein externer LDAP-Server verwendet wird, setzen Sie das Kennwort in Microsoft Active Directory zurück.
- Wenn ein externes SAML-Identity Provider verwendet wird, setzen Sie das Kennwort in Identity Provider zurück.
- Wenn Sie sich nicht mit einem anderen Systemadministratorkonto bei XClarity Administrator anmelden können oder kein anderes Systemadministratorkonto vorhanden ist, können Sie das Kennwort für einen lokalen Benutzer mit Wiederherstellungs- oder Supervisor-Berechtigungen zurücksetzen, indem Sie ein ISO-Image anhängen, das eine Konfigurationsdatei mit dem neuen Kennwort enthält. Weitere Informationen finden Sie unter Kennwort für eine lokale Wiederherstellung oder einen Supervisor-Benutzer vergessen in der Onlinedokumentation von XClarity Administrator.

Einen Benutzer freigeben

Sie können einen in Lenovo XClarity Administrator gesperrten Benutzeraccount entsperren. Ein Benutzeraccount kann vorübergehend gesperrt werden, wenn der Benutzer zu viele ungültige Anmeldeversuche durchgeführt hat.

Zu dieser Aufgabe

Die Sicherheitseinstellungen eines Benutzeraccounts steuern die Mindestdauer in Minuten, die vergehen müssen, bevor sich ein gesperrter Benutzer erneut anmelden kann. Wenn die Einstellung **Sperrzeitraum nach maximaler Anzahl von fehlgeschlagenen Anmeldeversuchen** auf `0` festgelegt ist, bleibt der Benutzeraccount gesperrt, bis er von einem Administrator entsperrt wird. Weitere Informationen zum Sperrzeitraum nach der maximalen Anzahl von fehlgeschlagenen Anmeldeversuchen finden Sie unter Die Sicherheitseinstellungen eines Benutzeraccounts ändern.

Sie können einen Benutzeraccount außerdem dauerhaft aktivieren oder deaktivieren. Siehe Einen Benutzer aktivieren oder deaktivieren für weitere Informationen.

Anmerkung: Sie müssen Supervisor-Rechte haben, um einen Benutzeraccount zu entsperren.

Tipp: Sie können XClarity Administrator zum Entsperren von Benutzeraccounts verwenden, auf dem lokalen Authentifizierungsserver verwaltet werden. Sie können mit XClarity Administrator keine Benutzeraccounts auf einem externen Authentifizierungsserver entsperren.

Vorgehensweise

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

- Wenn der lokale Authentifizierungsserver verwendet wird:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
  2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Lokale Benutzer**, um die Seite Benutzerverwaltung anzuzeigen.
  3. Wählen Sie den Benutzeraccount aus der Tabelle aus.
  4. Klicken Sie auf **Alle Aktionen → Account für ausgewählten Benutzer entsperren**.

- Wenn ein externer LDAP-Server verwendet wird, entsperren Sie das Benutzeraccount in Microsoft Active Directory.
- Wenn ein externes SAML-Identity Provider verwendet wird, entsperren Sie das Benutzeraccount in Identity Provider.

Aktive Benutzer überwachen

Sie können über die Dashboardseite feststellen, wer an der Lenovo XClarity Administrator-Webschnittstelle angemeldet ist.

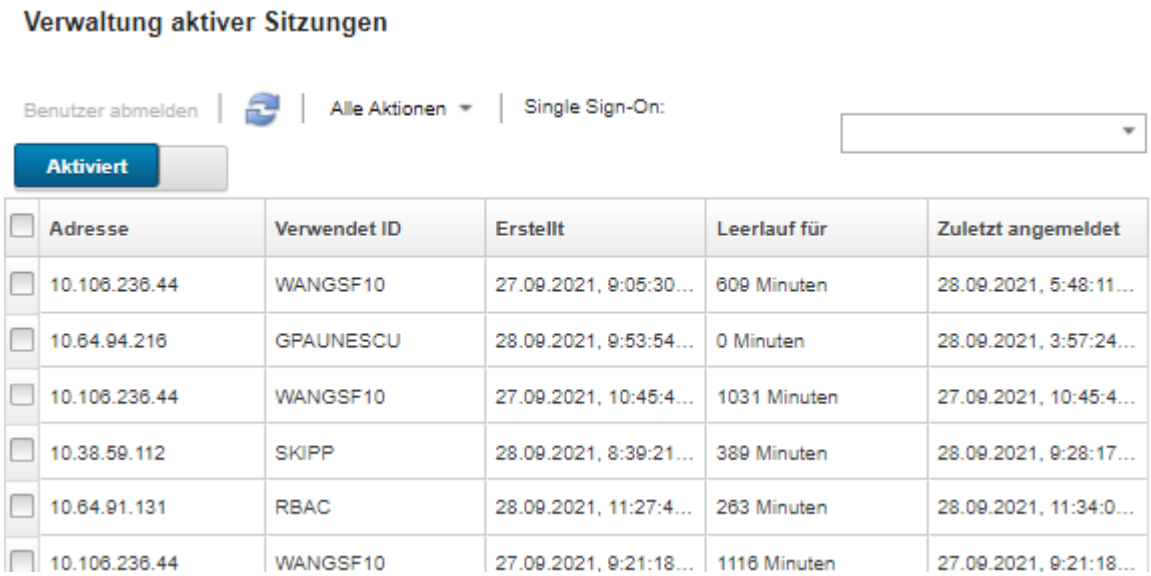
Vorgehensweise

- Sie können eine Liste der aktiven Benutzer und ihrer IP-Adressen abrufen, indem Sie in der XClarity Administrator-Menüleiste auf **Dashboard** klicken.

  Die aktiven Benutzersitzungen werden im Aktivitätsabschnitt aufgelistet.

- Sie können eine Liste aller aktiven Benutzer (außerdem aktiven Benutzer) und ihrer IP-Adressen abrufen, indem Sie in der XClarity Administrator-Menüliste auf **Verwaltung → Sicherheit** und dann auf **Aktive Sitzungen** klicken.

  Anmerkung: Benutzersitzungen, die länger als eine festgelegte Dauer inaktiv sind, werden automatisch abgemeldet. Sie können den Inaktivitätszeitraum festlegen, indem Sie auf **Verwaltung → Sicherheit** in der Menüleiste von XClarity Administrator klicken, die Option „Accountsicherheitseinstellungen“ auswählen und dann den Wert **Sitzungszeitlimit bei Webinaktivität** anpassen. Beachten Sie, dass die Änderung keine Auswirkungen auf aktive Benutzersitzungen hat. Sie wirkt sich nur auf Benutzersitzungen aus, die gestartet werden, nachdem die Einstellung geändert wurde.



Gespeicherte Anmeldeinformationen verwalten

Gespeicherte Anmeldeinformationen werden verwendet, um die Autorisierung und den Zugriff auf Gehäuse und Server zu verwalten, die durch Lenovo XClarity Administrator mit einer lokalen Authentifizierung verwaltet werden.

Vorbereitende Schritte

Sie müssen die Berechtigungen **lxc-supervisor** oder **lxc-security-admin** besitzen, um gespeicherte Anmeldeinformationen zu erstellen, zu ändern oder zu löschen.

Zu dieser Aufgabe

Bei den gespeicherten Anmeldeinformationen muss es sich um einen aktiven Benutzeraccount auf der Einheit oder um einen Benutzeraccount auf einem Active Directory-Server handeln.

Wenn Sie sich dazu entscheiden, Einheiten mit der lokalen Authentifizierung anstatt mit der verwalteten XClarity Administrator Authentifizierung zu verwalten, müssen Sie beim Verwaltungsprozess einen Account mit gespeicherten Anmeldeinformationen auswählen.

Wichtig: XClarity Administrator validiert nicht den Benutzernamen und das Kennwort, das Sie für die gespeicherten Anmeldeinformationen angegeben haben. Es liegt in Ihrer Verantwortung, sicherzustellen, dass die angegebenen Informationen einem aktiven Benutzeraccount auf der lokalen Einheit oder im Active Directory entsprechen (falls die verwaltete Einheit zur Verwendung von Active Directory für die Authentifizierung konfiguriert ist).

Achtung: Die gespeicherten Anmeldeinformationen müssen über Supervisorzugriff oder ausreichend Berechtigungen verfügen, um Konfigurationsänderungen auf der Einheit vorzunehmen. Wenn Sie versuchen, einen Server mit gespeicherten Anmeldeinformationen zu verwalten, die nicht über ausreichende Berechtigungen für die Einheit verfügen, ist der Verwaltungsprozess zwar möglicherweise erfolgreich, ggf. schlagen aber zusätzliche administrative Bestandsaktivitäten auf der Einheit fehl, da der Zugriff verweigert wird. Dies könnte dazu führen, dass Verbindungsprobleme mit der Einheit festgestellt werden.

Vorgehensweise

So fügen Sie gespeicherte Anmeldeinformationen zu XClarity Administrator hinzu:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**. Die Seite Sicherheit wird angezeigt.

Schritt 2. Klicken Sie auf **Gespeicherte Anmeldeinformationen** im Abschnitt „Verwaltete Authentifizierung“, um die Seite „Gespeicherte Anmeldeinformationen“ anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ), um gespeicherte Anmeldeinformationen zu erstellen. Das Dialogfenster Neue gespeicherte Anmeldeinformationen erstellen wird angezeigt.

Schritt 4. Tragen Sie die folgenden Informationen ein.
- Geben Sie einen Benutzernamen und optional eine Beschreibung für die gespeicherten Anmeldeinformationen ein.
- Geben Sie das Kennwort für die gespeicherten Anmeldeinformationen ein und bestätigen Sie dieses.
- Geben Sie optional das Kennwort für die mit RECOVERY_ID gespeicherten Anmeldeinformationen ein und bestätigen Sie dieses.

Schritt 5. Klicken Sie auf **Gespeicherte Anmeldeinformationen** erstellen.

Nach dieser Aufgabe

Der Account mit den gespeicherten Anmeldeinformationen wird in der Tabelle „Gespeicherte Anmeldeinformationen“ angezeigt. In der Tabelle wird die zugeordnete ID und eine Beschreibung für jeden Account mit gespeicherten Anmeldeinformationen angezeigt.

Über die Seite „Gespeicherte Anmeldeinformationen“ können Sie für einen ausgewählten Account mit gespeicherten Anmeldeinformationen die folgenden Aktionen ausführen:

- Ändern Sie den Benutzernamen, das Kennwort und eine Beschreibung für einen Account mit gespeicherten Anmeldeinformationen, indem Sie auf das Symbol **Bearbeiten** klicken ( ).

  Anmerkung: Wenn Sie eine Einheit mit gespeicherten Anmeldeinformationen verwalten und die verwaltete Authentifizierung aktivieren, können Sie die gespeicherten Anmeldeinformationen nicht bearbeiten.
- Löschen Sie den Account mit gespeicherten Anmeldeinformationen, indem Sie auf das Symbol **Löschen** klicken ( ).

Informationen zum Auflösen gespeicherter Anmeldeinformationen, die abgelaufen oder ungültig sind, finden Sie unter Abgelaufene oder ungültige gespeicherte Anmeldeinformationen für einen Server auflösen.

Rollen und Rollengruppen verwalten

Eine *Rolle* wird zur Steuerung des Benutzerzugriffs auf Ressourcen verwendet. Sie schränkt die Aktionen ein, die ein Benutzer für diese Ressourcen ausführen kann. Eine *Rollengruppe* ist eine Sammlung mit einer oder mehreren Rollen. Sie wird verwendet, um die Rollen mehreren Benutzern zuzuweisen. Die von Ihnen für eine Rollengruppe konfigurierten Rollen legen die Zugriffsebene für die Benutzer fest, die Mitglied der Rollengruppe sind. Jeder Lenovo XClarity Administrator-Benutzer muss in mindestens einer Rollengruppe Mitglied sein.

Angepasste Rolle erstellen

Ein *Rolle* ist ein Satz von *Berechtigungen* zum Ausführen einer bestimmter Aktion. Lenovo XClarity Administrator enthält mehrere vordefinierte (Standard-) Rollen. Sie können auch angepasste Rollen erstellen, mit denen ein eindeutiger Berechtigungssatz für die vom Benutzer ausführbaren Aktionen erzwungen wird.

Vorbereitende Schritte

Sie benötigen die Berechtigung **lxc-supervisor** oder **lxc-security-admin** für die Ausführung dieses Tasks.

Zu dieser Aufgabe

Um eine benutzerdefinierte Rolle zu erstellen, wählen Sie eine oder mehrere vordefinierte Rollen aus, die dem Umfang der Rolle, die Sie erstellen möchten, am nächsten kommen, und löschen Sie dann die einzelnen Berechtigungen, die Sie einschränken möchten. Dadurch wird sichergestellt, dass Sie alle gewünschten Berechtigungen erhalten und die Rolle ordnungsgemäß mit abhängigen Berechtigungen erstellt wird.

Einige XClarity Administrator-Berechtigungen sind von den entsprechenden Berechtigungen für das Verwaltungsmodul abhängig, um Aktionen auf verwalteten Einheiten auszuführen (siehe Berechtigungen für Verwaltungsmodul v1 und Berechtigungen für Verwaltungsmodul v2). Mit einer XClarity Administrator-Berechtigung können Sie möglicherweise eine Aktion auf einem verwalteten Gerät anfordern, das die Anforderung jedoch verweigert, wenn Sie nicht über die entsprechenden Berechtigungen für CMM, IMM oder XCC verfügen. Wenn Sie beispielsweise eine benutzerdefinierte Rolle für die Ausführung von Stromversorgungsaktionen auf verwalteten Einheiten erstellen, können Sie die Berechtigung **lxc-inventory-modify-device-power-state** hinzufügen und folgende Schritte ausführen:

- Fügen Sie für einen ThinkSystemserver-Server in einem Rack die Berechtigung **mm-power-and-restart-access-v1** hinzu.
- Fügen Sie für ein vollständiges Flex System Gehäuse (einschließlich Einheiten im Gehäuse) die Berechtigung **mm-power-and-restart-access-v1** hinzu.
- Fügen Sie für einen ThinkSystem-Server in einem Gehäuse **mm-power-and-restart-access-v1** und **mm-blade-operator-v2** sowie die Berechtigung **mm-blade-#-scope-v2** hinzu, die dem Zielserver entspricht.

Alle Rollen enthalten Leseberechtigungen. Keine angepasste Rolle kann eingeschränkter als die Rolle **lxc-operator** sein.

Wenn ein Benutzer keine Berechtigungen zum Ausführen bestimmter Aktionen hat, sind Menüelemente, Symbolleistensymbole und Schaltflächen, die diese Aktionen ausführen, deaktiviert (abgeblendet).

XClarity Administrator stellt für jede vordefinierte Rolle eine Rollengruppe mit dem gleichen Namen wie die Rolle zur Verfügung. Für neue Gruppen, die Sie erstellen, können Sie eine Rollengruppe erstellen. Weitere Informationen zu Rollengruppen finden Sie unter Angepasste Rollengruppe erstellen.

- **lxc-supervisor**. Benutzer, denen diese Rolle zugewiesen wird, können alle verfügbaren Vorgänge für den Verwaltungsserver und alle verwalteten Einheiten anzeigen, konfigurieren und durchführen.Benutzer, die denen diese Rolle zugeordnet wird, können immer auf alle verwalteten Einheiten zugreifen. Sie können den Zugriff auf Einheiten für diese Rolle nicht einschränken.

- **lxc-admin**. Benutzer, denen diese Rolle zugewiesen wird, können nicht-sicherheitsbezogene Einstellungen ändern und entsprechende nicht-sicherheitsbezogene Vorgänge für den Verwaltungsserver ausführen (inkl. dem Aktualisieren und Neustarten des Verwaltungsservers). Diese Rolle umfasst zudem die Möglichkeit, alle Konfigurations- und Statusinformationen zum Verwaltungsserver und den verwalteten Einheiten anzuzeigen.
- **lxc-security-admin**. Benutzer, denen diese Rolle zugeordnet wird, können Sicherheitseinstellungen ändern und sicherheitsrelevante Vorgänge für den Verwaltungsserver und die verwalteten Einheiten ausführen. Diese Rolle umfasst zudem die Möglichkeit, alle Konfigurations- und Statusinformationen zum Verwaltungsserver und den verwalteten Einheiten anzuzeigen.

  Benutzer, die denen diese Rolle zugeordnet wird, können immer auf alle verwalteten Einheiten zugreifen. Sie können den Zugriff auf Einheiten für diese Rolle nicht einschränken.
- **lxc-hw-admin**. Benutzer, denen diese Rolle zugewiesen wird, können für die verwaltete Einheiten nicht-sicherheitsbezogene Vorgänge durchführen (inkl. Aktualisierung und Neustart der verwalteten Einheiten). Diese Rolle umfasst zudem die Möglichkeit, alle Konfigurations- und Statusinformationen zum Verwaltungsserver und allen verwalteten Einheiten anzuzeigen.
- **lxc-fw-admin**. Benutzer, denen diese Rolle zugewiesen wird, können Firmware-Richtlinien erstellen und diese Richtlinien auf verwalteten Einheiten bereitstellen. Benutzer, denen diese Rolle nicht zugewiesen wurde, können nur die Richtlinieninformationen anzeigen.
- **lxc-os-admin**. Benutzer mit dieser Rolle können Betriebssysteme und Einheitentreiberaktualisierungen auf verwaltete Server herunterladen und dort implementieren. Benutzer, denen diese Rolle nicht zugewiesen wurde, können nur die Betriebssystem- und Einheitentreiberinformationen anzeigen.
- **lxc-service-admin**. Benutzer, denen diese Rolle zugewiesen werden, können Servicedateien für XClarity Administratorund verwaltete Einheiten sammeln und herunterladen. Benutzer, denen diese Rolle nicht zugewiesen werden, können Servicedaten sammeln, jedoch nicht herunterladen.
- **lxc-hw-manager**. Benutzer, denen diese Rolle zugewiesen wird, können neue Einheiten ermitteln und diese Einheiten unter der Verwaltungssteuerung von XClarity Administrator platzieren. Diese Rolle verbietet dem Benutzer das Ausführen von Vorgängen oder das Ändern von Konfigurationseinstellungen für den Verwaltungsserver sowie die verwalteten Einheiten, abgesehen von Vorgängen, die zum Ermitteln und Verwalten neuer Einheiten notwendig sind.
- **lxc-operator**. Benutzer, denen diese Rolle zugewiesen wird, können alle Konfigurations- und Statusinformationen zum Verwaltungsserver und den verwalteten Einheiten anzeigen. Diese Rolle verbietet dem Benutzer das Ausführen von Vorgängen oder das Ändern von Konfigurationseinstellungen für den Verwaltungsserver sowie verwaltete Einheiten.
- **lxc-recovery**. Benutzer, denen diese Rolle zugeordnet wird, können Sicherheitseinstellungen ändern und sicherheitsrelevante Vorgänge für den Verwaltungsserver ausführen. Diese Benutzer können sich zusätzlich direkt am XClarity Administrator authentifizieren. Dies gilt auch dann, wenn die Authentifizierungsmethode auf einen externen LDAP-Server festgelegt ist. Diese Rolle stellt einen Wiederherstellungsmechanismus im Fall eines Übertragungsfehlers mit dem externen LDAP-Server bereit, der die „Anmeldeinformationen“-Konfiguration verwendet.

  Benutzer, die denen diese Rolle zugeordnet wird, können immer auf alle verwalteten Einheiten zugreifen. Sie können den Zugriff auf Einheiten für diese Rolle nicht einschränken.

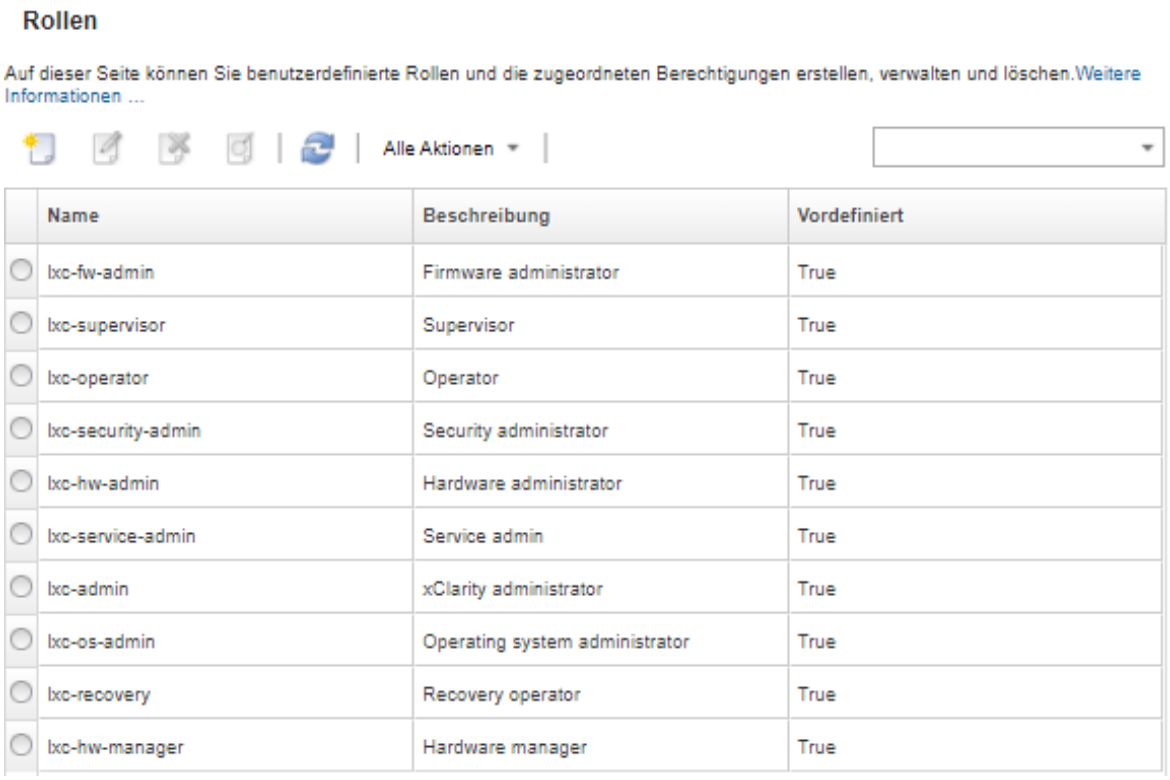
Die folgenden vordefinierten Rollen sind *reserviert* und können nicht verwendet werden, um neue Rollengruppen zu erstellen oder diese den neuen Benutzer zuzuweisen.
- **lxc-sysrdr**
- **lxc-sysmgr**

Vorgehensweise

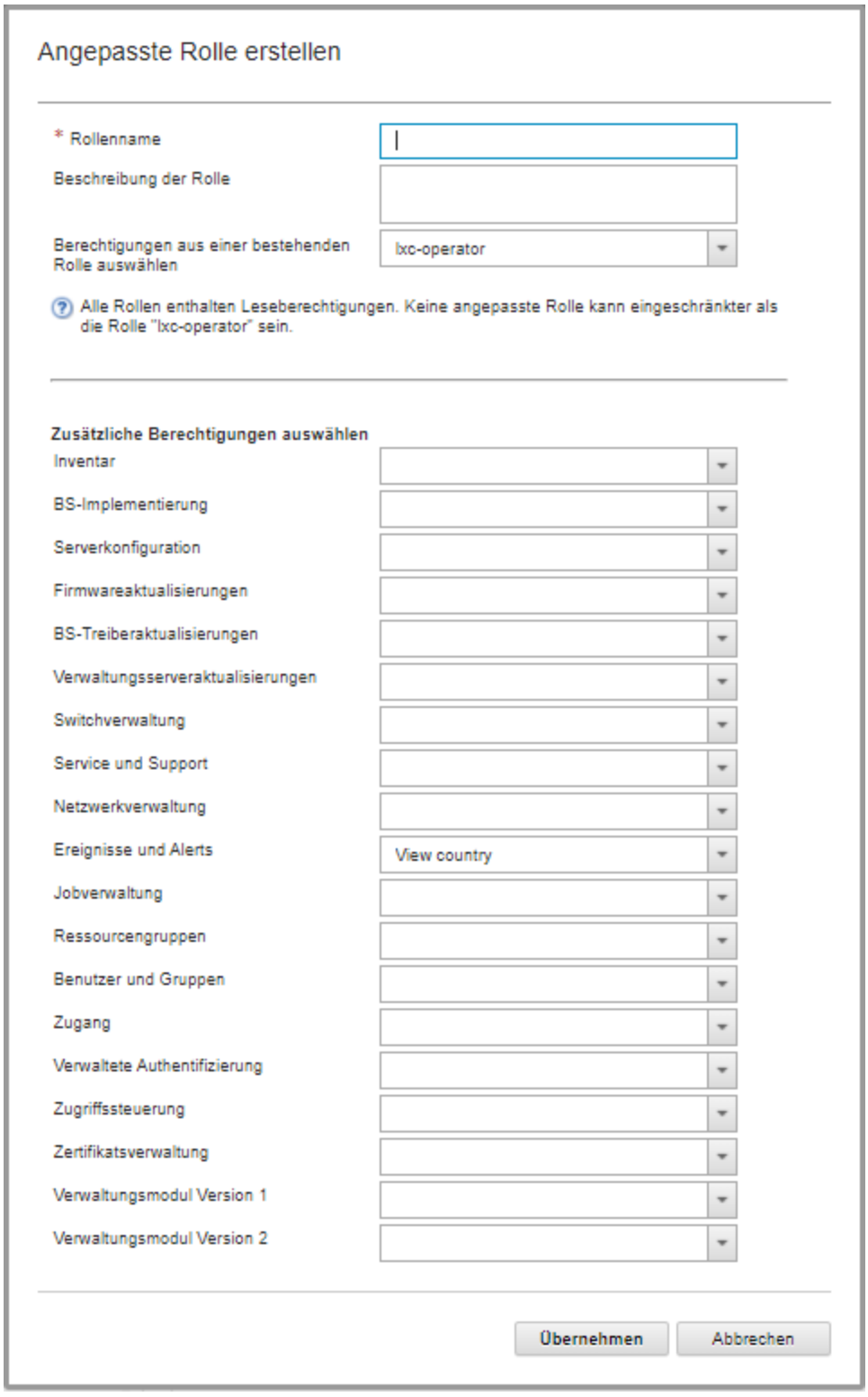
Führen Sie die folgenden Schritte aus, um eine angepasste Gruppe zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Rollen**, um die Seite „Rollenverwaltung“ anzuzeigen.



Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ), um eine Rolle zu erstellen. Das Dialogfenster Angepasste Rolle erstellen wird angezeigt.



Schritt 4. Geben Sie einen Rollennamen und eine Beschreibung ein.

Schritt 5. Wählen Sie eine vordefinierte Rolle als Ausgangspunkt für die angepasste Rolle aus.

Bei Auswahl einer vorhandenen Rolle werden deren zugehörige Berechtigungen in diesem Dialogfenster ausgewählt.

Schritt 6. Ändern Sie die Berechtigungen für die neue Rolle, indem Sie Berechtigungen im Dropdown-Menü **Weitere Berechtigungen auswählen** aktivieren oder deaktivieren.

Anmerkung: Wenn Sie alle Berechtigungen einer bestimmten Kategorie ausgewählt haben und dieser Kategorie bei einem XClarity Administrator-Update oder -Upgrade weitere Berechtigungen hinzugefügt werden, werden diese neuen Berechtigungen automatisch zur angepassten Rolle hinzugefügt.

Schritt 7. Klicken Sie auf **Erstellen**. Die neue Rolle wird zur Tabelle auf der Seite „Rollenverwaltung“ hinzugefügt.

Ergebnisse

Sie können außerdem die folgenden Aktionen ausführen.

- Zeigen Sie die Berechtigungen für eine bestimmte Rolle an, indem Sie die Rolle auswählen und auf das Symbol **Anzeigen** klicken ( ).
- Benennen Sie die angepasste Rolle um oder bearbeiten Sie diese, indem Sie auf das Symbol **Bearbeiten** ( ) klicken. Wenn Sie eine angepasste Rolle bearbeiten, können Sie die ausgewählten Berechtigungen, die Beschreibung und die Liste der Benutzer für diese Rolle ändern.

  Anmerkung: Vordefinierte Rollen können nicht geändert werden.
- Löschen Sie die vordefinierte oder angepasste Rolle über das Symbol **Löschen** ( ).
- Fügen Sie Rollen zu einer Rollengruppe hinzu oder entfernen Sie welche daraus (siehe Hinzufügen und Entfernen mehrerer Benutzer bei einer Rollengruppe).
- Stellen Sie alle gelöschten vordefinierten Rollen wieder her, indem Sie auf **Alle Aktionen** → **Standardrollen wiederherstellen** klicken.

Vordefinierte Berechtigungen

Lenovo XClarity Administrator bietet eine Reihe von *Berechtigungen*, mit denen Benutzer bestimmte Aktionen ausführen können. Die Berechtigungen sind auf Basis des Aktionstyps in Kategorien unterteilt.

Zugriffsberechtigungen

Diese Berechtigungen ermöglichen das Ändern von Verschlüsselungs- und SSL/TLS-Modi.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-sec-apply-crypto-settings	Verschlüsselungseinstellungen anwenden	lxc-recovery, lxc-security-admin, lxc-supervisor

Berechtigungen für die Zugriffssteuerung

Diese Berechtigungen ermöglichen die Steuerung des Zugriffs auf Ressourcen.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-sec-modify-resource-access-control	Einstellungen für Ressourcenzugriffssteuerung bearbeiten	lxc-recovery, lxc-security-admin, lxc-supervisor

Berechtigungen für die Zertifikatsverwaltung

Diese Berechtigungen ermöglichen das Verwalten von Sicherheitszertifikaten in Lenovo XClarity Administrator.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-sec-add-external-certificates	Externes Zertifikat hinzufügen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Vertrauenswürdiges Zertifikat hinzufügen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-certificate-signing	Zertifikatssignieranforderung (CSR) generieren	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	Vorhandenes externes Zertifikat löschen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Vorhandenes Zertifikat löschen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Stammzertifikat der Zertifizierungsstelle herunterladen	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	Serverzertifikat herunterladen	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Zertifikatsperrliste ändern oder austauschen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Stammzertifikat der Zertifizierungsstelle neu generieren	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Stammzertifikat der Zertifizierungsstelle neu generieren	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Serverzertifikat neu generieren	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Nicht vertrauenswürdige Zertifikate auflösen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Serverzertifikat hochladen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_view_certpol_settings	Zertifikatrichtlinieneinstellungen anzeigen	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_apply_certpol_settings	Zertifikatrichtlinieneinstellungen übernehmen	lxc-security-admin, lxc-supervisor

Berechtigungen für Überwachung und Ereignisse

Diese Berechtigungen werden für die Verwaltung von Ereignissen und Alerts benötigt.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-event-audit	Ereignis- und Prüfprotokolle verwalten	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Ereignisweiterleitungen erstellen und ändern	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Push-Services erstellen und ändern	lxc-admin, lxc-hw-admin, lxc-supervisor

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-monitoring-remove-event-forwarders	Ereignisweiterleitungen löschen	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-push-services	Push-Services löschen	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Ereignis-Schwellenwerte festlegen	lxc-admin, lxc-hw-admin, lxc-supervisor

Berechtigungen für Firmwareaktualisierungen

Diese Berechtigungen werden benötigt, um Firmwareaktualisierungen und UpdateXpress System Packs zu verwalten und zu übernehmen.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-fwUpdates-apply-assign-policy	Firmwarekonformitätsrichtlinie zu Einheiten zuordnen	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Firmwareaktualisierungen ausführen	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Firmwarekonformitätsrichtlinien erstellen, kopieren, bearbeiten und importieren	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	Konformitätsrichtlinien löschen	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Firmwareaktualisierungspakete löschen	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Firmwareaktualisierungspakete herunterladen und importieren und Katalog der Firmwareaktualisierungspakete aktualisieren	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Firmwareaktualisierungspakete exportieren	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Berechtigungen für Ressourcengruppen

Diese Berechtigungen werden für Ressourcengruppen verwendet.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-resource-create-edit-group	Ressourcengruppen erstellen und ändern	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Ressourcengruppen löschen	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Berechtigungen für den Bestand

Diese Berechtigungen werden für die Ermittlung und Verwaltung von Einheiten sowie zum Anzeigen des Einheitenbestands benötigt.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-dm-manage-device	Gehäuse, Server, Speicher und Switches verwalten	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Prüfung auf IP-Adressduplikate im gleichen Subnetz aktivieren oder deaktivieren	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	Stromversorgungsstatus von Einschüben, CMMs, Knoten, Speicher und Switches ändern	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Eigenschaften von Schränken, Einschüben, Gehäusen, CMMs, Knoten, Speicher und Switches ändern	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	PFA-Konfigurationseinstellungen (vorhergesagte Fehler) ändern	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Berechtigungen für die Jobverwaltung

Diese Berechtigungen werden für die Verwaltung von Jobs (Tasks) benötigt.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-tasks-remove-jobs	Jobs löschen	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Jobs planen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Berechtigungen für die verwaltete Authentifizierung

Diese Berechtigungen ermöglichen die Verwaltung der Authentifizierung, einschließlich der gespeicherten Anmeldeinformationen.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-sec-delete-stored-credentials	Gespeicherte Anmeldeinformationen löschen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Vorhandene gespeicherte Anmeldeinformationen bearbeiten	lxc-recovery, lxc-security-admin, lxc-supervisor

Berechtigungen für Verwaltungsmodul v1

Diese Berechtigungen sind den LDAP-Berechtigungsbits (Bitstrings) zugeordnet, die von Verwaltungsmodulen für Rack-Server und vollständige Flex System-Gehäuse (einschließlich aller Einheiten in diesem Gehäuse) erzwungen werden.

Von Lenovo XClarity Administrator werden diese Berechtigungen nicht erzwungen. Die Berechtigungen werden von den verwalteten Einheiten erzwungen, die einen XClarity Administrator-Benutzeraccount verwenden.

Wird die Einheit mit der *verwalteten Authentifizierung* (Authentifizierung erfolgt über den lokalen Authentifizierungsserver) verwaltet, nutzt der lokale Authentifizierungsserver diese Berechtigungen, um den verwalteten Einheiten mitzuteilen, welche Berechtigungen dem Benutzer bei der Anmeldung an der Einheit erteilt werden sollen.

Sie konfigurieren dieselben Berechtigungen auf einem externen LDAP-Server. Wenn Sie einen externen LDAP-Server mit XClarity Administrator verwenden, stellen Sie sicher, dass Sie Gruppen im externen LDAP-Server mit Namen hinzufügen, die den Rollengruppennamen in XClarity Administrator entsprechen, und dass die externen LDAP-Benutzer zu mindestens einer dieser Gruppen hinzugefügt werden. Externe LDAP-Benutzer müssen Teil einer LDAP-Gruppe mit einem Namen sein, der einer Rollengruppe von XClarity Administrator entspricht, die Rollen enthält, die den Bit-Zeichenfolgen des Verwaltungsmoduls zugeordnet sind. XClarity Administrator verwendet diese Gruppen, um die externen LDAP-Benutzer mit den Rollengruppen in XClarity Administrator und den Bit-Zeichenfolgen zu verknüpfen, die vom Verwaltungsmodul erzwungen werden. Wenn sich ein Benutzer dann mit einem externen LDAP-Benutzeraccount bei einer verwalteten Einheit anmeldet, weiß das Verwaltungsmodul, ob dem Benutzer Supervisor- oder Bediener-Berechtigungen gewährt werden sollen.

Anmerkung: Verwaltungsmodul v1-Berechtigungen werden für FlexSystem-Switches, für die keine sichere IOM aktiviert ist, RackSwitch-Switches, Speichereinheiten und ThinkServerserver-Server nicht unterstützt.

Informationen zu den LDAP-Berechtigungsbits für die einzelnen Verwaltungsmodule finden Sie in der Onlinedokumentation.
- LDAP konfigurieren in der CMM- und CMM2-Onlinedokumentation
- LDAP konfigurieren in der IMM- und IMM2-Onlinedokumentation
- LDAP konfigurieren in der XCC-Onlinedokumentation

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
mm-advanced-adaptor-configuration-v1	Erweiterte Adapterkonfiguration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Allgemeine Konfiguration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-clear-event-logs-v1	Ereignisprotokolle löschen	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Nicht zulassen	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	Netzwerk und Sicherheit	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Zugriff zum Einschalten/Neustart von Servern und Flex-Switches	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Fernsteuerungszugriff auf Server	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Zugriff auf ferne Konsole und virtuelle Datenträger von Servern	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Supervisorzugriff	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	Benutzerverwaltung	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Berechtigungen für Verwaltungsmodul v2

Diese Berechtigungen sind den LDAP-Berechtigungsbits (Bitstrings) zugeordnet, die von Verwaltungsmodulen für einzelne FlexSystem- und ThinkSystem-Einheiten in einem Gehäuse (Gehäuse, Server und Switches, für die sichere IOM aktiviert ist) erzwungen werden.

Von Lenovo XClarity Administrator werden diese Berechtigungen nicht erzwungen. Die Berechtigungen werden von den verwalteten Einheiten erzwungen, die einen XClarity Administrator-Benutzeraccount verwenden.

Wird die Einheit mit der *verwalteten Authentifizierung* (Authentifizierung erfolgt über den lokalen Authentifizierungsserver) verwaltet, nutzt der lokale Authentifizierungsserver diese Berechtigungen, um den verwalteten Einheiten mitzuteilen, welche Berechtigungen dem Benutzer bei der Anmeldung an der Einheit erteilt werden sollen.

Sie konfigurieren dieselben Berechtigungen auf einem externen LDAP-Server. Wenn Sie einen externen LDAP-Server mit XClarity Administrator verwenden, stellen Sie sicher, dass Sie Gruppen im externen LDAP-Server mit Namen hinzufügen, die den Rollengruppennamen in XClarity Administrator entsprechen, und dass die externen LDAP-Benutzer zu mindestens einer dieser Gruppen hinzugefügt werden. Externe LDAP-Benutzer müssen Teil einer LDAP-Gruppe mit einem Namen sein, der einer Rollengruppe von XClarity Administrator entspricht, die Rollen enthält, die den Bit-Zeichenfolgen des Verwaltungsmoduls zugeordnet sind. XClarity Administrator verwendet diese Gruppen, um die externen LDAP-Benutzer mit den Rollengruppen in XClarity Administrator und den Bit-Zeichenfolgen zu verknüpfen, die vom Verwaltungsmodul erzwungen werden. Wenn sich ein Benutzer dann mit einem externen LDAP-Benutzeraccount bei einer verwalteten Einheit anmeldet, weiß das Verwaltungsmodul, ob dem Benutzer Supervisor- oder Bediener-Berechtigungen gewährt werden sollen.

Anmerkungen:

- Sie müssen außerdem Berechtigungen für Verwaltungsmodul v1 für das gesamte Gehäuse festlegen (siehe Berechtigungen für Verwaltungsmodul v1).
- Berechtigungen für Verwaltungsmodul v2 werden für FlexSystem-Switches, für die keine sichere IOM aktiviert ist, nicht unterstützt.
- Stellen Sie für Lenovo ThinkSystem Gehäuse sicher, dass IMM2 der benutzerdefinierten Rolle die „Knotenverwaltung“ gewährt. Wenn Sie möchten, dass die benutzerdefinierte Rolle die Kontrolle über alle Einheiten im Lenovo ThinkSystem Gehäuse hat, stellen Sie sicher, dass IMM2 der benutzerdefinierten Rolle auch den Zugriff auf „Bereich von Knoten X“ gewährt.

Informationen zu den LDAP-Berechtigungsbits für die einzelnen Verwaltungsmodule finden Sie in der Onlinedokumentation.
- LDAP konfigurieren in der CMM- und CMM2-Onlinedokumentation
- LDAP konfigurieren in der IMM- und IMM2-Onlinedokumentation
- LDAP konfigurieren in der XCC-Onlinedokumentation

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
mm-blade-1-scope-v2	Bereich von Knoten 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Bereich von Knoten 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Bereich von Knoten 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Bereich von Knoten 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Bereich von Knoten 5	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Bereich von Knoten 6	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
mm-blade-7-scope-v2	Bereich von Knoten 7	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-8-scope-v2	Bereich von Knoten 8	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Bereich von Knoten 9	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	Bereich von Knoten 10	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Bereich von Knoten 11	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Bereich von Knoten 12	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	Bereich von Knoten 13	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Bereich von Knoten 14	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Knotenverwaltung	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Knotenkonfiguration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Bladebediener	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Fernpräsenz für Knoten	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	Gehäuseverwaltung	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Gehäusekonfiguration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	Account-Management für Gehäuseprotokolle	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Gehäusebediener	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Gehäusebereich	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	Benutzerverwaltung	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Nicht zulassen	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	Bereich von E/A-Modul 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
mm-io-module-2-scope-v2	Bereich von E/A-Modul 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-3-scope-v2	Bereich von E/A-Modul 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	Bereich von E/A-Modul 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	Switch-Verwaltung	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Switch-Konfiguration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-operator-v2	Switch-Bediener	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Supervisorzugriff	lxc-admin, lxc-hw-admin, lxc-supervisor

Berechtigungen für Verwaltungsserver

Diese Berechtigungen werden für Verwaltungsserveraktualisierungen benötigt.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-mgmtserverupdates-delete-updates	Verwaltungsserveraktualisierungen löschen	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Verwaltungsserveraktualisierungen herunterladen und importieren und Verwaltungsserverkatalog aktualisieren	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Verwaltungsserveraktualisierungen ausführen	lxc-admin, lxc-fw-admin, lxc-supervisor

Berechtigungen für die Netzwerkverwaltung

Diese Berechtigungen werden für die Konfiguration von Netzwerkeinstellungen verwendet.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-network-edit	Netzwerkzugriff ändern	lxc-admin, lxc-supervisor

Berechtigungen für BS-Implementierung

Diese Berechtigungen werden für die Verwaltung und Implementierung von Betriebssystemen benötigt.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-osdeploy-create-edit-remote-file-server	Eintrag für Remote-Dateiserver erstellen und bearbeiten	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	BS-Images und angepasste Dateien erstellen, importieren, exportieren und bearbeiten	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	BS-Images und angepasste Dateien löschen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-osdeploy-delete-remote-file-server	Eintrag für Remote-Dateiserver löschen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-global-settings	Informationen im Dialogfenster „Globale Einstellungen“ bearbeiten **Anmerkung:** Die Änderung der globalen IP-Zuweisungseinstellungen wirkt sich auf die Netzwerkeinstellungen aus. Daher müssen Sie auch über die Berechtigungen **lxc-osdeploy-edit-settings-and-deploy-os-images** verfügen, um Änderungen an den globalen IP-Zuordnungseinstellungen vornehmen zu können.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Implementierungseinstellungen ändern und BS-Images auf mindestens einem oder mehreren Servern implementieren	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Berechtigungen für BS-Treiberaktualisierungen

Diese Berechtigungen werden benötigt, um Aktualisierungen für BS-Einheitentreiber zu verwalten und zu übernehmen.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-osDriverUpdates-apply-assign-uxsp	UXSP der BS-Einheitentreiber den Einheiten zuweisen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	BS-Authentifizierung prüfen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Konformität der BS-Einheitentreiber prüfen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Aktualisierungen für BS-Einheitentreiber ausführen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Aktualisierungspakete für BS-Einheitentreiber löschen	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Aktualisierungspakete für BS-Einheitentreiber herunterladen und importieren und UXSP-Katalog für BS-Einheitentreiber aktualisieren	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Benutzer- und Gruppenberechtigungen

Diese Berechtigungen ermöglichen das Verwalten von Benutzeraccounts und Gruppen.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-sec-apply-saml-settings	SAML-Einstellungen anwenden	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Rollengruppe löschen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	Rolle löschen	lxc-recovery, lxc-security-admin, lxc-supervisor

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-sec-delete-users	Benutzer löschen	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	Sicherheitseinstellungen für Account ändern	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	LDAP-Einstellungen anwenden	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Rollengruppe ändern	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Rolle ändern	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Benutzer ändern	lxc-recovery, lxc-security-admin, lxc-supervisor

Berechtigungen für Serverkonfiguration

Diese Berechtigungen werden für die Bereitstellung oder Vorabbereitstellung von Servern mithilfe von Konfigurationsmustern verwendet.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-cp-edit-management-ip	Management-IP-Adressen für Gehäuse ändern	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Einstellungen für Konfigurationsmuster festlegen	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Adressenpools verwalten	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Muster verwalten	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Platzhalter verwalten	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Muster implementieren, Platzhalter für Gehäuse implementieren und Profile verwalten	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Lokalen Speicher zurücksetzen und Intel Optane DCPMM-Sicherheitsvorgang anwenden	lxc-admin, lxc-hw-admin, lxc-supervisor

Service-Berechtigungen

Diese Berechtigungen werden benötigt, um Supportkontakte für jede verwaltete Einheit zu definieren, Servicedateien zu sammeln und an die Lenovo Unterstützung zu senden, automatische Benachrichtigungen der Service-Provider für bestimmte wartungsfähige Ereignissen bei bestimmten Einheiten einzurichten, den Service-Ticketstatus und Garantieinformationen anzuzeigen sowie Servicedaten zu erfassen und weiterzuleiten.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-ss-alter-backup-credentials	FFDC-Anmeldeinformationen für Sicherung ändern	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Call Home ausführen	lxc-admin, lxc-hw-admin, lxc-supervisor

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-ss-change-service-recovery-password	Kennwort zur Service-Wiederherstellung ändern	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Service-Tickets ändern	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	Service-Tickets löschen	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Service-Weiterleiter ausführen	lxc-admin, lxc-hw-admin, lxc-supervisor

Berechtigungen für Switch-Konfiguration

Diese Berechtigungen werden zum Konfigurieren von Switches sowie zum Sichern und Wiederherstellen der Switch-Konfigurationsdaten benötigt.

Name der Berechtigung	Beschreibung der Berechtigung	Standardrollen
lxc-netcfg-template-management	Switch-Konfigurationsvorlagen erstellen, ändern, löschen und implementieren sowie Switch-Konfigurationsimplementierungen löschen	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Switch-Konfigurationsdatendateien sichern, wiederherstellen, löschen, exportieren und importieren	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Switch-Portstatus ändern	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Angepasste Rollengruppe erstellen

Eine *Rollengruppe* ist ein Satz von Rollen und ein Satz von Benutzern, die Mitglieder desselben Rollensatzes sind. Die für jeden Benutzer der Rollengruppe gewährte Zugriffsebene basiert auf den Rollen, die dieser Rollengruppe zugeordnet sind. XClarity Administrator enthält die folgenden vordefinierten Rollengruppen, die den vordefinierten Rollen entsprechen. Sie können auch angepasste Rollengruppen erstellen.

Zu dieser Aufgabe

Jeder XClarity Administrator-Benutzer muss in mindestens einer Rollengruppe Mitglied sein.

Die folgenden Rollengruppen sind in XClarity Administrator vordefiniert.

- **LXC-SUPERVISOR**. Enthält die Rolle **lxc-supervisor**.
- **LXC-ADMIN**. Enthält die Rolle **lxca-admin**.
- **LXC-SECURITY-ADMIN**. Enthält die Rolle **lxc-security-admin**.
- **LXC-HW-ADMIN**. Enthält die Rolle **lxc-hw-admin**.
- **LXC-FW-ADMIN**. Enthält die Rolle **lxc-fw-admin**.
- **LXC-OS-ADMIN**. Enthält die Rolle **lxc-os-admin**.
- **LXC-SERVICE-ADMIN**. Enthält die Rolle **lxc-service-admin**.
- **LXC-HW-MANAGER**. Enthält die Rolle **lxc-hw-manager**.
- **LXC-OPERATOR**. Enthält die Rolle **lxc-operator**.
- **LXC-RECOVERY**. Enthält die Rolle **lxc-recovery**.

Die folgenden vordefinierten Rollen sind *reserviert* und können nicht verwendet werden, um neue Rollengruppen zu erstellen oder diese den neuen Benutzer zuzuweisen.

- **lxc-sysrdr**
- **lxc-sysmgr**

Vorgehensweise

So erstellen Sie eine Rollengruppe:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Rollengruppen**, um die Gruppen-Verwaltungsseite anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ), um eine Rollengruppe zu erstellen. Der Dialog Neue Rollengruppe erstellen wird angezeigt.

Schritt 4. Geben Sie einen Gruppennamen und eine Beschreibung ein.

Anmerkung: Tipp: Für den Gruppennamen können Sie Buchstaben, Zahlen, Leerzeichen, Unterstriche, Bindestriche und Punkte verwenden.

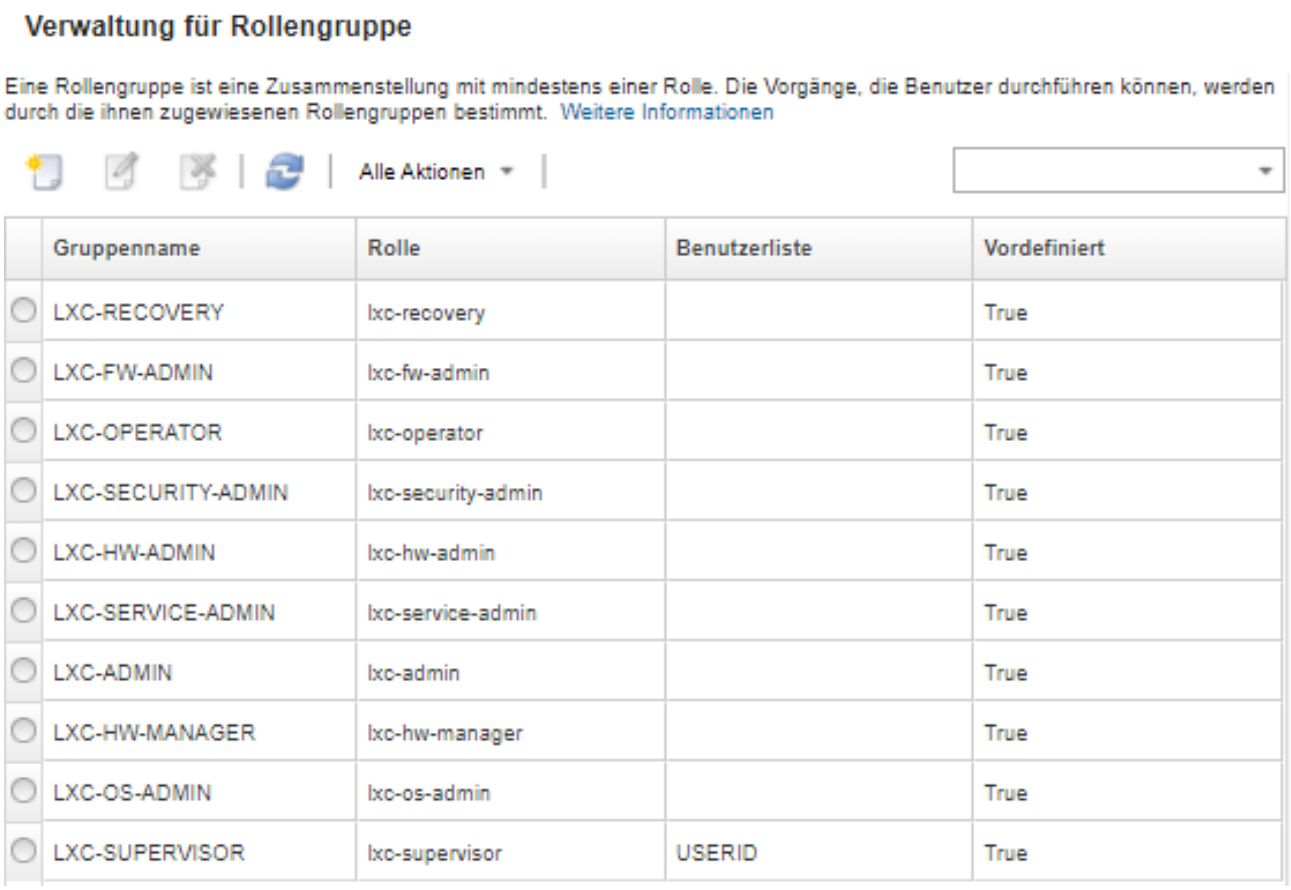
Schritt 5. Wählen Sie eine oder mehrere Rollen aus, die Sie dieser Rollengruppe zuweisen.

Schritt 6. Wählen Sie mindestens einen Benutzer als Mitglied dieser Rollengruppe aus.

Schritt 7. Klicken Sie auf **Erstellen**. Die Rollengruppe wird zur Tabelle auf der Seite „Gruppenverwaltung“ hinzugefügt.

Ergebnisse

Die Rollengruppe wird in der Tabelle „Rollengruppen“ angezeigt. Die Tabelle zeigt die zugeordneten Autorisierungsrollen und die Mitglieder jede Rollengruppe an.



Nachdem Sie eine Rollengruppe erstell haben, können Sie die folgenden Aktionen für eine ausgewählte Rollengruppe ausführen:

- Sie können Rollen zu dieser Rollengruppe hinzufügen oder daraus entfernen, indem Sie auf das Symbol **Bearbeiten** klicken ( ).
- Hinzufügen oder Entfernen von Benutzern als Mitglieder der Rollengruppe (siehe „Hinzufügen und Entfernen mehrerer Benutzer bei einer Rollengruppe“ auf Seite 59).
- Exportieren von Informationen zu Rollengruppen einschließlich Rollengruppen-Zugriffsberechtigungen über **Alle Aktionen → Als CSV exportieren**.
- Löschen Sie die Rollengruppe über das Symbol **Löschen** ( ).Vordefinierte Rollengruppen können nicht gelöscht werden.

Nachdem eine Rollengruppe erstellt, bearbeitet oder gelöscht wurde, wird die entsprechende Änderung sofort für jede verwaltete Einheit bereitgestellt.

Hinzufügen und Entfernen mehrerer Benutzer bei einer Rollengruppe

Sie können die Mitgliedschaft in einer Rollengruppe ändern, indem Sie mehrere Benutzer hinzufügen oder entfernen.

Vorgehensweise

Gehen Sie wie folgt vor, um Benutzer aus einer Rollengruppe zu entfernen:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Rollengruppen**, um die Gruppen-Verwaltungsseite anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Bearbeiten** (), um die Rollengruppe zu bearbeiten. Das Dialogfenster Rollengruppe bearbeiten wird angezeigt.

Schritt 4. Klicken Sie auf die Dropdown-Liste **Benutzerliste** und wählen Sie die Benutzer aus, die entfernt werden sollen (oder heben Sie die Auswahl für die Benutzer auf, die nicht entfernt werden sollen).

Schritt 5. Klicken Sie auf **Speichern**. Die Spalte **Benutzerliste** zeigt die aktuelle Benutzermitgliedschaft in der Rollengruppe an.

Zugriff auf Einheiten verwalten

Die Zugriffssteuerung auf Einheiten ist standardmäßig deaktiviert und wird erst wirksam, wenn Sie sie aktivieren.

Wenn Einheiten zunächst von Lenovo XClarity Administrator verwaltet werden, hat ein vordefinierter Satz von Rollengruppen standardmäßig die Zugriffsberechtigung für die Einheiten. Dieser vordefinierte Satz ist standardmäßig leer, bis er konfiguriert wird.

Sie können die Rollengruppen ändern, die auf bestimmte verwaltete Einheiten zugreifen können. Wenn bestimmten Rollengruppen eine Berechtigung erteilt wird, können nur diejenigen Benutzer diese bestimmten Einheiten sehen und verwenden, die Mitglieder dieser Rollengruppen sind.

Zugriff auf bestimmte Einheiten steuern

Wenn Einheiten zunächst von Lenovo XClarity Administrator verwaltet werden, hat ein vordefinierter Satz von Rollengruppen standardmäßig die Zugriffsberechtigung für die Einheiten. Sie können die Rollengruppen ändern, die auf bestimmte verwaltete Einheiten zugreifen können. Wenn bestimmten Rollengruppen eine Berechtigung erteilt wird, können nur diejenigen Benutzer diese bestimmten Einheiten sehen und verwenden, die Mitglieder dieser Rollengruppen sind.

Vorbereitende Schritte

Nur Benutzer mit der Berechtigung **lxc-supervisor**, **lxc-security-admin** oder **lxc-recovery** können diese Aktion ausführen.

Zu dieser Aufgabe

Die Zugriffssteuerung wird auf einzelnen Einheiten festgelegt. Sie wird nicht für Container festgelegt, wie z. B. Racks und Ressourcengruppen.

Für Komponenten in einem Gehäuse müssen Benutzer mindestens Lesezugriff für das Gehäuse haben, um die Komponenten in diesem Gehäuse anzeigen zu können. Wenn Benutzer nicht mindestens Lesezugriff für das Gehäuse haben, können sie die Gehäusekomponenten möglicherweise in einigen, jedoch nicht allen Ansichten sehen.

Unabhängig davon, ob sie in einer Rollengruppe sind, der explizit Zugriff auf diese Ressource gewährt wurde, können Benutzer mit der Berechtigung **lxc-supervisor** alle Ressourcen sehen und verwenden. Bei der Rollengruppe **lxc-supervisor** ist es nicht möglich, den Zugriff auf Ressourcen zu entfernen.

Wenn ein Benutzer nicht Mitglied einer Rollengruppe ist, die Zugriff auf eine bestimmte verwaltete Einheit hat, kann der Benutzer diese bestimmte Einheit nicht sehen oder verwenden. Dazu zählt das Starten der Management-Controller-Webschnittstelle über Lenovo XClarity Administrator. Bei Flex- und System x-Einheiten können Benutzer sich nicht direkt an einem CMM oder Management-Controller anmelden, auf den sie keinen Zugriff haben.

Die Standard-Zugriffssteuerungseinstellungen werden verwendet, um Zugriffsberechtigungen auf Einheiten festzulegen, wenn sie zunächst von XClarity Administrator verwaltet werden und die Zugriffsberechtigungen

für eine bestimmte Einheit auf die Standardeinstellungen zurückgesetzt werden. Das Ändern der Standard-Zugriffssteuerungseinstellungen ändert nicht automatisch die Zugriffsberechtigungen auf Einheiten, die bereits verwaltet werden.

Wichtig:

- Wenn ein Benutzer Mitglied von mehr als einer Rollengruppe ist und die Rollengruppen verschiedenen Einheiten zugeordnet sind, können sich die Aktionen unterscheiden, die der Benutzer auf den jeweiligen Einheiten ausführen darf. Wenn der Benutzer z. B. Mitglied der Standardrollengruppen „LXC-FW-ADMIN“ und „LXC-OS-ADMIN“ ist und der Rollengruppe „LXC-FW-ADMIN“ Zugriff auf Server A gewährt wurde, der Rollengruppe „LXC-OS-ADMIN“ jedoch nicht, könnte dieser Benutzer die Firmware auf Server A aktualisieren, aber kein Betriebssystem auf Server A implementieren. Wenn der Rollengruppe „LXC-OS-ADMIN“ Zugriff auf Server B gewährt wurde, der Rollengruppe „LXC-FW-ADMIN“ jedoch nicht, könnte derselbe Benutzer auf Server B ein Betriebssystem implementieren, aber keine Firmware auf Server B aktualisieren.
- Wenn Sie den Zugriff auf eine Einheit beschränken, die eine übergeordnete Ressource aufweist (z. B. einen Server oder Switch in einem Flex-Gehäuse), muss ein Benutzer mindestens Leseberechtigungen für die übergeordnete Ressource haben, um vollständig mit der Einheit interagieren zu können. Falls der Benutzer mindestens Lesezugriff auf die Einheit, aber nicht auf das übergeordnete Element hat, kann er keine Ansichten für den Einheitenbestand anzeigen, aber Informationen zur Einheit (wie Jobs und Ereignisse) in anderen Ansichten finden.

  Beispielsweise können Sie für das übergeordnete Element eine Rollengruppe erstellen und dieser die Rolle **lxc-operator** zuweisen. Nehmen Sie alle Benutzer, die Zugriff auf die untergeordneten Elemente (z. B. einen Server oder Switch in einem Flex-Gehäuse) haben sollen, in diese Rollengruppe auf. Binden Sie anschließend diese Rollengruppe als eine der Gruppen, die Zugriff auf das übergeordnete Element haben, ein.

Vorgehensweise

Gehen Sie wie folgt vor, um den Zugriff auf bestimmte Einheiten zu steuern, indem Sie diesen Einheiten Rollengruppen zuordnen.

Schritt 1. Klicken Sie im Hauptmenü von Lenovo XClarity Administrator auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im linken Navigationsfenster auf **Ressourcenanzeige**. Die Seite „Ressourcenanzeige“ wird angezeigt.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Einheiten zu erleichtern. Darüber hinaus können Sie einen Einheitentyp im Dropdown-Menü **Ressourcentyp** auswählen, eine Rollengruppe im Dropdown-Menü **Rollengruppen** auswählen, eine Ressourcengruppe im Dropdown-Menü **Ressourcengruppen** auswählen und Text im Feld **Filter** eingeben (z. B. einen Ressourcennamen oder -typ), um nur die Einheiten anzuzeigen, die die ausgewählten Kriterien erfüllen.

Schritt 3. Wählen Sie mindestens eine Einheit aus, für die der Zugriff gesteuert werden soll.

Schritt 4. Klicken Sie auf das Symbol **Bearbeiten** (). Das Dialogfenster „Ressource bearbeiten“ wird mit den Zieleinheiten angezeigt, die im Feld **Ressourcenname** aufgeführt sind.

Schritt 5. Wählen Sie in der Dropdown-Liste **Rollengruppen** die Rollengruppen aus, denen Sie den Zugriff auf die Zieleinheiten erteilen möchten.

Anmerkung: Wenn die Einheit eine übergeordnete Ressource aufweist (z. B. einen Server oder Switch in einem Flex-Gehäuse), können Sie den Zugriff für die Einheit (rechten Spalte) und die übergeordnete Ressource (linke Spalte) angeben.

Schritt 6. Legen Sie **Öffentlicher Zugriff** auf `No` fest. Dies bedeutet, dass nur Benutzer auf die Zieleinheiten zugreifen können, die Mitglieder der ausgewählten Rollengruppen sind.

Schritt 7. Klicken Sie auf **Speichern**.

Schritt 8. Klicken Sie nach dem Zuweisen der Berechtigungen auf die Umschalt-Schaltfläche **Deaktiviert**, um die **Ressourcenzugriffssteuerung** zu aktivieren.

Sie können die Ressourcenzugriffssteuerung jederzeit aktivieren – sowohl bevor als auch nachdem Sie den Zugriff auf bestimmte Einheiten konfiguriert haben. Wenn diese Einstellung aktiviert ist, ist die in der Tabelle angezeigte Konfiguration wirksam. Dazu zählt auch die Zugriffsverweigerung für Benutzer ohne supervisor-Berechtigung für alle Einheiten, denen keine Gruppen mit Zugriffsberechtigung zugeordnet sind.

Nach dieser Aufgabe

Sie können den Zugriff auf Einheiten auch mit den folgenden Aktionen steuern:

- Ändern Sie die Berechtigungen zu den Standardrollengruppen und der Standardeinstellung für den öffentlichen Zugriff, indem Sie auf das Symbol **Bearbeiten** ( ) und anschließend auf **Auf Standardwerte zurücksetzen** klicken.
- Ändern Sie die Standardrollengruppe und Standardeinstellung für den öffentlichen Zugriff (siehe Standardberechtigungen ändern).
- Deaktivieren Sie die Ressourcenzugriffssteuerung, indem Sie auf die Umschalt-Schaltfläche **Aktiviert** klicken und so die **Ressourcenzugriffssteuerung** deaktivieren. Anschließend haben alle Rollengruppen Zugriff auf alle verwalteten Einheiten.

Ressourcenzugriffssteuerung deaktivieren

Sie können die Zugriffssteuerung für alle Einheiten oder bestimmte Einheiten deaktivieren, sodass alle Benutzer diese Einheiten sehen und verwenden können.

Zu dieser Aufgabe

Nur Benutzer mit der Berechtigung **lxc-supervisor**, **lxc-security-admin** oder **lxc-recovery** können diese Aktion ausführen.

Vorgehensweise

Gehen Sie wie folgt vor, um die Ressourcenzugriffssteuerung zu deaktivieren.

- Für alle verwalteten Einheiten
  1. Klicken Sie im Hauptmenü von Lenovo XClarity Administrator auf **Verwaltung → Sicherheit**.
  2. Klicken Sie im linken Navigationsfenster auf **Ressourcenanzeige**. Die Seite „Ressourcenanzeige“ wird angezeigt.
  3. Klicken Sie auf die Umschalt-Schaltfläche **Aktiviert**, um die **Ressourcenzugriffssteuerung** zu deaktivieren.
- Für bestimmte verwaltete Einheiten
  1. Klicken Sie im Hauptmenü von XClarity Administrator auf **Verwaltung → Sicherheit**.
  2. Klicken Sie im linken Navigationsfenster auf **Ressourcenanzeige**. Die Seite „Ressourcenanzeige“ wird angezeigt.

     Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Einheiten zu erleichtern. Darüber hinaus können Sie einen Einheitentyp im Dropdown-Menü **Ressourcentyp** auswählen, eine Rollengruppe im Dropdown-Menü **Rollengruppen** auswählen, eine Ressourcengruppe im Dropdown-Menü **Ressourcengruppen** auswählen und Text im Feld **Filter** eingeben (z. B. einen

Ressourcennamen oder -typ), um nur die Einheiten anzuzeigen, die die ausgewählten Kriterien erfüllen.

3. Wählen Sie mindestens eine Einheit aus, für die der Zugriff geändert werden soll.
4. Klicken Sie auf das Symbol **Bearbeiten** (). Das Dialogfenster „Ressource bearbeiten“ wird mit den ausgewählten Einheiten angezeigt, die im Feld **Ressourcenname** aufgeführt sind.
5. Legen Sie **Öffentlicher Zugriff** auf `Yes` fest. Dies bedeutet, dass alle Rollengruppen auf die Zieleinheiten zugreifen können, unabhängig von den Rollengruppen, die in der Dropdown-Liste **Rollengruppen** aufgeführt sind.
6. Klicken Sie auf **Speichern**.

Standardberechtigungen ändern

Es gibt zwei Einstellungen, die bestimmen, ob Rollengruppen auf Einheiten zugreifen können, wenn sie zunächst von Lenovo XClarity Administrator verwaltet werden: „Öffentlicher Zugriff“ und „Rollengruppen“. Die Einstellung für den öffentlichen Zugriff bestimmt, ob alle oder nur bestimmte Rollengruppen auf die Zieleinheiten zugreifen können. Diese Einstellung ist standardmäßig auf `Yes` festgelegt, was bedeutet, dass alle Rollengruppen auf die Zieleinheiten zugreifen können. Sie können das Standardverhalten ändern, indem Sie die Einstellung für den öffentlichen Zugriff zu `No` ändern und anschließend Rollengruppen auswählen, die auf die Zieleinheiten zugreifen können sollen.

Zu dieser Aufgabe

Nur Benutzer mit der Berechtigung **lxc-supervisor**, **lxc-security-admin** oder **lxc-recovery** können diese Aktion ausführen.

Benutzer mit Berechtigungen **lxc-supervisor**, **lxc-security-admin** oder **lxc-recovery** können auf alle verwalteten Einheiten zugreifen. Bei diesen Rollengruppen ist es nicht möglich, den Zugriff auf Einheiten zu entfernen.

Die Standard-Zugriffssteuerungseinstellungen werden verwendet, um Zugriffsberechtigungen auf Einheiten festzulegen, wenn sie zunächst von XClarity Administrator verwaltet werden und die Zugriffsberechtigungen für eine bestimmte Einheit auf die Standardeinstellungen zurückgesetzt werden. Das Ändern der Standard-Zugriffssteuerungseinstellungen ändert nicht automatisch die Zugriffsberechtigungen auf Einheiten, die bereits verwaltet werden.

Vorgehensweise

Führen Sie zum Ändern der Standardzugriffssteuerungen die folgenden Schritte aus.

Schritt 1. Klicken Sie im Hauptmenü von XClarity Administrator auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im linken Navigationsfenster auf **Ressourcenanzeige**. Die Seite „Ressourcenanzeige“ wird angezeigt.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Einheiten zu erleichtern. Darüber hinaus können Sie einen Einheitentyp im Dropdown-Menü **Ressourcentyp** auswählen, eine Rollengruppe im Dropdown-Menü **Rollengruppen** auswählen, eine Ressourcengruppe im Dropdown-Menü **Ressourcengruppen** auswählen und Text im Feld **Filter** eingeben (z. B. einen Ressourcennamen oder -typ), um nur die Einheiten anzuzeigen, die die ausgewählten Kriterien erfüllen.

Schritt 3. Klicken Sie auf **Alle Aktionen → Standardressourcen bearbeiten**. Das Dialogfenster „Standardressourcen bearbeiten“ wird angezeigt.

Schritt 4. Wählen Sie in der Dropdown-Liste **Rollengruppen** die Rollengruppen aus, die Sie als Standardgruppe festlegen möchten.

Schritt 5. Wählen Sie die Standardeinstellung **Öffentlicher Zugriff** aus.

- **Ja**. Wenn eine Einheit zum ersten Mal verwaltet wird, können alle Rollengruppen auf die Einheit zugreifen, unabhängig von den Rollengruppen, die in der Dropdown-Liste **Rollengruppen** aufgeführt sind.
- **Nein**. Wenn eine Einheit zum ersten Mal verwaltet wird, können standardmäßig nur Rollengruppen auf die Einheit zugreifen, die in der Dropdown-Liste **Rollengruppen** aufgeführt sind.

Schritt 6. Klicken Sie auf **Speichern**.

Eine sichere Umgebung implementieren

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

Zu dieser Aufgabe

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

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

- Die physische Sicherheit Ihrer Umgebung ist wichtig, daher sollten Sie den Zugang zu den Räumlichkeiten und Racks, die Hardware für die Systemverwaltung enthalten, beschränken.
- Schützen Sie Ihre Netzwerkhardware und -daten mithilfe einer softwarebasierten Firewall vor bekannten und neuen Sicherheitsbedrohungen wie Viren und unbefugten Zugriffe.
- Ändern Sie nicht die Standardsicherheitseinstellungen für Netzwerkswitches und Pass-through-Module. Mit den werkseitigen Standardeinstellungen für diese Komponenten wird die Verwendung nicht sicherer Protokolle deaktiviert und die Verwendung signierter Firmwareaktualisierungen erzwungen.
- Die Verwaltungsanwendungen für die CMMS, Baseboard-Management-Controlle, FSPs und Switches lassen nur signierte Firmwareaktualisierungspakete für diese Komponenten zu. So ist sichergestellt, dass nur vertrauenswürdiger Code installiert wird.
- Die Berechtigung zum Aktualisieren von Firmwarekomponenten sollte Benutzern vorbehalten sein, die dazu berechtigt sind.
- Sorgen Sie dafür, dass zumindest kritische Firmwareaktualisierungen installiert werden. Nach jeder Änderung sollte eine Sicherungskopie der Konfiguration erstellt werden.
- Stellen Sie sicher, dass alle sicherheitsspezifischen Updates für DNS-Server unverzüglich installiert werden und der Schutz dieser Server immer aktuell ist.
- Weisen Sie Ihre Benutzer an, keine Zertifikate zu akzeptieren, die nicht vertrauenswürdig sind. Siehe Mit Sicherheitszertifikaten arbeiten für weitere Informationen.
- Für die Flex System-Hardware sind Optionen für den Manipulationsnachweis verfügbar. Installieren Sie für Hardware in nicht verschlossenen Racks oder in frei zugänglichen Bereichen die Optionen für den Manipulationsnachweis, um unbefugte Zugriffe abwehren und feststellen zu können. Weitere Informationen zu Optionen für den Manipulationsnachweis finden Sie in der Dokumentation für die Flex System-Produkte.
- Bringen Sie die Hardware für die Systemverwaltung nach Möglichkeit in einem eigenen Teilnetz unter. In der Regel sollten keine Benutzer, sondern nur Administratoren Zugang zu dieser Hardware haben.

- Verwenden Sie keine Kennwörter, die leicht zu erraten sind, wie beispielsweise „Kennwort“ oder den Namen Ihres Unternehmens. Bewahren Sie die Kennwörter an einem sicheren Ort auf und schränken Sie den Zugriff auf die Kennwörter ein. Führen Sie eine Kennwortrichtlinie für Ihr Unternehmen ein.

  Wichtig: Der Standardbenutzername und das Standardkennwort sollten auf jeden Fall geändert werden. Für alle Benutzer sollten strikte Kennwortrichtlinien gelten.
- Richten Sie für Benutzer Startkennwörter ein. Auf diese Weise können Sie den Zugriff auf die Daten und Konfigurationsprogramme der Server steuern. Weitere Informationen zu Startkennwörtern finden Sie in der Dokumentation der Server.
- Setzen Sie die verschiedenen Berechtigungsstufen ein, die für die verschiedenen Benutzer in Ihrer Umgebung vorhanden sind. Es dürfen nicht alle Benutzer dieselbe Supervisor-Benutzer-ID verwenden.
- Stellen Sie sicher, dass Ihre Umgebung die folgenden NIST 800-131A-Kriterien für eine sichere Kommunikation erfüllt:
  - Verwendung von Secure Sockets Layer (SSL) über das Protokoll TLS v1.2
  - Verwendung der Hashfunktion SHA-256 oder besser für digitale Signaturen und der Hashfunktion SHA-1 oder besser für andere Anwendungen
  - Verwenden Sie RSA-2048 oder besser bzw. von durch NIST genehmigte elliptische Kurven mit mindestens 224 Bit.
  - Verwenden Sie die von NIST genehmigte symmetrische Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit.
  - Verwenden Sie die von NIST genehmigten Zufallszahlengeneratoren.
  - Bieten Sie Unterstützung für Diffie-Hellman- und/oder Elliptic Curve Diffie-Hellman-Schlüsselaustauschmechanismen (soweit möglich).

  Weitere Informationen zu den Verschlüsselungseinstellungen finden Sie unter Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren. Weitere Informationen zu NIST-Einstellungen finden Sie unter NIST SP 800-131A-Konformität implementieren.

Die Sicherheitseinstellungen eines Benutzeraccounts ändern

Die Benutzeraccount-Sicherheitseinstellungen steuern die Komplexität von Kennwörtern, die Sperrung von Accounts und das Web-Sitzungszeitlimit bei Deaktivität. Sie können die Werte für die Einstellungen ändern.

Vorgehensweise

So überschreiben Sie die aktuellen Benutzeraccount-Sicherheitseinstellungen:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Accountsicherheitseinstellungen**, um die Seite „Benutzerverwaltung“ anzuzeigen.

Schritt 3. Wählen Sie für jede zu ändernde Einstellung einen neuen Wert aus.

Tabelle 1. Sicherheitseinstellungen für Account

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standard-werte
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. **Anmerkung:** Diese Einstellung gilt nur, wenn die Benutzeraccounts über den lokalen Authentifizierungsserver verwaltet werden. Sie werden nicht verwendet, wenn ein externer Authentifizierungsserver verwendet wird.	**0 – 365**	**90**
Warndauer vor Kennwortablauf	Zeitraum (in Tagen) vor Ablauf des Kennworts, ab dem Nutzer Warnungen über den bevorstehenden Ablauf des Benutzerkennworts erhalten Beträgt dieser Wert **0**, werden Benutzer nicht gewarnt. **Anmerkung:** Diese Einstellung gilt nur, wenn die Benutzeraccounts über den lokalen Authentifizierungsserver verwaltet werden. Sie werden nicht verwendet, wenn ein externer Authentifizierungsserver verwendet wird.	**0 –** *Maximal-einstellung für Kennwort-ablauf*	**5**
Mindestwiederverwen-dungszyklus des Kennworts	Mindestanzahl der Male, bei denen ein Benutzer bei der Änderung des Passworts ein einzigartiges Passwort eingeben muss, bevor ein Passwort erneut verwendet werden kann. Wird dieser Wert auf **0** festgelegt, können die Benutzer die Kennwörter umgehend wiederverwenden.	**0 – 10**	**5**
Mindestintervall für Kennwortänderung	Mindestzeitspanne (in Stunden), die vergehen muss, bevor ein Benutzer ein Kennwort erneut ändern kann. Der festgelegte Wert für diese Einstellung darf den Wert der Kennwortablaufdauer nicht überschreiten. Wird dieser Wert auf **0** festgelegt, können die Benutzer die Kennwörter umgehend ändern.	**0 – 1440**	**24**
Maximale Anzahl an Anmeldefehlern	Maximale Anzahl fehlgeschlagener Anmeldeversuche, bevor der Benutzeraccount gesperrt wird. Der festgelegte Wert für den Sperrzeitraum nach der maximalen Anzahl von fehlgeschlagenen Anmeldeversuchen bestimmt, wie lange ein Benutzeraccount gesperrt bleibt. Gesperrte Konten können nicht genutzt werden, um auf das System zuzugreifen, auch, wenn ein gültiges Passwort eingegeben wird. Beträgt dieser Wert **0**, werden Konten niemals gesperrt. Der Zähler für fehlgeschlagene Anmeldeversuche wird nach einem erfolgreichen Anmeldeversuch zurückgesetzt.	**0 – 100**	**20**

Tabelle 1. Sicherheitseinstellungen für Account (Forts.)

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standard-werte
Sperrzeitraum nach maximaler Anzahl von fehlgeschlagenen Anmeldeversuchen	Mindestdauer in Minuten, die vergehen muss, bevor sich ein gesperrter Benutzer erneut anmelden kann Beträgt der Wert **0** bleibt das Konto gesperrt, bis es von einem Administrator entsperrt wird. Beträgt der Wert 0, ist Ihr System möglicherweise gegenüber schwerwiegenden Denial of Service-Angriffen verwundbar, mit denen durch absichtlich fehlerhafte Anmeldeversuche eine permanente Sperrung von Accounts herbeigeführt werden kann. **Tipp:** Jeder Benutzer mit der Rolle Supervisor kann einen Benutzeraccount entsperren. Siehe Einen Benutzer freigeben für weitere Informationen. **Anmerkung:** Diese Einstellung gilt nur, wenn die Benutzeraccounts über den lokalen Authentifizierungsserver verwaltet werden. Sie werden nicht verwendet, wenn ein externer Authentifizierungsserver verwendet wird.	**0 – 2880**	**60**
Sitzungszeitlimit bei Webinaktivität	Zeitraum in Minuten, über den eine Benutzersitzung mit dem XClarity Administrator inaktiv sein kann, bevor der Benutzer abgemeldet wird. Beträgt dieser Wert **0**, laufen Benutzersitzungen nie ab. **Anmerkung:** Wenn Sie diesen Wert ändern, sind nur Benutzersitzungen betroffen, die nach Änderung der Einstellung gestartet wurden.	**0 – 1440**	**1440**
Mindestlänge des Kennworts	Mindestanzahl von Zeichen, die für ein gültiges Passwort verwendet werden können.	**8 – 20**	**8**

Tabelle 1. Sicherheitseinstellungen für Account (Forts.)

Sicherheitseinstellung	Beschreibung	Zulässige Werte	Standard-werte
Anzahl der Komplexitätsregeln, die bei der Erstellung eines neuen Kennworts befolgt werden müssen	Anzahl der Komplexitätsregeln, die bei der Erstellung eines neuen Kennworts befolgt werden müssen 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. XClarity Administrator unterstützt die folgenden Komplexitätsregeln für Kennwörter. • (1) Es muss mindestens ein Buchstabe und es dürfen nicht mehr als zwei aufeinanderfolgende Zeichen enthalten sein, einschließlich Abfolgen von Buchstaben, Ziffern und Tasten auf der QWERTZ-Tastatur (z. B. sind „abc“, „123“ und „asd“ nicht zulässig). • (2) Es muss mindestens eine Zahl (0–9) enthalten sein. • (3) Sie müssen mindestens *zwei* der folgenden Zeichen enthalten: – Großbuchstaben (A – Z) – Kleinbuchstaben (a – z) – Sonderzeichen ; @ _ ! ' $ & + • (4) Es darf keine Wiederholung oder Umkehrung des Benutzernamens sein. • (5) Es dürfen nicht mehr als zwei identische Zeichen hintereinander enthalten sein (z. B. sind „aaa“, „111“ und „...“ nicht zulässig). Wenn der Wert auf **0** festgelegt ist, müssen die Kennwörter keine der Komplexitätsregeln einhalten.	**0 – 5**	**4**
Maximale Anzahl aktiver Sitzungen für einen bestimmten Benutzer	Maximale Anzahl aktiver Sitzungen für einen bestimmten Benutzer, die zu einem bestimmten Zeitpunkt zulässig sind Ist dieser Wert auf **0** festgelegt, ist die Anzahl zulässiger aktiver Sitzungen für einen bestimmten Benutzer unbegrenzt.	**1 – 20**	**3**
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 Administrator anmeldet.	**Ja** oder **Nein**	**Ja**

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

Nach dieser Aufgabe

Sobald sie gespeichert wurden, sind die neuen Einstellungen wirksam. Wenn Sie die Einstellung für das Sitzungszeitlimit bei Webdeaktivität ändern, betrifft dies auch aktive Sitzungen.

Wenn Sie Kennwortrichtlinien ändern, werden diese Richtlinien beim nächsten Anmelden eines Benutzers oder bei einer Kennwortänderung aktiv.

Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren

Sie können die SSL/TLS-Version und die Verschlüsselungseinstellung für den Verwaltungsserver konfigurieren.

Vorbereitende Schritte

Lesen Sie die Hinweise zur Verschlüsselung, bevor Sie die Einstellungen auf dem Verwaltungsserver ändern (siehe Verschlüsselungsverwaltung in der XClarity Administrator Onlinedokumentation).

Zu dieser Aufgabe

Der *Verschlüsselungsmodus* bestimmt, wie sich die sichere Kommunikation zwischen XClarity Administrator und allen verwalteten Systemen vollzieht. Wenn die sichere Kommunikation implementiert ist, legt der Modus die Länge des Verschlüsselungsschlüssels fest.

Anmerkung: Unabhängig davon, welchen Verschlüsselungsmodus Sie auswählen, werden immer NIST-konforme Zufallszahlengeneratoren verwendet. Für die symmetrische Verschlüsselung kommen nur Schlüssel mit einer Mindestlänge von 128 Bit zum Einsatz.

Informationen zum Ändern der Sicherheitseinstellung für verwaltete Einheiten finden Sie unter Sicherheitseinstellungen für einen verwalteten Server konfigurieren.

Vorgehensweise

Gehen Sie wie folgt vor, um die Verschlüsselungseinstellungen auf dem Verwaltungsserver zu ändern.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.

Schritt 2. Wählen Sie einen der folgenden Verschlüsselungsmodi für eine sichere Kommunikation aus:

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

  Beachten Sie bei Auswahl dieses Modus Folgendes:

  – Für alle Ports außer Port 8443 sind alle TLS-CBC-Codierschlüssel und alle Codierschlüssel deaktiviert, die kein Perfect Forward Secrecy unterstützen.
  – Ereignisbenachrichtigungen werden möglicherweise nicht erfolgreich an einige Mobilgeräteabonnements weitergeleitet (siehe Ereignisse an mobile Einheiten weiterleiten). Externe Services wie Android und iOS legen SHA-1-signierte Zertifikate vor; dieser Algorithmus entspricht nicht den strikten Anforderungen von NIST SP 800-131A. Dementsprechend können bei Verbindungen zu diesen Services Zertifikatsausnahmen oder Handshakefehler auftreten.

  Weitere Informationen über die Konformität mit NIST SP 800-131A finden Sie unter NIST SP 800-131A-Konformität implementieren.

Schritt 3. Wählen Sie die Mindest-TLS-Protokollversion aus, die für Clientverbindungen mit anderen Servern (z. B. dem LDAP-Server) verwendet werden muss. Die folgenden Optionen stehen zur Verfügung.

- **TLS1.2**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.2.
- **TLS1.3**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.3.

Schritt 4. Wählen Sie die Mindest-TLS-Protokollversion aus, die für Serververbindungen (z. B. den Web-Server) verwendet werden muss. Die folgenden Optionen stehen zur Verfügung.

- **TLS1.2**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.2.
- **TLS1.3**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.3.

Schritt 5. Wählen Sie die Mindestversion des TLS-Protokolls für die Betriebssystemimplementierung und Einheitentreiberaktualisierungen von XClarity Administrator. Die folgenden Optionen stehen zur Verfügung.

- **TLS1.2**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.2.
- **TLS1.3**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.3.

Anmerkung: Nur Betriebssysteme mit einem Installationsvorgang, der den ausgewählten Verschlüsselungsalgorithmus oder stärker unterstützt, können über XClarity Administrator implementiert und aktualisiert werden.

Schritt 6. Wählen Sie die Länge des Verschlüsselungsschlüssels und den Hashalgorithmus aus, der für alle Teile des Zertifikats verwendet werden soll, einschließlich CA-Stammzertifikat, Serverzertifikat und CSR für extern signierte Zertifikate.

- **RSA-2048/SHA-256** (Standard)

  Dieser Modus kann verwendet werden, wenn verwaltete Einheiten im Modus „Kompatibilität“, „NIST SP 800-131A“ oder „Standardsicherheit“ sind. Dieser Modus kann *nicht* verwendet werden, wenn sich eine oder mehrere verwaltete Einheiten im Modus **„Enterprise Strikt“-Sicherheit** befinden.

- **RSA-3072/SHA-384**

  Dieser Modus ist erforderlich, wenn verwaltete Einheiten im Modus **„Enterprise Strikt“-Sicherheit** sind.

  Wichtig: Nur Server mit XCC2 unterstützen RSA-3072/SHA-384-Zertifikatsignaturen. Nach der Konfiguration von XClarity Administrator mit einem RSA-3072/SHA-384-basierten Zertifikat wird die Verwaltung aller Nicht-XCC2 Einheiten aufgehoben. Für die Verwaltung von Nicht-XCC2 Einheiten benötigen Sie eine separate XClarity Administrator-Instanz.

Schritt 7. Klicken Sie auf **Übernehmen**.

Schritt 8. Starten Sie XClarity Administrator neu (siehe Neustart von XClarity Administrator).

Schritt 9. Wenn Sie die Länge des Verschlüsselungsschlüssels geändert haben, generieren Sie das Stammzertifikat der Zertifizierungsstelle neu. Verwenden Sie dabei die richtigen Schlüssellänge und den korrekten Hashalgorithmus (siehe Selbst signiertes Lenovo XClarity Administrator Serverzertifikat neu generieren oder wiederherstellen oder Angepasste Serverzertifikate in Lenovo XClarity Administrator implementieren).

Nach dieser Aufgabe

Wenn Sie einen Alert erhalten, dass das Serverzertifikat für eine verwaltete Einheit nicht vertrauenswürdig ist, finden Sie weitere Informationen hierzu unter Ein nicht vertrauenswürdiges Serverzertifikat beheben.

Sicherheitseinstellungen für einen verwalteten Server konfigurieren

Sie können die SSL/TLS-Version und die Verschlüsselungseinstellung für verwaltete Server konfigurieren.

Zu dieser Aufgabe

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

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

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

Vorgehensweise

Gehen Sie wie folgt vor, um die Sicherheitseinstellungen für bestimmte verwaltete Server zu ändern.

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Server**. Die Seite Server wird aufgerufen, die eine Tabellenansicht aller verwalteten Server enthält.

Schritt 2. Wählen Sie einen oder mehrere Server aus.

Schritt 3. Konfigurieren Sie den Sicherheitsmodus.

1. Klicken Sie auf **Alle Aktionen → Sicherheit → Systemsicherheitsmodus festlegen**, um das Dialogfenster Systemsicherheitsmodus festlegen anzuzeigen.

   Im Dialogfenster wird die Anzahl der Server aufgeführt, die für jeden Modus festgelegt werden können. Bewegen Sie den Cursor über die einzelnen Zahlen, um ein Popup mit einer Liste der anwendbaren Servernamen anzuzeigen.

2. Wählen Sie den Sicherheitsmodus aus. Es kann einen der folgenden Werte aufweisen.

   - **Kompatibilität für Sicherheit**. Wählen Sie diesen Modus aus, wenn Services und Clients eine Verschlüsselung erfordern, die nicht CNSA/FIPS entspricht. Dieser Modus unterstützt

eine Vielzahl von Verschlüsselungsalgorithmen und ermöglicht die Aktivierung aller Services.

- **NIST SP 800-131A**. Wählen Sie diesen Modus aus, um die Einhaltung des Standards NIST SP 800-131A sicherzustellen. Eingeschlossen sind hier einschränkende RSA-Schlüssel bis 2048 Bit oder höher und einschränkende Hashwerte für digitale Signaturen für SHA-256 oder länger. Des Weiteren muss sichergestellt werden, dass nur NIST-zertifizierte, symmetrische Verschlüsselungsalgorithmen verwendet werden. Für diesen Modus muss der SSL/TLS-Modus auf **TLS 1.2 Server Client** festgelegt werden.

  Dieser Modus wird *nicht* für Server mit XCC2 unterstützt.

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

- **„Enterprise Strikt“-Sicherheit**. (Nur Server mit XCC2) Dies ist der sicherste Modus. Wählen Sie diesen Modus aus, um die Einhaltung des CNSA-Standards sicherzustellen. Es sind nur Services zulässig, die die Verschlüsselung auf CNSA-Ebene unterstützen. Unsichere Services sind standardmäßig deaktiviert und können nicht aktiviert werden. Dieser Modus erfordert Zertifikate auf CNSA-Ebene.

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

  Wichtig:

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

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

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

3. Klicken Sie auf **Übernehmen**.

Schritt 4. Konfigurieren Sie die Mindest-TLS-Version.

1. Klicken Sie auf **Alle Aktionen → Sicherheit → System-TLS-Version festlegen**, um das Dialogfenster System TLS-Version festlegen anzuzeigen.

2. Legen Sie die Mindest-TLS-Protokollversion fest, die für Clientverbindungen mit anderen Servern (z. B. LDAP-Client zu LDAP-Server) verwendet werden muss. Der Wert wird auf ausgewählten Einheiten konfiguriert, die diese Einstellung unterstützen. Die folgenden Optionen stehen zur Verfügung.
   - **TLS1.2**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.2.
   - **TLS1.3**. Erzwingt die Verwendung des Verschlüsselungsprotokolls TLS v1.3.

   Anmerkung: System x und CMM-Einheiten unterstützen nur TLS v1.2.
3. Klicken Sie auf **Übernehmen**.

Mit Sicherheitszertifikaten arbeiten

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

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

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

XClarity Administrator bietet verschiedene Services, die eingehende SSL/TLS-Verbindungen akzeptieren. Wenn sich ein Client, z. B. eine verwaltete Einheit oder ein Webbrowser, mit einem dieser Services verbindet, stellt XClarity Administrator 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 Administrator nicht in der Liste des Client enthalten ist, trennt der Client die Verbindung mit XClarity Administrator, damit keine vertraulichen Informationen mit einer nicht vertrauenswürdigen Quelle ausgetauscht werden.

XClarity Administrator fungiert bei der Kommunikation mit verwalteten Einheiten und externen Services als Client. Wenn XClarity Administrator eine Verbindung mit einer Einheit oder einem externen Service herstellt, stellen diese ihr jeweiliges Serverzertifikat für die Identifikation von XClarity Administrator bereit. XClarity

Administrator hält eine Liste von vertrauenswürdigen Zertifikaten vor. Wenn das *vertrauenswürdige Zertifikat*, das von der verwalteten Einheit oder dem externen Service bereitgestellt wird, nicht in der Liste vorhanden ist, trennt XClarity Administrator die entsprechende Verbindung, damit keine vertraulichen Informationen mit einer nicht vertrauenswürdigen Quelle ausgetauscht werden.

Die folgende Zertifikatskategorie wird von XClarity Administrator 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 Administrator verwaltet wird. Es ist nicht notwendig, das Stammzertifikat neu zu generieren, sofern kein Schlüssel kompromittiert wurde oder eine Unternehmensrichtlinie besteht, nach der alle Zertifikate regelmäßig ersetzt werden müssen (siehe Selbst signiertes Lenovo XClarity Administrator Serverzertifikat neu generieren oder wiederherstellen).

  Bei der Erstkonfiguration wird auch ein separater Schlüssel generiert, ein Serverzertifikat erstellt und signiert und ein Zertifikat erstellt, das durch die interne Zertifizierungsstelle signiert wird. Dieses Zertifikat dient als standardmäßiges XClarity Administrator-Serverzertifikat. Es wird automatisch jedes Mal neu generiert, wenn XClarity Administrator ermittelt, dass seine Netzwerkadressen (IP- oder DNS-Adressen) sich geändert haben. So wird sichergestellt, dass das Zertifikat die korrekten Adressen für den Server enthält. Das Zertifikat kann nach Bedarf angepasst und generiert werden (siehe Selbst signiertes Lenovo XClarity Administrator Serverzertifikat neu generieren oder wiederherstellen).

  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 Administrator importieren (siehe Angepasste Serverzertifikate in Lenovo XClarity Administrator implementieren).

  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 Zertifizierungsstellenzertifikat in einen Webbrowser importieren).
- **Vom Betriebssystem implementiertes Zertifikat**. Der Betriebssystem-Implementierungsservice verwendet ein separates Zertifikat, um zu gewährleisten, dass der Betriebssystem-Installer während der Installation des Systems eine sichere Verbindung mit dem Implementierungsservice herstellen kann. Wenn der Schlüssel kompromittiert wurde, können Sie ihn neu generieren, indem Sie den Verwaltungsserver neu starten.

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

- **Vertrauenswürdige Zertifikate**.

  Dieser Truststore verwaltet Zertifikate, die zum Herstellen einer sicheren Verbindung zu lokalen Ressourcen verwendet werden, wenn XClarity Administrator als Client fungiert. Beispiele für lokale Ressourcen sind verwaltete Einheiten, lokale Software bei der Ereignisweiterleitung und ein externer LDAP-Server.
- **Zertifikate für externe Services**. Dieser Truststore verwaltet Zertifikate, die zum Herstellen einer sicheren Verbindung mit externen Services verwendet werden, wenn XClarity Administrator als Client fungiert. Beispiele für externe Services sind die Lenovo Onlineunterstützungsservices, die zum Abrufen von Garantieinformationen oder Erstellen von Service-Tickets verwendet werden, externe Software (z. B. Splunk), an die Ereignisse weitergeleitet werden können, und Push-Benachrichtigungsserver von Apple und Google, wenn in Lenovo XClarity Mobile Push-Benachrichtigungen für eine iOS- oder Android-Einheit aktiviert sind. Er enthält vorkonfigurierte, vertrauenswürdige Zertifikate von Stammzertifizierungsstellen von bestimmten, allgemein vertrauenswürdigen und weltweit bekannten Zertifizierungsstellen (z. B. Digicert und Globalsign).

Wenn Sie XClarity Administrator 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.

XClarity Administrator unterstützt RSA-3072/SHA-384-, RSA-2048/SHA-256- und ECDSA p256/SHA-256-Zertifikatsignaturen. Andere Algorithmen wie ein stärkerer SHA-1 oder SHA-Hashes können abhängig von Ihrer Konfiguration unterstützt werden. Ziehen Sie den ausgewählten Verschlüsselungsmodus in XClarity Administrator (siehe Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren), die ausgewählten Sicherheitseinstellungen für verwaltete Server (Sicherheitseinstellungen für einen verwalteten Server konfigurieren) und die Funktionen von anderer Software und Einheiten in Ihrer Umgebung in Betracht. ECDSA-Zertifikate, die auf bestimmten (einschließlich p256), aber nicht allen elliptischen Kurven basieren, werden auf der Seite „Vertrauenswürdige Zertifikate“ und in der Signierungskette des XClarity Administrator-Zertifikats unterstützt, aber werden aktuell *nicht* für die Verwendung durch das XClarity Administrator-Serverzertifikat unterstützt.

Anmerkung: XClarity Administrator verwendet RSA-3072/SHA-384-Zertifikatsignaturen für Server mit XCC2 im „Strikt“-Modus.

Ein angepasstes, extern signiertes Serverzertifikat installieren

Sie können ein von einer privaten oder einer kommerziellen Zertifizierungsstelle (Certificate Authority, CA) signiertes Serverzertifikat verwenden.

Vorbereitende Schritte

Stellen Sie sicher, dass es sich bei der Stammzertifizierungsstelle um eine von Ihrer Organisation generierte handelt, die für das Signieren von Zertifikaten innerhalb dieser Organisation verwendet wird, oder eine allgemein vertrauenswürdige und weltweit bekannte Zertifizierungsstelle (siehe Webseite „Liste der vertrauenswürdigen Zertifizierungsstellen“).

Stellen Sie sicher, dass die Algorithmen für die Schlüssel und Signaturen des CA-Stammzertifikats unterstützt werden. Es werden nur RSA-3072/SHA-384- und RSA-2048/SHA-256-Signaturen unterstützt. RSA-PSS-Signaturen werden derzeit nicht unterstützt.

Stellen Sie sicher, dass auf allen verwalteten Einheiten die aktuelle Firmware installiert ist, bevor Sie einen Task starten, der möglicherweise die Verbindungen zwischen den Einheiten beeinträchtigt. Informationen zu Firmware-Upgrades auf verwalteten Einheiten finden Sie unter Firmware auf verwalteten Einheiten aktualisieren.

Überprüfen Sie, ob XClarity Administrator mit allen verwalteten Einheiten erfolgreich kommuniziert. Klicken Sie dazu auf **Hardware** und dann auf den Einheitentyp (Gehäuse oder Server). Es wird eine Seite mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs angezeigt. Wenn eine Einheit den Status „Offline“ hat, stellen Sie sicher, dass die Netzwerkverbindung zwischen dem Verwaltungsserver und der Einheit funktioniert, und lösen Sie ggf. nicht vertrauenswürdige Serverzertifikate nach Bedarf auf (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).

Zu dieser Aufgabe

Wenn Sie ein angepasstes, extern signiertes Serverzertifikat in XClarity Administrator oder einem Baseboard Management Controller oder CMM installieren, müssen Sie das Zertifikatspaket bereitstellen, das die vollständige CA-Signierungskette enthält.

Wenn Sie ein angepasstes Serverzertifikat in einem nicht durch XClarity Administrator verwalteten Gehäuse oder Server installieren, müssen Sie das Zertifikatspaket zuerst auf dem CMM installieren, bevor Sie seine Installation auf allen Management-Controllern im CMM ausführen.

Wenn Sie ein angepasstes Serverzertifikat auf einem verwalteten Gehäuse installieren, fügen Sie zuerst dem XClarity Administrator-Truststore die CA-Signierungskette hinzu und installieren das Serverzertifikat auf jedem Management-Controller und dem CMM. Anschließend laden Sie das Serverzertifikat in XClarity Administrator hoch. Beachten Sie, dass dies einfach umgangen werden kann, indem alle CA-Stammzertifikate, aber nicht jeder Zertifikatskette von jeder verwalteten Einheit als vertrauenswürdig gekennzeichnet/hinzugefügt werden. Die Anzahl der importierten Zertifikate sollte mit der Anzahl der CA-Stammzertifikate (CA-Stammzertifikate + alle dazwischenliegenden Zertifizierungsstellenzertifikate) übereinstimmen. Siehe Angepasste Serverzertifikate in verwaltete Einheiten implementieren für weitere Informationen.

Sie müssen das CA-Stammzertifikat und alle Zwischenzertifikate jeweils einzeln zum XClarity Administrator-Truststore hinzufügen. Die Reihenfolge ist irrelevant. Jedes Zertifikat muss einmal installiert werden. Wenn alle Einheiten dieselbe Zertifizierungsstelle und Zwischenzertifikate verwenden, müssen die Zertifizierungsstelle und alle Zwischenzertifikate einmal im XClarity Administrator-Truststore installiert sein. Wenn mehr als eine Zertifizierungsstelle oder eine Zwischenzertifizierungsstelle verwendet werden, müssen Sie sicherstellen, dass alle eindeutigen CA-Stammzertifikate oder Zwischenzertifikate, die in der Signierungskette einer verwalteten Einheit verwendet werden, mit den unten stehenden Schritten importiert werden.

Tipp: Wenn das neue Serverzertifikat nicht von einem vertrauenswürdigen Drittanbieter signiert wurde, wird das nächste Mal, wenn Sie eine Verbindung mit XClarity Administrator herstellen, im Browser eine Sicherheitsmeldung angezeigt. In einem Dialogfeld werden Sie aufgefordert, das neue Zertifikat im Browser zu akzeptieren. Sie können ein heruntergeladenes Serverzertifikat in die Liste mit vertrauenswürdigen Zertifikaten im Webbrowser importieren, um die Sicherheitsmeldungen zu vermeiden. Weitere Informationen zum Importieren von Serverzertifikaten finden Sie unter Zertifizierungsstellenzertifikat in einen Webbrowser importieren.

Angepasste Serverzertifikate in Lenovo XClarity Administrator implementieren

Sie können eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) zum Signieren durch die Zertifizierungsstelle Ihrer Organisation oder eine unabhängige Zertifizierungsstelle generieren. Die Zertifikatssignieranforderung erstellt eine vollständige Zertifikatskette, die Sie importieren und anstelle der eindeutigen, intern signierten Standardzertifikate verwenden können.

Vorbereitende Schritte

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

Achtung: Wenn NIST SP 800-131A aktiviert ist (siehe NIST SP 800-131A-Konformität implementieren) und Sie benutzerdefinierte oder extern signierte Zertifikate in einem NIST verwenden oder verwenden möchten, müssen alle Zertifikate in der Kette auf SHA-256-Hashfunktionen basieren.

Wenn das Serverzertifikat hochgeladen wurde, versucht XClarity Administrator, das neue CA-Zertifikat für alle verwalteten Einheiten bereitzustellen. Ist der Bereitstellungsprozess erfolgreich, wird das neue Serverzertifikat sofort von XClarity Administrator verwendet. Wenn der Vorgang fehlschlägt, erhalten Sie Fehlernachrichten. Mithilfe dieser Nachrichten können Sie Probleme manuell korrigieren, bevor Sie das neu importierte Serverzertifikat übernehmen. Nachdem die Fehler behoben sind, schließen Sie die Installation des zuvor hochgeladenen Zertifikats ab.

Anmerkung: Wenn XClarity Administrator bereits ein Zertifikat genutzt hat, das von derselben Stammzertifizierungsstelle signiert wurde, muss das CA-Zertifikat nicht an die Einheiten gesendet werden. XClarity Administrator beginnt direkt mit der Verwendung des Zertifikats.

Nach dem Hochladen eines Zertifikats in XClarity Administrator v1.1.0 und früher wurde der Web-Server neu gestartet und alle Browsersitzungen wurden automatisch beendet. Seit XClarity Administrator v1.1.1 wird das neue Zertifikat verwendet, ohne aktuelle Sitzungen zu schließen. Alle neuen Sitzungen werden mit dem neuen Zertifikat gestartet. Starten Sie den Webbrowser neu. Jetzt können Sie überprüfen, dass das neue Zertifikat verwendet wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein angepasstes, extern signiertes Serverzertifikat zu generieren und in Lenovo XClarity Administrator zu implementieren.

Schritt 1. Erstellen Sie eine Zertifikatssignieranforderung (CSR) für XClarity Administrator und laden Sie sie herunter.

a. Wählen Sie in der Menüleiste von XClarity Administrator die Optionen **Verwaltung → Sicherheit** aus, um die Seite Sicherheit aufzurufen.

b. Klicken Sie im Zertifikatsverwaltungsabschnitt auf **Serverzertifikat**, um die gleichnamige Seite anzuzeigen.

c. Wählen Sie die Registerkarte **Zertifikatssignieranforderung (CSR) generieren** aus.

d. Geben Sie Daten in die Felder für die Anforderung ein.
   - Land oder Region
   - Staat oder Bundesland
   - Ort oder Standort
   - Anordnung
   - Organisationseinheit (optional)
   - Allgemeiner Name

   Achtung: Wählen Sie einen allgemeinen Namen aus, der mit der IP-Adresse oder dem Hostnamen übereinstimmt, die von XClarity Administrator zum Herstellen der Verbindung mit der verwalteten Einheit verwendet werden. Ein falscher Wert kann zu Verbindungen führen, die nicht vertrauenswürdig sind.

e. Passen Sie die alternativen Namen (SANs) an, die beim Generieren der Zertifikatssignieranforderung zur Erweiterung X.509 „subjectAltName“ hinzugefügt werden.

   Standardmäßig definiert XClarity Administrator automatisch alternative Namen (SANs) für die Zertifikatssignieranforderung auf Basis der IP-Adresse und des Hostnamens, die von den Netzwerkschnittstellen des Gastbetriebssystems von XClarity Administrator erkannt werden. Sie können diese SAN-Werte anpassen, löschen oder ergänzen.

   Der Name, den Sie angeben, muss für den ausgewählten Typ gültig sein:
   - **directoryName** (z. B. `cn=lxca-example,ou=dcg,dc=company,dc=com`)
   - **dNSName** (z. B. `lxca-example.dcg.company.com`)
   - **ipAddress** (z. B. `192.0.2.0`)
   - **registeredID** (z. B. `1.2.3.4.55.6.5.99`)

- **rfc822Name** (z. B. `example@company.com`)
- **uniformResourceIdentifier** (z. B. `https://lxca-dev.dcg.company.com/example`)

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

f. Klicken Sie auf **CSR-Datei generieren**. Das Serverzertifikat ist im Dialogfenster Zertifikatssignieranforderung zu sehen.

g. Wählen Sie **In Datei speichern** aus, um das Serverzertifikat auf dem Host-Server zu sichern.

Schritt 2. Übermitteln Sie die Zertifikatssignieranforderung an eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA). Die Zertifizierungsstelle signiert die Zertifikatssignieranforderung und antwortet mit einem Serverzertifikat.

Schritt 3. Laden Sie das extern signierte Serverzertifikat in XClarity Administrator hoch. Der Zertifikatsinhalt muss ein Paket sein, in dem das CA-Stammzertifikat, alle Zwischenzertifikate und das Serverzertifikat enthalten sind.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, um die Seite „Sicherheit“ anzuzeigen.

b. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Serverzertifikat**.

c. Wechseln Sie auf die Registerkarte **Zertifikat hochladen**.

d. Wählen Sie **Zertifikat hochladen** aus, um das gleichnamige Dialogfeld anzuzeigen.

e. Geben Sie eine Zertifikatspaketdatei im Format PEM, DER oder PKCS7 an oder fügen Sie das Zertifikatspaket im PEM-Format ein.

f. Klicken Sie auf **Hochladen**, um das Serverzertifikat hochzuladen und das Zertifikat im XClarity Administrator-Truststore zu speichern.

Angepasste Serverzertifikate in verwaltete Einheiten implementieren

Sie können angepasste Serverzertifikate in verwaltete Einheiten implementieren, indem Sie das extern signierte Zertifikatspaket mithilfe des CMMs und des Management-Controllers für diese Einheiten hochladen und installieren.

Vorbereitende Schritte

Stellen Sie sicher, dass die neueste Firmware auf allen verwalteten Einheiten installiert ist (siehe Firmware auf verwalteten Einheiten aktualisieren).

Wenn Sie eine Zertifikatssignieranforderung (CSR) für angepasste Zertifikate generieren, müssen Sie einen allgemeinen Namen auswählen, der mit der zur Ermittlung der Einheit verwendeten IP-Adresse oder dem Hostnamen übereinstimmt. Ein falscher Wert kann zu Verbindungen führen, die nicht vertrauenswürdig sind.

Stellen Sie sicher, dass Sie ein Zertifikatspaket abrufen, das die gesamte Signierungskette enthält – vom Endserverzertifikat bis zum Stammzertifikat (Basiszertifikat) der vertrauenswürdigen Zertifizierungsstelle, das verwendet werden kann, um die gesamte vertrauenswürdige Zertifikatkette zu überprüfen.

Ändern Sie das Lenovo XClarity Administrator-Serverzertifikat nicht, während eine verwaltete Einheit „offline“ ist. Sie müssen die Verbindung wiederherstellen, bevor Sie Lenovo XClarity Administrator bearbeiten. Andernfalls können zusätzliche Schritte erforderlich werden, um die Konnektivitätsprobleme zu beheben (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).

Zu dieser Aufgabe

Dieser Abschnitt enthält Empfehlungen, die dazu dienen, eine erfolgreiche, unterbrechungsfreie Kommunikation zwischen Lenovo XClarity Administrator und den verwalteten Einheiten zu gewährleisten. Detaillierte Anweisungen dazu, wie Sie eine Zertifikatssignieranforderung generieren und ein signiertes Zertifikat importieren, finden Sie in der Dokumentation zu Ihrer Einheit.

Wenn Lenovo XClarity Administrator ein oder mehrere Gehäuse, Rack-Server und Tower-Server verwaltet und die intern signierten Lenovo XClarity Administrator-Standardzertifikate derzeit auf Lenovo XClarity Administrator und den verwalteten Einheiten installiert sind, können Sie angepasste Serverzertifikate implementieren.

Wenn das extern signierte Serverzertifikat auf der Einheit installiert wird, *bevor* Sie versuchen, die Einheit durch Lenovo XClarity Administrator zu verwalten, sind keine weiteren Schritte erforderlich. Um ein angepasstes Serverzertifikat in Einheiten zu implementieren, für die das Lenovo XClarity Administrator-Management verwendet wird, müssen Sie einen der folgenden Schritte ausführen, damit eine fortlaufende Konnektivität zwischen dem Verwaltungsserver und den Einheiten sichergestellt wird.

Vorgehensweise

Führen Sie eine der folgenden Optionen aus, um das angepasste, extern signierte Serverzertifikat in verwalteten Gehäusen oder Servern zu implementieren.

- Wenn Lenovo XClarity Administrator ein Zertifikat verwendet, das von derselben Zertifizierungsstelle wie die verwalteten Einheiten signiert wurde, führen Sie die Schritte in Angepasste Serverzertifikate in Lenovo XClarity Administrator implementieren aus, *bevor* Sie die Zertifikate auf den verwalteten Einheiten installieren. Durch die Installation der Lenovo XClarity Administrator-Zertifikatskette von derselben Zertifizierungsstelle als Erstes wird sichergestellt, dass sich die Zertifikatskette im Lenovo XClarity Administrator-Truststore befindet und Lenovo XClarity Administrator den Einheiten nach der Installation der extern signierten Zertifikate vertrauen kann.
- Fügen Sie dem Lenovo XClarity Administrator-Truststore die extern signierten Zertifikate in den CA-Signierungsketten hinzu.

  Sie müssen das CA-Stammzertifikat und alle Zwischenzertifikate jeweils einzeln zum Lenovo XClarity Administrator-Truststore hinzufügen. Die Reihenfolge ist irrelevant. Jedes Zertifikat muss einmal installiert werden. Wenn alle Einheiten dieselbe Zertifizierungsstelle und Zwischenzertifikate verwenden, müssen die Zertifizierungsstelle und alle Zwischenzertifikate einmal im Lenovo XClarity Administrator-Truststore installiert sein. Wenn mehr als eine Zertifizierungsstelle oder eine Zwischenzertifizierungsstelle verwendet werden, müssen Sie sicherstellen, dass alle eindeutigen CA-Stammzertifikate oder Zwischenzertifikate, die in der Signierungskette einer verwalteten Einheit verwendet werden, mit den unten stehenden Schritten importiert werden.

  Anmerkung: Fügen Sie während dieser Schritte keine Nicht-CA-Serverzertifikate hinzu.

  Führen Sie die folgenden Schritte für jedes Zertifikat im Paket aus.

  1. Wählen Sie in der Lenovo XClarity Administrator-Menüleiste **Verwaltung → Sicherheit** aus, um die Seite „Sicherheit“ anzuzeigen.
  2. Klicken Sie unter der Zertifikatsverwaltung in der linken Navigation auf **Vertrauenswürdige Zertifikate**.
  3. Wählen Sie das Symbol **Erstellen** ( ) aus, um das Dialogfeld Zertifikat hinzufügen anzuzeigen.
  4. Geben Sie eine Zertifikatsdatei im Format PEM oder DER an oder fügen Sie das Zertifikatspaket im PEM-Format ein.
  5. Klicken Sie auf **Erstellen**, um die Zertifikaterstellung abzuschließen.

Nach der Installation der CA-Signierungskette vertraut Lenovo XClarity Administrator Verbindungen zu CIM-Servern auf dem CMM und dem Management-Controller, auf denen das extern signierte Serverzertifikat installiert ist.

- Importieren Sie die extern signierten Zertifikate in die verwalteten Einheiten.

  Anmerkung: Wenn die erforderlichen Zertifikate nicht im Lenovo XClarity Administrator-Truststore vorliegen, geht die Konnektivität zwischen Lenovo XClarity Administrator und der verwalteten Einheit verloren. Führen Sie die Schritte in Ein nicht vertrauenswürdiges Serverzertifikat beheben aus, um die Verbindung wiederherzustellen.

  Wichtig: Diese Option geht mit einem temporären Verbindungsausfall einher. Daher wird eine der vorherigen Möglichkeiten empfohlen.

Selbst signiertes Lenovo XClarity Administrator Serverzertifikat neu generieren oder wiederherstellen

Sie können ein neues Zertifizierungsstellen- oder Serverzertifikat generieren, um das aktuelle, selbst signierte Zertifikat zu ersetzen, oder ein von Lenovo XClarity Administrator generiertes Zertifikat wiederherstellen, wenn XClarity Administrator derzeit ein angepasstes extern signiertes Serverzertifikat verwendet. Das neue, selbst signierte Serverzertifikat wird dann von den Authentifizierungs-, HTTPS- und CIM-Servern auf XClarity Administrator genutzt. Es wird auch automatisch auf allen verwalteten Einheiten bereitgestellt.

Vorbereitende Schritte

Wenn Sie das XClarity Administrator Zertifikat neu generieren oder hochladen, wird XClarity Administrator neu gestartet.

Das neue CA-Zertifikat wird nach der Generierung automatisch in die Truststores sämtlicher CMMs und Baseboard Management Controller in allen verwalteten Gehäusen, Rack- und Tower-Servern implementiert, um vertrauenswürdige Authentifizierungsserververbindungen zu gewährleisten. Wenn beim Implementieren des CA-Stammzertifikats ein Fehler auftritt, laden Sie es von der Zertifizierungsstellenseite herunter und importieren Sie es manuell in den Truststore aller verwalteten Einheiten, für die es nicht erfolgreich bereitgestellt werden konnte, bevor Sie ein neues Serverzertifikat generieren.

Wenn Sie das CA-Zertifikat neu generieren möchten, planen Sie Zeit ein, um es zu generieren, mögliche Bereitstellungsfehler zu beheben und das Serverzertifikat zeitnah neu zu generieren.

Nachdem Sie ein neues CA-Stammzertifikat generiert haben, kann es u. U. zu Kommunikationsfehlern kommen oder Sie können sich bei einer Einheit erst anmelden, wenn das Serverzertifikat neu generiert und signiert wurde.

Wichtig: In XClarity Administrator v1.1.1 und früher müssen Sie das CA-Stammzertifikat in den Truststore jedes CMMs und Management-Controllers importieren. Weitere Informationen zum Importieren des CA-Stammzertifikats finden Sie in der Dokumentation für das CMM und den Management-Controller.

Vorgehensweise

Gehen Sie wie folgt vor, um ein selbst signiertes Serverzertifikat auf XClarity Administrator wiederherzustellen.

Anmerkung: Das derzeit in XClarity Administrator verwendete Serverzertifikat, ob selbst oder extern signiert, wird weiterhin genutzt, bis ein neues Serverzertifikat neu generiert und signiert wurde.

Schritt 1. **Optional**: Generieren Sie ein neues CA-Stammzertifikat.

a. Wählen Sie in der XClarity Administrator-Menüleiste **Verwaltung → Sicherheit** aus, um die Seite Sicherheit anzuzeigen.

b. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Zertifizierungsstelle**.

c. Wählen Sie **Stammzertifikat der Zertifizierungsstelle neu generieren** aus.

Wenn der Zertifizierungsstellenschlüssel und das -zertifikat erfolgreich neu generiert wurden, sehen Sie ein Dialogfenster mit dem Status der Jobs, die dazu dienen, das Zertifikat für alle CMMs und Management-Controller als vertrauenswürdiges LDAP-Zertifikat bereitzustellen (für Converged-, NeXtScale- und System x-Server). In diesem Dialogfenster und auf der Jobüberwachungsseite wird der Erfolg oder Misserfolg von jedem dieser Bereitstellungsjobs angezeigt.

Wenn einer der Jobs fehlschlägt, schließen Sie die folgenden Schritte zum Herunterladen des CA-Stammzertifikats ab. Importieren Sie dann das Stammzertifikat manuell als vertrauenswürdiges LDAP-Zertifikat in die Einheiten, bei denen ein Fehler aufgetreten ist.

Schritt 2. **Optional**: Laden Sie das CA-Stammzertifikat auf das Hostsystem herunter und importieren Sie es in den Webbrowser.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, um die Seite „Sicherheit“ anzuzeigen.

b. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Zertifizierungsstelle**.

c. Wählen Sie **Stammzertifikat der Zertifizierungsstelle herunterladen** aus. Das aktuelle CA-Stammzertifikat wird im Dialogfenster „Zertifizierungsstellen-Stammzertifikat“ angezeigt.

d. Wählen Sie **In Datei speichern** aus, um das CA-Stammzertifikat auf dem Hostsystem zu speichern.

e. Befolgen Sie die Anweisungen für Ihren Webbrowser und die Webbrowser, die andere Benutzer für den Zugriff auf XClarity Administrator verwenden, um das Zertifikat als vertrauenswürdige Stammzertifizierungsstelle zu importieren.

Schritt 3. Generieren Sie ein neues Serverzertifikat und signieren Sie das Zertifikat mit dem neuen CA-Stammzertifikat.

a. Klicken Sie auf der Seite „Sicherheit“ im Abschnitt für die Zertifikatsverwaltung auf **Serverzertifikat**.

b. Wechseln Sie auf die Registerkarte **Serverzertifikat neu generieren**.

c. Füllen Sie die Felder auf der Seite „Serverzertifikat neu generieren“ aus:
   - Land oder Region
   - Staat oder Bundesland
   - Ort oder Standort
   - Anordnung
   - Organisationseinheit
   - Allgemeiner Name
   - Ungültig vor Datum
   - Ungültig vor Zeit
   - Ungültig nach Datum
   - Ungültig nach Zeit

d. Klicken Sie auf **Zertifikat neu generieren**.

e. Wenn Sie selbst signierte Zertifikate auf den verwalteten CMMs und den Management-Controllern (für Converged-, NeXtScale-, ThinkSystem- und System x-Server) neu generieren: Importieren Sie nach der Neugenerierung des Zertifikats auf allen Einheiten das neue Einheitenzertifikat in den XClarity Administrator-Truststore (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben). Alternativ können Sie das Zertifikat manuell von der Einheit herunterladen und es in XClarity Administrator auf der Seite Vertrauenswürdige Zertifikate importieren.

In XClarity Administrator v1.1.0 und früher startet der Web-Server nach der Neugenerierung eines Zertifikats neu und alle Browsersitzungen werden automatisch geschlossen. In XClarity Administrator v1.1.1 und höher beginnt XClarity Administrator mit der Verwendung des neuen Zertifikats, ohne die vorhandenen Sitzungen zu beenden. Neue Sitzungen werden mit dem neuen Zertifikat gestartet. Starten Sie den Webbrowser neu. Jetzt können Sie überprüfen, dass das neue Zertifikat verwendet wird.

Schritt 4. Wenn Sie selbst signierte Zertifikate auf den verwalteten CMMs und den Management-Controllern (für Converged-, NeXtScale-, ThinkSystem- und System x-Server) neu generieren: Importieren Sie nach der Neugenerierung des Zertifikats auf allen Einheiten das neue Einheitenzertifikat in den XClarity Administrator-Truststore (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben). Alternativ können Sie das Zertifikat manuell von der Einheit herunterladen und es in XClarity Administrator auf der Seite Vertrauenswürdige Zertifikate importieren.

Ein nicht vertrauenswürdiges Serverzertifikat beheben

Das Serverzertifikat, das zur Herstellung einer sicheren Verbindung mit einer verwalteten Einheit verwendet wird, kann zu einem nicht vertrauenswürdiges Zertifikat werden. Wenn die Ursache des Problems eine zurückgestufte CA-Stammzertifikatsversion der Einheit oder ein selbst signiertes Einheitenzertifikat im Lenovo XClarity Administrator-Truststore ist, kann XClarity Administrator das nicht vertrauenswürdige Serverzertifikat auflösen.

Zu dieser Aufgabe

Wenn eine verwaltete Einheit nicht vertrauenswürdig wird, verhindert XClarity Administrator die Kommunikation mit dieser Einheit und hindert Sie daran, Verwaltungs- oder Bestandsvorgänge darauf auszuführen.

Vorgehensweise

Um ein nicht vertrauenswürdiges Serverzertifikat für eine verwaltete Einheit aufzulösen, gehen Sie wie folgt vor.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware** und dann auf den Einheitentyp (**Gehäuse**, **Server**, **Speicher** oder **Schalter**.) Es wird eine Seite mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs angezeigt.

Schritt 2. Wählen Sie die entsprechende Einheit im „Offline“-Status aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen**.

Schritt 4. Wählen Sie **Zertifikat installieren** aus.

XClarity Administrator ruft das aktuelle Zertifikat von der Zieleinheit ab. Wenn sich dieses Zertifikat vom vertrauenswürdigen Zertifikat für diese Einheit im XClarity Administrator-Truststore unterscheidet, wird das neue Zertifikat im XClarity Administrator-Truststore gespeichert und ersetzt das vorherige Zertifikat für diese Einheit.

Wenn das Problem dadurch nicht gelöst wird, stellen Sie sicher, dass die Netzwerkverbindung zwischen XClarity Administrator und der Einheit funktioniert.

Das Serverzertifikat herunterladen

Sie können eine Kopie des aktuellen Serverzertifikats im Format PEM oder DER auf das lokale System herunterladen. Anschließend können Sie das Zertifikat in den Webbrowser oder eine andere Anwendung importieren (zum Beispiel Lenovo XClarity Mobile oder Lenovo XClarity Integrator).

Vorgehensweise

Gehen Sie wie folgt vor, um das Serverzertifikat herunterzuladen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, um die Seite „Sicherheit“ anzuzeigen.

Schritt 2. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Serverzertifikat**. Die Seite „Serverzertifikat“ wird angezeigt.

Schritt 3. Wechseln Sie auf die Registerkarte **Zertifikat herunterladen**.

Schritt 4. Klicken Sie auf **Zertifikat herunterladen**.

Schritt 5. Wählen Sie **Als „DER“ speichern** oder **Als „PEM“ speichern** aus, um das Serverzertifikat in einem der beiden Dateiformate auf dem lokalen System zu speichern.

Zertifizierungsstellenzertifikat in einen Webbrowser importieren

Möglicherweise erhalten Sie Sicherheitswarnmeldungen, wenn Sie im Webbrowser auf Lenovo XClarity Administrator zugreifen. Sie können dies vermeiden, indem Sie eine Kopie des aktuellen Zertifikats der Zertifizierungsstelle (Certificate Authority, CA) im Format PEM oder DER auf Ihr lokales System herunterladen und dieses Zertifikat in die Liste mit vertrauenswürdigen Zertifikaten im Webbrowser importieren.

Zu dieser Aufgabe

XClarity Administrator unterstützt RSA-3072/SHA-384-, RSA-2048/SHA-256- und ECDSA p256/SHA-256-Zertifikatsignaturen. Andere Algorithmen wie ein stärkerer SHA-1 oder SHA-Hashes können abhängig von Ihrer Konfiguration unterstützt werden. Ziehen Sie den ausgewählten Verschlüsselungsmodus in XClarity Administrator (siehe Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren), die ausgewählten Sicherheitseinstellungen für verwaltete Server (Sicherheitseinstellungen für einen verwalteten Server konfigurieren) und die Funktionen von anderer Software und Einheiten in Ihrer Umgebung in Betracht. ECDSA-Zertifikate, die auf bestimmten (einschließlich p256), aber nicht allen elliptischen Kurven basieren, werden auf der Seite „Vertrauenswürdige Zertifikate“ und in der Signierungskette des XClarity Administrator-Zertifikats unterstützt, aber werden aktuell *nicht* für die Verwendung durch das XClarity Administrator-Serverzertifikat unterstützt.

Anmerkung: XClarity Administrator verwendet RSA-3072/SHA-384-Zertifikatsignaturen für Server mit XCC2 im „Strikt“-Modus.

Vorgehensweise

Gehen Sie wie folgt vor, um das Serverzertifikat herunterzuladen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, um die Seite „Sicherheit“ anzuzeigen.

Schritt 2. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Zertifizierungsstelle**. Die Seite Zertifizierungsstelle wird angezeigt.

Schritt 3. Wählen Sie **Stammzertifikat der Zertifizierungsstelle herunterladen** aus.

Schritt 4. Wählen Sie **Als „DER“ speichern** oder **Als „PEM“ speichern** aus, um das Serverzertifikat in einem der beiden Dateiformate auf dem lokalen System zu speichern.

Schritt 5. Importieren Sie das heruntergeladene Zertifikat in die Liste der vertrauenswürdigen Stammzertifizierungsstellen für Ihren Browser.

- **Firefox:**
  1. Öffnen Sie den Browser und klicken Sie auf **Extras → Einstellungen → Erweitert**.
  2. Wählen Sie **Zertifikate** aus.
  3. Klicken Sie auf **Zertifikate anzeigen**.
  4. Wählen Sie **Importieren** aus und navigieren Sie zur Position des heruntergeladenen Zertifikats.
  5. Markieren Sie das Zertifikat und klicken Sie auf **Öffnen**.

- **Internet Explorer:**
  1. Öffnen Sie den Browser und wählen Sie **Extras → Internetoptionen → Inhalte** aus.
  2. Klicken Sie auf **Zertifikate**, um eine Liste aller aktuell vertrauenswürdigen Zertifikate anzuzeigen.
  3. Wenn Sie auf **Importieren** klicken, wird der Zertifikatimport-Assistent gestartet.
  4. Schließen Sie den Vorgang im Assistenten ab, um das Zertifikat zu importieren.

Eine Zertifikatswiderrufliste hinzufügen und ersetzen

Eine *Zertifikatswiderrufliste* ist eine Liste von Zertifikaten, die widerrufen wurden und nicht mehr vertrauenswürdig sind. Ein Zertifikat kann widerrufen werden, wenn es nicht ordnungsgemäß von der Zertifizierungsstelle ausgegeben wurde oder wenn sein Schlüssel unrechtmäßig weitergegeben, verloren oder gestohlen wurde.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine neue Zertifikatswiderrufliste hinzuzufügen oder eine vorhandene Zertifikatswiderrufliste zu ersetzen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, um die Seite „Sicherheit“ anzuzeigen.

Schritt 2. Klicken Sie unter der Zertifikatsverwaltung in der linken Navigation auf **Zertifikatswiderruflisten**. Die Seite „Zertifikatswiderruflisten“ wird mit einer Liste aller Zertifikatswiderruflisten angezeigt.

Schritt 3. Klicken Sie auf **CLR hinzufügen/ersetzen**, um eine Zertifikatswiderrufliste hinzuzufügen, oder wählen Sie eine Zertifikatswiderrufliste aus und klicken Sie auf **CLR hinzufügen/ersetzen**, um die Zertifikatswiderrufliste zu ersetzen.

Schritt 4. Geben Sie eine Zertifikatswiderruflisten-Datei im Format PEM oder DER an oder fügen Sie das Zertifikatspaket im PEM-Format ein.

Schritt 5. Klicken Sie auf **Erstellen**, um die Zertifikatswiderrufliste zu erstellen.

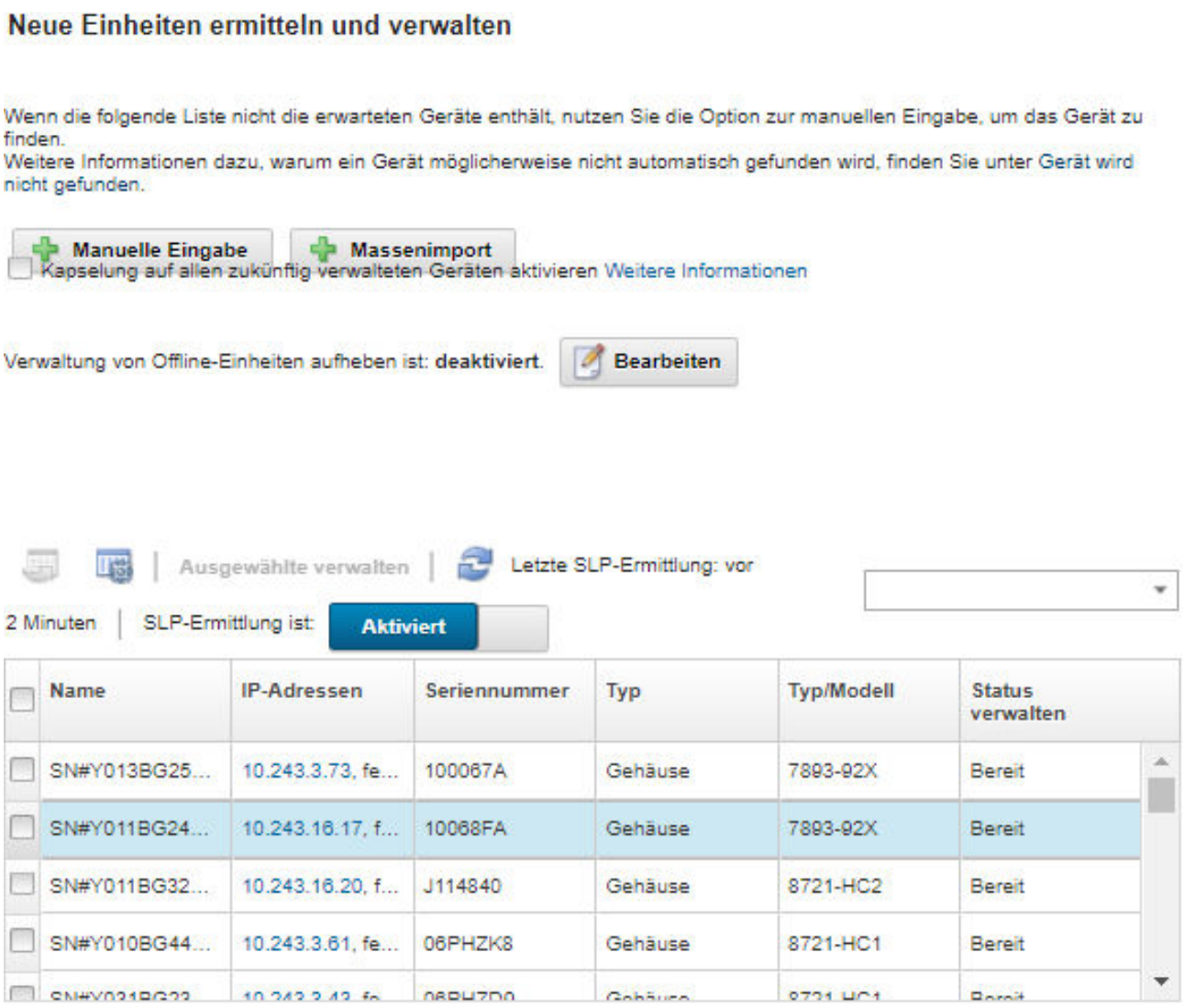
Kapselung aktivieren

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

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

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

Sie können die Kapselung im Rahmen des Verwaltungsprozesses über das Kontrollkästchen **Kapselung auf allen zukünftig verwalteten Geräten aktivieren** auf der Seite Neue Einheiten ermitteln und verwalten global für alle Einheiten aktivieren oder deaktivieren. Die Kapselung ist standardmäßig deaktiviert.



Sie können die Kapselung auch jederzeit für bestimmte verwaltete Einheiten individuell aktivieren und deaktivieren. Wechseln Sie dafür zur Übersichtsseite, wählen Sie die Einheit aus und klicken Sie auf **Aktionen → Kapselung aktivieren** oder **Aktionen → Kapselung deaktivieren**.

Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.

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

NIST SP 800-131A-Konformität implementieren

Wenn Ihr System NIST SP 800-131A-konform sein muss, können Sie mithilfe von Lenovo XClarity Administrator beginnen, auf eine vollständig konforme Umgebung hinzuarbeiten.

Zu dieser Aufgabe

In der Veröffentlichung „Special Publication 800-131A (SP800-131A)“ des National Institute of Standards and Technology (NIST SP 800-131A) ist definiert, wie die sichere Kommunikation erfolgen soll. Bessere Algorithmen und länger Schlüssel für mehr Sicherheit sind kennzeichnend für diesen Standard. Der Standard NIST SP 800-131A setzt voraus, dass die strikte Einhaltung des Standards durch eine entsprechende Benutzerkonfiguration gegeben ist.

Anmerkungen: Die folgenden Flex System-Komponenten bieten derzeit keine Unterstützung für NIST SP 800-131A. Die Kommunikation zwischen XClarity Administrator oder dem CMM und diesen Komponenten ist nicht konform:
- Skalierbarer Flex System EN4023 10 Gb Switch
- Flex System EN6131 40 Gb Ethernet Switch
- Flex System FC3171 8 Gb SAN Switch
- Skalierbarer Flex System FC5022 16 Gb SAN Switch
- Flex System IB6131 Infiniband Switch

Anmerkung: Wenn ein SAML-Identity Provider für die Authentifizierung verwendet wird, verwendet XClarity Administrator SHA-1 zum Signieren der Signatur in den Metadaten. Die Verwendung des SHA-1-Algorithmus für digitale Signaturen ist nicht konform mit NIST SP 800-131A.

Vorgehensweise

Gehen Sie wie folgt vor, um NIST SP 800-131A-Konformität zu implementieren.

Schritt 1. Stellen Sie sicher, dass die Einheiten die folgenden Kriterien erfüllen:

- Verwendung von Secure Sockets Layer (SSL) über das Protokoll TLS v1.2
- Verwendung der Hashfunktion SHA-256 oder besser für digitale Signaturen und der Hashfunktion SHA-1 oder besser für andere Anwendungen
- Verwenden Sie RSA-2048 oder besser bzw. von durch NIST genehmigte elliptische Kurven mit mindestens 224 Bit.
- Verwenden Sie die von NIST genehmigte symmetrische Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit.
- Verwenden Sie die von NIST genehmigten Zufallszahlengeneratoren.
- Bieten Sie Unterstützung für Diffie-Hellman- und/oder Elliptic Curve Diffie-Hellman-Schlüsselaustauschmechanismen (soweit möglich).

Schritt 2. Konfigurieren Sie die Verschlüsselungseinstellungen in Lenovo XClarity Administrator. Es gibt zwei Einstellungen in Bezug auf NIST SP 800-131A-Konformität:

- Der *SSL/TLS-Modus* gibt die Protokolle an, die für eine sichere Kommunikation verwendet werden sollen. XClarity Administrator unterstützt die Einstellung **TLS 1.2 Server und Client**, um das Verschlüsselungsprotokoll in XClarity Administrator und auf allen verwalteten Einheiten auf TLS 1.2 zu beschränken.
- Wenn die sichere Kommunikation implementiert ist, legt der *Verschlüsselungsmodus* die Länge des zu verwendenden Verschlüsselungsschlüssels fest. Sie können den Verschlüsselungsmodus auf **NIST SP 800-131A** festlegen. Allerdings können Sie dann möglicherweise bestimmte Betriebssysteme nicht über XClarity Administrator bereitstellen, da die eingeschränkten Einstellungen von einigen Betriebssystem-Installationsprogrammen nicht unterstützt werden. Um das Bereitstellen eines Betriebssystems zu unterstützen, können Sie eine Ausnahme für die Betriebssystembereitstellung zulassen.

Wenn Sie Verschlüsselungseinstellungen ändern, stellt XClarity Administrator die neuen Einstellungen auf allen verwalteten Einheiten bereit und versucht, alle neuen Zertifikate auf diesen Einheiten aufzulösen.

Anmerkung: Wenn Verschlüsselungseinstellungen geändert wurden, müssen Sie XClarity Administrator manuell neu starten, damit die Änderungen wirksam werden und um eventuell ausgefallene Services wiederherzustellen (siehe Neustart von XClarity Administrator).

Weitere Informationen zu diesen Einstellungen finden Sie unter Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren.

Schritt 3. Verwenden Sie einen Webbrowser, der das Protokoll TLS1.2 und SHA-256-Hashfunktionen unterstützt, und aktivieren Sie diese Einstellungen im Webbrowser.

Anmerkung: Wenn Sie benutzerdefinierte oder extern signierte Zertifikate verwenden möchten, müssen alle Zertifikate in der Kette auf SHA-256-Hashfunktionen basieren.

Schritt 4. Verwenden Sie für die gesamte Kommunikation verschlüsselte Protokolle. Unverschlüsselte Protokolle wie Telnet, FTP und VNC sollten für die Remote-Kommunikation mit verwalteten XClarity Administrator-Einheiten nicht verwendet werden.

VMware-Tools verwenden

Das Paket mit VMware-Tools wird auf dem Gastsystem der virtuellen Maschine installiert, wenn Sie Lenovo XClarity Administrator 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.

Netzwerkzugriff konfigurieren

Bei der Erstkonfiguration von Lenovo XClarity Administrator konfigurieren Sie bis zu zwei Netzwerkschnittstellen. Darüber hinaus müssen Sie angeben, welche dieser Schnittstellen zum Bereitstellen von Betriebssystemen verwendet werden soll. Sie können diese Einstellungen nach der Erstkonfiguration ändern.

Vorbereitende Schritte

Achtung:

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

  Anmerkung: Wenn diese Option aktiviert ist, führt XClarity Administrator einen ARP-Scan aus, um aktive IPv4-Komponenten im selben Subnetz zu finden. Wenn Sie den ARP-Scan verhindern möchten, deaktivieren Sie **Doppelte IP-Adressen prüfen**.
- Wenn XClarity Administrator als eine virtuelle Einheit ausgeführt wird und die Netzwerkschnittstelle für das Verwaltungsnetzwerk für die Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert ist, ändert sich möglicherweise die IP-Adresse der Verwaltungsschnittstelle, wenn die DHCP-Zugangsberechtigung abläuft. Ist das der Fall, müssen Sie die Gehäuse-, Rack- und Tower-Server-Verwaltung zunächst aufheben und anschließend erneut aufnehmen. Sie können dieses Problem vermeiden, indem Sie entweder für die Verwaltungsschnittstelle eine statische IP-Adresse angeben oder

den DHCP-Server so konfigurieren, dass die DHCP-Adresse auf einer MAC-Adresse basiert oder die DHCP-Zugangsberechtigung nicht abläuft.

- Wenn Sie *nicht* beabsichtigen, XClarity Administrator zum Implementieren des Betriebssystems oder Aktualisieren von BS-Einheitentreibern zu verwenden, können Sie Samba- und Apache-Server deaktivieren, indem für die Netzwerkschnittstelle die Option **Nur Hardware ermitteln und verwalten** konfigurieren. Beachten Sie, dass der Verwaltungsserver nach dem Ändern der Einstellungen für die Netzwerkschnittstelle neu gestartet wird.
- Wenn XClarity Administrator als Container ausgeführt wird.
  - Sie können nur die Überprüfung auf doppelte IP-Adressen aktivieren oder deaktivieren, die Netzwerkschnittstellenrollen ändern und Proxyeinstellungen ändern. Alle anderen Netzwerkeinstellungen (einschließlich IP-Adresse, Gateway und DNS) werden in der Containerkonfiguration definiert.
  - Stellen Sie sicher, dass ein macvlan-Netzwerk auf dem Hostsystem eingerichtet ist.

Zu dieser Aufgabe

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

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

    Anmerkung: Wenn Sie für die Implementierung von BS-Betriebssystemen und Aktualisierungen von BS-Einheitentreibern ein separates Netzwerk verwenden, können Sie eine Verbindung von der zweiten Netzwerkschnittstelle mit diesem Netzwerk anstelle des Datennetzwerks konfigurieren. Wenn jedoch das Betriebssystem auf jedem Server keinen Zugriff auf das Datennetzwerk hat, konfigurieren Sie eine zusätzliche Schnittstelle auf den Servern, um die Verbindung vom Hostbetriebssystem zum Datennetzwerk für die BS-Implementierung sowie Aktualisierungen von BS-Einheitentreibern bereitzustellen, falls erforderlich.
- Wenn zwei Netzwerkschnittstellen (Eth0 und Eth1) vorhanden sind:
  - Die erste Netzwerkschnittstelle (in der Regel die Eth0-Schnittstelle) muss mit dem Verwaltungsnetzwerk verbunden und für die Unterstützung der Einheitenermittlung und -verwaltung (einschließlich Serverkonfiguration und Firmwareaktualisierungen) konfiguriert sein. Sie muss mit CMMs und Flex-Switches in sämtlichen verwalteten Gehäusen, den Management-Controllern in allen verwalteten Servern und mit sämtlichen RackSwitch-Switches kommunizieren können.

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

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

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

Tabelle 2. Rolle jeder Netzwerkschnittstelle auf Basis der Netzwerktopologie

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

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

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

Weitere Informationen zu XClarity Administrator-Netzwerkschnittstellen und IPv6-Adresseinschränkungen finden Sie unter Hinweise zum Netzwerkbetrieb in der Onlinedokumentation von XClarity Administrator.

Vorgehensweise

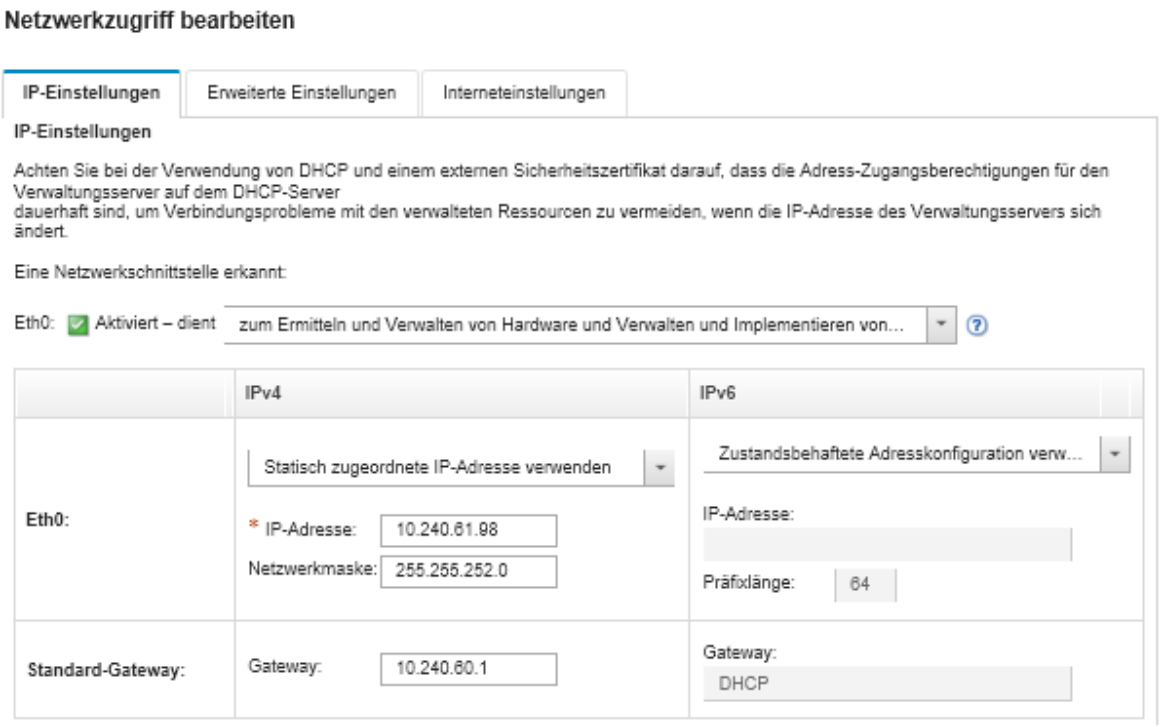
Gehen Sie wie folgt vor, um Netzwerkzugriff zu konfigurieren.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Netzwerkzugriff**. Die aktuellen Netzwerkeinstellungen werden angezeigt.

Schritt 2. Sie können optional die Prüfung auf doppelte IP-Adressen im selben Subnetz aktivieren, indem Sie auf die Umschalt-Schaltfläche **Doppelte IP-Adressen prüfen** klicken.

Bei Aktivierung löst XClarity Administrator einen Alert aus, wenn Sie versuchen, die IP-Adresse von XClarity Administrator zu ändern oder eine Einheit zu verwalten, die dieselbe IP-Adresse wie eine andere verwaltete Einheit oder eine andere Einheit im selben Subnetz hat.

Schritt 3. Klicken Sie auf **Netzwerkzugriff bearbeiten**, um die Seite Netzwerkzugriff bearbeiten anzuzeigen.



Schritt 4. Wenn Sie Betriebssysteme über XClarity Administrator bereitstellen und auch BS-Einheitentreiber aktualisieren möchten, geben Sie die für die Betriebssystemverwaltung zu verwendende Netzwerkschnittstelle an.

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

Schritt 5. (XClarity Administrator nur als virtuelle Einheit) Ändern Sie die IP-Einstellungen.

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

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

  Anmerkung: Weitere Informationen über IPv6-Adresseinschränkungen finden Sie unter IPv6-Konfigurationseinschränkungen in der Onlinedokumentation von XClarity Administrator.

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

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

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

c. Geben Sie das Standard-Gateway an.

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

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

Tipps:

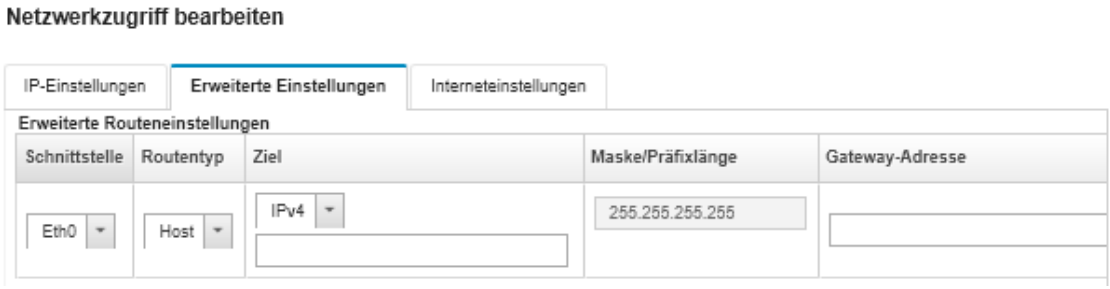
- Stellen Sie sicher, dass das Gateway mit einem Subnetz der Netzwerkschnittstellen übereinstimmt. Das Standard-Gateway wird automatisch über diese Netzwerkschnittstelle festgelegt.
- Wenn Sie zu einem von DHCP bereitgestellten Gateway zurückkehren möchten, deaktivieren Sie das Kontrollkästchen **Gateway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

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

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

Schritt 6. (XClarity Administrator nur als virtuelle Einheit) Optional können Sie die erweiterten Einstellungen ändern.

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



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

Gehen Sie wie folgt vor, um eine oder mehrere Routen zu definieren.
1. Wählen Sie die Schnittstelle aus.
2. Geben Sie den Routentyp an (Route zu einem anderen Host oder zu einem Netzwerk).
3. Geben Sie den Zielhost oder die Netzwerkadresse für die Route an.

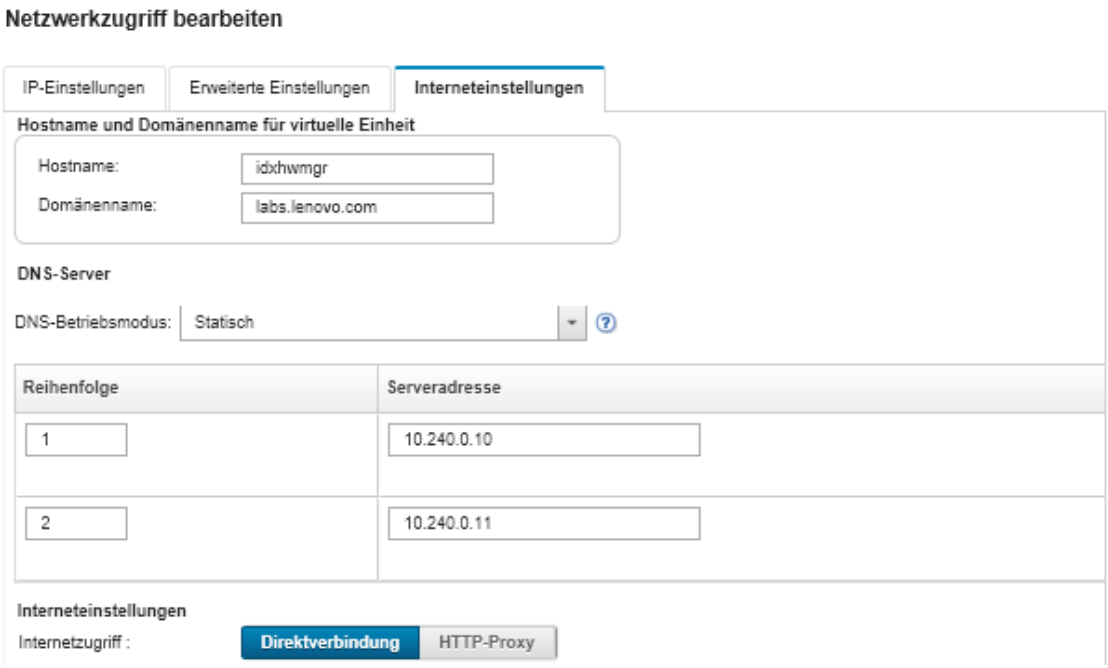
4. Geben Sie die Subnetzmaske der Zieladresse an.
5. Geben Sie die Gateway-Adresse für die zu sendenden Pakete an.

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

Schritt 7. Ändern Sie bei Bedarf die DNS- und Proxy-Einstellungen.

Wenn XClarity Administrator als Container konfiguriert ist, können über die Webschnittstelle nur Proxy-Einstellungen geändert werden. Die DNS-Einstellungen werden im Container definiert.

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



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

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

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

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

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

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

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

Wenn Sie einen HTTP-Proxy verwenden, geben Sie Daten in den folgenden Feldern an:

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

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

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

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

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

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

Schritt 8. Klicken Sie auf **Neu starten**, um den Verwaltungsserver neu zu starten.

Schritt 9. Klicken Sie auf **Verbindung testen**, um die Netzwerkeinstellungen zu überprüfen.

Datum und Uhrzeit einstellen

Sie können das Datum und die Uhrzeit festlegen, die für Lenovo XClarity Administrator verwendet werden.

Vorbereitende Schritte

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

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

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

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

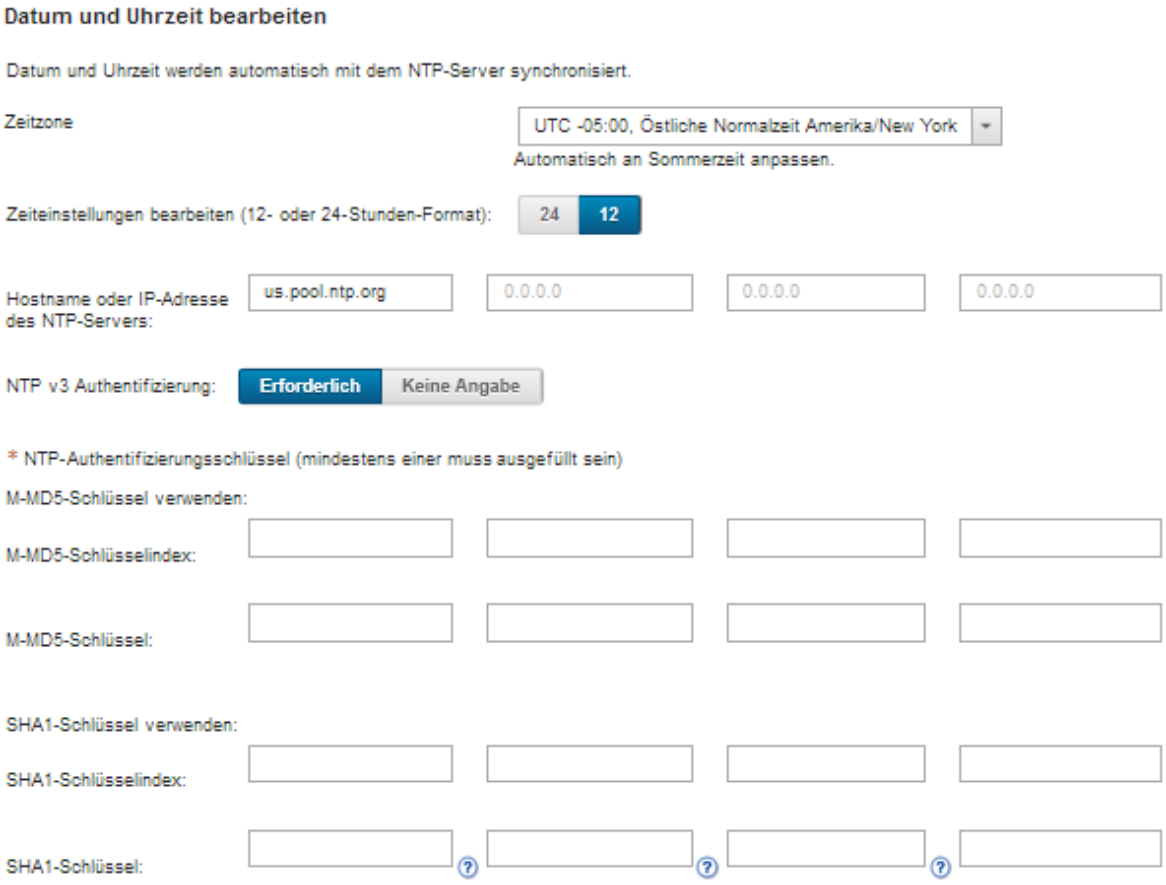
- Befolgen Sie für ESXi die Anweisungen auf der VMware – Website zur Deaktivierung der Zeitsynchronisation.
- Klicken Sie bei Hyper-V im Hyper-V-Manager mit der rechten Maustaste auf die virtuelle XClarity Administrator-Maschine und klicken Sie anschließend auf **Einstellungen**. Klicken Sie im Dialogfeld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

Vorgehensweise

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

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Datum und Uhrzeit**. Die Seite Datum und Uhrzeit wird angezeigt. Diese Seite zeigt das aktuelle Datum und die Uhrzeit für XClarity Administrator an.

Schritt 2. Klicken Sie auf **Datum und Uhrzeit bearbeiten**, um die gleichnamige Seite anzuzeigen.



Schritt 3. Geben Sie Daten in das Dialogfenster „Datum und Uhrzeit“ ein.

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

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

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

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

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

Bestandseinstellungen festlegen

Sie können Bestandseinstellungen für verwaltete Einheiten festlegen, einschließlich für Bestand, der zur Anzeige des Einheitennamens verwendet wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Bestandseinstellungen für verwaltete Einheiten vorzunehmen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Bestandseinstellungen**. Die Seite „Bestandseinstellungen“ wird angezeigt.

Schritt 2. Wählen Sie die Eigenschaft aus, die für den in der Lenovo XClarity Administrator Benutzerschnittstelle angezeigten Einheitennamen verwendet werden soll. Sie können eine der folgenden Eigenschaften auswählen.
- **Vordefinierte Reihenfolge (Standard)**
- **Benutzerdefinierter Name**
- **DNS-Hostname**
- **Hostname**
- **IPv4-Adresse**
- **Seriennummer**

Falls **Vordefinierte Reihenfolge** ausgewählt ist, wird der Einheitenname basierend auf der Reihenfolge der Eigenschaften in der vorherigen Liste ausgewählt. Falls eine Einheit beispielsweise einen benutzerdefinierten Namen aufweist, wird dieser Name angezeigt. Falls eine Einheit keinen benutzerdefinierten Namen aufweist, wird der DNS-Hostname angezeigt. Falls eine Einheit keinen benutzerdefinierten Namen oder DNS-Hostnamen aufweist, wird der Hostname angezeigt.

Anmerkung: Wird ein anderer Wert als der Standardwert ausgewählt, wird der Name, der in der Lenovo XClarity Administrator Benutzerschnittstelle angezeigt wird, für alle Einheiten in die ausgewählte Eigenschaft geändert. Der benutzerdefinierte Name, welcher der Einheit zugewiesen ist, wird nicht geändert.

Schritt 3. Klicken Sie optional auf **Aktivieren**, um die Raster (Tabellen) mithilfe des Werts zu sortieren, der für den Gerätenamen ausgewählt wurde.

Schritt 4. Wählen Sie die bevorzugte Reihenfolge der Rack-Nummerierung aus: entweder von oben nach unten (z. B. 1 – 52) oder von unten nach oben (z. B. 52 – 1).

Anmerkung: Wenn Sie die Reihenfolge der Nummerierung ändern, wird die Position einer Einheit innerhalb des Racks nicht geändert.

Schritt 5. Klicken Sie auf **Übernehmen**.

Nach dieser Aufgabe

Sie können Schwellenwerteinstellungen für das Auslösen von Alerts und Ereignissen festlegen, wenn ein bestimmter Wert wie die Lebensdauer einer SSD in einem ThinkSystem- oder ThinkServer-Server eine Warnung oder einen kritischen Wert überschreitet (siehe Schwellenwerteinstellungen für die Generierung von Alerts und Ereignissen festlegen).

Schwellenwerteinstellungen für die Generierung von Alerts und Ereignissen festlegen

Sie können Schwellenwerteinstellungen für das Auslösen von Alerts und Ereignissen festlegen, wenn ein bestimmter Wert wie die Lebensdauer einer SSD in einem ThinkSystem- oder ThinkServer-Server eine Warnung oder einen kritischen Wert überschreitet.

Vorgehensweise

Gehen Sie wie folgt vor, um bestimmte Servicedateien an den Service Provider weiterzuleiten.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Überwachung → Alerts**, um die Seite Alerts anzuzeigen.

Schritt 2. Klicken Sie auf das Symbol **Schwellenwerteinstellungen** (), um das Dialogfeld „Schwellenwerteinstellungen“ anzuzeigen.

Schritt 3. Ändern Sie die Warn- und kritischen Schwellenwerte für die verbleibende Lebensdauer der SSDs in ThinkSystem- und ThinkServer-Servern.

Die verbleibende Lebensdauer der SSDs wird mit den SMART-Zählern der Hersteller berechnet. Die Standardwerte sind 30 % für den Warnungsschwellenwert und 20 % für den kritischen Schwellenwert.

Schritt 4. Wählen Sie Umschalt-Schaltfläche **Aktiviert** aus, um einen Alert und ein Ereignis zu generieren, wenn einer der beiden Schwellenwerte erreicht wird.

Schritt 5. Klicken Sie auf **Übernehmen**.

Automatische Problembenachrichtigung an den Lenovo-Support (Call-Home-Funktion) einrichten

Sie können mithilfe der Call-Home-Funktion-Funktion einen Service-Weiterleiter erstellen, der automatisch Servicedaten für jede beliebige verwaltete Einheit an den Lenovo-Support sendet. Dies dient der Problembehebung in Fällen, bei denen bestimmte wartungsfähige Ereignisse (z. B. ein nicht wiederherstellbarer Speicher) von bestimmten verwalteten Einheiten übermittelt werden. Dieser Service-Weiterleiter heißt „Standard-Call-Home-Funktion.“

Lenovo setzt sich für Ihre Sicherheit ein. Wenn diese Option aktiviert ist, Call-Home-Funktion Lenovo-Support Center wenn eine Einheit einen Hardwareausfall meldet oder Sie sich entscheiden, einen manuellen Call-Home-Funktion zu initiieren. Service Daten, die Sie normalerweise manuell auf die Lenovo Unterstützungswebsite hochladen, werden automatisch mit TLS 1.2 oder höher über HTTPS an Lenovo-Support Center gesendet. Ihre Geschäftsdaten werden nicht übertragen. Der Zugriff auf Servicedaten in Lenovo-Support Center ist auf autorisiertes Servicepersonal beschränkt.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an die Lenovo Unterstützung übertragen können.

Stellen Sie sicher, dass alle von Lenovo XClarity Administrator 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 Administrator.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen von Call-Home-Funktion hergestellt werden kann. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn XClarity Administrator 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 Netzwerkzugriff konfigurierenNetzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Wenn Sie Call-Home-Funktion konfiguriert haben, wird der **standardmäßige Lenovo Call-Home**-Service-Weiterleiter zur Seite Service-Weiterleiter hinzugefügt. Sie können diesen Weiterleiter bearbeiten, um zusätzliche Einstellungen zu konfigurieren, einschließlich der Geräte, die mit diesem Weiterleiter verknüpft werden sollen. Standardmäßig werden alle Geräte abgeglichen. Wenn keine vGeräte angegeben sind, leitet Call-Home-Funktion *keine* Problembenachrichtigungen an den Lenovo Support weiter.

Zu dieser Aufgabe

Mit einem *Service-Weiterleiter* wird festgelegt, an welchen Empfänger die Servicedatendateien nach einem aufgetretenen wartungsfähigen Ereignis gesendet werden sollen. Sie können bis zu 50 Service-Weiterleiter definieren.

- **Ist kein Call-Home-Funktion Service-Weiterleiter konfiguriert**, können Sie ein Service-Ticket manuell öffnen und Servicedateien an das Lenovo-Support Center übertragen. Folgen Sie dazu den Anweisungen unter Website für neue Serviceanforderung. Weitere Informationen über das Sammeln und den Download von Servicedateien finden Sie unter XClarity Administrator-Diagnosedateien herunterladen und Diagnosedateien für eine Einheit erfassen und herunterladen in der Onlinedokumentation von XClarity Administrator.
- **Sofern ein Call-Home-Funktion Service-Weiterleiter konfiguriert, aber nicht aktiviert ist**, können Sie ein Service-Ticket *manuell* mithilfe der Call-Home-Funktion-Funktion öffnen, um Servicedateien zu sammeln und an das Lenovo-Support Center zu senden. Weitere Informationen finden Sie unter Service-Ticket öffnen in der Onlinedokumentation von XClarity Administrator.
- **Wenn ein Call-Home-Funktion Service-Weiterleiters konfiguriert und aktiviert ist**, erfasst XClarity Administrator beim Auftreten eines wartungsfähigen Ereignisses *automatisch* Servicedaten, öffnet ein Service-Ticket und überträgt Servicedateien an das Lenovo-Support Center, damit das Problem behoben werden kann.

  Wichtig: Wenn Sie einen Call-Home-Funktion Service-Weiterleiter in Lenovo XClarity Administrator aktivieren, wird Call-Home-Funktion auf allen verwalteten Einheiten deaktiviert, damit keine doppelten Problemdatensätze generiert werden. Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden oder wenn Sie Call-Home-Funktion in XClarity Administrator deaktivieren möchten, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren – anstatt Call-Home-Funktion später auf jeder einzelnen Einheit erneut zu aktivieren. Weitere Informationen dazu, wie Sie Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren, wenn die Serviceweiterleitung für Call-Home-Funktion deaktiviert ist, finden Sie unter Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren in der Onlinedokumentation zu XClarity Administrator.Für Server mit XCC2 speichert XClarity Administrator Servicedaten in zwei Dateien im Repository.

  – **Servicedateien**. (.zip) Diese Datei enthält Serviceinformationen und Bestandsdaten in einem leicht lesbaren Format. Diese Datei wird automatisch an das Lenovo-Support Center gesendet, wenn ein wartungsfähiges Ereignis auftritt.

  – **Debugdatei**. (.tzz) Die Datei enthält alle Serviceinformationen, den Bestand und die Debugprotokolle für die Verwendung durch die Lenovo Unterstützung. Sie können diese Datei manuell an die Lenovo Unterstützung senden, wenn weitere Informationen zur Lösung eines Problems erforderlich sind.

  Bei anderen Einheiten speichert XClarity Administrator Servicedaten (einschließlich Serviceinformationen, Bestand und Debugprotokolle) in einer einzelnen Servicedatei im Repository. Diese Datei wird an das Lenovo-Support Center gesendet, wenn ein wartungsfähiges Ereignis auftritt.

  Obwohl XClarity Administrator Call-Home-Funktion für ThinkAgile und ThinkSystem Einheiten unterstützt, unterstützt der Baseboard Management Controller für manche ThinkAgile und ThinkSystem Einheiten kein Call-Home-Funktion. Daher können Sie die Call-Home-Funktion auf diesen Einheiten weder aktivieren noch deaktivieren. Die Call-Home-Funktion kann nur für diese Einheiten auf der Ebene XClarity Administrator aktiviert werden.

  Die Call-Home-Funktion wird für wiederholte Ereignisse für alle Einheiten unterdrückt, wenn bereits ein Service-Ticket für dieses Ereignis auf dieser Einheit erstellt wurde. Die Call-Home-Funktion wird auch für ähnliche Ereignisse für die ThinkAgile und ThinkSystem Einheiten unterdrückt, wenn bereits ein Service-Ticket für ein Ereignis auf dieser Einheit erstellt wurde. ThinkAgile und ThinkSystem Ereignisse sind Zeichenfolgen mit 16 Zeichen im folgenden Format *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (z. B. `806F010D0401FFFF`). Ereignisse ähneln sich, wenn Sie über denselben

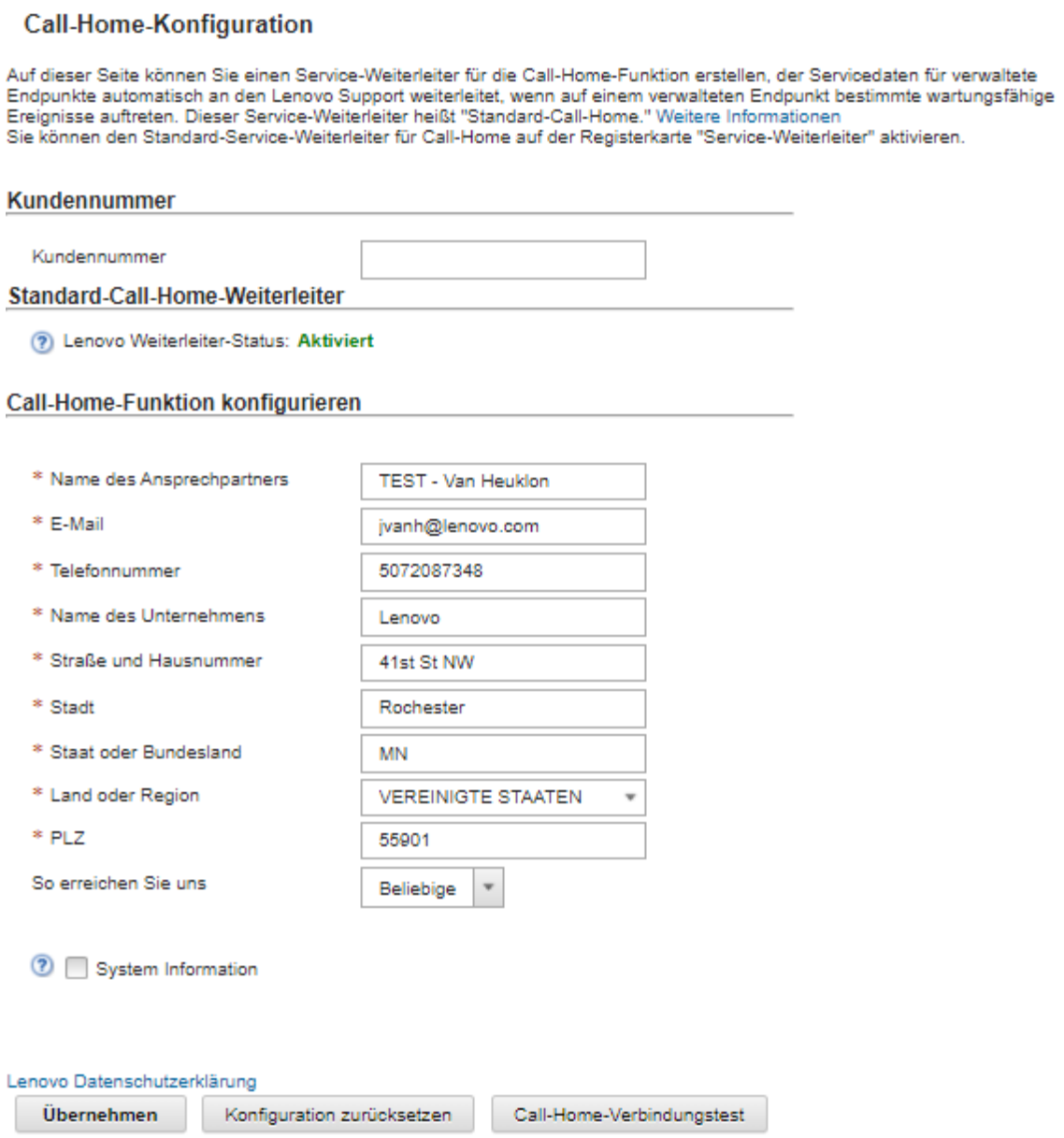
Lesetyp, denselben Sensortyp und dieselbe Entitäts-ID verfügen. Wenn z. B. auf einer bestimmten ThinkAgile oder ThinkSystem Einheit ein Service-Ticket für Ereignis 806F010D0401FFFF erstellt wurde, werden alle Ereignisse, die auf dieser Einheit mit Ereignis-IDs wie *xx*6F01*xx*04*xxxxxx* auftreten (wobei es sich bei *x* um irgendein alphanumerisches Zeichen handeln kann) unterdrückt.

Weitere Informationen über die Anzeige von Service-Tickets, die von einem Call-Home-Funktion Service-Weiterleiter automatisch geöffnet wurden, finden Sie unter Service-Tickets und Status anzeigen in der Onlinedokumentation von XClarity Administrator.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Service-Weiterleiter für Call-Home-Funktion einzurichten.

- Richten Sie Call-Home-Funktion für alle verwalteten Einheiten (aktuelle und zukünftige) ein:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.
  2. Klicken Sie im linken Navigationsbereich auf **Call-Home-Konfiguration**, um die Seite Call-Home-Konfiguration zu öffnen.



3. (Optional) Geben Sie die standardmäßige Lenovo Kundennummer an, die beim Melden von Problemen mit XClarity Administrator verwendet werden soll.

   Tipp: Ihre Kundennummer finden Sie in der E-Mail mit dem Berechtigungsnachweis, die Sie beim Kauf von Lenovo XClarity Pro erhalten haben.
4. Geben Sie die Kontakt- und Standortinformationen ein.
5. Wählen Sie die bevorzugte Kontaktmethode für die Lenovo Unterstützung aus.
6. (Optional) Geben Sie die Systeminformationen an.
7. Klicken Sie auf **Übernehmen**.

   Für die Call-Home-Funktion-Funktion wird unter Verwendung der angegebenen Kontaktinformationen ein Service-Weiterleiter mit dem Namen „Standard-Call Home“ für alle verwalteten Einheiten erstellt.
8. Aktivieren und testen Sie den Service-Weiterleiter „Standard-Call Home“.

a. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.

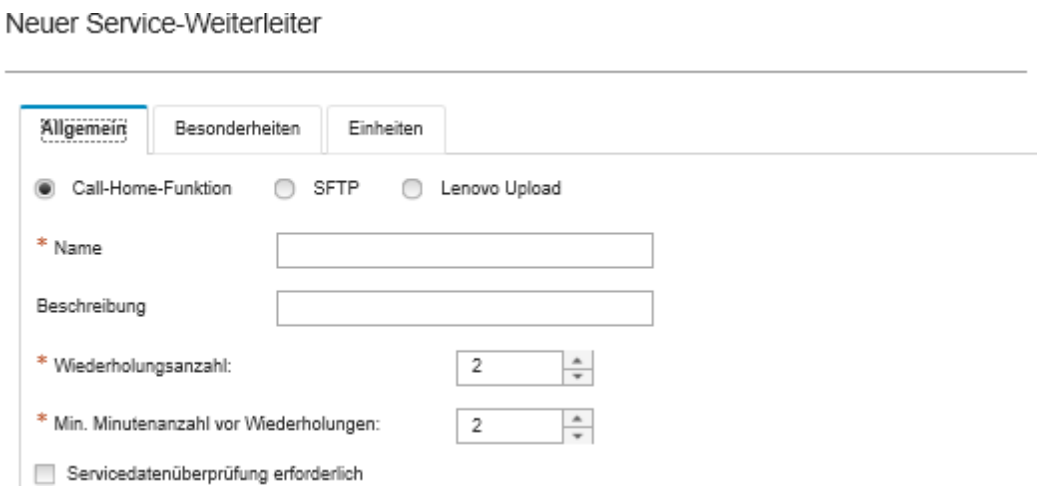
b. Wählen Sie **Aktivieren** in der Spalte **Status** des Service-Weiterleiters „Standard-Call Home“ aus.

c. Markieren Sie den Service-Weiterleiter „Standard-Call Home“ und klicken Sie auf **Service-Weiterleiter testen**, um ein Testereignis für den Service-Weiterleiter zu generieren und die Kommunikation zwischen der XClarity Administrator und dem Lenovo Unterstützungszentrum zu überprüfen.

Sie können den Testfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken.

Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

- Richten Sie Call-Home-Funktion für bestimmte verwaltete Einheiten ein:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.
  2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.
  3. Klicken Sie auf das Symbol **Service-Weiterleiter** erstellen ( ), um das Dialogfenster Neuer Service-Weiterleiter zu öffnen.
  4. Klicken Sie auf die Registerkarte **Allgemein**.



a. Wählen Sie die **Call-Home-Funktion** als Service-Weiterleiter aus:

b. Geben Sie den Namen des Service-Weiterleiters und eine Beschreibung ein.

c. Geben Sie an, wie häufig die automatische Benachrichtigung wiederholt werden soll. Der Standardwert ist 2.

d. Geben Sie an, wie viele Minuten zwischen den Wiederholungen verstreichen sollen. Der Standardwert ist 2.

e. (Optional) Klicken Sie auf **Servicedatenüberprüfung erforderlich**, wenn die Servicedatendateien vor dem Versenden überprüft werden sollen. Optional können Sie die E-Mail-Adresse des Kontakts angeben, der bei einer erforderlichen Prüfung der Servicedateien benachrichtigt werden soll.

  5. Klicken Sie auf die Registerkarte **Bestimmt** und geben Sie die Kontakt- und Systeminformationen an.

Tipp: Um dieselben Kontakt- und Standortinformationen zu verwenden, die auf der Seite „Call-Home-Konfiguration“ konfiguriert sind, wählen Sie im Dropdown-Menü **Konfiguration** die Option **Allgemeine Konfiguration** aus.

6. Klicken Sie auf die Registerkarte **Einheiten** und wählen Sie die verwalteten Einheiten und Ressourcengruppen aus, für die dieser Service-Weiterleiter Servicedateien weiterleiten soll.

   Tipp: Um Servicedateien für alle verwalteten Einheiten (derzeitige und künftige) weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Geräte abgleichen**.
7. Klicken Sie auf **Erstellen**. Der Service-Weiterleiter wird zur Seite Service und Support hinzugefügt.
8. Wählen Sie auf der Seite Service-Weiterleiter in der Spalte **Status** die Option **Aktivieren** aus, um den Service-Weiterleiter zu aktivieren.
9. Markieren Sie den Service-Weiterleiter und klicken Sie auf **Service-Weiterleiter testen**, um für den Service-Weiterleiter ein Testereignis zu generieren und die Kommunikation zwischen XClarity Administrator und dem Lenovo Unterstützungszentrum zu überprüfen.

   Sie können den Testfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken.

   Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

Nach dieser Aufgabe

Auf der Seite Service und Support können Sie zudem folgende Aktionen ausführen:

- Wenn die Option **Servicedatenüberprüfung erforderlich** ausgewählt ist und bei einer der verwalteten Einheiten dieses Service-Weiterleiters ein wartungsfähiges Ereignis aufgetreten ist, müssen Sie die Servicedateien prüfen, bevor diese an den Service Provider weitergeleitet werden. Weitere Informationen finden Sie unter Diagnosedaten an den Lenovo Support senden in der Onlinedokumentation von XClarity Administrator.
- Ermitteln Sie, ob die Call-Home-Funktion auf einer verwalteten Einheit aktiviert oder deaktiviert ist. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen** und überprüfen Sie den Status in der Spalte **Call-Home-Funktion-Status**.

  Tipp: Wenn „Status unbekannt“ in der Spalte **Call-Home-Funktion-Status** angezeigt wird, aktualisieren Sie den Webbrowser, damit der richtige Status angegeben wird.
- Definieren Sie die Support-Kontakt- und Standortinformationen einer bestimmten verwalteten Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Kontaktprofil erstellen** ( ) oder **Kontaktprofil bearbeiten** ( ). Die Kontakt- und Standortinformationen für die verwaltete Einheit werden in das Service-Ticket eingebunden, den dieCall-Home-Funktion an das Lenovo-Support Center sendet. Sofern eindeutige Kontakt- und Standortinformationen für eine verwaltete Einheit angegeben sind, werden diese in das Service-Ticket aufgenommen. Andernfalls werden die allgemeinen Informationen herangezogen, die für die XClarity AdministratorCall-Home-Funktion-Konfiguration angegeben sind (auf der Seite **Call-Home-FunktionKonfiguration** oder **Service-Weiterleiter**) angegeben sind. Siehe Lenovo-Support Center für weitere Informationen. Weitere Informationen finden Sie unter Support-Kontakte für eine Einheit definieren in der Onlinedokumentation von XClarity Administrator.
- Zeigen Sie die Service-Tickets an, die an das Lenovo-Support Center übermittelt wurden. Klicken Sie dazu im linken Navigationsbereich auf **Status des Service-Tickets**. Auf dieser Seite werden die automatisch oder manuell von einem Call-Home-Funktion Service-Weiterleiter geöffneten Service-Tickets, der Status sowie die Servicedateien angezeigt, die an das Lenovo-Support Center übertragen wurden. Weitere Informationen finden Sie unter Service-Tickets und Status anzeigen in der Onlinedokumentation von XClarity Administrator.
- Sammeln Sie die Servicedaten für eine bestimmte Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Servicedaten sammeln** ( ). Weitere Informationen finden Sie unter Diagnosedateien für eine Einheit erfassen und herunterladen in der Onlinedokumentation von XClarity Administrator.

- 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. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf **Alle Aktionen → Call-Home-Funktion manuell ausführen**.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.

  Weitere Informationen finden Sie unter Service-Ticket öffnen in der Onlinedokumentation von XClarity Administrator.
- Aktivieren Sie die Call-Home-Funktion wieder auf allen verwalteten Einheiten. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen** und anschließend auf **Alle Aktionen → Call-Home-Funktion auf allen Einheiten aktivieren**.

  Wenn Sie einen Call-Home-Funktion Service-Weiterleiter in Lenovo XClarity Administrator aktivieren, wird Call-Home-Funktion auf allen verwalteten Einheiten deaktiviert, damit keine doppelten Problemdatensätze generiert werden. Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden oder wenn Sie Call-Home-Funktion in XClarity Administrator deaktivieren möchten, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren – anstatt Call-Home-Funktion später auf jeder einzelnen Einheit erneut zu aktivieren.

  Weitere Informationen finden Sie unter Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren in der Onlinedokumentation von XClarity Administrator.

Automatische Problembenachrichtigung an einen bevorzugten Service Provider einrichten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Diagnosedateien für eine bestimmte Gruppe an verwalteten Einheiten automatisch an Ihren bevorzugten Service Provider gesendet werden (einschließlich der Lenovo Unterstützung, die Call-Home-Funktion verwendet), wenn bestimmte wartungsfähige Ereignisse von verwalteten Einheiten empfangen werden (wie ein nicht behebbaren Speicherfehler). Auf diese Weise kann das Problem behoben werden.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an die Lenovo Unterstützung übertragen können.

Stellen Sie sicher, dass alle von XClarity Administrator benötigten Ports (darunter auch die Ports, die für die Call-Home-Funktion erforderlich sind) zur Verfügung stehen, bevor Sie die einen Service-Weiterleiter konfigurieren. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen des Service Providers hergestellt werden kann.

Wenn Sie Lenovo-Support verwenden möchten, stellen Sie sicher, dass eine Verbindung zu den Internetadressen von Call-Home-Funktion hergestellt werden kann. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn XClarity Administrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss es sich um einen Non-Termination-Proxy handeln. Weitere Informationen über die Proxy-Einrichtung finden Sie unter Netzwerkzugriff konfigurierenNetzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Zu dieser Aufgabe

Mit einem *Service-Weiterleiter* wird festgelegt, an welchen Empfänger die Servicedatendateien nach einem aufgetretenen wartungsfähigen Ereignis gesendet werden sollen. Sie können bis zu 50 Service-Weiterleiter definieren.

Sie können für jeden Service-Weiterleiter automatisch Servicedaten an den Lenovo Support (*Call-Home-Funktion* genannt), an Ihren Lenovo Kundendiensttechniker mithilfe der Lenovo Upload-Funktionalität oder an einen anderen Service Provider senden. Informationen zum Einrichten eines Service-Weiterleiters für Call-Home-Funktion finden Sie unter Automatische Problembenachrichtigung an den Lenovo-Support (Call-Home-Funktion) einrichten und Automatische Problembenachrichtigung an einen bevorzugten Service Provider einrichten. Informationen zur Einrichten eines Service-Weiterleiters für die Lenovo Upload-Funktionalität finden Sie unter Automatische Problembenachrichtigung an die Lenovo Upload-Funktionalität in der Onlinedokumentation von XClarity Administrator.

Ist für SFTP ein Service-Weiterleiter konfiguriert und aktiviert, erfasst XClarity Administrator *automatisch* die Servicedatendateien und übermittelt sie an die angegebene SFTP-Site des bevorzugten Service Providers.

Für Server mit XCC2 speichert XClarity Administrator Servicedaten in zwei Dateien im Repository.

- **Servicedateien**. (.zip) Diese Datei enthält Serviceinformationen und Bestandsdaten in einem leicht lesbaren Format. Diese Datei wird automatisch an Ihren bevorzugten Service-Provider gesendet, wenn ein wartungsfähiges Ereignis auftritt.
- **Debugdatei**. (.tzz) Die Datei enthält alle Serviceinformationen, Bestand und Debugprotokolle zur Verwendung durch den Lenovo Support. Sie können diese Datei manuell an den Lenovo Support senden, wenn zusätzliche Informationen zur Problemlösung erforderlich sind.

Bei anderen Einheiten speichert XClarity Administrator Servicedaten (einschließlich Serviceinformationen, Bestand und Debugprotokolle) in einer einzelnen Servicedatei im Repository. Diese Datei wird an Ihren bevorzugten Service-Provider gesendet, wenn ein wartungsfähiges Ereignis auftritt.

Anmerkung: Falls die SFTP-Funktion bei mehreren Service-Weiterleitern für dieselbe Einheit konfiguriert ist, überträgt nur ein Service-Weiterleiter Servicedaten. Die verwendete Adresse und der verwendete Port hängen davon ab, welcher Service-Weiterleiter zuerst ausgelöst wird.

Vorgehensweise

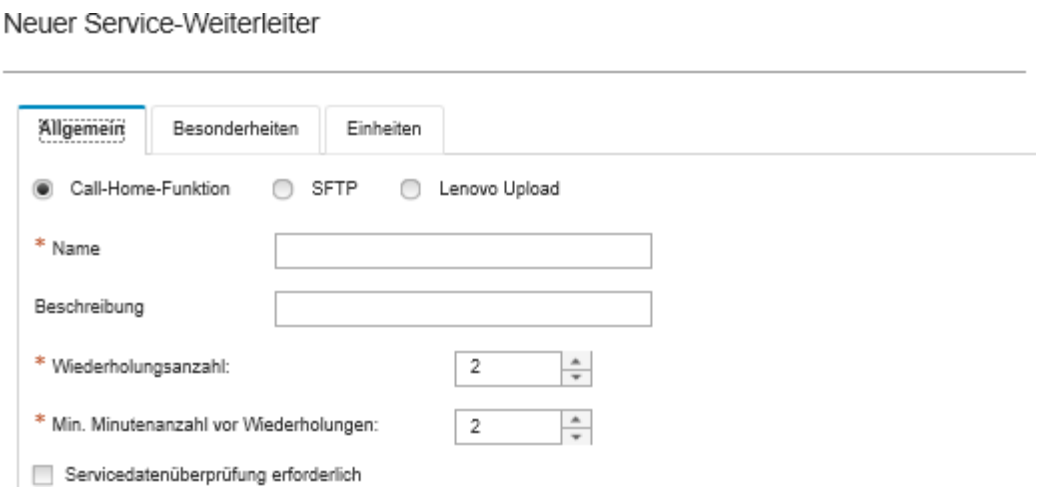
Gehen Sie wie folgt vor, um einen Service-Weiterleiter zu definieren und zu aktivieren.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite Service und Support wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.

Schritt 3. Klicken Sie auf das Symbol **Service-Weiterleiter erstellen** ( ), um das Dialogfenster Neuer Service-Weiterleiter zu öffnen.

Schritt 4. Klicken Sie auf die Registerkarte **Allgemein**.



1. Wählen Sie **SFTP** für den Service-Weiterleiter aus:
2. Geben Sie den Namen des Service-Weiterleiters und eine Beschreibung ein.
3. Geben Sie an, wie häufig die automatische Benachrichtigung wiederholt werden soll. Der Standardwert ist 2.
4. Geben Sie an, wie viele Minuten zwischen den Wiederholungen verstreichen sollen. Der Standardwert ist 2.
5. (Optional) Klicken Sie auf **Servicedatenüberprüfung erforderlich**, wenn die Servicedateien vor dem Versenden überprüft werden sollen. Optional können Sie die E-Mail-Adresse des Kontakts angeben, der bei einer erforderlichen Prüfung der Servicedatendateien benachrichtigt werden soll.

Schritt 5. Klicken Sie auf die Registerkarte **Bestimmt** und geben Sie die folgenden Informationen an:
- IP-Adresse und Portnummer des SFTP-Servers
- Benutzer-ID und Kennwort für die Authentifizierung am SFTP-Server

Schritt 6. Klicken Sie auf die Registerkarte **Einheit** und wählen Sie die verwalteten Einheiten und Ressourcengruppen aus, für die dieser Service-Weiterleiter Servicedaten weiterleiten soll.

Tipp: Um Servicedaten für alle verwalteten Einheiten (derzeitige und künftige) weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Geräte abgleichen**.

Schritt 7. Klicken Sie auf **Erstellen**. Der Service-Weiterleiter wird zur Seite Service und Support hinzugefügt.

Schritt 8. Wählen Sie auf der Seite Service und Support in der Spalte **Status** die Option **Aktivieren** aus, um den Service-Weiterleiter zu aktivieren.

Schritt 9. Um zu verhindern, dass wartungsfähige Ereignisse, die in der Liste der ausgeschlossenen Ereignisse aufgeführt sind, automatisch Problemberichte öffnen, wählen Sie **Nein** neben der Frage **Sollen bei ausgeschlossenen Ereignissen Problemberichte geöffnet werden?** aus.

Schritt 10. Markieren Sie den Service-Weiterleiter und klicken Sie auf **Service-Weiterleiter testen**, um für den Service-Weiterleiter ein Testereignis zu generieren und die Kommunikation zwischen XClarity Administrator und den einzelnen Service Providern zu überprüfen.

Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

Nach dieser Aufgabe

Auf der Seite Service und Support können Sie zudem folgende Aktionen ausführen:

- Wenn die Option **Servicedatenüberprüfung erforderlich** ausgewählt ist und bei einer der verwalteten Einheiten dieses Service-Weiterleiters ein wartungsfähiges Ereignis aufgetreten ist, müssen Sie die

Servicedateien prüfen, bevor diese an den Service Provider weitergeleitet werden. Weitere Informationen finden Sie unter Diagnosedateien überprüfen in der Onlinedokumentation von XClarity Administrator.

- Bearbeiten Sie die Informationen für den Service-Weiterleiter. Klicken Sie dazu im linken Navigationsbereich auf **Service-Weiterleiter** und dann auf das Symbol **Service-Weiterleiter bearbeiten** ( ).
- Aktivieren oder deaktivieren Sie einen Service-Provider. Klicken Sie dazu auf **Service-Weiterleiter** und wählen Sie in der Spalte **Status** entweder **Aktivieren** oder **Deaktivieren** aus.
- Löschen Sie den Service-Provider. Klicken Sie dazu auf **Service-Weiterleiter** und auf das Symbol **Service-Weiterleiter löschen** ( ).
- Definieren Sie die Support-Kontakt- und Standortinformationen einer bestimmten verwalteten Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Kontaktprofil erstellen** ( ) oder **Kontaktprofil bearbeiten** ( ). Die Kontakt- und Standortinformationen für die verwaltete Einheit werden in den Problemdatensatz eingebunden, der im Lenovo-Support Center von der Call-Home-Funktion erstellt wird. Sofern eindeutige Kontakt- und Standortinformationen für eine verwaltete Einheit angegeben sind, werden diese in den Problemdatensatz einbezogen. Andernfalls werden die allgemeinen Informationen herangezogen, die in XClarity Administrator in der Call-Home-Konfiguration angegeben sind (auf der Seite **Call-Home-Konfiguration** oder der Seite **Service-Weiterleiter**). Weitere Informationen finden Sie unter Support-Kontakte für eine Einheit definieren in der Onlinedokumentation von XClarity Administrator.
- Sammeln Sie die Servicedaten für eine bestimmte Einheit. Klicken Sie dazu auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Servicedaten sammeln** ( ). Weitere Informationen finden Sie unter Diagnosedateien für eine Einheit erfassen und herunterladen in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen über diese Service und Support-Aufgaben finden Sie unter Mit Service und Support arbeiten in der Onlinedokumentation von XClarity Administrator.

XClarity Administrator als Hub mit dem TruScale-Portal verbinden

Sie können Lenovo XClarity Administrator als Verwaltungshub mit dem Lenovo TruScale-Portal verbinden.

Vorbereitende Schritte

Achtung: Diese Konfigurationsschritte sind nur für Lenovo Service-Mitarbeiter vorgesehen.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Administrator als Verwaltungshub mit dem Lenovo TruScale-Portal zu verbinden.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Hub-Konfiguration**, um die Seite Hub-Konfiguration aufzurufen.

Schritt 2. Erstellen Sie einen Registrierungsschlüssel, indem Sie auf **Registrierungsanforderung generieren** klicken. Das Dialogfenster Registrierungsanforderung generieren wird angezeigt.

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

Schritt 4. Klicken Sie auf **Registrierungsschlüssel installieren**, um das Dialogfenster Registrierungsschlüssel installieren anzuzeigen.

Schritt 5. Fügen Sie den Registrierungsschlüssel in das Feld **Registrierungsschlüssel** ein.

Schritt 6. Klicken Sie auf **Senden**.

Nach dieser Aufgabe

Sie können den Registrierungsschlüssel deinstallieren, indem Sie auf **Konfiguration zurücksetzen** klicken.

Systemdaten und -einstellungen sichern, wiederherstellen und migrieren

Sie können Lenovo XClarity Administrator verwenden, um Systemdaten und -einstellungen und importierte Dateien wie Betriebssystem-Images, Firmwareaktualisierungen und BS-Einheitentreiber zu sichern und wiederherzustellen.

Lenovo XClarity Administrator sichern

Wenn bereits Sicherungsverfahren für virtuelle Hosts vorhanden sind, müssen Sie sicherstellen, dass Ihre Verfahren Lenovo XClarity Administrator einschließen.

Vorbereitende Schritte

Achtung: Achten Sie darauf, dass Sie alle aktiven Benutzer benachrichtigen, bevor Sie die Sicherung starten. XClarity Administrator ist während der Sicherung stillgelegt, um zu verhindern, dass Daten geändert werden. Daher können Sie nicht auf XClarity Administrator zugreifen, während die Sicherung durchgeführt wird.

Stellen Sie sicher, dass das Zertifizierungsstellenzertifikat über die virtuelle XClarity Administrator Einheit heruntergeladen und in Ihren Webbrowser importiert wurde (siehe Zertifizierungsstellenzertifikat in einen Webbrowser importieren).

Stellen Sie sicher, dass alle laufenden Jobs abgeschlossen sind und dass keine Jobs anstehen. Wenn gerade Jobs ausgeführt werden, können Sie die laufenden Jobs beenden und mit dem Erstellen der Sicherung fortfahren.

Stellen Sie sicher, dass die DNS-Server korrekt konfiguriert sind. Andernfalls funktionieren SMTP und NTP möglicherweise nach der Wiederherstellung der Sicherung nicht ordnungsgemäß.

Stellen Sie sicher, dass auf dem Verwaltungsserver genügend Speicherplatz für die Sicherung verfügbar ist. Wenn dies nicht der Fall ist, geben Sie Speicherplatz frei, indem Sie XClarity Administrator-Ressourcen löschen (einschließlich vorheriger Sicherungen, die nicht mehr benötigt werden; siehe Plattenspeicher verwalten) oder legen Sie fest, dass eine neue Sicherung ohne Betriebssystem-Images, Firmwareaktualisierungen und BS-Einheitentreibern erstellt wird.

Stellen Sie sicher, dass die BS-Implementierung auf der entsprechenden Netzwerkschnittstelle (eth1 oder eth0) konfiguriert ist, wenn Sie BS-Images sichern möchten (siehe Netzwerkzugriff konfigurieren).

Zu dieser Aufgabe

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

- Bevor Sie XClarity Administrator aktualisieren
- Wenn Sie neue Gehäuse oder Rack-Server verwalten
- Wenn Sie Benutzer zu XClarity Administrator hinzufügen
- Wenn Sie neue Konfigurationsmuster erstellen und implementieren

Stellen Sie sicher, dass Sie XClarity Administrator regelmäßig sichern.

Es wird empfohlen, Sicherungen auf Ihr lokales System herunterzuladen. Wenn das Hostbetriebssystem unerwartet herunterfährt, ist eine Authentifizierung bei XClarity Administrator eventuell nicht möglich,

nachdem das Hostbetriebssystem neu gestartet wurde. Sie können dieses Problem lösen, indem Sie XClarity Administrator aus der letzten Sicherung auf Ihr lokales System wiederherstellen (siehe Lenovo XClarity Administrator wiederherstellen.).

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Administrator zu sichern.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Daten sichern und wiederherstellen**. Die Seite „Daten sichern und wiederherstellen“ wird angezeigt.

Schritt 2. Klicken Sie auf das Symbol **Sichern** (). Das Dialogfenster Daten und Einstellungen sichern wird angezeigt.

Schritt 3. Geben Sie eine Beschreibung für diese Sicherung ein.

Schritt 4. Wählen Sie den Speicherort zum Erstellen der Sicherung aus. Dies kann das lokale Repository oder eine Remote-Freigabe sein.

Die Sicherung wird standardmäßig im lokalen Repository erstellt. Sie können eine Sicherung des lokalen Repository auf eine Remote-Freigabe kopieren, indem Sie auf das Symbol **Sicherung kopieren** () klicken.

Wenn Sie eine Remote-Freigabe auswählen, wird die Sicherung zunächst im lokalen Repository erstellt. Die Sicherung wird anschließend in die ausgewählte Remote-Freigabe kopiert und die lokale Kopie wird gelöscht. Weitere Informationen finden Sie unter Remote-Freigaben verwalten.

Schritt 5. Geben Sie optional an, dass Betriebssystem-Images, Firmwareaktualisierungen und Betriebssystem-Einheitentreiber enthalten sein sollen.

Schritt 6. Legen Sie den Verschlüsselungstext für die Sicherung fest.

Achtung: Notieren Sie sich den Verschlüsseltungstext. Der Verschlüsselungstext ist erforderlich, um die Sicherung auf dieser oder einer anderen XClarity Administrator-Instanz wiederherzustellen. Wenn Sie den Verschlüsselungstext vergessen, gibt es keine Möglichkeit, ihn wiederherzustellen.

Schritt 7. Klicken Sie auf **Sichern**, um Daten und Einstellungen sofort zu sichern, oder klicken Sie auf **Zeitplan**, um diese Sicherung geplant zu einem späteren Zeitpunkt auszuführen.

Achtung: Wenn Sie die Sicherung sofort starten, dürfen Sie die Registerkarte oder das Browserfenster nicht schließen oder aktualisieren, bevor der Prozess abgeschlossen ist. Andernfalls kann die Sicherung möglicherweise nicht erstellt werden.

Das Erstellen der Sicherung kann eine Weile dauern. Eine Fortschrittsleiste zeigt den Status der Jobs an.

Wenn Sie die Sicherung auf einer Remote-Freigabe erstellen, können Sie den Fortschritt auf der Seite „Jobs“ überwachen (siehe Jobs überwachen).

Wenn Sie eine Sicherung planen, wird der Verwaltungsserver während der Sicherung vorübergehend heruntergefahren. Nachdem der Verwaltungsserver wieder online ist, können Sie den Fortschritt der Sicherung auf der Seite „Jobs“ überwachen.

Schritt 8. Melden Sie sich bei XClarity Administrator an, um mit der Verwaltung Ihrer Einheiten fortzufahren.

Nach dieser Aufgabe

Auf der Seite „Daten sichern und wiederherstellen“ können Sie die folgenden Aktionen ausführen:

- Sie können XClarity Administrator-Sicherungen von oder auf eine Remote-Freigabe kopieren. Klicken Sie dazu auf das Symbol **Sicherung kopieren** ().
- Löschen Sie ausgewählte Sicherungen, die nicht mehr benötigt werden, aus dem lokalen Repository oder von der Remote-Freigaben, indem Sie auf das Symbol **Sicherung löschen** () klicken.
- Wiederherstellen von Systemdaten und -einstellungen auf diesem Verwaltungsserver (siehe Lenovo XClarity Administrator wiederherstellen).
- Importieren oder exportieren Sie Sicherungen vom lokalen System, indem Sie auf das Symbol **Sicherung importieren** () oder **Sicherung exportieren** () klicken.
- Weiterleiten von ausgewählten Sicherungen zu einer neuen XClarity Administrator-Instanz (siehe Systemdaten und -einstellungen auf eine andere XClarity Administrator-Instanz migrieren).

Lenovo XClarity Administrator wiederherstellen

Sie können gesicherten Daten und Einstellungen verwenden, um Lenovo XClarity Administrator in einen vorherigen Zustand wiederherzustellen.

Vorbereitende Schritte

Achtung: Achten Sie darauf, dass Sie alle aktiven Benutzer benachrichtigen, bevor Sie die Sicherung starten. XClarity Administrator ist während der Sicherung stillgelegt, um zu verhindern, dass Daten geändert werden. Daher können Sie nicht auf XClarity Administrator zugreifen, während die Sicherung durchgeführt wird

Laden Sie das Zertifizierungsstellenzertifikat über die virtuelle XClarity Administrator-Einheit herunter und importieren Sie das Zertifikat im Webbrowser (siehe Zertifizierungsstellenzertifikat in einen Webbrowser importieren).

Stellen Sie sicher, dass alle laufenden Jobs abgeschlossen sind und dass keine Jobs anstehen.

Sie können eine Sicherung nur zur selben XClarity Administrator-Version wiederherstellen, die zum Erstellen der Sicherung verwendet wurde.

Zu dieser Aufgabe

Achtung:

- Dabei werden alle Änderungen seit Erstellen der Sicherung gelöscht.
- Zum Wiederherstellen der Daten wird die virtuelle Einheit in ihren ursprünglichen bereinigten Zustand zurückgesetzt. Alle aktuellen Einstellungen, Einheitenbestände und Dateien (Betriebssystem-Images, Firmwareaktualisierungen und BS-Einheitentreiber) werden vor dem Wiederherstellen der Sicherungsdaten gelöscht. Daten und Einstellungen aus der Sicherung werden nicht mit den aktuellen Daten und Einstellungen der virtuellen Einheit kombiniert. Wenn Sie Einheitenbestand, Betriebssystem-Images, Firmwareaktualisierungen und BS-Einheitentreiber nicht wiederherstellen möchten, sind nach Abschluss der Wiederherstellung nur die standardmäßigen XClarity Administrator-Daten vorhanden.

Das Wiederherstellen einer Sicherung löscht keine Sicherungen in der XClarity Administrator-Instanz.

Das Wiederherstellen einer Sicherung ändert keine Daten oder Einstellungen auf den verwalteten Einheiten. Wenn Sie z. B. die Verwaltung einer Einheit aufheben und dann eine vorherige Sicherung wiederherstellen, bei der die Einheit noch mit XClarity Administrator verwaltet wurde, können nach Abschluss der Wiederherstellung Verbindungsprobleme mit dieser Einheit auftreten. Dasselbe gilt, wenn Sie eine Einheit verwalten und dann eine vorherige Sicherung wiederherstellen, bei der die Einheit noch nicht verwaltet wurde. In diesem Fall müssen Sie möglicherweise die Konfiguration der Einheit manuell bearbeiten, um den

Verwaltungsstatus rückgängig zu machen, oder die Option **Erzwingen** verwenden, wenn Sie versuchen, sie erneut in XClarity Administrator zu verwalten.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Administrator wiederherzustellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Daten sichern und wiederherstellen**. Die Seite „Daten sichern und wiederherstellen“ wird angezeigt.

Schritt 2. Gehen Sie wie folgt vor, wenn Sie das Sicherungspaket in Ihr lokales System exportiert und von XClarity Administrator gelöscht haben.

a. Klicken Sie auf der Seite „Daten sichern und wiederherstellen“ auf das Symbol **Sicherung importieren** (), um das Dialogfenster „Sicherung importieren“ anzuzeigen.

b. Klicken Sie auf **Durchsuchen**, um die Sicherung zu finden, die Sie von einer XClarity Administrator-Instanz exportiert haben.

c. Klicken Sie auf **Importieren**, um die Sicherung auf dem Ziel-XClarity Administrator hochzuladen.

Das Importieren der Sicherung kann eine Weile dauern. Eine Fortschrittsleiste zeigt den Status der Jobs an.

Achtung: Wenn Sie die Registerkarte oder das Browserfenster schließen oder aktualisieren, bevor der Prozess abgeschlossen ist, schlägt der Prozess möglicherweise fehl.

d. Wenn der Import abgeschlossen ist, geben Sie den Verschlüsselungstext der Sicherung ein.

Anmerkung: Wenn Sie nicht über den Verschlüsselungstext verfügen, müssen Sie eine neue Sicherung in XClarity Administrator erstellen (siehe Lenovo XClarity Administrator sichern).

Schritt 3. Wählen Sie die Sicherung aus, die wiederhergestellt werden soll, und klicken Sie auf das Symbol **Sicherung wiederherstellen** (). Das Dialogfenster Daten wiederherstellen wird angezeigt.

Schritt 4. Legen Sie den Verschlüsselungstext für die Sicherung fest.

Schritt 5. Klicken Sie auf **Bestätigen**.

Schritt 6. Überprüfen Sie im Dialogfenster „Datenwiederherstellung bestätigen“, dass alle Informationen korrekt sind.

Schritt 7. Im Dialogfenster „Wiederherstellungsoptionen“ können Sie optional festlegen, dass auch Betriebssystem-Images, Firmwareaktualisierungen, BS-Einheitentreiber, Netzwerkeinstellungen und Einheitenbestand importiert werden sollen.

Achtung: Lesen Sie sorgfältig alle Warnungen, die in diesem Dialogfenster angezeigt werden.

Schritt 8. Klicken Sie auf **Bestätigen**, um mit der Datenwiederherstellung zu beginnen.

Das Wiederherstellen von Daten und Einstellungen kann eine Weile dauern. Eine Fortschrittsleiste zeigt den Status der Jobs an.

Wenn die Wiederherstellung der Daten abgeschlossen ist, werden Sie zur Anmeldeseite umgeleitet.

Achtung: Wenn Sie die Registerkarte oder das Browserfenster schließen oder aktualisieren, bevor der Prozess abgeschlossen ist, schlägt der Prozess möglicherweise fehl.

Schritt 9. Melden Sie sich bei XClarity Administrator an, um mit der Verwaltung Ihrer Einheiten fortzufahren.

Systemdaten und -einstellungen auf eine andere XClarity Administrator-Instanz migrieren

Sie können die gesicherten Systemdaten und -einstellungen auf eine neue Lenovo XClarity Administrator-Instanz migrieren, die sich im selben oder einem anderen Netzwerk befindet.

Vorbereitende Schritte

Der Zielverwaltungsserver muss eine *neue* XClarity Administrator-Instanz mit derselben Version wie der Verwaltungsserver sein, der zum Erstellen der Sicherung verwendet wurde, und muss sich im Assistenten für die Erstkonfiguration befinden, ohne dass bereits Schritte abgeschlossen wurden. Weitere Informationen finden Sie unter XClarity Administrator installieren und einrichten in der Onlinedokumentation von XClarity Administrator.

Achten Sie darauf, dass Sie alle aktiven Benutzer benachrichtigen, bevor Sie die Sicherung starten. XClarity Administrator ist während der Sicherung stillgelegt, um zu verhindern, dass Daten geändert werden. Daher können Sie nicht auf XClarity Administrator zugreifen, während die Sicherung durchgeführt wird.

Laden Sie das Zertifizierungsstellenzertifikat über XClarity Administrator herunter und importieren Sie das Zertifikat im Webbrowser (siehe Plattenspeicher verwalten in der Onlinedokumentation von XClarity Administrator).

Sicherungen im Sicherungs-Repository des Quellverwaltungsservers werden nicht auf den Zielverwaltungsserver migriert. Exportieren Sie vor der Migration von Dateien und Einstellungen alle Sicherungen auf Ihr lokales System, die Sie benötigen könnten.

Zu dieser Aufgabe

Alle Änderungen am Quellverwaltungsserver, die nach dem Erstellen der Sicherung durchgeführt wurden, werden nicht auf den Zielverwaltungsserver migriert.

Das Wiederherstellen einer Sicherung ändert keine Daten oder Einstellungen auf den verwalteten Einheiten. Wenn Sie z. B. die Verwaltung einer Einheit aufheben und dann eine vorherige Sicherung wiederherstellen, bei der die Einheit noch mit XClarity Administrator verwaltet wurde, können nach Abschluss der Wiederherstellung Verbindungsprobleme mit dieser Einheit auftreten. Dasselbe gilt, wenn Sie eine Einheit verwalten und dann eine vorherige Sicherung wiederherstellen, bei der die Einheit noch nicht verwaltet wurde. In diesem Fall müssen Sie möglicherweise die Konfiguration der Einheit manuell bearbeiten, um den Verwaltungsstatus rückgängig zu machen, oder die Option **Erzwingen** verwenden, wenn Sie versuchen, sie erneut in XClarity Administrator zu verwalten.

Anmerkungen: Wenn XClarity Administrator als Container ausgeführt wird, können die auf dem Host für den einen Container erstellten Datenträger von einem anderen Container als Datenträger verwendet werden. Nachdem die Datenträger an den neuen (Ziel-)Container gebunden wurden, können sie nicht mehr vom ursprünglichen (Quell-)Container verwendet werden.

1. Konfigurieren Sie die Datei `docker-compose.yml` so, dass der Zielcontainer dieselbe IP-Adresse und denselben Containernamen wie der Quellcontainer verwendet.
2. Stoppen Sie den Quellcontainer mit dem folgenden Befehl.
   ```
   docker-compose -p ${CONTAINER_NAME} down
   ```
3. Starten Sie den Zielcontainer mit dem folgenden Befehl. Dabei ist <*env_filename*> der Name der Datei mit Umgebungsvariablen. Wenn der Zielcontainer gestartet wird, werden die Datenträger an den XClarity Administrator Zielcontainer gebunden und XClarity Administrator verwendet Systemdaten und -einstellungen von diesen Datenträgern.
   COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <`*ENV_FILENAME*`> up -d`

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Administrator wiederherzustellen.

Schritt 1. Wenn Quell- und Ziel-XClarity Administrator sich im selben Netzwerk befinden, führen Sie die folgenden Schritte aus.

a. Klicken Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Daten sichern und wiederherstellen**. Die Seite „Daten sichern und wiederherstellen“ wird angezeigt.

b. Klicken Sie auf das Symbol **Sicherung weiterleiten** (), um das Dialogfenster „Daten weiterleiten“ anzuzeigen.

c. Geben Sie die aktuelle IP-Adresse des Ziel-XClarity Administrator an.

d. Klicken Sie auf **Fortfahren**, um die Sicherung auf dem Ziel-XClarity Administrator hochzuladen.

Das Hochladen der Sicherung kann eine Weile dauern. Eine Fortschrittsleiste zeigt den Status der Jobs an.

Achtung: Wenn Sie die Registerkarte oder das Browserfenster schließen oder aktualisieren, bevor der Prozess abgeschlossen ist, wird das Paket möglicherweise nicht hochgeladen.

Schritt 2. Wenn Quell- und Ziel-XClarity Administrator sich *nicht* im selben Netzwerk befinden, führen Sie die folgenden Schritte aus.

a. Klicken Sie in der Menüleiste des Quell-XClarity Administrator auf **Verwaltung → Daten sichern und wiederherstellen**. Klicken Sie auf der Seite „Daten sichern und wiederherstellen“ auf das Symbol **Sicherung exportieren** (), um die Sicherung auf Ihr lokales System zu exportieren.

Das Exportieren der Sicherung kann eine Weile dauern.

b. Kopieren Sie die exportierte Sicherung des Quellverwaltungsservers auf ein System im selben Netzwerk wie der Zielverwaltungsserver.

c. Klicken Sie auf der Assistentenseite des Ziel-XClarity Administrator auf das Symbol **Sicherung importieren** (), um das Dialogfenster „Datenpaket importieren“ anzuzeigen.

d. Klicken Sie auf **Durchsuchen**, um die Sicherung zu finden, die Sie vom Quell-XClarity Administrator exportiert haben.

e. Klicken Sie auf **Hochladen**, um die Sicherung auf dem Ziel-XClarity Administrator zu importieren.

Das Importieren der Sicherung kann eine Weile dauern. Eine Fortschrittsleiste zeigt den Status der Jobs an.

Achtung: Wenn Sie die Registerkarte oder das Browserfenster schließen oder aktualisieren, bevor der Prozess abgeschlossen ist, schlägt der Prozess möglicherweise fehl.

Schritt 3. Wenn der Import abgeschlossen ist, geben Sie den Verschlüsselungstext der Sicherung ein.

Anmerkung: Wenn Sie nicht über den Verschlüsselungstext verfügen, müssen Sie eine neue Sicherung im Quell-XClarity Administrator erstellen (siehe Lenovo XClarity Administrator sichern).

Schritt 4. Überprüfen Sie im Dialogfenster „Datenwiederherstellung bestätigen“, dass alle Informationen korrekt sind.

Schritt 5. Klicken Sie auf **Bestätigen**, um mit dem Laden von Systemdaten und -einstellungen zu beginnen.

Schritt 6. Im Dialogfenster „Wiederherstellungsoptionen“ können Sie optional festlegen, dass auch Betriebssystem-Images, Firmwareaktualisierungen, BS-Einheitentreiber, Netzwerkeinstellungen und Einheitenbestand importiert werden sollen.

Achtung: Lesen Sie sorgfältig alle Warnungen, die in diesem Dialogfenster angezeigt werden.

Schritt 7. Wenn Sie Netzwerkeinstellungen oder Einheitenbestand importieren möchten, fahren Sie den Quellverwaltungsserver des Quell-XClarity Administrator herunter, indem Sie **Verwaltung → Verwaltungsserver herunterfahren → Herunterfahren** auswählen.

Überprüfen Sie, dass die virtuelle Quelleinheit vor dem Fortfahren heruntergefahren wurde.

Schritt 8. Klicken Sie beim Ziel-XClarity Administrator auf **Bestätigen**, um mit dem Laden von Daten und Einstellungen aus dem Paket zu beginnen.

Wenn Sie Netzwerkeinstellungen importieren möchten, werden nach Abschluss der Migration die IP-Adressen des Quell-XClarity Administrator dem Ziel-XClarity Administrator neu zugewiesen.

Achtung: Wenn das Quell-XClarity Administrator DHCP verwendet, müssen Sie die MAC-Adressen des Ziel-XClarity Administrator mit den entsprechenden IP-Adressen des Quell-XClarity Administrator beim DHCP-Server verknüpfen. Warten Sie nach einer Veränderung des DHCP-Servers mindestens 15 Minuten, bevor Sie fortfahren.

Schritt 9. Warten Sie, bis der Fortschrittsbalken „Daten und Einstellungen aus dem Paket laden“ voll ist.

Wenn die Migration der Daten abgeschlossen ist, werden Sie zur Anmeldeseite umgeleitet.

Achtung: Wenn Sie die Registerkarte oder das Browserfenster schließen oder aktualisieren, bevor der Prozess abgeschlossen ist, schlägt der Prozess möglicherweise fehl.

Schritt 10. Melden Sie sich beim Ziel-XClarity Administrator an, um mit der Verwaltung Ihrer Einheiten fortzufahren.

Plattenspeicher verwalten

Sie können den von Lenovo XClarity Administrator belegten Festplattenspeicher verwalten, indem Sie große Datendateien verschieben, die nicht unmittelbar für eine Remote-Freigabe erforderlich sind, oder indem Sie nicht mehr benötigte Ressourcen löschen.

Zu dieser Aufgabe

Um festzustellen, wie viel Plattenspeicherplatz derzeit verwendet wird, klicken Sie der Menüleiste von XClarity Administrator auf **Dashboard**. Die Speicherplatzbelegung im Repository und Remote-Freigaben wird im Aktivitätsabschnitt von XClarity Administrator aufgeführt.

Vorgehensweise

Führen Sie einen oder mehrere der folgenden Schritte aus, um Speicherplatz freizugeben, indem Sie Dateien zu einer Remote-Freigabe verschieben und nicht benötigte Ressourcen löschen.

- **Nicht mehr benötigte Ressourcen löschen**

  Sie können Dateien, die nicht mehr benötigt werden, schnell aus dem lokalen Repository löschen, indem Sie die folgenden Schritte ausführen.

  1. Wählen Sie in der XClarity Administrator-Menüleiste **Verwaltung → Datenträger bereinigen** aus, um die Seite Datenträger bereinigen anzuzeigen.
  2. Wählen Sie die Dateien aus, die Sie löschen möchten. Die Überschrift des Abschnitts gibt an, wie viel Speicherplatz freigegeben wird, wenn die Dateien gelöscht werden.

- **Betriebssystembezogene Dateien**

  Sie können BS-Images, Bootoptionsdateien und Softwaredateien löschen.

- **Firmwareaktualisierungen**

  Sie können Nutzlastdateien für alle BS-Einheitentreiber löschen, die mit UpdateXpress System Packs (UXSPs) verknüpft sind, sowie einzelne Einheitentreiber, die sich im Status „Heruntergeladen“ befinden.

  Sie können Nutzlastdateien für einzelne Firmwareaktualisierungen löschen, die sich im Status „Heruntergeladen“ befinden und nicht in einer Firmwarekonformitätsrichtlinie verwendet werden.

  Sie können Nutzlastdateien für Verwaltungsserveraktualisierungen löschen, die den Status „Heruntergeladen“ aufweisen.

  Anmerkung: Wenn sich das Repository für Firmwareaktualisierungen auf einer Remote-Freigabe befindet, können Sie die Datenträgerbereinigungsfunktion nicht verwenden, um einzelne Firmwareaktualisierungen und UXSPs zu löschen.

- **Servicedatendateien**

  Wenn ein Service-Ereignis auf einer Einheit auftritt, werden automatisch Servicedaten für diese Einheit erfasst. Servicedaten werden automatisch immer dann für den Verwaltungsserver erfasst, wenn eine Ausnahme im XClarity Administrator auftritt. Wenn XClarity Administrator und die verwalteten Einheiten ordnungsgemäß funktionieren, sollten Sie diese Archive in regelmäßigen Abständen löschen.

  Wenn Verwaltungsserveraktualisierungen erfolgreich ausgeführt werden, werden die Aktualisierungsdateien automatisch aus dem Repository entfernt.

3. Klicken Sie auf **Ausgewählte löschen**.
4. Überprüfen Sie die Liste der ausgewählten Dateien und klicken Sie auf **Löschen**.

- **Firmwareaktualisierungspakete zu einem Remote-Repository verschieben**

  Standardmäßig verwendet Lenovo XClarity Administrator ein lokales (internes) Repository zum Speichern von Firmwareaktualisierungen. Sie können Speicherplatz freigeben, der für das lokale XClarity Administrator Repository zur Verfügung steht, indem Sie eine angehängte Remote-Freigabe über das SSH File System (SSHFS) als Remote-Repository verwenden. Sie können dann Firmwareaktualisierungsdateien direkt aus dem Remote-Repository verwenden, um die Firmwarekonformität auf Ihren Einheiten zu erhalten. Weitere Informationen hierzu finden Sie unter Remote-Repository für Firmwareaktualisierungen verwenden.

  Wenn Sie die Position des Firmwareaktualisierungs-Repositorys ändern, können Sie festlegen, dass alle Firmwareaktualisierungen aus dem ursprünglichen Repository in das neue Repository kopiert werden.

  Die Firmwareaktualisierungsdateien im ursprünglichen Repository werden nach dem Wechseln der Positionen *nicht* automatisch gelöscht.

  Tipp: Das Repository für Remote-Aktualisierungen kann von mehreren XClarity Administrator Verwaltungsservern gemeinsam genutzt werden.

  Gehen Sie wie folgt vor, um Firmwareaktualisierungen in ein Remote-Firmwareaktualisierungs-Repository zu verschieben.

  1. Fügen Sie eine Remote-Freigabe zu XClarity Administrator hinzu (siehe Remote-Freigaben verwalten).
  2. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Repository**. Die Seite Repository für Firmwareaktualisierungen wird angezeigt.

3. Klicken Sie auf **Alle Aktionen → Repository-Position wechseln**, um das Dialogfeld „Repository-Position wechseln“ anzuzeigen.
4. Wählen Sie die gerade erstellte Remote-Freigabe aus der Dropdown-Liste **Repository-Position** aus.
5. Wählen Sie **Aktualisierungspakete aus aktuellem Repository in neues Repository kopieren** aus, um die Firmwareaktualisierungsdateien in die neue Repository-Position zu kopieren, bevor die Repository-Position gewechselt wird.
6. Klicken Sie auf **OK**.

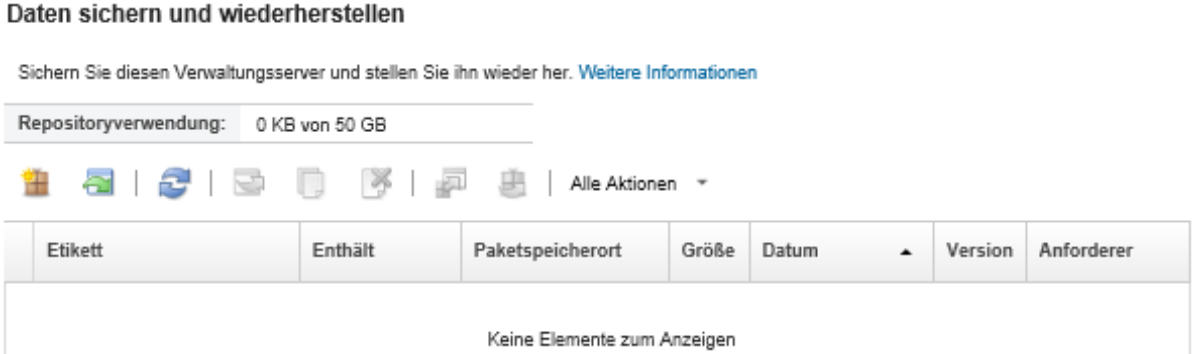
   Es wird ein Job erstellt, um Firmwareaktualisierungspakete in das neue Repository zu kopieren. Sie können den Jobfortschritt überwachen, indem Sie in der XClarity Administrator-Menüleiste auf **Überwachung → Jobs** klicken.
7. Bereinigen Sie die Firmwareaktualisierungsdateien im lokalen Repository.
   a. Wechseln Sie die Position zum lokalen Repository, indem Sie auf **Alle Aktionen → Repository-Position wechseln** klicken und **Lokales Repository** als Repository-Position auswählen. Klicken Sie dann auf **OK**.
   b. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen**, klicken Sie auf das Kontrollkästchen „Alle auswählen“ in der Tabelle, um alle Firmwareaktualisierungen auszuwählen, und klicken Sie dann auf das Symbol **Vollständige Aktualisierungspakete löschen** ( ).
   c. Klicken Sie auf die Registerkarte **UpdateXpress System Pack (UXSP)**, klicken Sie auf das Kontrollkästchen „Alle auswählen“ in der Tabelle, um alle UXSPs auszuwählen, und klicken Sie dann auf das Symbol **UXSP und zugehörige Richtlinie löschen** ( ).
   d. Wechseln Sie die Position zurück zum Remote-Repository, indem Sie auf **Alle Aktionen → Repository-Position wechseln** klicken und das neue Remote-Repository als Repository-Position auswählen. Klicken Sie dann auf **OK**.

- **XClarity Administrator-Sicherungsdateien zu einer Remote-Freigabe verschieben**

  Sie können Festplattenspeicher, der für das lokale Repository von XClarity Administrator zur Verfügung steht, freigeben. Verschieben Sie dazu XClarity Administrator-Sicherungen zu einer Remote-Freigabe. Sie können die Dateien allerdings nicht direkt auf der Remote-Freigabe verwenden. Um die Dateien zu verwenden, müssen Sie sie zurück in das lokale Repository von XClarity Administrator verschieben. Weitere Informationen zu Remote-Freigaben finden Sie unter Remote-Freigaben verwalten.

  Wichtig: Es wird empfohlen, Sicherungen vor dem Löschen der Sicherungen in XClarity Administrator auf Ihr lokales System herunterzuladen oder Sicherungen auf eine Remote-Freigabe zu kopieren.

  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Daten sichern und wiederherstellen**, um die Seite Daten sichern und wiederherstellen anzuzeigen.



  Die Spalte **Paketposition** zeigt an, ob die Sicherung entweder im lokalen Repository von XClarity Administrator oder auf einer Remote-Freigabe gespeichert ist.

2. Wählen Sie die Sicherung aus und klicken Sie auf das Symbol **Sicherung kopieren** (), um das Dialogfeld Sicherung kopieren anzuzeigen.
3. Wählen Sie die Remote-Freigabe für die Sicherung aus.
4. Klicken Sie auf **Kopieren**.
5. Sie können den Kopierfortschritt auf der Seite Jobs überwachen. Wenn der Kopiervorgang abgeschlossen ist, wählen Sie die Sicherung erneut aus und klicken Sie auf das Symbol **Sicherung löschen** (), um das Dialogfeld Sicherung löschen anzuzeigen.
6. Wählen Sie „Lokal“ als Position aus.
7. Klicken Sie auf **Löschen**.

Remote-Freigaben verwalten

Sie können Remote-Freigaben anhängen und dann große Datendateien, z. B. Lenovo XClarity Administrator Sicherungen und Firmwareaktualisierungen, aus dem lokalen Repository in die Remote-Freigabe verschieben, um Festplattenspeicher zu verwalten, der für den Verwaltungsserver zur Verfügung steht.

Vorbereitende Schritte

Wenn XClarity Administrator als Container ausgeführt wird, werden Remote-Freigaben während der Installation mithilfe der YML-Datei an den Container angehängt (siehe XClarity Administrator in VMware ESXi-basierten Umgebungen installieren in der XClarity Administrator Onlinedokumentation).

Wenn XClarity Administrator als virtuelle Einheit ausgeführt wird, müssen Sie die **lxc-supervisor**-Berechtigung haben, um eine Remote-Freigabe anhängen oder abhängen zu können.

Stellen Sie sicher, dass eine stabile, schnelle Netzwerkverbindung zwischen dem Dateiserver und XClarity Administrator besteht.

Wird XClarity Administrator als Container ausgeführt, werden Remote-Freigaben nicht unterstützt.

Zu dieser Aufgabe

Sie müssen separate Remote-Freigaben verwenden, um XClarity Administrator Sicherungen und Firmwareaktualisierungen zu speichern.

Sie können die XClarity Administrator Sicherungsdateien nicht direkt aus der Remote-Freigabe verwenden. Um die Sicherungsdateien zu verwenden, müssen Sie sie zurück in das lokale Repository verschieben.

Derzeit wird nur SSHFS unterstützt.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Remote-Freigabe beim Ausführen von XClarity Administrator als virtuelle Einheit hinzuzufügen.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Remote-Freigabe**. Die Seite Remote-Freigabe wird angezeigt.
2. Klicken Sie auf das Symbol **Erstellen** (), um eine Remote-Freigabe zu erstellen. Das Dialogfenster Remote-Freigabe erstellen wird angezeigt.
3. Geben Sie die IP-Adresse des Dateiservers an, der die Remote-Freigabe hostet.
4. Geben Sie die gespeicherten Anmeldeinformationen für den Zugriff auf die Remote-Freigabe an.

Tipp: Informationen zum Erstellen von gespeicherten Anmeldeinformationen finden Sie unter Gespeicherte Anmeldeinformationen verwalten.

5. Geben Sie für die Verwendung mit der Remote-Freigabe den Mountpunkt (lokales Verzeichnis) auf dem Verwaltungsserver an.

   Wichtig: Der Pfad muss mit „/mnt“ beginnen.
6. Geben Sie zum Anhängen als Remote-Freigabe auf dem Verwaltungsserver das gemeinsam genutzte Verzeichnis (Remote-Server-Pfad) an.
7. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

- Hängen Sie die Remote-Freigabe ab, indem Sie die Remote-Freigabe auswählen und auf das Symbol **Löschen** ( ) klicken.
- Verschieben Sie XClarity Administrator Sicherungsdateien von einer und in eine Remote-Freigabe (siehe Plattenspeicher verwalten).
- Konfigurieren Sie XClarity Administrator für die Verwendung einer Remote-Freigabe als Firmwareaktualisierungs-Repository (siehe Remote-Repository für Firmwareaktualisierungen verwenden).

Die Sprache der Benutzerschnittstelle ändern

Sie können die Sprache der Benutzerschnittstelle ändern, nachdem Sie sich angemeldet haben.

Vorgehensweise

Klicken Sie in der Lenovo XClarity Administrator-Titelleiste auf das Benutzeraktionen-Menü (ADMIN_USER) und anschließend auf **Sprache ändern**. Wählen Sie die Sprache aus, die Sie anzeigen möchten, und klicken Sie dann auf **Schließen**.

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

Herunterfahren von XClarity Administrator

Wenn Lenovo XClarity Administrator herunterfährt, geht die Verbindung zu Lenovo XClarity Administrator verloren.

Vorbereitende Schritte

Sie müssen die Berechtigung **lxc-supervisor** oder **lxc-admin** haben, um eine XClarity Administrator virtuelle Einheit herunterfahren zu können.

Stellen Sie sicher, dass aktuell keine Jobs laufen. Alle aktuell laufenden Jobs werden beim Herunterfahren abgebrochen. Weitere Informationen zum Anzeigen des Jobprotokolls finden Sie unter Jobs überwachen.

Vorgehensweise

So fahren Sie Lenovo XClarity Administrator herunter:

- **Container**

  Führen Sie den folgenden Befehl aus, um den Container zu stoppen.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```

- **Virtuelle Einheiten**
  1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Verwaltung → Verwaltungsserver herunterfahren**.

     Ein Bestätigungsdialog mit einer Liste von aktuell ausgeführten Jobs wird angezeigt. Wenn Sie XClarity Administrator herunterfahren, werden diese Jobs abgebrochen.
  2. Klicken Sie auf **Herunterfahren**.

Nach dieser Aufgabe

Informationen dazu, wie Sie XClarity Administrator nach dem Herunterfahren erneut starten, finden Sie unter Neustart von XClarity Administrator.

Neustart von XClarity Administrator

Sie können Lenovo XClarity Administrator nach dem Herunterfahren über die Webschnittstelle oder über den Hypervisor neu starten.

Vorbereitende Schritte

Sie müssen die Berechtigung **lxc-supervisor** oder **lxc-admin** haben, um XClarity Administrator neu starten zu können.

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.

Zu dieser Aufgabe

Es gibt verschiedene Situationen, in denen ein Neustart von Lenovo XClarity Administrator erforderlich ist:
- Bei der Wiederherstellung eines Serverzertifikats
- Beim Hochladen eines neuen Serverzertifikats

Vorgehensweise

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

- **Container**

  Führen Sie die folgenden Befehle aus, um den Container zu stoppen und dann zu starten. Dabei ist *<env_filename>* der Name der Datei mit Umgebungsvariablen.

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

- **Virtuelle Einheiten**
  - Neustart von Lenovo XClarity Administrator über die Webschnittstelle:
    1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Verwaltungsserver herunterfahren**.

       Ein Bestätigungsdialog mit einer Liste von aktuell ausgeführten Jobs wird angezeigt. Wenn Sie Lenovo XClarity Administrator neu starten, werden diese Jobs abgebrochen.
    2. Klicken Sie auf **Neu starten**.

       Wenn Lenovo XClarity Administrator herunterfährt, geht die Verbindung zu Lenovo XClarity Administrator verloren.

3. Warten Sie einige Minuten auf den Neustart von Lenovo XClarity Administrator. Melden Sie sich dann wieder an.

– Neustart von Lenovo XClarity Administrator über den Hypervisor nach einem Herunterfahren:
  – 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 **Starten**. Beim Start der virtuellen Maschine werden die IPv4- und IPv6-Adressen für die einzelnen Schnittstellen aufgeführt, wie im folgenden Beispiel dargestellt.

       Der eth0-Verwaltungsport von XClarity Administrator verwendet standardmäßig eine DHCP-IP-Adresse. Am Ende des Bootprozesses von XClarity Administrator können Sie eine statische IP-Adresse für den eth0-Verwaltungsport festlegen, indem Sie nach der Aufforderung „1“ eingeben, wie im folgenden Beispiel dargestellt. Die Eingabeaufforderung ist 150 Sekunden verfügbar, bis der Anmeldedialog angezeigt wird. Wenn Sie sofort zum Anmeldedialog fortfahren möchten, geben Sie bei der Eingabeaufforderung „x“ ein.

       Wichtig:

       - Wenn Sie die statischen IP-Adresseneinstellungen ändern, haben Sie maximal 60 Sekunden Zeit, um die neuen Einstellungen vorzunehmen. Stellen Sie sicher, dass Sie über die erforderlichen IP-Informationen verfügen, bevor Sie fortfahren.
         – Für die IPv4-Einstellungen müssen Sie die IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse haben.
         – Für die IPv6-Einstellungen müssen Sie die IP-Adresse und die Länge des Präfixes haben.
       - Falls Sie keinen DHCP-Server nutzen, können Sie eine Konfigurationsdatei verwenden, um die IP-Einstellungen für den eth0-Verwaltungsport von XClarity Administrator anzugeben, mit dem auf XClarity Administrator zugegriffen werden soll. Weitere Informationen finden Sie im Abschnitt „Nächste Schritte“ weiter unten.
       - Wenn Sie die IP-Adresseinstellungen über die Konsole ändern, wird XClarity Administrator neu gestartet, damit die neuen Einstellungen angewendet werden.
       - Für die Anmeldung ist keine Aktion erforderlich. Die Nachricht für die Konsolenanmeldung können Sie ignorieren. Die Konsolenschnittstelle ist nicht zur Verwendung durch den Kunden geeignet.
       - Möglicherweise wird die Nachricht `TCP: eth0: Treiber hat eine vermutete GRO-Implementierung, die TCP-Leistung ist möglicherweise beeinträchtigt` auf der Konsole angezeigt. Die Leistung der virtuellen Maschine ist nicht betroffen, Sie können diese Warnung ignorieren.

       Achtung: Das Ändern der IP-Adresse des Verwaltungsports von XClarity Administrator nach der Verwaltung von Einheiten kann dazu führen, dass die Einheiten in XClarity Administrator in den Offlinestatus versetzt werden. Wenn Sie die IP-Adresse ändern möchten, sobald XClarity Administrator betriebsbereit ist, stellen Sie sicher, dass die Verwaltung aller Einheiten aufgehoben wird, bevor Sie die IP-Adresse ändern.

```
------------------------------------------
Lenovo XClarity Administrator  Version x.x.x
------------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0
```

```
eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Melden Sie sich bei Lenovo XClarity Administrator an (siehe Bei XClarity Administrator anmelden).

– VMware ESXi

1. Stellen Sie über VMware vSphere Clientdie Verbindung zum Host her.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Ein/Aus → Einschalten**.
3. Klicken Sie auf die Registerkarte **Konsole**. Beim Start der virtuellen Maschine werden die IPv4- und IPv6-Adressen für die einzelnen Schnittstellen aufgeführt, wie im folgenden Beispiel dargestellt.

   Der eth0-Verwaltungsport von XClarity Administrator verwendet standardmäßig eine DHCP-IP-Adresse. Am Ende des Bootprozesses von XClarity Administrator können Sie eine statische IP-Adresse für den eth0-Verwaltungsport festlegen, indem Sie nach der Aufforderung „1“ eingeben, wie im folgenden Beispiel dargestellt. Die Eingabeaufforderung ist 150 Sekunden verfügbar, bis der Anmeldedialog angezeigt wird. Wenn Sie sofort zum Anmeldedialog fortfahren möchten, geben Sie bei der Eingabeaufforderung „x“ ein.

   Wichtig:

   - Wenn Sie die statischen IP-Adresseneinstellungen ändern, haben Sie maximal 60 Sekunden Zeit, um die neuen Einstellungen vorzunehmen. Stellen Sie sicher, dass Sie über die erforderlichen IP-Informationen verfügen, bevor Sie fortfahren.
     – Für die IPv4-Einstellungen müssen Sie die IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse haben.
     – Für die IPv6-Einstellungen müssen Sie die IP-Adresse und die Länge des Präfixes haben.
   - Falls Sie keinen DHCP-Server nutzen, können Sie eine Konfigurationsdatei verwenden, um die IP-Einstellungen für den eth0-Verwaltungsport von XClarity Administrator anzugeben, mit dem auf XClarity Administrator zugegriffen werden soll. Weitere Informationen finden Sie im Abschnitt „Nächste Schritte“ weiter unten.
   - Wenn Sie die IP-Adresseinstellungen über die Konsole ändern, wird XClarity Administrator neu gestartet, damit die neuen Einstellungen angewendet werden.
   - Für die Anmeldung ist keine Aktion erforderlich. Die Nachricht für die Konsolenanmeldung können Sie ignorieren. Die Konsolenschnittstelle ist nicht zur Verwendung durch den Kunden geeignet.
   - Möglicherweise wird die Nachricht `TCP: eth0: Treiber hat eine vermutete GRO-Implementierung, die TCP-Leistung ist möglicherweise beeinträchtigt` auf der Konsole angezeigt. Die Leistung der virtuellen Maschine ist nicht betroffen, Sie können diese Warnung ignorieren.

   Achtung: Das Ändern der IP-Adresse des Verwaltungsports von XClarity Administrator nach der Verwaltung von Einheiten kann dazu führen, dass die Einheiten in XClarity Administrator in den Offlinestatus versetzt werden. Wenn Sie die IP-Adresse ändern möchten, sobald XClarity

Administrator betriebsbereit ist, stellen Sie sicher, dass die Verwaltung aller Einheiten aufgehoben wird, bevor Sie die IP-Adresse ändern.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Melden Sie sich bei Lenovo XClarity Administrator an (siehe Bei XClarity Administrator anmelden).

Nach dieser Aufgabe

Beim Neustart sammelt Lenovo XClarity Administrator 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.

Kapitel 3. Einheiten und Aktivitäten überwachen

Sie können Einheiten und Aktivitäten über das Dashboard, Alerts und Prüfprotokolle sowie Jobprotokolle überwachen.

Übersicht über Ihre Umgebung anzeigen

Das Dashboard zeigt den Status aller verwalteten Einheiten, eine Übersicht aller bereitstellungsbezogenen Tasks und Informationen zu Lenovo XClarity Administrator-Ressourcen und -Aktivitäten an.

Weitere Informationen: XClarity Administrator: Überwachung

Vorgehensweise

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Dashboard**.

Schritt 2. Erweitern Sie den Hardwarestatus, den Bereitstellungsstatus oder den Abschnitt mit Administratoraktivitäten, um weitere Informationen zu dem entsprechenden Bereich zu erhalten.

Übersicht über Ihren Hardwarestatus anzeigen

Im Abschnitt „Hardwarestatus“ wird der Status aller verwalteten Einheiten angezeigt.

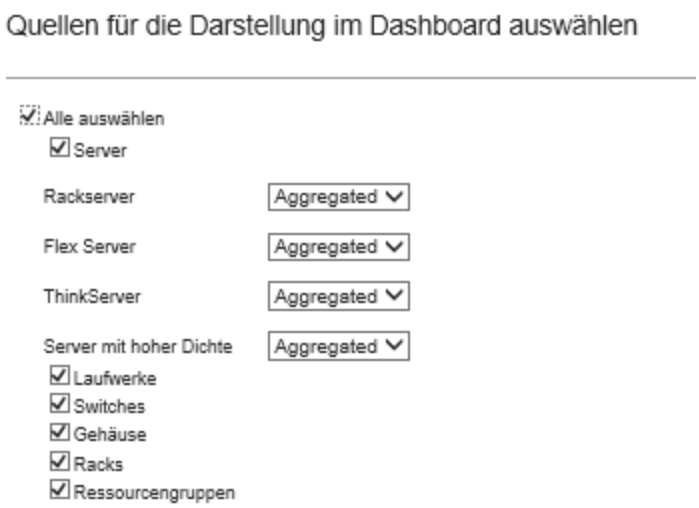
Vorgehensweise

Weitere Informationen zu allen Einheiten dieses Typs erhalten Sie, indem Sie auf die Nummer unter dem entsprechenden Einheitentyp klicken.

Um ausführliche Informationen nur für Einheiten dieses Typs und mit diesem Status anzuzeigen, klicken Sie auf das Symbol oder die Nummer neben dem Symbol für den Status.

- **Server**. Zeigt die Gesamtzahl der von XClarity Administrator verwalteten Server (Rechenknoten, Rack-Server und Tower-Server) sowie die Anzahl der Server mit dem Status „Normal“, „Warnung“ bzw. „Kritisch“ an. Siehe Den Status eines verwalteten Servers anzeigen für weitere Informationen.
- **Speicher**. Zeigt die Gesamtzahl der von XClarity Administrator verwalteten Speichereinheiten sowie die Anzahl der Speichereinheiten mit dem Status „Normal“, „Warnung“ bzw. „Kritisch“ an. Siehe Status von Speichereinheiten anzeigen für weitere Informationen.
- **Switches**. Zeigt die Gesamtzahl der von XClarity Administrator verwalteten RackSwitch- und Flex System-Switches sowie die Anzahl der Switches mit dem Status „Normal“, „Warnung“ bzw. „Kritisch“ an. Weitere Informationen hierzu finden Sie im Abschnitt Status von Switches anzeigen
- **Gehäuse**. Zeigt die Gesamtzahl der von XClarity Administrator verwalteten Flex-Gehäuse sowie die Anzahl der Flex-Gehäuse mit dem Status „Normal“, „Warnung“ bzw. „Kritisch“ an. Siehe Den Status eines verwalteten Gehäuses anzeigen für weitere Informationen.
- **Racks**. Zeigt die Anzahl der in XClarity Administrator erstellten Racks sowie die Anzahl der Racks mit Einheiten an, die „Normal“, „Warnung“ bzw. „Kritisch“ als höchsten Status aufweisen. Siehe Status von Einheiten in einem Rack anzeigen für weitere Informationen.
- **Ressourcengruppen**. Zeigt die Anzahl der Ressourcengruppen an, die von XClarity Administrator verwaltet werden, sowie die Anzahl der Ressourcengruppen mit Einheiten an, die „Normal“, „Warnung“ bzw. „Kritisch“ als höchsten Status aufweisen. Siehe Status von Einheiten in einer Ressourcengruppe anzeigen für weitere Informationen.

Um die Hardwareressourcen anzupassen, die im Dashboard angezeigt werden, klicken Sie auf das Symbol **Anpassen** (). Sie können die Einheitentypen auswählen, die ein- oder ausgeblendet werden sollen. Sie können auch auswählen, ob Server in einer einzigen Zusammenfassung aggregiert, separate Übersichten für jeden Servertyp (Rack- und Tower-, Flex System-, ThinkServer- und NeXtScale-Server) angezeigt oder bestimmte Arten von Servern ausgelassen werden sollen.



Übersicht über Ihren Bereitstellungsstatus anzeigen

Der Abschnitt „Bereitstellungsstatus“ bietet eine Übersicht über alle Tasks, die mit der Bereitstellung von Einheiten in Zusammenhang stehen.

Vorgehensweise

- **Konfigurationsmuster**. Zeigt Details zur Anzahl der Server mit Profilen an, einschließlich der folgenden Statistiken.

  Anmerkung: Wenn der Verwaltungsserver nicht lizenzkonform ist, sind alle Werte 0 (siehe Lizenz für den vollständigen Funktionsumfang installieren in der Onlinedokumentation von XClarity Administrator).

  – Die Anzahl der Server, die mit ihrem Serverprofil kompatibel sind. Sie können auf die Zahl klicken, um die Seite „Konfigurationsmuster: Serverprofile“ mit einer Liste der konformen Server anzuzeigen.

  – Die Anzahl der Server, die nicht mit ihrem Serverprofil kompatibel sind. Sie können auf die Zahl klicken, um die Seite „Konfigurationsmuster: Serverprofile“ mit einer Liste der nicht konformen Server anzuzeigen.

  – Die Anzahl der Geräte, für die der Konformitätsstatus unbekannt ist. Sie können auf die Zahl klicken, um die Seite „Konfigurationsmuster: Serverprofile“ mit einer Liste der Server mit unbekannter Konformität anzuzeigen.

    Anmerkung: Der Compliance-Status ist unbekannt, typischerweise nach einer teilweisen Profilbereitstellung, wenn Lenovo XClarity Administrator die Konfigurationsinformationen nicht vom Server erfasst hat. Aktualisieren Sie das Serverinventar oder besuchen Sie die Seite mit den Details zum Serverprofil erneut, um das Erfassen von Konfigurationsinformationen vom Server zu erzwingen.

  – Die Anzahl der Server, denen ein Serverprofil zugewiesen ist. Sie können auf die Zahl klicken, um die Seite „Konfigurationsmuster: Serverprofile“ mit einer Liste der Server mit Profil anzuzeigen.

  – Die Anzahl der Server, denen kein Serverprofil zugewiesen ist. Sie können auf die Zahl klicken, um die Seite „Konfigurationsmuster: Servermuster“ mit einer Liste der Servermuster anzuzeigen, die auf Servern ohne Profil implementiert werden können.

  – Die Anzahl der Servermuster, die derzeit implementiert werden.

  Klicken Sie zur Anzeige von Trenddaten für Konfigurationsmuster auf **Trenddaten anzeigen** (siehe Trends im Bereitstellungsstatus überwachen).

  Weitere Informationen zu Konfigurationsmustern und Serverprofilen finden Sie unter Server mithilfe von Konfigurationsmustern konfigurieren.

- **Betriebssystem-Images**. Zeigt Details zu Betriebssystemimplementierungen einschließlich der folgenden Statistiken an.

  Anmerkung: Wenn der Verwaltungsserver nicht lizenzkonform ist, sind alle Werte 0 (siehe Lizenz für den vollständigen Funktionsumfang installieren in der Onlinedokumentation von XClarity Administrator).

  – Die Anzahl der BS-Images im Repository. Sie können auf die Zahl klicken, um die Seite „Betriebssysteme implementieren: BS-Images verwalten“ mit einer Liste der Betriebssysteme anzuzeigen.

  – Die Anzahl der aktuell laufenden BS-Implementierungen. Sie können auf die Zahl klicken, um die Seite „Betriebssysteme implementieren: BS-Images bereitstellen“ mit einer Liste der Einheiten anzuzeigen, für die ein Betriebssystem installiert wird.

- **Firmwareaktualisierungen**. Zeigt Details zu Firmwareaktualisierungen an, einschließlich der folgenden Statistiken.

  – Die Anzahl der konformen Einheiten. Sie können auf die Nummer klicken, um die Seite „Firmwareaktualisierungen: Übernehmen/Aktivieren“ mit einer Liste der konformen Einheiten anzuzeigen.

  – Die Anzahl der nicht konformen Einheiten. Sie können auf die Nummer klicken, um die Seite „Firmwareaktualisierungen: Übernehmen/Aktivieren“ mit einer Liste der nicht konformen Einheiten anzuzeigen.

  – Die Anzahl von Einheiten, denen keine Firmwarekonformitätsrichtlinie zugeordnet ist. Sie können auf die Nummer klicken, um die Seite „Firmwareaktualisierungen: Übernehmen/Aktivieren“ mit einer Liste der Einheiten ohne Konformitätsrichtlinie anzuzeigen.

    Über diese Seite können Sie jeder Einheit eine Firmwarekonformitätsrichtlinie zuweisen, indem Sie in der Spalte **Zugeordnete Konformitätsrichtlinie** eine Richtlinie auswählen.

  – Die Anzahl der Einheiten, für die keine Aktualisierungen unterstützt werden. Sie können auf die Nummer klicken, um die Seite „Firmwareaktualisierungen: Übernehmen/Aktivieren“ mit einer Liste der Einheiten anzuzeigen, für die keine Aktualisierungen unterstützt werden.

  – Die Anzahl der laufenden Aktualisierungen.

  – Die Anzahl der Einheiten mit ausstehender Firmware. Sie können auf die Nummer klicken, um die Seite „Firmwareaktualisierungen: Übernehmen/Aktivieren“ mit einer Liste der Einheiten anzuzeigen, für die Aktualisierungen mit ausstehender Aktivierung vorhanden sind.

  Klicken Sie zur Anzeige von Trenddaten für Firmwareaktualisierungen auf **Trenddaten anzeigen** (siehe Trends im Bereitstellungsstatus überwachen).

  Weitere Informationen zu Firmwareaktualisierungen und Konformitätsrichtlinien finden Sie unter Firmware auf verwalteten Einheiten aktualisieren.

Übersicht über Lenovo XClarity Administrator-Aktivitäten anzeigen

Im Aktivitätsabschnitt von XClarity Administrator werden Informationen zu aktiven Jobs, aktiven Sitzungen und Systemressourcen in XClarity Administrator angezeigt.

Vorgehensweise

- **Jobs**. Zeigt die Anzahl der aktiven Jobs an, die derzeit ausgeführt werden. Weitere Informationen zu Jobs finden Sie unter Jobs überwachen.
- **Aktive Sitzungen**. Zeigt die Benutzer-ID und die IP-Adresse für jede aktive XClarity Administrator-Sitzung an. Weitere Informationen zu Benutzern finden Sie unter Benutzeraccounts verwalten.
- **Ressourcennutzung**. Zeigt die Prozessorauslastung, Speicherbelegung und Datenträgerkapazität auf dem Hostsystem und Remote-Dateifreigaben an. Weitere Informationen zu Systemressourcen finden Sie unter Systemressourcen überwachen.

Systemressourcen überwachen

Sie können die Prozessorbelegung, die Speicherauslastung und die Datenträgerkapazität auf dem Hostsystem über die Seite „Dashboard“ ermitteln.

Vorbereitende Schritte

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

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

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

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

Anmerkungen:

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

Vorgehensweise

Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Dashboard**.

Die Ressourcenauslastung auf dem Hostsystem wird im Aktivitätsabschnitt von XClarity Administrator aufgeführt.

Prozessor

Das Nutzungsmaß gibt die Anzahl der XClarity Administrator-Prozesse an, die gleichzeitig auf die Prozessoren auf dem Host zugreifen.

Tipp: Das Nutzungsmaß kann gelegentlich auf „Hoch“ oder „Sehr hoch“ ansteigen. Wenn die Auslastung länger als 30 Minuten auf diesem Niveau bleibt, sollten Sie im Jobprotokoll überprüfen, ob laufende Jobs durchgeführt werden (siehe Jobs überwachen).

Das Gesamtkapazitätsmaß gibt die Anzahl der Prozessoren an, die auf dem Host verfügbar sind.

Hauptspeicher

Das Nutzungsmaß gibt die Speichermenge an, die aktuell von XClarity Administrator verwendet wird.

Das Gesamtkapazitätsmaß gibt die Gesamtkapazität des verfügbaren Speichers auf dem Host an.

Benutzerdaten

Das Nutzungsmaß gibt den Plattenspeicherplatz an, der aktuell von XClarity Administrator auf dem Hostsystem verwendet wird.

Das Gesamtkapazitätsmaß gibt die Gesamtkapazität des Speichers (verwendet und nicht verwendet) an, der für Benutzerdaten reserviert ist, z. B. Betriebssysteme und Firmwareaktualisierungen.

Weitere Informationen zum Verwalten von Festplattenspeicher finden Sie unter Plattenspeicher verwalten.

Achtung: Wenn die zugeordneten Ressourcen nicht ausreichen, um die aktuelle Anzahl an verwalteten Einheiten bei guter Leistung zu verarbeiten, sollten Sie die Ressourcenzuordnung erhöhen. Weitere Informationen zu den empfohlenen Hardwareanforderungen basierend auf der Anzahl der verwalteten Einheiten in Ihrer Umgebung finden Sie unter Unterstützte Hostsysteme in der Onlinedokumentation von XClarity Administrator.

Trends im Bereitstellungsstatus überwachen

Lenovo XClarity Administrator erfasst regelmäßig den Bereitstellungsstatus für alle verwalteten Einheiten, einschließlich Konformität und aktiven Jobs für Firmwareaktualisierungen und Konfigurationsmuster, damit Sie Trends für einen bestimmten Zeitraum überwachen können.

Zu dieser Aufgabe

Sie müssen die Berechtigung **lxc-admin** oder **lxc-supervisor** haben, um Trenddaten anzeigen zu können.

Die folgenden Daten werden gesammelt:

- **Firmwareaktualisierungen**
  - **Konforme Einheiten**. Anzahl der Einheiten, die mit ihrer Firmwarekonformitätsrichtlinie konform sind.
  - **Nicht konforme Einheiten**. Anzahl der Einheiten, die nicht mit ihrer Firmwarekonformitätsrichtlinie konform sind.
  - **Einheiten ohne Richtlinien**. Anzahl der Einheiten, denen keine Firmwarekonformitätsrichtlinie zugeordnet ist.
  - **Nicht für Aktualisierung unterstützte Einheiten**. Anzahl der Einheiten, für die keine Firmwareaktualisierungen unterstützt werden.
  - **Aktualisierungen in Bearbeitung**. Anzahl der Einheiten, für die keine Firmwareaktualisierungen in Bearbeitung sind.
- **Konfigurationsmuster**
  - **Server mit Profilen**. Anzahl der Einheiten, denen ein Serverprofil zugewiesen ist.
  - **Server ohne Profile**. Anzahl der Einheiten, denen kein Serverprofil zugewiesen ist.
  - **Konforme Server**. Anzahl der Einheiten, die mit ihrem zugewiesenen Serverprofil kompatibel sind.
  - **Nicht konforme Server**. Anzahl der Einheiten, die nicht mit ihrem zugewiesenen Serverprofil konform sind.
  - **Servermuster in Bearbeitung**. Anzahl der Einheiten, für die Aktualisierungen des Konfigurationsmuster in Bearbeitung sind.

Vorgehensweise

Gehen Sie wie folgt vor, um Trends im Bereitstellungsstatus anzuzeigen.

Schritt 1. Wählen Sie in der XClarity Administrator-Menüleiste **Dashboard** aus, um die Seite Dashboard anzuzeigen.

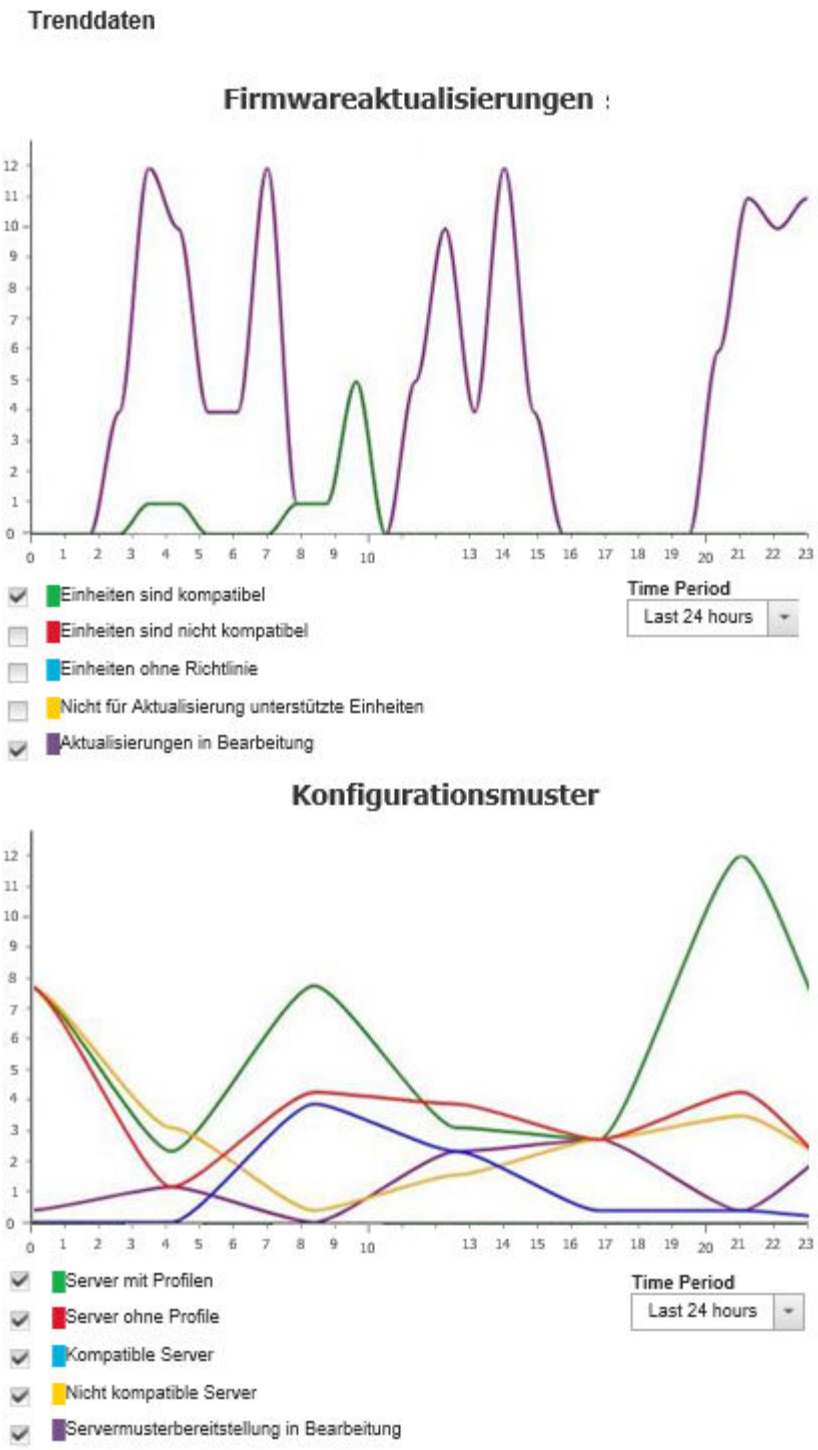
Schritt 2. Klicken Sie auf den Link **Trenddaten**, um das Dialogfenster „Schwellenwerteinstellungen“ anzuzeigen.

Schritt 3. Wählen oder blenden Sie Daten aus, um die gewünschten Daten anzuzeigen.

Schritt 4. Wählen Sie den Zeitraum aus, den Sie anzeigen möchten.

- **24 Stunden**. Zeigt die Daten der vergangenen 24 Stunden an. Jeder Datenpunkt gibt den Durchschnittswert eines Zeitraums von 1 Stunde an.
- **1 Monat**. Zeigt die Daten der vergangenen 30 Tage an. Jeder Datenpunkt gibt den Durchschnittswert eines Zeitraums von 24 Stunden an.

Die Trenddaten werden als Diagramm für den ausgewählten Zeitraum angezeigt.



Metrikenverlauf überwachen

Lenovo XClarity Administrator erfasst regelmäßig Metrikdaten für verwaltete ThinkSystem und ThinkAgile Einheiten, damit Sie den aktuellen Status Ihrer Umgebung analysieren können.

Vorbereitende Schritte

Historische Metriken werden nur für ThinkSystem Server (außer SR635, SR645, SR655 und SR665) unterstützt.

Es werden nur SSDs in ThinkAgile und ThinkSystem Servern (außer SR635 und SR655) unterstützt, auf denen die XCC-Firmware ausgeführt wird, die nach April 2019 veröffentlicht wurde.

Integrierte SATA-Treiber werden nicht unterstützt.

NVMe-Laufwerke müssen die Spezifikation NVMe Management Interface (NVMe-MI) unterstützen.

Zu dieser Aufgabe

Die folgenden Metriken werden erfasst.

- **SSD-Überwachung** Diese Berichtskarte enthält die folgenden Statistiken und Diagramme.
  - Die Gesamtzahl der SSDs in den verwalteten Einheiten (je nach Bereich)
  - Die Anzahl der analysierten SSDs
  - Die Anzahl der SSDs, die nicht analysiert werden können
  - Ein Kreisdiagramm mit der Anzahl der Einheiten mit SSDs, deren verbleibende Lebensdauer in einem bestimmten Bereich liegt
    - Verbleibende Lebensdauer ≤ 10 %. Anzahl der SSDs mit 10 % oder weniger verbleibender Lebensdauer
    - Verbleibende Lebensdauer 11–50 %. Anzahl der SSDs mit 11–50 % verbleibender Lebensdauer
    - Verbleibende Lebensdauer 51–100 %. Anzahl der SSDs mit mehr als 50 % verbleibender Lebensdauer
- **Systemauslastung** Diese Berichtskarte enthält die folgenden Statistiken und Diagramme.
  - Die aktuelle Prozessorauslastung in Prozent
  - Die aktuelle Speicherauslastung in Prozent
  - Ein Liniendiagramm mit der Prozessor- und Speicherauslastung in einem bestimmten Zeitraum
- **Energieverbrauch** Diese Berichtskarte enthält die folgenden Statistiken und Diagramme.
  - Die aktuelle Gesamteingangsleistung für alle Netzteile in Watt
  - Ein Liniendiagramm, das die Gesamteingangsleistung im Laufe der Zeit anzeigt
- **Einheitentemperatur** Diese Berichtskarte enthält die folgenden Statistiken und Diagramme.
  - Die aktuelle Höchsttemperatur der eintretenden Luft in Celsius
  - Ein Liniendiagramm, das die maximale Temperatur im Laufe der Zeit anzeigt

Sie können den Mauszeiger über jede farbige Linie im Kreisdiagramm, jeden Punkt im Liniendiagramm oder die Zahl neben den einzelnen Metriken bewegen, um weitere Informationen zu den Metriken zu erhalten. Sie können Metriken im Diagramm einblenden oder ausblenden, indem Sie auf das Farbsymbol in der Legende klicken. Sie können auch auf eine verlinkte Zahl oder Option beim Symbol **Einstellungen** () oben rechts auf der Karte klicken, um eine Liste aller Einheiten mit Metriken anzuzeigen, die den ausgewählten Kriterien entsprechen.

Vorgehensweise

Gehen Sie wie folgt vor, um das Flussdiagramm für eine bestimmte Aktivität anzuzeigen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Metrikenverlauf**, um die Seite Metrikenverlauf mit Berichtskarten für jeden Metriktyp anzuzeigen.

Schritt 2. Wählen Sie alle oder eine bestimmte Gruppe von Einheiten aus.

Einheiten in den Wartungsmodus versetzen

Wenn sich ein Gerät im Wartungsmodus befindet, schließt Lenovo XClarity Administrator alle Ereignisse und Alerts für dieses Gerät aus allen Seiten aus, auf denen Ereignisse und Alerts angezeigt werden. Ausgeschlossene Alerts werden weiterhin protokolliert, sind aber ausgeblendet.

Zu dieser Aufgabe

Es werden nur die Ereignisse und Alerts ausgeschlossen, die für eine Einheit generiert wurden, während sich diese im Wartungsmodus befand. Es werden die Ereignisse und Alerts angezeigt, wie generiert wurden, bevor die Einheit in den Wartungsmodus versetzt wurde.

Wird ein Gerät in den Wartungsmodus und anschließend wieder in den Servicemodus versetzt, kann dies dazu führen, dass der Bestand für dieses Gerät nicht mehr auf dem neuesten Stand ist. Falls Abweichungen auftreten, können Sie den Bestand auf der Einheitenseite aktualisieren, indem Sie die Einheit auswählen und auf **Alle Aktionen → Bestand → Bestand aktualisieren** klicken.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um Einheiten in den Wartungsmodus zu versetzen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite Service und Support wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Endpunktaktionen**, um die Seite Endpunktaktionen anzuzeigen.

Schritt 3. Wählen Sie ein oder mehrere Einheiten aus, die in den Wartungsmodus versetzt werden sollen.

Schritt 4. Klicken Sie auf **Aktionen → Wartung**, um das Dialogfeld Wartungsmodus mode anzuzeigen.

Schritt 5. Wählen Sie das Datum und die Uhrzeit aus, zu dem/zu der das Gerät vom Wartungsmodus wieder in den Servicemodus versetzt werden soll.

Wählen Sie **Unbegrenzt** aus, wenn das Gerät nicht wieder in den Servicemodus versetzt werden soll.

Schritt 6. Klicken Sie auf **Bestätigen**. Die Spalte „Wartung“ in der Tabelle wird für dieses Gerät in „Ja“ geändert.

Nach dieser Aufgabe

Wenn Sie die Wartung für das Gerät abgeschlossen haben, können Sie es wieder in den Servicemodus versetzen, indem Sie das Gerät auswählen, auf **Aktionen → Wartung** und dann auf das Dialogfeld **Wartung ausschalten** klicken. Wenn Sie das Gerät nicht manuell wieder im Servicemodus versetzen, wird es nach Ablauf des angegebenen Enddatums. bzw. der angegebenen Endzeit automatisch in den Servicemodus versetzt.

Mit Alerts arbeiten

Alerts sind Hardware- oder Verwaltungsbedingungen, die eine Überprüfung und Benutzeraktion erfordern. Lenovo XClarity Administrator ruft die verwalteten Einheiten asynchron ab und zeigt Alerts, die von diesen Einheiten empfangen wurden.

Weitere Informationen:  XClarity Administrator: Überwachung

Zu dieser Aufgabe

In der Regel wird ein entsprechendes Ereignis im Ereignisprotokoll gespeichert, wenn ein Alert empfangen wird. Es ist möglich, einen Alert ohne ein entsprechendes Ereignis im Ereignisprotokoll zu haben (selbst wenn das Protokoll abgeschlossen ist). Ereignisse, die auftreten, bevor Sie ein Gehäuse verwalten, werden nicht im Ereignisprotokoll angezeigt. Allerdings werden die Alerts für das Gehäuse im Alertprotokoll angezeigt, da Lenovo XClarity Administrator das CMM abruft, nachdem das Gehäuse verwaltet wurde.

Aktive Alerts anzeigen

Sie können eine Liste aller aktiven Hardware- und Verwaltungsalerts anzeigen.

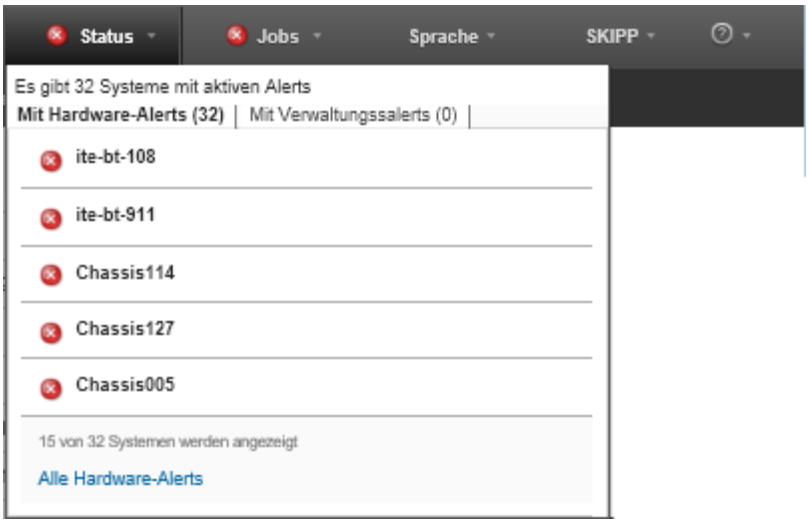
Zu dieser Aufgabe

Anmerkung: Alerts für Lenovo Storage-Einheiten stehen nur auf Englisch verfügbar, selbst wenn die Ländereinstellung für Lenovo XClarity Administrator auf eine andere Sprache festgelegt ist. Verwenden Sie ein externes Übersetzungssystem, um die Nachrichten bei Bedarf manuell zu übersetzen.

Vorgehensweise

Führen Sie eines der folgenden Verfahren durch, um die aktiven Alerts anzuzeigen.

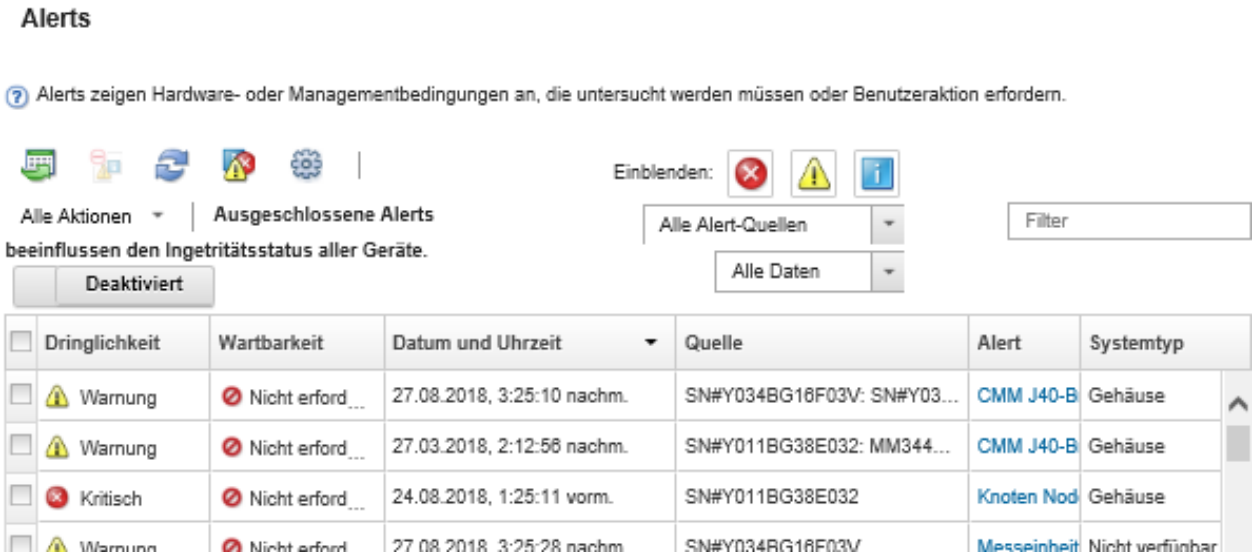
- So zeigen Sie Alerts nur für verwaltete Einheiten an (als *Hardware-Alerts* bekannt):
  1. Klicken Sie in der XClarity Administrator-Titelleiste auf das Pulldown-Menü **Status**, um eine Zusammenfassung der Hardware- und Verwaltungsalerts anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Mit Hardware-Alerts**, um eine Zusammenfassung der Alerts für jede verwaltete Einheit anzuzeigen.



  3. Bewegen Sie den Cursor über eine Einheit, die unter dieser Registerkarte aufgelistet ist, um eine Liste der Alerts für diese Einheit anzuzeigen.
  4. Klicken Sie auf den Link **Alle Hardware-Alerts**, um die Seite „Alerts“ mit einer gefilterten Liste aller Hardware-Alerts anzuzeigen.
- So zeigen Sie nur Alerts von XClarity Administrator an (als *Verwaltungsalerts* bekannt):
  1. Klicken Sie in der XClarity Administrator-Titelleiste auf das Pulldown-Menü **Status**, um eine Zusammenfassung der Hardware- und Verwaltungsalerts anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Mit Verwaltungsalerts**, um eine Zusammenfassung aller CMM- und XClarity Administrator-Alerts anzuzeigen.

3. Bewegen Sie den Cursor über eine Einheit, die unter dieser Registerkarte aufgelistet ist, um eine Liste der Alerts für diese Einheit anzuzeigen.
4. Klicken Sie auf den Link **Alle Verwaltungssalerts**, um die Seite „Alerts“ mit einer gefilterten Liste aller CMM- und XClarity Administrator-Alerts anzuzeigen.

- Um alle Alerts in XClarity Administrator anzuzeigen, klicken Sie auf **Überwachung → Alerts** in der XClarity Administrator-Menüleiste. Die Seite „Alerts“ wird mit einer Liste aller aktiven Alerts angezeigt.

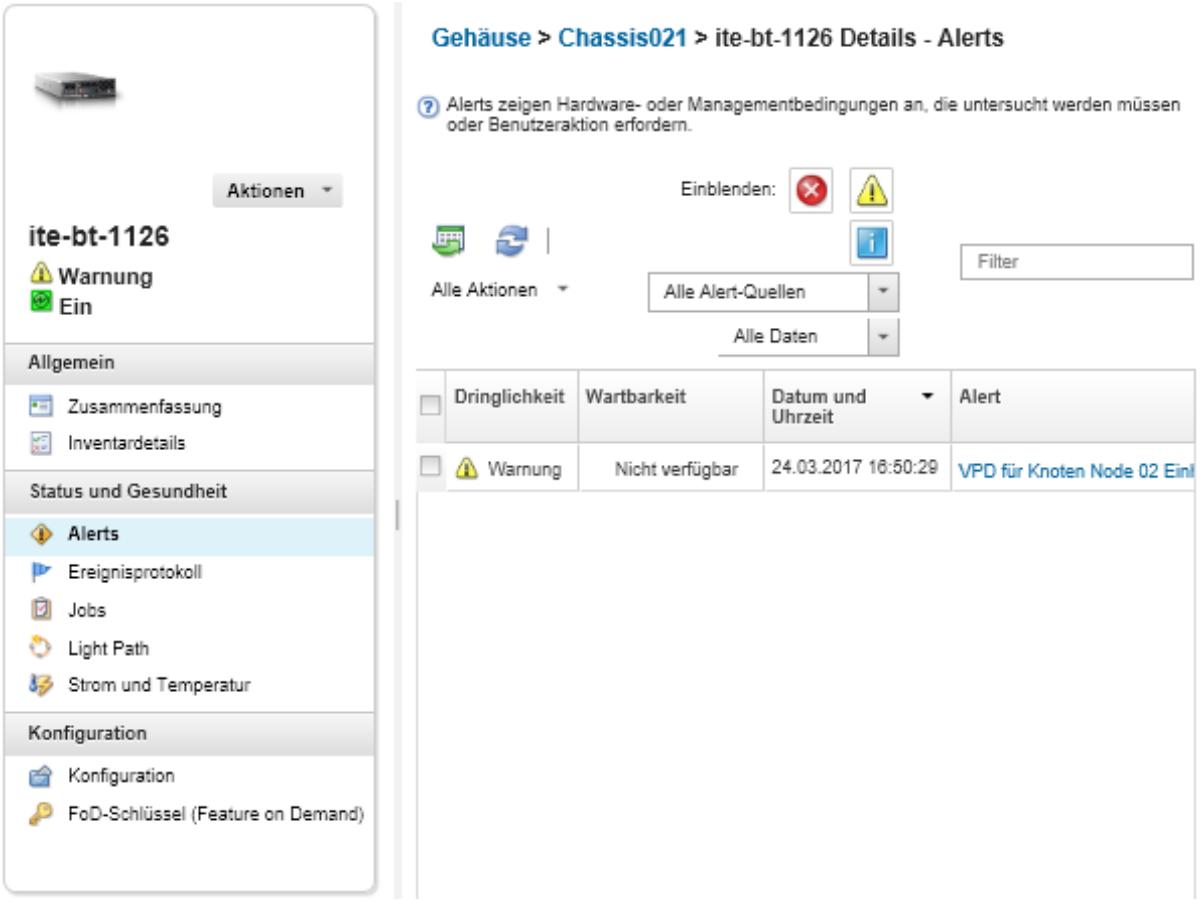


- So zeigen Sie Alerts für eine bestimmte Einheit an:
  1. Klicken Sie in der Menüleiste XClarity Administrator auf **Hardware** und anschließend auf einen Einheitentyp. Es wird eine Seite mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs angezeigt. Klicken Sie beispielsweise auf **Hardware → Server**, um die Seite Server anzuzeigen.
  2. Klicken Sie auf eine bestimmte Einheit, um die Zusammenfassungsseite für die Einheit anzuzeigen.
  3. Klicken Sie unter „Status und Zustand“ auf **Alerts**, um eine Liste aller Alerts anzuzeigen, die dieser Einheit zugeordnet sind.

     Anmerkungen: Die Spalte „Wartbarkeit“ kann „Nicht verfügbar“ anzeigen, wenn:

     – Der Alert auf der Einheit aufgetreten ist, bevor XClarity Administrator mit der Verwaltung begonnen hat

     – Das Ereignisprotokoll wurde abgeschlossen und das Ereignis, das diesem Alert zugeordnet ist, befindet sich nicht mehr im Ereignisprotokoll.



Ergebnisse

Über diese Seite „Alerts“ können Sie die folgenden Aktionen ausführen:

- Die Liste der Alerts durch Klicken auf das Symbol **Aktualisieren** ( ) aktualisieren

  Tipp: Das Alertprotokoll wird alle 30 Sekunden automatisch aktualisiert, wenn neue Alerts erkannt werden.
- Auf den Link in der Spalte **Alert** klicken, um Informationen zu einem bestimmten Alert (einschließlich einer Erläuterung und Benutzeraktion) und zu der Einheit anzuzeigen, die die Quelle des Alerts ist (wie der Universally Unique Identifier). Ein Dialogfenster mit Informationen zu den Alerteigenschaften und Details wird angezeigt.

  Anmerkung: Wenn die Erläuterungen und Wiederherstellungsaktionen für einen Alert nicht auf der Registerkarte **Details** angezeigt werden, gehen Sie zu Lenovo Flex System-Onlinedokumentation und suchen Sie nach der Alert-ID (zum Beispiel `FQXHMSE0004G`). Die Website enthält immer die aktuellen Informationen.
- Standardmäßig beeinflussen ausgeschlossene Alerts nicht den Allgemeinzustand von verwalteten Einheiten. Sie können ausgeschlossene Alerts zulassen, um den Integritätsstatus der verwalteten Einheiten über die Seite „Alerts“ zu beeinflussen, indem Sie auf den Schalter klicken, um **Ausgeschlossene Alerts beeinflussen Integritätsstatus für alle Einheiten** zu aktivieren.
- Sie können Schwellenwerteinstellungen für das Auslösen von Alerts und Ereignissen festlegen, wenn ein bestimmter Wert wie die Lebensdauer einer SSD in einem ThinkSystem- oder ThinkServer-Server eine Warnung oder einen kritischen Wert überschreitet (siehe Schwellenwerteinstellungen für die Generierung von Alerts und Ereignissen festlegen).

- Das Alertprotokoll durch Klicken auf das Symbol **Als CSV exportieren** () exportieren.

  Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.
- Schließen Sie bestimmte Alerts aus allen Seiten aus, auf denen Alerts angezeigt werden (siehe Alerts ausschließen).
- Liste der Alerts eingrenzen, die auf der aktuellen Seite angezeigt werden:
  - Alerts mit einem bestimmten Schweregrad durch Klicken auf die folgenden Symbole anzeigen oder einblenden:
    - Symbol für **Kritische Alerts** ()
    - Symbol für **Warnalerts** ()
    - Symbol für **Informationsalerts** ()
  - Ausschließlich Alerts aus bestimmten Quellen anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Alert-Quellen
    - Hardware-Ereignisse
    - Management-Ereignisse
    - Service Center-Ereignisse
    - Für Kunden wartungsfähige Ereignisse
    - Nicht wartungsfähige Ereignisse
  - Nur Alerts mit einem bestimmten Datum und einer bestimmten Uhrzeit anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Daten
    - Vergangene zwei Stunden
    - Vergangene 24 Stunden
    - Letzte Woche
    - Letzter Monat
  - Nur Alerts anzeigen, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
  - Alerts durch Klicken auf eine Spaltenüberschrift spaltenweise sortieren

Alerts ausschließen

Wenn bestimmte Alerts für Sie nicht relevant sind, können Sie diese Alerts auf allen Seiten ausschließen, auf denen Alerts angezeigt werden. Ausgeschlossene Alerts werden weiterhin im Protokoll festgehalten, aber auf den Seiten mit Alerts ausgeblendet, einschließlich Protokollansichten und Gerätestatus.

Zu dieser Aufgabe

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

Sie können Einheiten in den Wartungsmodus versetzen, sodass alle Ereignisse und Alerts für diese Einheiten ausgeschlossen sind (siehe Einheiten in den Wartungsmodus versetzen).

Einschränkung: Nur Benutzer mit Administratorberechtigung können Alerts ausschließen und wiederherstellen.

Wichtig: Wenn Sie Statusalerts ausschließen, ändert sich der Gerätestatus in der Gerätezusammenfassung und auf den Detailseiten nicht.

VorgehensweiseGehen Sie wie folgt vor, um Alerts aus den Alertprotokollen auszuschließen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Alerts**. Die Seite Alerts wird angezeigt.

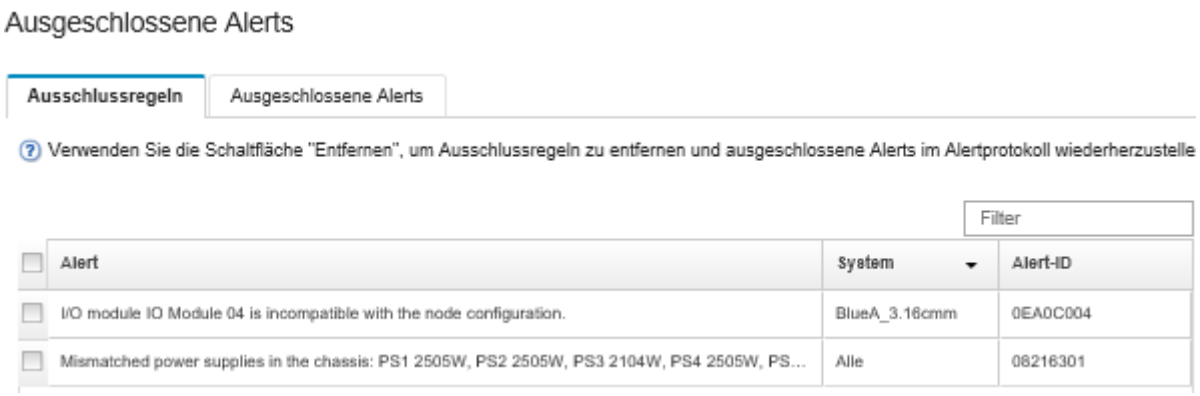
Schritt 2. Wählen Sie die auszuschließenden Alerts aus und klicken Sie auf das Symbol **Alerts ausschließen** (). Das Dialogfenster „Ereignisse ausschließen“ wird angezeigt.

Schritt 3. Wählen Sie eine der folgenden Optionen:
- **Ausgewählte Alerts von allen Systemen ausschließen**. Schließt die ausgewählten Alerts von allen verwalteten Einheiten aus.
- **Nur Alerts aus Systemen im Bereich der ausgewählten Instanzen ausschließen**. Schließt die ausgewählten Alerts von den verwalteten Einheiten aus, auf die sich die ausgewählten Alerts beziehen.

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

Nach dieser Aufgabe

Wenn Sie Alerts ausschließen, erstellt Lenovo XClarity Administrator Ausschlussregeln basierend auf den von Ihnen bereitgestellten Angaben. Sie können eine Liste der Ausschlussregeln und ausgeschlossenen Alerts über die Seite „Alerts“ anzeigen. Klicken Sie dazu auf das Symbol **Ausgeschlossene/Bestätigte Alerts anzeigen** (). Klicken Sie im Dialogfenster Ausgeschlossene/Bestätigte Alerts auf die Registerkarte **Ausschlussregeln**, um die Liste der Ausschlussregeln anzuzeigen, oder klicken Sie auf die Registerkarte **Ausgeschlossene Alerts**, um die Liste der ausgeschlossenen Alerts anzuzeigen.



Standardmäßig beeinflussen ausgeschlossene Alerts nicht den Allgemeinzustand von verwalteten Einheiten. Sie können ausgeschlossene Alerts zulassen, um den Integritätsstatus der verwalteten Einheiten über die Seite „Alerts“ zu beeinflussen, indem Sie auf den Schalter klicken, um **Ausgeschlossene/Bestätigte Alerts anzeigen** zu aktivieren.

Sie können Alerts wiederherstellen, die vom Alertprotokoll ausgeschlossen wurden, indem Sie die entsprechende Ausschlussregel entfernen. Um eine Ausschlussregel zu entfernen, klicken Sie auf das **Ausgeschlossene Alerts anzeigen**-Symbol (). Das Dialogfenster „Ausgeschlossene Alerts“ wird angezeigt. Wählen Sie die wiederherzustellenden Ausschlussregeln oder ausgeschlossenen Alerts aus und klicken Sie auf **Entfernen**.

Einen Alert beheben

Lenovo XClarity Administrator enthält Informationen über die geeigneten Maßnahmen zum Beheben von Alerts.

VorgehensweiseGehen Sie wie folgt vor, um ein Alert zu beheben.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Überwachung → Alerts**, um die Seite Alerts anzuzeigen.

Schritt 2. Suchen Sie den Alert im Alertprotokoll.

Schritt 3. Klicken Sie auf den Link in der Spalte **Alert**, um Informationen zum Alert (einschließlich einer Erläuterung und Wiederherstellungsaktionen) und Eigenschaften für die Einheit anzuzeigen, die die Quelle des Alerts ist (wie der Universally Unique Identifier).

Schritt 4. Führen Sie die auf der Registerkarte **Details** aufgelisteten Wiederherstellungsaktionen aus, um den Alert zu beheben. Das folgende Beispiel zeigt Wiederherstellungsaktionen für ein Ereignis.

Ändern Sie die Sicherheitsrichtlinieneinstellung auf dem referenzierten verwalteten Gehäuse, sodass sie mit der aktuellen Sicherheitsrichtlinie auf dem Verwaltungsserver übereinstimmen.

Um die Sicherheitsrichtlinie auf dem Gehäuse zu ändern, öffnen Sie eine Sitzung der Befehlszeilenschnittstelle auf dem Chassis Management Module (CMM) und führen Sie einen der folgenden Befehle aus:

- Ändern der Sicherheitsrichtlinie in `Secure`:
  `security -p secure -T mm[p]`
- Ändern der Sicherheitsrichtlinie in `Legacy`:
  `security -p legacy -T mm[p]`

Anmerkung: Wenn die Erläuterungen und Wiederherstellungsaktionen für einen Alert nicht auf der Registerkarte **Details** angezeigt werden, gehen Sie zu Lenovo Flex System-Onlinedokumentation und suchen Sie nach der Alert-ID (zum Beispiel `FQXHMSE0004G`). Die Website enthält immer die aktuellen Informationen.

Wenn Sie die empfohlenen Aktionen ausführen und das Problem weiterhin auftritt, wenden Sie sich an den Lenovo-Support.

Alerts bestätigen

Wenn ein aktiver Alert bestätigt wird, wird er auf den Seiten aufgelistet, auf denen Alerts angezeigt werden, hat aber keinen Einfluss auf den Wertigkeitsstatus der entsprechenden Einheit.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Alert zu bestätigen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Alerts**. Die Seite Alerts wird angezeigt.

Schritt 2. Wählen Sie die zu bestätigenden Alerts aus.

Schritt 3. Klicken Sie auf das Symbol **Alerts bestätigen** ( ).

Nach dieser Aufgabe

- Sie können eine Liste der bestätigten Alerts über die Seite „Alerts“ anzeigen. Klicken Sie auf das Symbol **Ausgeschlossene/Bestätigte Alerts anzeigen** ( ), um das Dialogfenster „Ausgeschlossene/Bestätigte Alerts“ anzuzeigen, und klicken Sie dann auf die Registerkarte **Bestätigte Alerts**.
- Sie können die Bestätigung eines aktiven Alerts entfernen. Klicken Sie dazu auf das Symbol **Ausgeschlossene/Bestätigte Alerts anzeigen** ( ), um das Dialogfenster „Ausgeschlossene/Bestätigte Alerts“ anzuzeigen, und klicken Sie dann auf die Registerkarte **Bestätigte Alerts**. Wählen Sie die Alerts aus und klicken Sie auf das Symbol **Bestätigung entfernen** ( ).

Ereignisse handhaben

Über Lenovo XClarity Administrator haben Sie Zugriff auf ein Ereignisprotokoll und ein Prüfprotokoll.

Weitere Informationen: XClarity Administrator: Überwachung

Zu dieser Aufgabe

Das *Ereignisprotokoll* enthält eine Liste aller archivierten Hardware- und Verwaltungsereignisse.

Das *Prüfprotokoll* stellt eine historische Aufzeichnung aller Benutzeraktionen dar, z. B. Anmelden an Lenovo XClarity Administrator, Erstellen eines neuen Benutzers und Ändern eines Benutzerkennworts. Sie können das Prüfprotokoll verwenden, um die Authentifizierung und Kontrollen in IT-Systemen zu verfolgen und zu dokumentieren.

Ereignisse im Ereignisprotokoll überwachen

Das *Ereignisprotokoll* enthält eine Liste aller archivierten Hardware- und Verwaltungsereignisse.

Zu dieser Aufgabe

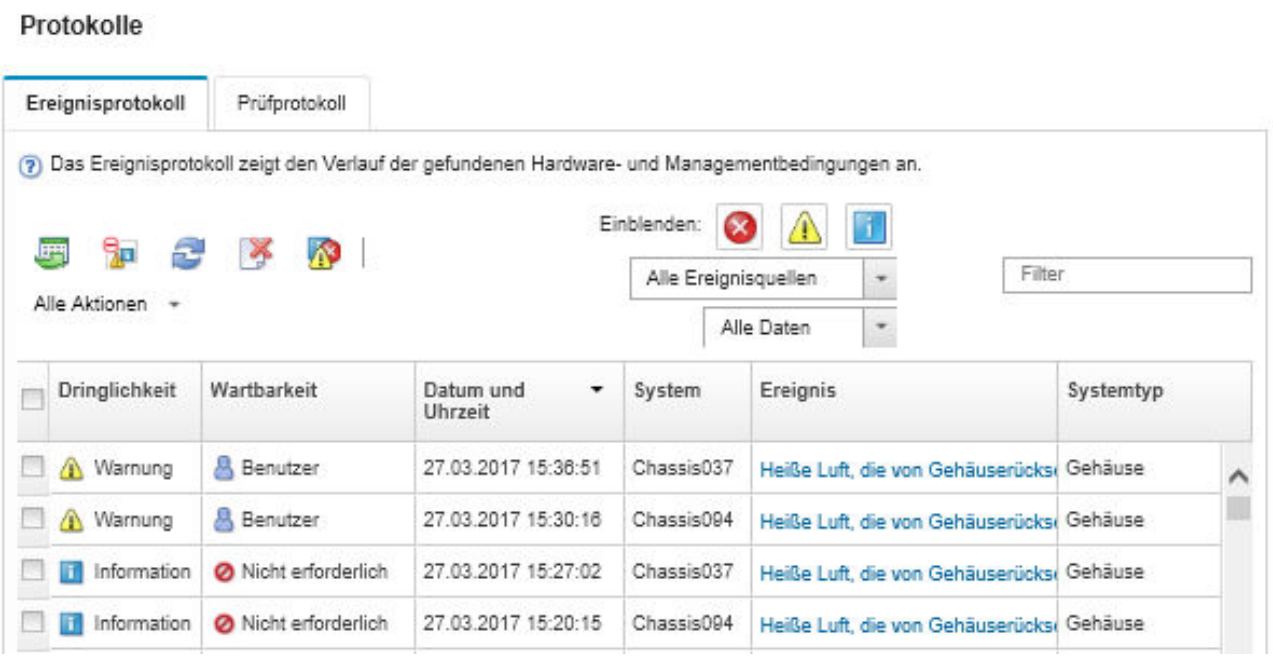
Das Ereignisprotokoll enthält Informations- und Nicht-Informationsereignisse. Die Anzahl an Einträgen für jedes dieser Ereignisse ist variabel, bis die maximale Anzahl von 50.000 Ereignissen im Ereignisprotokoll erreicht wird. Zu diesem Zeitpunkt gibt es maximal 25.000 Informations- und 25.000 Nicht-Informationsereignisse. Beispiel: Zu Beginn gab es 0 Ereignisse im Ereignisprotokoll. Die empfangenen Ereignisse teilen sich wie folgt auf: 20.000 Informationsereignisse und 30.000 Nicht-Informationsereignisse. Wenn das nächste Ereignis empfangen wird, wird jedes Mal das älteste Informationsereignis gelöscht. Dies gilt auch, wenn ein Nicht-Informationsereignis vorhanden ist, das älter ist. Dies führt dazu, dass das Protokoll nach einer gewissen Zeit ausgeglichen ist, d. h., es enthält 25.000 Einträge jedes Ereignistyps.

Lenovo XClarity Administrator sendet ein Ereignis, wenn das Ereignisprotokoll 80 Prozent der maximalen Größe erreicht und ein weiteres Ereignis, wenn die Summe der Ereignis- und Prüfprotokolle 100 Prozent der maximalen Größe erreicht.

Tipp: Sie können das Ereignisprotokoll exportieren, um sicherzustellen, dass Ihnen eine vollständige Aufzeichnung aller Hardware- und Verwaltungsereignisse vorliegt. Klicken Sie zum Exportieren des Ereignisprotokolls auf das Symbol für **Als CSV exportieren** ( ).

Vorgehensweise

Um das Ereignisprotokoll anzuzeigen, klicken Sie auf **Überwachung → Ereignisprotokolle** in der Menüleiste von Lenovo XClarity Administrator und dann die Registerkarte **Ereignisprotokoll**. Die Seite „Ereignisprotokoll“ wird angezeigt.



Die Spalte **Wartbarkeit** gibt an, ob die Einheit gewartet werden muss. Diese Spalte kann einen der folgenden Werte aufweisen:

- **Nicht erforderlich**. Das Ereignis ist informativ und erfordert keine Aktion.
- **Benutzer**. Führen Sie die entsprechende Wiederherstellungsaktion durch, um das Problem zu beheben.

  Um Informationen über ein bestimmtes Ereignis anzuzeigen, klicken Sie auf den Link in der Spalte **Ereignis**. Es wird ein Dialogfenster angezeigt mit Informationen zu den Eigenschaften der Einheit, die das Ereignis gesendet hat, Details zum Ereignis und Wiederherstellungsaktionen.
- **Unterstützung**. Wenn Call-Home-Funktion in Lenovo XClarity Administrator aktiviert ist, wird das Ereignis in der Regel zum Lenovo-Support Center gesendet. Ausnahme: Es existiert bereits ein offenes Service-Ticket mit dieser Ereignis-ID für die Einheit.

  Wenn Call-Home-Funktion nicht aktiviert ist, wird empfohlen, dass Sie manuell ein Service-Ticket öffnen, um das Problem zu beheben (siehe Service-Ticket öffnen in der Onlinedokumentation von Lenovo XClarity Administrator).

Ergebnisse

Über die Seite „Ereignisprotokoll“ können Sie die folgenden Aktionen ausführen:

- Zeigen Sie die Quelle des Ereignisses an, indem Sie in der Spalte **Quelle** auf den Link klicken.
- Liste der Ereignisse durch Klicken auf das Symbol **Aktualisieren** ( ) aktualisieren.

  Tipp: Das Ereignisprotokoll wird alle 30 Sekunden automatisch aktualisiert, wenn neue Ereignisse erkannt werden.
- Wählen Sie zum Löschen aller Ereignisse im Ereignisprotokoll **Alle Aktionen → Ereignisprotokoll löschen** aus.
- Details über ein bestimmtes Ereignis durch Klicken auf den Link in der Spalte **Ereignis** und dann Klicken auf die Registerkarte **Details** anzeigen
- Ereignisprotokoll durch Klicken auf das Symbol **Als CSV exportieren** ( ) exportieren.

Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.

- Schließen Sie bestimmte Ereignisse von allen Seiten aus, auf denen Ereignisse angezeigt werden (siehe Ereignisse ausschließen).
- Liste der Hardware- und Verwaltungsereignisse eingrenzen, die auf der aktuellen Seite angezeigt werden:
  - Ereignisse mit einem bestimmten Schweregrad durch Klicken auf die folgenden Symbole in der Dropdown-Liste anzeigen oder einblenden:
    - Symbol für **Kritische Ereignisse** ( )
    - Symbol für **Warnereignisse** ( )
    - Symbol für **Informationsereignisse** ( )
  - Ausschließlich Ereignisse aus bestimmten Quellen anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Alert-Quellen
    - Hardware-Ereignisse
    - Management-Ereignisse
    - Wartungsfähige Ereignisse
    - Für Kunden wartungsfähige Ereignisse
    - Nicht wartungsfähige Ereignisse
  - Nur Ereignisse mit einem bestimmten Datum und einer bestimmten Uhrzeit anzeigen. Sie können eine der folgenden Optionen auswählen:
    - Alle Daten
    - Vergangene 2 Stunden
    - Vergangene 24 Stunden
    - Letzte Woche
    - Letzter Monat
    - Custom

    Wenn Sie **Angepasst** auswählen, können Sie Hardware- und Verwaltungsereignisse filtern, die zwischen einem benutzerdefinierten Startdatum und dem aktuellen Datum ausgelöst wurden.
  - Nur Ereignisse anzeigen, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
  - Ereignisse durch Klicken auf eine Spaltenüberschrift spaltenweise sortieren.

Ereignisse im Prüfprotokoll überwachen

Das *Prüfprotokoll* stellt eine historische Aufzeichnung aller Benutzeraktionen dar, z. B. Anmelden an Lenovo XClarity Administrator, Erstellen eines neuen Benutzers und Ändern eines Benutzerkennworts. Sie können das Prüfprotokoll verwenden, um die Authentifizierung und Kontrollen in IT-Systemen zu verfolgen und zu dokumentieren.

Zu dieser Aufgabe

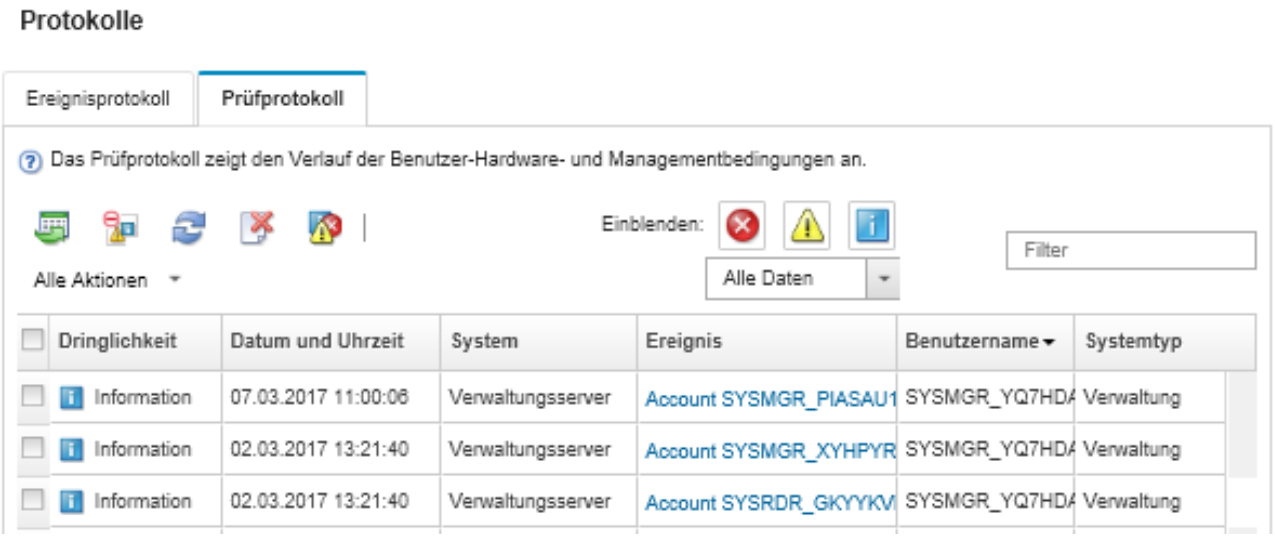
Das Prüfprotokoll kann maximal 50.000 Ereignisse enthalten. Wenn die maximale Größe erreicht ist, wird das älteste Ereignis im Protokoll gelöscht und das neue Ereignis zum Protokoll hinzugefügt.

XClarity Administrator sendet ein Ereignis, wenn das Prüfprotokoll 80 Prozent der maximalen Größe erreicht und ein weiteres Ereignis, wenn die Summe der Ereignis- und Prüfprotokolle 100 Prozent der maximalen Größe erreicht.

Tipp: Sie können das Prüfprotokoll exportieren, um sicherzustellen, dass Ihnen eine vollständige Aufzeichnung aller Prüfereignisse vorliegt. Um das Prüfprotokoll zu exportieren, klicken Sie auf das Symbol für **Als CSV exportieren** ( ).

Vorgehensweise

Um das Prüfprotokoll anzuzeigen, klicken Sie auf **Überwachung → Ereignisprotokolle** in der Menüleiste von XClarity Administrator und dann auf die Registerkarte **Prüfprotokoll**. Die Seite Prüfprotokoll wird angezeigt.



Um Informationen über ein bestimmtes Prüfereignis anzuzeigen, klicken Sie auf den Link in der Spalte **Ereignis**. Es wird ein Dialogfenster angezeigt mit Informationen zu den Eigenschaften der Einheit, die das Ereignis gesendet hat, Details zum Ereignis und Wiederherstellungsaktionen.

Ergebnisse

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Zeigen Sie die Quelle des Prüfereignisses an, indem Sie in der Spalte **Quelle** auf den Link klicken.
- Liste der Prüfereignisse durch Klicken auf das Symbol **Aktualisieren** ( ) aktualisieren.

  Tipp: Das Ereignisprotokoll wird alle 30 Sekunden automatisch aktualisiert, wenn neue Ereignisse erkannt werden.
- Details über ein bestimmtes Prüfereignis durch Klicken auf den Link in der Spalte **Ereignis** und dann Klicken auf die Registerkarte **Details** anzeigen
- Prüfprotokoll durch Klicken auf das Symbol **Als CSV exportieren** ( ) exportieren.

  Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.
- Schließen Sie bestimmte Prüfereignisse von allen Seiten aus, auf denen Ereignisse angezeigt werden (siehe Ereignisse ausschließen).
- Liste der Prüfereignisse eingrenzen, die auf der aktuellen Seite angezeigt werden:
  - Ereignisse mit einem bestimmten Schweregrad durch Klicken auf die folgenden Symbole anzeigen oder einblenden:

  - Symbol für **Kritische Ereignisse** ()
  - Symbol für **Warnereignisse** ()
  - Symbol für **Informationsereignisse** ()
- Nur Ereignisse mit einem bestimmten Datum und einer bestimmten Uhrzeit anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
  - Alle Daten
  - Vergangene 2 Stunden
  - Vergangene 24 Stunden
  - Letzte Woche
  - Letzter Monat
  - Custom

  Wenn Sie **Angepasst** auswählen, können Sie Hardware- und Verwaltungsereignisse filtern, die zwischen einem benutzerdefinierten Startdatum und dem aktuellen Datum ausgelöst wurden.
- Nur Ereignisse anzeigen, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
- Ereignisse durch Klicken auf eine Spaltenüberschrift spaltenweise sortieren.

Ein Ereignis beheben

Lenovo XClarity Administrator enthält Informationen über die geeigneten Maßnahmen zum Beheben von Ereignissen.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Ereignis zu beheben.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisprotokolle**, um die Seite Protokolle anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisprotokoll**.

Schritt 3. Suchen Sie das Ereignis im Ereignisprotokoll.

Schritt 4. Klicken Sie auf den Link in der Spalte **Ereignis**, um Informationen zu diesem Ereignis (einschließlich Erläuterungen und Wiederherstellungsaktionen) und zu der Einheit anzuzeigen, die das Ereignis ausgelöst hat.

Schritt 5. Klicken Sie auf die Registerkarte **Details**.

Schritt 6. Führen Sie die auf der Registerkarte **Details** angegebenen Wiederherstellungsaktionen aus, um das Ereignis zu beheben.

Anmerkung: Wenn die Erläuterungen und Wiederherstellungsaktionen für ein Ereignis nicht angezeigt werden, rufen Sie die Lenovo Flex System-Onlinedokumentation auf und suchen Sie nach dem Ereignisnamen. Die Website enthält immer die aktuellen Informationen.

Wenn Sie die empfohlenen Aktionen ausführen und das Problem weiterhin auftritt, wenden Sie sich an den Lenovo-Support.

Ereignisse ausschließen

Wenn bestimmte Ereignisse für Sie nicht relevant sind, können Sie diese Ereignisse auf allen Seiten ausschließen, auf denen Ereignisse angezeigt werden. Ausgeschlossene Ereignisse werden weiterhin im Protokoll festgehalten, aber auf den Seiten mit Ereignissen ausgeblendet.

Zu dieser Aufgabe

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

Sie können Einheiten in den Wartungsmodus versetzen, sodass alle Ereignisse und Alerts für diese Einheiten ausgeschlossen sind (siehe Einheiten in den Wartungsmodus versetzen).

Einschränkung: Nur Benutzer mit Administratorberechtigung können Ereignisse ausschließen und wiederherstellen.

Vorgehensweise

Gehen Sie wie folgt vor, um Ereignisse aus den Ereignisprotokollen auszuschließen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisprotokolle** und wählen Sie dann die Registerkarte **Ereignisprotokoll** aus. Die Seite „Ereignisprotokolle“ wird angezeigt.

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

Schritt 3. Wählen Sie eine der folgenden Optionen:
- **Ausgewählte Ereignisse von allen Systemen ausschließen**. Schließt die ausgewählten Ereignisse von allen verwalteten Einheiten aus.
- **Nur Ereignisse aus Systemen 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 Lenovo XClarity Administrator Ausschlussregeln basierend auf den von Ihnen bereitgestellten Angaben.

- Zeigen Sie eine Liste der Ausschlussregeln und ausgeschlossenen Ereignisse über die Seite für Protokolle an. Klicken Sie dazu auf das **Ausgeschlossene Ereignisse anzeigen**-Symbol ( ). Klicken Sie im Dialogfenster Ausgeschlossene Ereignisse auf die Registerkarte **Ausschlussregeln**, um die Ausschlussregeln anzuzeigen, oder klicken Sie auf die Registerkarte **Ausgeschlossene Ereignisse**, um ausgeschlossene Ereignisse anzuzeigen.

- Stellen Sie Ereignisse wieder her, die vom Ereignisprotokoll ausgeschlossen wurden, indem Sie die entsprechende Ausschlussregel entfernen. Um eine Ausschlussregel zu entfernen, klicken Sie auf das

Ausgeschlossene Ereignisse anzeigen-Symbol ( ). Das Dialogfenster Ausgeschlossene Ereignisse wird angezeigt. Wählen Sie die wiederherzustellenden Ausschlussregeln aus und klicken Sie auf **Ausschlüsse entfernen**.

- Vermeiden Sie, das wartungsfähige Ereignisse, die sich in der Liste ausgeschlossener Ereignisse befinden, automatisch Problemberichte senden, in dem Sie auf **Verwaltung → Service und Support** in der Lenovo XClarity Administrator Menüleiste klicken. Klicken Sie anschließend auf die Registerkarte **Service-Weiterleiter** und wählen Sie dann **Nein** neben der Frage **Sollen bei ausgeschlossenen Ereignissen Problemberichte geöffnet werden?** aus.

Ereignisse weiterleiten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisse an mobile Einheiten und verbundene Anwendungen in Ihrer Umgebung weitergeleitet werden. Dies hilft beim Erfassen und Überwachen von Hardwarestatus- und Laufzeitproblemen für Ihre Hardwareumgebung.

Weitere Informationen: XClarity Administrator: Überwachung

Ereignisse an syslog, Remote-SNMP-Manager, E-Mail und andere Ereignisservices weiterleiten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisse an verbundene Anwendungen in Ihrer Umgebung weitergeleitet werden. Dies hilft beim Erfassen und Überwachen von Hardwarestatus- und Laufzeitproblemen für Ihre Hardwareumgebung. Basierend auf der Einheit, Ereignisklasse, Ereigniswertigkeit und Komponente können Sie festlegen, in welchem Umfang Ereignisse weitergeleitet werden.

Zu dieser Aufgabe

Lenovo XClarity Administrator kann Ereignisse für eine oder mehrere Einheiten weiterleiten. Bei Prüfereignissen können Sie auswählen, ob alle oder keine der Prüfereignisse weitergeleitet werden. Es ist nicht möglich, bestimmte Prüfereignisse weiterzuleiten. Bei Hardware- und Verwaltungsereignissen können Sie auswählen, dass Ereignisse für eine oder mehrere Wertigkeiten (kritische, Warn- und Informationsereignisse) und für eine oder mehrere Komponenten (z. B. Plattenlaufwerke, Prozessoren und Adapter) weitergeleitet werden.

Lenovo XClarity Administrator verwendet Ereignisweiterleitungen zum Weiterleiten von Ereignissen. Eine *Ereignisweiterleitung* enthält Informationen zum zu verwendenden Protokoll, zum Empfänger, zu den zu überwachenden Einheiten und zu den weiterzuleitenden Ereignissen. Nachdem Sie eine Ereignisweiterleitung erstellt und aktiviert, startet Lenovo XClarity Administrator die Überwachung der eingehenden Ereignisse basierend auf den Filterkriterien. Wenn eine Übereinstimmung gefunden wird, wird das Ereignis basierend auf dem zugeordneten Protokoll weitergeleitet.

Die folgenden Protokolle werden unterstützt:

- **Azure Log Analytics**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an Microsoft Azure Log Analytics weiter.
- **E-Mail**. Lenovo XClarity Administrator leitet die überwachten Ereignisse per SMTP an eine oder mehrere E-Mail-Adressen weiter. Die E-Mail enthält Informationen zum Ereignis, den Hostnamen der Quelleinheit sowie Links zur Lenovo XClarity Administrator-Webschnittstelle und zur Lenovo XClarity Mobile-App.
- **FTP**. Leitet die überwachten Ereignisse über das Netzwerk an einen FTP-Server weiter.
- **REST**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an einen REST-Webservice weiter.
- **SNMP**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an einen Remote-SNMP-Manager weiter. SNMPv1- und SNMPv3-Traps werden unterstützt.

Informationen über die MIB-Datei (Management Information Base), in der die von Lenovo XClarity Administrator generierten SNMP-Traps beschrieben werden, finden Sie unter Datei „lenovoMgrAlert.mib“Datei „lenovoMgrAlert.mib“ in der Onlinedokumentation von Lenovo XClarity Administrator.

- **Syslog**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an einen zentralen Protokollserver weiter, wobei systemeigene Tools für die syslog-Überwachung verwendet werden können.

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Anmerkung: Ereignisse werden nicht übermittelt, wenn beispielsweise keine funktionsfähige Verbindung zwischen Lenovo XClarity Administrator und der Ereignisweiterleitung vorhanden ist oder wenn der Port blockiert ist.

Ereignisweiterleitung an Azure Log Analytics einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an Azure Log Analytics konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für Azure Log Analytics zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **Azure Log Analytics** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen und optional eine Beschreibung für die Ereignisweiterleitung ein.
- Geben Sie den Primärschlüssel für die Azure Log Analytics-Schnittstelle ein.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- **Optional**: 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.
  - **Keine Angabe**. Es wird keine Authentifizierung verwendet.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für Azure Log Analytics-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für Azure Log Analytics-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Klicken Sie auf die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse zulassen**, um das Weiterleiten ausgeschlossener Ergebnisse zu erlauben oder zu verhindern.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID

auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Übereinstimmung nach Ereigniskategorie**.
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.
- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.

- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Benachrichtigungen über neue Alerts wurden gesendet.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

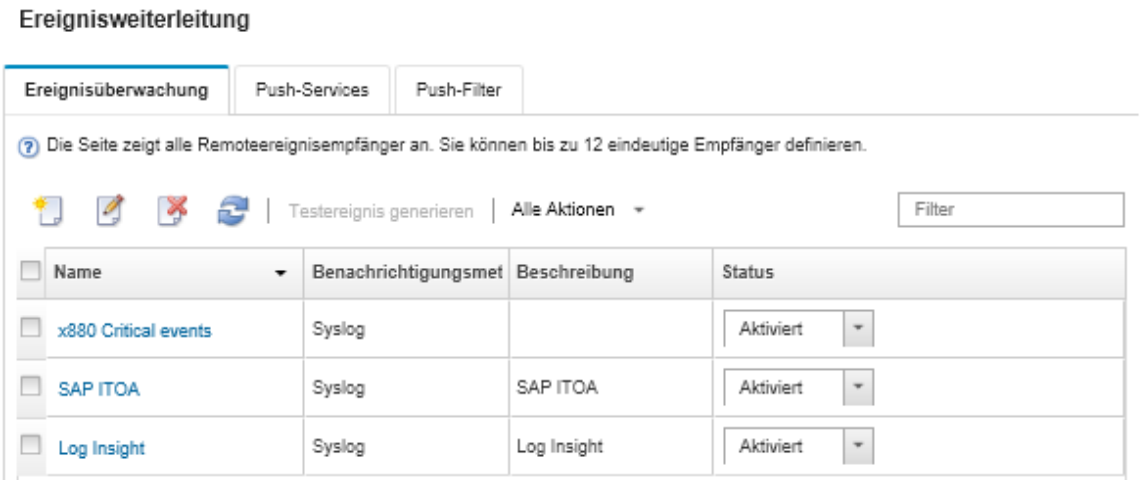
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden Azure Log Analytics-Server weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** () klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** () klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen E-Mail-Service über SMTP einrichten

Sie können Lenovo XClarity Administrator so konfigurieren, dass bestimmte Ereignisse über SMTP an einen E-Mail-Service weitergeleitet werden.

Vorbereitende Schritte

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 einer Ereignisweiterleitung an einen Gmail-Webservice die Informationen im Abschnitt Ereignisweiterleitung an einen Gmail-SMTP-Service einrichtenEreignisweiterleitung an syslog, Remote- SNMP-Manager oder E-Mail einrichten der Onlinedokumentation von Lenovo XClarity Administrator durch.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für E-Mail über SMTP zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** (). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **E-Mail** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen, den Zielhost und optional eine Beschreibung der Ereignisweiterleitung 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.

  Wählen Sie zum Senden der E-Mail an den Support-Kontakt, der für die Einheit zugewiesen ist, **Support-Kontakt-E-Mail verwenden** (siehe Support-Kontakte für eine Einheit definieren in der Onlinedokumentation von XClarity Administrator).
- **Optional:** Geben Sie die E-Mail-Adresse des Absenders der E-Mail ein (zum Beispiel `john@company.com`).

  Wenn Sie keine E-Mail-Adresse angeben, wird standardmäßig `LXCA.`*<source_identifier>*`@`*<smtp_host>* als Absenderadresse verwendet.

  Wenn Sie nur die Absenderdomäne angeben, wird *<LXCA_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 Administrator definiert haben, lehnt der SMTP-Server unter Umständen weitergeleitete Ereignisse ab. Wenn XClarity Administrator 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 (`LXCA.`*<source_identifier>*`@`*<smtp_host>*) abgelehnt. In diesem Fall müssen Sie im Feld **Absender** mindestens einen Domänennamen angeben.
- **Optional:** Um eine sichere Verbindung zum SMTP-Server herzustellen, wählen Sie die folgenden Verbindungstypen aus:
  – **SSL**. Verwendet bei der Kommunikation das SSL-Protokoll.
  – **STARTTLS**. Verwendet TLS, um eine sichere Kommunikation über einen unsicheren Kanal aufzubauen.

  Wenn einer dieser Verbindungstypen ausgewählt ist, versucht LXCA, das Zertifikat des SMTP-Servers herunterzuladen und in seinen Truststore zu importieren. Sie werden aufgefordert, das Hinzufügen dieses Zertifikat zum Truststore zu akzeptieren.
- **Optional:** 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.
  – **NTLM**. Verwendet das Protokoll „NT LAN Manager (NTLM)“, um sich mithilfe der angegebenen Benutzer-ID, des Kennworts und des Domänennamens am angegebenen SMTP-Server zu authentifizieren.

- **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 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten, die im E-Mail-Text weitergeleitet werden sollen, und das Format des E-Mail-Betreffs auszuwählen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für E-Mail-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für die E-Mail-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

E-Mail-Betreff

```
[[DeviceName]]-[[EventMessage]]
```

E-Mail-Text

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Klicken Sie auf die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse zulassen**, um das Weiterleiten ausgeschlossener Ergebnisse zu erlauben oder zu verhindern.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Übereinstimmung nach Ereigniskategorie**.
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.
- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.

- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Benachrichtigungen über neue Alerts wurden gesendet.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

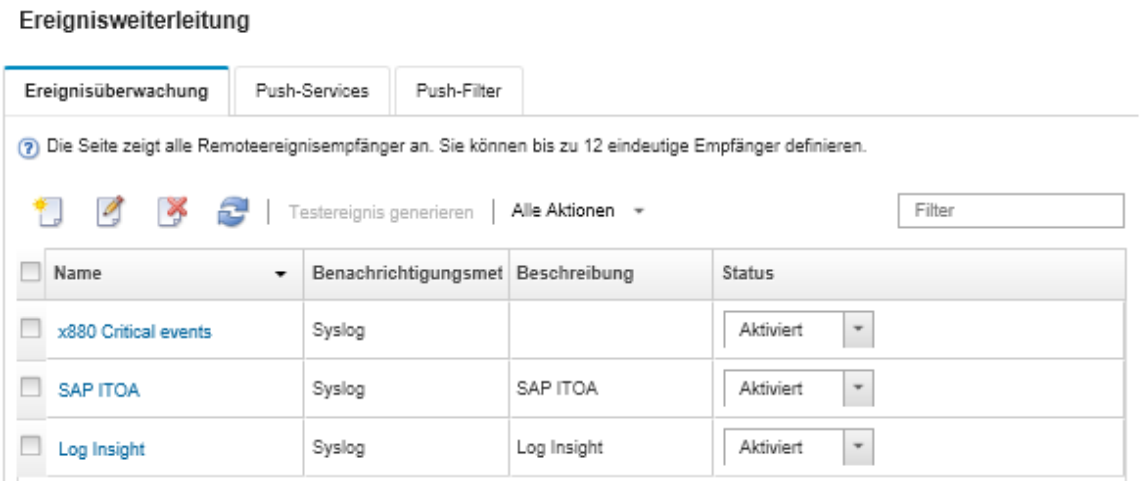
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden E-Mail-Service weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen SMTP-Service für Gmail einrichten

Sie können Lenovo XClarity Administrator so einrichten, dass überwachte Ereignis an einen webbasierten E-Mail-Service wie 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 gültiges Benutzeraccount und 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
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 gültiges Benutzeraccount und 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 gültiges 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.
   e. Klicken Sie in den Suchergebnissen auf **GMAIL-API**.
   f. Klicken Sie auf **Aktivieren**.
   g. Klicken Sie auf die Registerkarte **Anmeldeinformationen**.
   h. Klicken Sie auf **OAuth-Zustimmung**.

i. Geben Sie im Feld **Benutzern angezeigter Produktname** einen Namen ein und klicken Sie auf **Speichern**.

j. Klicken Sie auf **Anmeldeinformationen erstellen → OAuth-Client-ID**.

k. Wählen Sie **Sonstige** aus und geben einen Namen ein.

l. Klicken Sie auf **Erstellen**. Im Dialogfenster OAuth-Client werden Ihre Client-ID und der geheime Clientschlüssel angezeigt.

m. Notieren Sie die Client-ID und den geheimen Clientschlüssel für die spätere Verwendung.

n. 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=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --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
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;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/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
   Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_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 Administrator mit dem neuen Token zu aktualisieren.

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

Parameter	Wert
Host	smtp.gmail.com
Port	587
SSL	Löschen
STARTTLS	Auswählen
Authentifizierung	OAUTH2
Benutzer	Gültige E-Mail-Adresse für Gmail
Token	Sicherheitstoken
Absenderadresse	(optional)

Ereignisweiterleitung an einen FTP-Server einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an einen FTP-Server konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für einen FTP-Server zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **FTP** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen, den Zielhost und optional eine Beschreibung der Ereignisweiterleitungen ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 21.

- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- **Optional:** Geben Sie die Zeichenfolge an, die aus dem Dateiinhalt entfernt werden soll.
- Geben Sie das Dateinamenformat ein, das für die Datei verwendet werden soll, die das weitergeleitete Ereignis enthält. Das Standardformat ist `event_[[EventSequenceID]].txt`.

  Anmerkung: Jede Datei enthält Informationen zu einem einzelnen Ereignis.
- Geben Sie den Pfad auf dem Remote-FTP-Server ein, auf den die Datei hochgeladen werden soll.
- Wählen Sie den Zeichensatz, entweder **UTF-8** oder **Big5**. UTF-8 ist der Standardwert.
- Wählen Sie den Authentifizierungstyp aus. Es kann einen der folgenden Werte aufweisen.
  - **Anonym**. Es wird keine Authentifizierung verwendet. (Standardwert)
  - **Allgemein**. Authentifiziert den FTP-Server mithilfe der angegebenen Benutzer-ID und des Kennworts.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für FTP-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für FTP-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n"
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Klicken Sie auf die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse zulassen**, um das Weiterleiten ausgeschlossener Ergebnisse zu erlauben oder zu verhindern.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Übereinstimmung nach Ereigniskategorie**.
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.

- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Benachrichtigungen über neue Alerts wurden gesendet.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

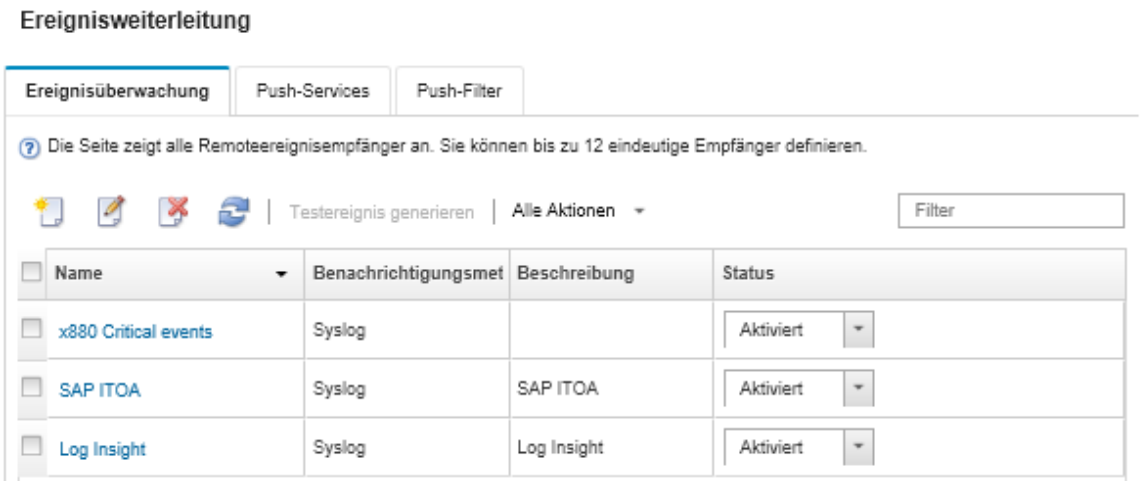
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden FTP-Server weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen REST-Web-Service einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an einen REST-Web-Service konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für einen REST-Web-Service zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** (). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **REST** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Ressourcenpfad ein, auf dem der Weiterleiter die Ereignisse senden soll (z. B. /rest/test).
- Wählen Sie das Protokoll aus, das für die Ereignisweiterleitung verwendet werden soll. Es kann einen der folgenden Werte aufweisen.
  - **HTTP**
  - **HTTPS**
- Wählen Sie die REST-Methode aus. Es kann einen der folgenden Werte aufweisen.
  - **PUT**
  - **POST**
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- **Optional:** 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.
  - **Keine Angabe**. Es wird keine Authentifizierung verwendet.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für REST-Web-Service-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für REST-Web-Service-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
{\"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]]\"}"
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Klicken Sie auf die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse zulassen**, um das Weiterleiten ausgeschlossener Ergebnisse zu erlauben oder zu verhindern.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Übereinstimmung nach Ereigniskategorie**.
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.
- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.

- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Benachrichtigungen über neue Alerts wurden gesendet.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

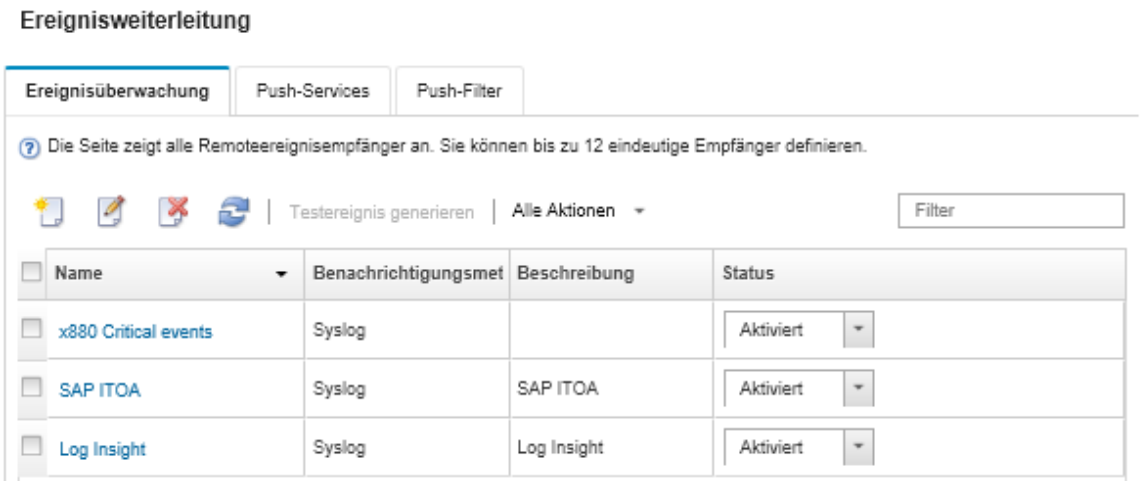
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden REST-Web-Service weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen Remote-SNMPv1- oder SNMPv3-Manager einrichten

Sie können Lenovo XClarity Administrator so konfigurieren, dass bestimmte Ereignisse an einen Remote-SNMPv1 oder SNMPv3-Manager weitergeleitet werden.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Informationen zur XClarity Administrator-MIB finden Sie unter Datei „lenovoMgrAlert.mib“.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für einen Remote-SNMPv1 oder SNMPv3-Manager zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **SNMPv1** oder **SNMPv3** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen und den Zielhost für die Ereignisweiterleitung ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist `162`.
- **Optional**: Geben Sie zusätzliche Informationen wie die Beschreibung, den Namen des Ansprechpartners und die Position ein.
- Wählen Sie die SNMP-Version. Es kann einen der folgenden Werte aufweisen.
  - **SNMPv1**. Wenn Sie diese Version auswählen, müssen Sie das Community-Kennwort angeben, das zusammen mit der SNMP-Anforderung an die Einheit gesendet wird.
  - **SNMPv3**. Dies ist die Standardversion, die für eine größere Sicherheit empfohlen wird. Geben Sie bei Auswahl von SNMPv3 optional die Werte für Benutzer-ID, Authentifizierungstyp und -kennwort und Datenschutztyp und -kennwort an.

    Wenn der SNMPv3-Trap-Empfänger die Engine-ID für die Instanz von XClarity Administrator benötigt, können Sie diese wie folgt herausfinden:

    1. Stellen Sie sicher, dass die Verbindungsparameter (Benutzername, AuthProtokoll, AuthKennwort, DSProtokoll, DSKennwort) mit den in XClarity Administrator definierten Werten übereinstimmen.
    2. Führen Sie mithilfe Ihrer bevorzugten Software (wie snmpwalk) eine SNMP-GET-Anforderung auf dem XClarity Administrator-Server durch. Nutzen Sie hierzu eine der folgenden Objektkennungen:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots: 1.3.6.1.6.3.10.2.1.2.0

       Verwenden Sie für den `snmpget`-Befehl das folgende Format. Beachten Sie, dass der Authentifizierungstyp für den -a Weiterleiter SHA oder leer (keine Authentifizierung) sein kann.
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDE
       ```

       Wenn die XClarity Administrator-IP-Adresse beispielsweise 192.0.1.0 lautet, der Authentifizierungstyp SHA und der Datenschutztyp AES ist, zeigt der folgende Befehl die EngineID an.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_
       ```

       Die folgende Beispielantwort wird zurückgegeben. In diesem Beispiel ist die engineID 0x80001370017F00000134C27E12.
       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.

- **Optional**: Wenn eine Trap-Authentifizierung erforderlich ist, geben Sie die Benutzer-ID und das Authentifizierungskennwort ein. Als Remote-SNMP-Manager muss die gleiche Benutzer-ID und das gleiche Kennwort eingegeben werden, zu dem auch die Traps weitergeleitet werden sollen.
- Wählen Sie das Authentifizierungsprotokoll aus, das vom Remote-SNMP-Manager verwendet wird, um den Trap-Sender zu verifizieren. Dies kann einer der folgenden Werte sein:
  - **SHA**. Verwendet das SHA-Protokoll, um sich mithilfe der angegebenen Benutzer-ID, des Kennworts und des Domänennamens am angegebenen SNMP-Server zu authentifizieren.
  - **Keine Angabe**. Es wird keine Authentifizierung verwendet.
- Wenn eine Trap-Verschlüsselung erforderlich ist, geben Sie den Datenschutztyp (Verschlüsselungsprotokoll) und das Kennwort ein. Es kann einen der folgenden Werte aufweisen. Als Remote-SNMP-Manager muss das gleiche Protokoll und das gleiche Kennwort eingegeben werden, zu dem die Traps weitergeleitet werden sollen.
  - **AES**
  - **DES**
  - **Keine Angabe**

Schritt 5. Klicken Sie auf die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse zulassen**, um das Weiterleiten ausgeschlossener Ergebnisse zu erlauben oder zu verhindern.

Schritt 6. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 7. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 8. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 9. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 10. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Übereinstimmung nach Ereigniskategorie**.
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.

1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 11. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.

- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Benachrichtigungen über neue Alerts wurden gesendet.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 12. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 13. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 14. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 15. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

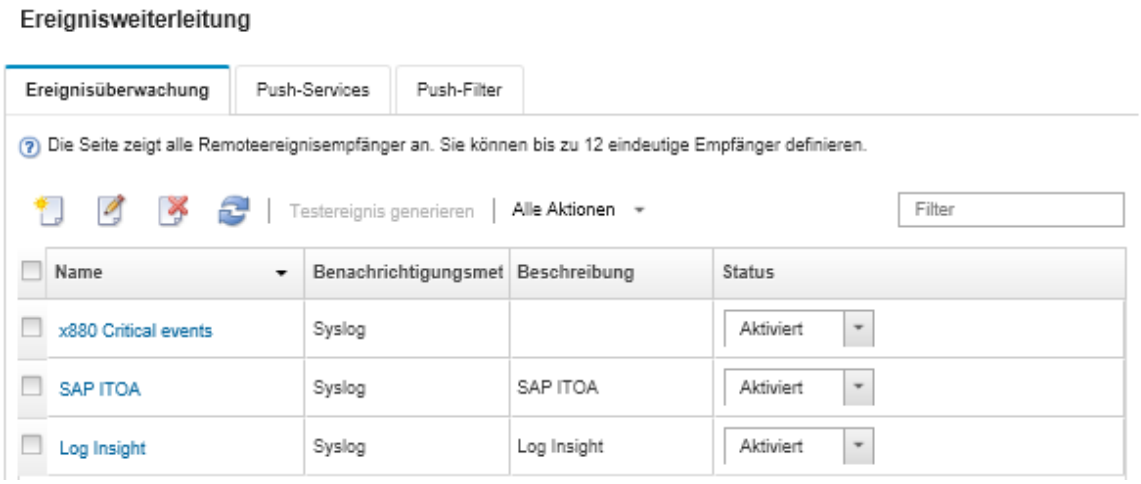
1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.

- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 16. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 17. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden Remote-SNMP-Manager weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).
- Laden Sie die MIB-Datei herunter, die Informationen zu SNMP-Traps enthält, indem Sie auf das Symbol **Erstellen** ( ) und dann auf **MIB-Datei herunterladen** auf der Registerkarte „Allgemein“ des Dialogfelds „Neue Ereignisweiterleitung“ klicken.

Datei „lenovoMgrAlert.mib“

Diese MIB-Datei (Management Information Base) beschreibt die SNMP-Traps, die von Lenovo XClarity Administrator generiert werden, einschließlich der Alerts, die von XClarity Administrator und verwalteten Einheiten ausgelöst wurden. Diese MIB-Datei kann in jedem SNMP-Trap-Manager kompiliert werden, sodass von XClarity Administrator gesendete SNMP-Traps sinnvoll wiedergegeben werden können.

Sie können die MIB-Datei von der Webschnittstelle herunterladen. Klicken Sie dazu in der Menüleiste auf **Überwachung → Ereignisweiterleitung** und dann auf das Symbol **Erstellen** ( ). Wählen Sie **SNMP** als Typ der Ereignisweiterleitung aus und klicken Sie dann unten im Dialogfenster auf **MIB-Datei herunterladen**.

Die folgenden Objekte sind in allen ausgehenden SNMP-Traps enthalten. Einige SNMP-Traps enthalten möglicherweise zusätzliche Objekte. Alle Objekte sind in der MIB-Datei beschrieben. Beachten Sie, dass die Wiederherstellungsinformationen nicht im Trap enthalten sind.

Anmerkung: Diese Liste kann in den verschiedenen Versionen von XClarity Administrator unterschiedlich sein.

- **mgrTrapAppId**. Dies ist der „Lenovo Event Manager“.
- **mgrTrapCommonEvtID**. Allgemeine Ereignis-ID
- **mgrTrapDateTime**. Das lokalisierte Datum und die Uhrzeit, die darstellen, wann das Ereignis aufgetreten ist
- **mgrTrapEventClass**. Ereignisquelle Hierbei kann es sich um Prüfung, Kühlung, Power, Datenträger, Hauptspeicher, Prozessoren, System, Test, Adapter, Erweiterung, IO-Modul oder Blade handeln.
- **mgrTrapEvtID**. Die eindeutige Kennung für das Ereignis
- **mgrTrapFailFRUs**. Eine durch Komma getrennte Liste der fehlerhaften FRU-UUIDs, falls zutreffend
- **mgrTrapFailSNs**. Eine durch Kommas getrennte Liste mit den Seriennummern der ausgefallenen FRUs, falls zutreffend
- **mgrTrapFullyQualifiedDomainName**. Der vollständig qualifizierte Domänenname: der Hostname und der Domänenname
- **mgrTrapID**. Trap-ID
- **mgrTrapMsgText**. Nachrichtentext (nur Englisch)
- **mgrTrapMsgID**. Nachrichten-ID
- **mgrTrapMtm**. Modelltyp der Einheit, die das Ereignis ausgelöst hat
- **mgrTrapService**. Wartbarkeitanzeige. Hierbei gibt es die Optionen 000 (Unbekannt), 100 (Keine), 200 (Service Center) oder 300 (Kunde)
- **mgrTrapSeverity**. Schweregradanzeige. Hierbei gibt es die Optionen Information, Warnung, Untergeordnet, Übergeordnet oder Kritisch
- **mgrTrapSN**. Seriennummer der Einheit, die das Ereignis ausgelöst hat
- **mgrTrapSrcIP**. IP-Adresse der Einheit, von der das ausgelöste Ereignis empfangen wurde
- **mgrTrapSrcLoc**. Position der Einheit, die das Ereignis ausgelöst hat, nur in Englisch (zum Beispiel Slot#xx)
- **mgrTrapSrcName**. Hostname oder Anzeigename der Einheit, die das Ereignis ausgelöst hat
- **mgrTrapSysContact**. Benutzerkonfigurierte Kontakt-ID
- **mgrTrapSysLocation**. Benutzerkonfigurierte Informationen zum Standort der Einheit
- **mgrTrapSystemName**. Einheitenname, Komponentenname und Steckplatzposition
- **mgrTrapTxtId**. Hostname oder IP-Adresse des Lenovo Event Manager-Servers, der den Trap ausgelöst hat
- **mgrTrapUserid**. Benutzer-ID, die dem Ereignis zugeordnet ist (wenn es sich um ein internes Ereignis handelt und die Ereignisklasse „Prüfung“ ist)
- **mgrTrapUuid**. UUID der Einheit, die das Ereignis ausgelöst hat

Ereignisweiterleitung an ein Syslog einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an ein Syslog konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für ein Syslog zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **Syslog** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen, den Zielhost und optional eine Beschreibung der Ereignisweiterleitung 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 können Sie das Format des Zeitstempels im Syslog auswählen. 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 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für Sylog-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für Sylog-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Klicken Sie auf die Umschalt-Schaltfläche **Ausgeschlossene Ereignisse zulassen**, um das Weiterleiten ausgeschlossener Ergebnisse zu erlauben oder zu verhindern.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Übereinstimmung nach Ereigniskategorie**.
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.

- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Benachrichtigungen über neue Alerts wurden gesendet.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

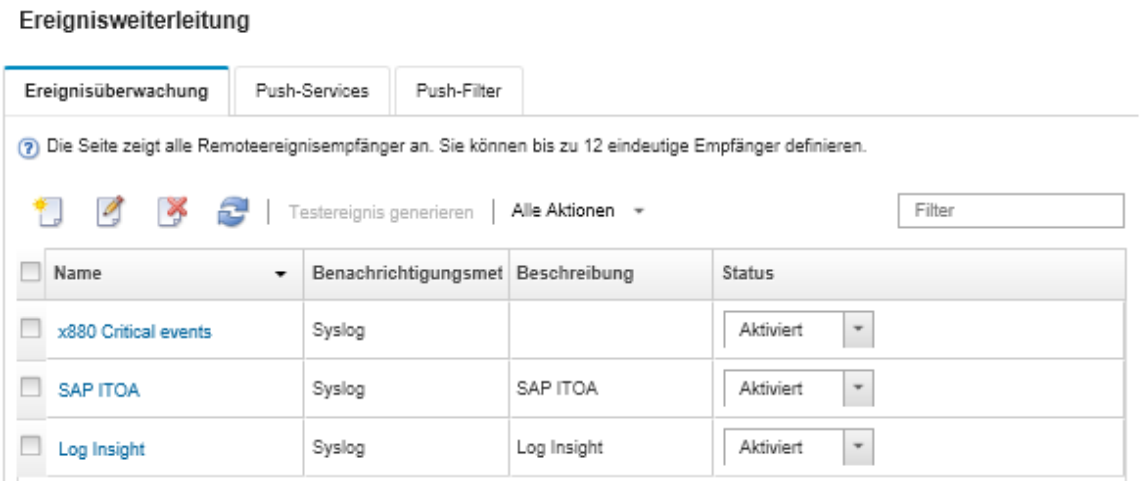
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an das entsprechende Syslog weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung aussetzen

Sie können die Ereignisweiterleitung aussetzen, indem Sie die Ereignisweiterleitung deaktivieren. Das Aussetzen der Ereignisweiterleitung unterbricht die Überwachung der eingehenden Ereignisse. Ereignisse, die empfangen werden, während die Überwachung ausgesetzt ist, werden nicht weitergeleitet.

Zu dieser Aufgabe

Der Status „Deaktiviert“ ist nicht permanent. Wenn der Verwaltungsknoten erneut gestartet wird, werden alle Ereignisweiterleitungen aktiviert.

Vorgehensweise

Gehen Sie wie folgt vor, um die Weiterleitung von Ereignissen zu deaktivieren.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Ereignisweiterleitung“ wird angezeigt.

Schritt 2. Wählen Sie für jede Ereignisweiterleitung, die ausgesetzt werden soll, in der Spalte **Status** die Option **Deaktivieren** aus.

Ereignisse an mobile Einheiten weiterleiten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisbenachrichtigungen per Push an mobile Einheiten übertragen werden.

Vorbereitende Schritte

Die folgenden Voraussetzungen müssen erfüllt sein, damit Ereignisse an mobile Einheiten weitergeleitet werden:

- Stellen Sie sicher, dass ein gültiger DNS-Server konfiguriert ist, damit Lenovo XClarity Administrator eine Verbindung zu den Push-Servern von Apple bzw. Google herstellen kann. Klicken Sie zum Konfigurieren auf **Verwaltung → Netzwerkzugriff → Netzwerkzugriff bearbeiten** und wählen Sie dann die Registerkarte **Interneteinstellungen** aus (siehe Netzwerkzugriff konfigurieren).
- Stellen Sie sicher, dass alle für die Ereignisverwaltung erforderlichen Ports im Netzwerk und in den Firewalls geöffnet sind. Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von Lenovo XClarity Administrator.

Zu dieser Aufgabe

Wenn die Lenovo XClarity Mobile-App auf einer mobilen Einheit installiert ist, können Sie festlegen, dass jede angeschlossene Lenovo XClarity Administrator-Instanz Ereignisbenachrichtigungen per Push an diese mobile Einheit überträgt. Wenn Push-Benachrichtigungen für eine bestimmte Instanz aktiviert sind, wird in Lenovo XClarity Administrator ein Abonnement für diese mobile Einheit erstellt.

Sie können die Ereignisse definieren, die per Push an die mobile Einheit übertragen werden, indem Sie für jede Lenovo XClarity Administrator-Instanz vordefinierte oder angepasste Ereignisfilter zuordnen. Die vordefinierten globalen Ereignisfilter sind standardmäßig aktiviert. Lenovo XClarity Administrator beginnt die Überwachung für eingehende Ereignisse anhand der Filterkriterien. Wenn eine Übereinstimmung gefunden wird, wird das Ereignis an die mobile Einheit weitergeleitet.

Weitere Informationen zu Lenovo XClarity Mobile und den unterstützten mobilen Einheiten finden Sie unter Lenovo XClarity Mobile-App verwenden.

Vorgehensweise

Um Push-Benachrichtigungen für diese mobile Einheit einzurichten, führen Sie in der Lenovo XClarity Mobile-App auf der mobilen Einheit die folgenden Schritte aus.

Schritt 1. Aktivieren Sie Push-Benachrichtigungen:

- Sie können Push-Benachrichtigungen aktivieren, wenn Sie eine Verbindung zu einer Lenovo XClarity Administrator-Instanz herstellen. Push-Benachrichtigungen sind standardmäßig aktiviert.
- Sie können Push-Benachrichtigungen für vorhandene Verbindungen aktivieren, indem Sie einen oder mehrere Ereignisfilter aktivieren.

Schritt 2. Weisen Sie globale Ereignisfilter zu, um anzugeben, welche Ereignisse an die mobile Einheit weitergeleitet werden sollen:

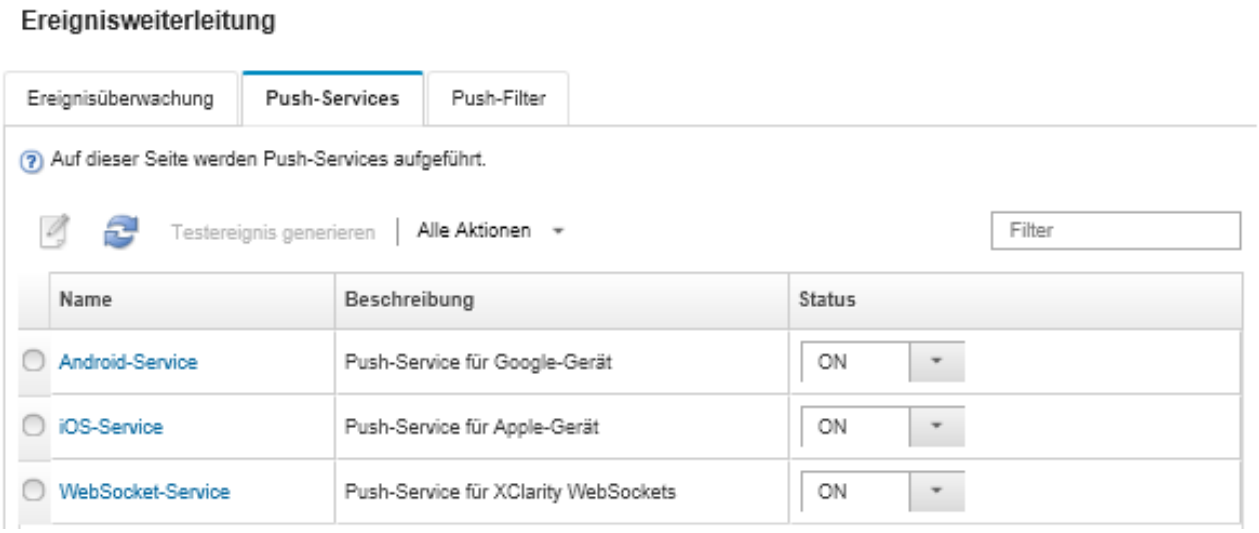
Anmerkung: Das Hinzufügen und Entfernen globaler Filter aus dem Abonnement ist nur über die Lenovo XClarity Mobile-App möglich. Sie können globale Filter nur über die Webschnittstelle von Lenovo XClarity Administrator erstellen. Informationen zum Erstellen von angepassten globalen Ereignisfiltern finden Sie unter Ereignisfilter für mobile Einheiten und WebSockets erstellen.

1. Tippen Sie auf **Einstellungen → Push-Benachrichtigungen**. Es wird eine Liste der Lenovo XClarity Administrator-Verbindungen angezeigt.

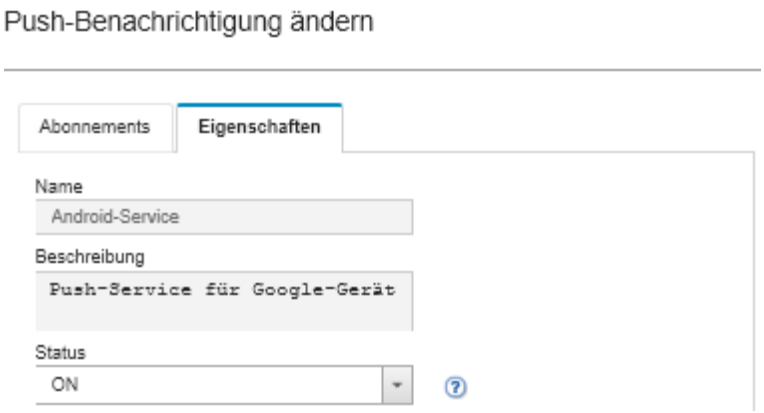
2. Tippen Sie auf die Instanz von Lenovo XClarity Administrator, um eine Liste der Push-Filter anzuzeigen.
3. Aktivieren Sie die Ereignisfilter für die Ereignisse, die für die Lenovo XClarity Administrator-Instanz an die mobile Einheit per Push übertragen werden sollen.
4. Tippen Sie auf **Test-Push-Benachrichtigung durch Berühren generieren**, um zu überprüfen, ob die Ereignisbenachrichtigungen ordnungsgemäß per Push übertragen werden.

Ergebnisse

Sie können Abonnements über die Seite „Ereignisweiterleitung“ der Lenovo XClarity Administrator-Webschnittstelle verwalten. Klicken Sie auf **Überwachung → Ereignisweiterleitung**, um die Seite „Ereignisweiterleitung“ anzuzeigen.



- Sie können die Eigenschaften für den Benachrichtigungs-Service der Einheit auf der Seite „Ereignisweiterleitung“ auf der Registerkarte **Push-Service** ändern. Klicken Sie dazu auf den Link für den Push-Benachrichtigungs-Service (Google oder Apple) in der Spalte **Name**, um das Dialogfenster „Push-Benachrichtigung ändern“ anzuzeigen. Klicken Sie dann auf die Registerkarte **Eigenschaften**.

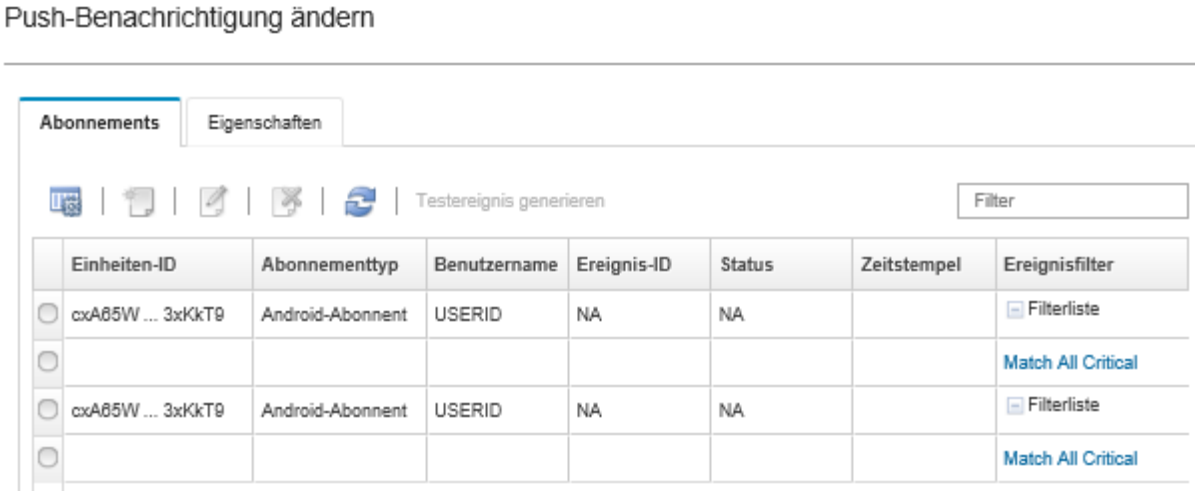


- Sie können Abonnements aktivieren und deaktivieren:
  - Zum Aktivieren und Deaktivieren aller Abonnements für einen bestimmten Einheitenbenachrichtigungs-Service legen Sie auf der Seite „Ereignisweiterleitung“ auf der Registerkarte **Push-Service** in der Tabelle für den Benachrichtigungs-Service dieser Einheit den Status **EIN** oder **AUS** fest.

  - Zum Aktivieren und Deaktivieren aller Abonnements für eine bestimmte Einheit tippen Sie in der Lenovo XClarity Mobile-App auf **Einstellungen → Push-Benachrichtigung** und aktivieren bzw. deaktivieren Sie dann die Option „Aktiviert“ für Push-Benachrichtigungen.
  - Zum Aktivieren und Deaktivieren eines bestimmten Abonnements tippen Sie in der Lenovo XClarity Mobile-App auf **Einstellungen → Push-Benachrichtigung** und dann auf eine Lenovo XClarity Administrator-Verbindung. Aktivieren Sie mindestens einen Ereignisfilter oder deaktivieren Sie alle Ereignisfilter.
- Sie können auf der Seite „Ereignisweiterleitung“ über die Registerkarte **Push-Service** ein Testereignis für alle Abonnements für einen bestimmten mobilen Service generieren, indem Sie den mobilen Service auswählen und auf **Testereignis generieren** klicken.
- Sie können eine Liste der aktuellen Abonnements anzeigen. Klicken Sie auf der Seite „Ereignisweiterleitung“ auf der Registerkarte **Push-Service** auf den Link für den Benachrichtigungs-Service der Einheit (Android oder iOS) in der Spalte **Name**, um das Dialogfenster Push-Benachrichtigung ändern anzuzeigen. Klicken Sie dann auf die Registerkarte **Abonnements**. Die einzelnen Abonnements werden über die Einheiten-ID identifiziert.

  Tipps:

  - Die Einheiten-ID besteht aus den ersten und letzten 6 Ziffern der Pushregistrierungskennung. Die Pushregistrierungskennung finden Sie in der Lenovo XClarity Mobile-App, indem Sie auf **Einstellungen → Info → Pushregistrierungskennung** tippen.
  - Wenn Sie als Benutzer mit einer der folgenden Rollen angemeldet sind, werden alle Abonnements angezeigt. Andernfalls werden nur Abonnements für den angemeldeten Benutzer angezeigt.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- Sie können die Liste der Ereignisfilter anzeigen, die dem Abonnement zugeordnet sind. Erweitern Sie dazu im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** die **Filterliste** in der Spalte **Ereignisfilter** für das Abonnement.



- Sie können im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** Ereignisfilter für ein bestimmtes Abonnement erstellen, indem Sie das Abonnement auswählen und auf das Symbol für **Erstellen** ( ) klicken.

  Anmerkung: Diese Ereignisfilter gelten nur ein bestimmtes Abonnement und können nicht von anderen Abonnements verwendet werden.

Sie können auch einen Ereignisfilter bearbeiten oder entfernen, indem Sie den Ereignisfilter auswählen und auf das Symbol für **Bearbeiten** () bzw. das Symbol für **Entfernen** () klicken.

- Im Dialogfenster „Push-Benachrichtigung ändern“ können Sie auf der Registerkarte **Abonnements** den Status des zuletzt versuchten Push-Vorgangs für ein bestimmtes Abonnement ermitteln. Die Spalte **Zeitstempel** gibt Datum und Uhrzeit des letzten Push-Vorgangs an. Der **Status** gibt an, ob die Push-Benachrichtigung erfolgreich an den Push-Service übermittelt wurde. Es ist kein Status im Hinblick darauf verfügbar, ob die Push-Benachrichtigung erfolgreich vom Service an die Einheit übermittelt wurde. Wenn die Übermittlung an den Push-Service nicht erfolgreich war, werden in der Statusspalte weitere Informationen zum Fehler angezeigt.
- Sie können im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** ein Testereignis für ein bestimmtes Abonnement generieren, indem Sie das Abonnement auswählen und auf **Testereignis generieren** klicken.
- Sie können im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** ein Abonnement entfernen, indem Sie das Abonnement auswählen und auf das Symbol für **Entfernen** () klicken.

Ereignisweiterleitung an WebSocket-Services

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisbenachrichtigungen an WebSocket-Services gepusht werden.

Zu dieser Aufgabe

Die WebSocket-Abonnements werden nicht dauerhaft in Lenovo XClarity Administrator gespeichert. Wenn Lenovo XClarity Administrator neu gestartet wird, müssen die WebSocket-Abonnements erneuert werden.

Vorgehensweise

Um Ereignisbenachrichtigungen an einen WebSocket-Service zu pushen, führen Sie die folgenden Schritte durch.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Ereignisweiterleitung“ wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Push-Services**.

Schritt 3. Klicken Sie in der Spalte **Name** auf den Link für den **WebSocket-Service**. Das Dialogfenster „Push-Benachrichtigung ändern“ wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Abonnements**.

Schritt 5. Klicken Sie auf das Symbol **Erstellen** ().

Schritt 6. Geben Sie die IP-Adresse des Zielhosts ein.

Schritt 7. Klicken Sie auf **Erstellen**.

Schritt 8. Wählen Sie das neue Abonnement aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den WebSocket-Service weitergeleitet werden.

Ergebnisse

Über die Registerkarte **Abonnements** auf dem Dialogfeld „Push-Benachrichtigung ändern“ können Sie die folgenden Aktionen für ein ausgewähltes WebSocket-Abonnement ausführen:

- Aktualisieren Sie die Liste der WebSocket-Services, indem Sie auf Symbol **Aktualisieren** () klicken.
- Abonnements durch Auswahl der Abonnements und Klicken auf das Symbol **Löschen** () löschen

- Status des letzten versuchten Pushs eines bestimmten Abonnements durch Anzeigen des Inhalts der Spalte **Status** ermitteln. Wenn der Versuch fehlgeschlagen ist, enthält diese Spalte eine Nachricht, die den Fehler beschreibt.

Über die Registerkarte **Eigenschaften** auf dem Dialogfeld Push-Benachrichtigung ändern können Sie die folgenden Aktionen ausführen:

- Eigenschaften des WebSocket-Services ändern, einschließlich der Verbindungsleerlaufzeit, der maximalen Puffergröße, der maximalen Anzahl an Abonnenten und des Registrierungstimeout-Zeitraums
- den WebSocket-Service durch Klicken auf **Standardwerte wiederherstellen** auf die Standardeinstellungen zurücksetzen
- das Pushen der Ereignisbenachrichtigungen für alle Abonnements des WebSocket-Services durch Setzen des **Status** auf „Aus“ aussetzen

Über die Registerkarte **Push-Service** auf der Seite „Ereignisweiterleitung“ können Sie für alle WebSocket-Abonnements ein Testereignis generieren, indem Sie den WebSocket-Service auswählen und auf **Testereignis generieren** klicken.

Ereignisfilter für mobile Einheiten und WebSockets erstellen

Sie können globale Ereignisfilter erstellen, die in einem oder mehreren Abonnements für mobile Einheiten und WebSockets verwendet werden können. Sie können auch Ereignisfilter erstellen, die nur für ein Abonnement gelten.

Vorbereitende Schritte

Zum Erstellen von Ereignisfiltern sind Supervisorberechtigungen erforderlich.

Sie können maximal 20 globale Ereignisfilter erstellen.

Zu dieser Aufgabe

Die folgenden globalen Ereignisfilter sind vordefiniert:

- **Alle kritischen Ereignisse abgleichen**. Dieser Filter findet Übereinstimmungen mit allen kritischen Ereignissen, die von einer verwalteten Einheit oder XClarity Administrator generiert werden.
- **Alle Warnungen abgleichen**. Dieser Filter findet Übereinstimmungen mit allen Warnereignissen, die von einer verwalteten Einheit oder XClarity Administrator generiert werden.

Vorgehensweise

Gehen Sie wie folgt vor, um einen globalen Ereignisfilter zu erstellen.

- Erstellen Sie einen globalen Ereignisfilter, der von jedem beliebigen Abonnement verwendet werden kann.
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Ereignisweiterleitung“ wird angezeigt.
  2. Klicken Sie auf die Registerkarte **Push-Filter**.
  3. Klicken Sie auf das Symbol **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds „Neuer Ereignisfilter“ wird angezeigt.
  4. Geben Sie den Namen und eine Optionsbeschreibung für diesen Ereignisfilter an.
  5. Klicken Sie auf **Weiter**, um die Registerkarte **Systeme** anzuzeigen.
  6. Wählen Sie die Einheiten aus, die Sie überwachen möchten.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

7. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.
8. Wählen Sie die Komponenten und Schweregrade aus, für die Sie Ereignisse weiterleiten möchten.

   Tipp:
   - Um alle Hardwareereignisse weiterzuleiten, wählen Sie **Alle Ereignisse abgleichen** aus.
   - Um Prüfereignisse weiterzuleiten, wählen Sie **Alle Prüfereignisse einschließen** aus.
   - Um Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
9. Klicken Sie auf **Erstellen**.

- Erstellen Sie einen Ereignisfilter für ein bestimmtes Abonnement:
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Neue Ereignisweiterleitung“ wird angezeigt.
  2. Klicken Sie auf die Registerkarte **Push-Filter**.
  3. Wählen Sie in der Tabellenspalte „Name“ den Link für den Typ der mobilen Einheit (Android oder iOS) aus. Das Dialogfenster „Push-Benachrichtigung ändern“ wird angezeigt.
  4. Klicken Sie auf die Registerkarte **Abonnements**, um eine Liste der aktiven Abonnements anzuzeigen.
  5. Wählen Sie das Abonnement aus und klicken Sie auf das Symbol **Erstellen** ( ). Das Dialogfenster „Neuer Ereignisfilter“ wird mit der Registerkarte **Allgemein** angezeigt.
  6. Geben Sie den Namen und eine Optionsbeschreibung für diesen Ereignisfilter an.
  7. Klicken Sie auf **Weiter**, um die Registerkarte **Systeme** anzuzeigen.
  8. Wählen Sie die Einheiten aus, die Sie überwachen möchten.

     Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.
  9. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.
  10. Wählen Sie die Komponenten und Schweregrade aus, für die Sie Ereignisse weiterleiten möchten.

      Tipp:
      - Um alle Hardwareereignisse weiterzuleiten, wählen Sie **Alle Ereignisse abgleichen** aus.
      - Um Prüfereignisse weiterzuleiten, wählen Sie **Alle Prüfereignisse einschließen** aus.
      - Um Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  11. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

Über die Registerkarte „Push-Filter“ der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für einen ausgewählten Ereignisfilter ausführen:

- Aktualisieren Sie die Liste der Ereignisfilter durch Klicken auf das Symbol für **Aktualisieren** ().
- Zeigen Sie Details zu einem bestimmten Ereignisfilter an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien von Ereignisfiltern, indem Sie auf das Symbol für **Bearbeiten** () klicken.

Löschen Sie den Ereignisfilter, indem Sie auf das Symbol für **Löschen** () klicken.

Mit Jobs arbeiten

Jobs sind länger laufende Tasks, die auf einer oder mehreren Einheiten ausgeführt werden. Sie können bestimmte Jobs planen, damit sie nur einmal (sofort oder zu einem späteren Zeitpunkt), wiederkehrend oder nur bei Auftreten eines bestimmten Ereignisses ausgeführt werden.

Jobs werden im Hintergrund ausgeführt. Sie können den Status jedes Jobs im Jobprotokoll anzeigen.

Jobs überwachen

Sie können ein Protokoll aller Jobs anzeigen, die von Lenovo XClarity Administrator gestartet wurden. Das Jobprotokoll umfasst Jobs, die aktiv oder abgeschlossen sind oder Fehler enthalten.

Zu dieser Aufgabe

Jobs sind länger laufende Tasks, die auf einer oder mehreren Einheiten ausgeführt werden. Wenn Sie beispielsweise ein Betriebssystem auf mehreren Servern implementieren, wird jede Serverimplementierung als separater Job aufgelistet.

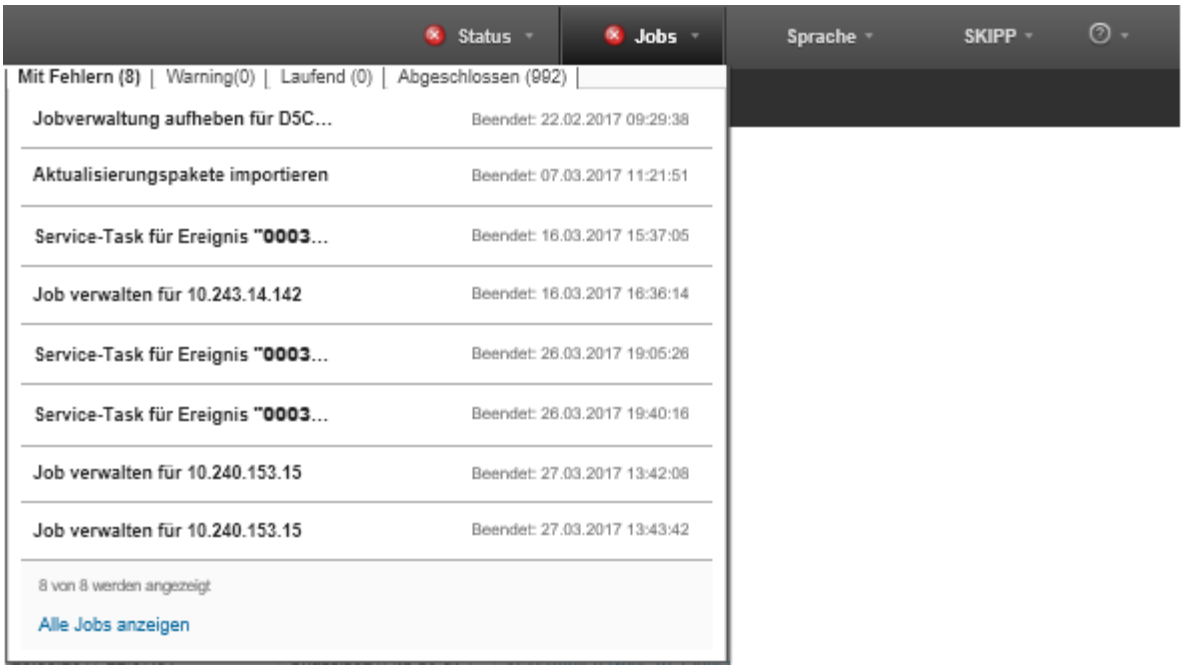
Jobs werden im Hintergrund ausgeführt. Sie können den Status jedes Jobs im Jobprotokoll anzeigen.

Das Jobprotokoll enthält Informationen zu jedem Job. Das Protokoll kann maximal 1.000 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.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um das Jobprotokoll anzuzeigen.

- Klicken Sie auf der Titelleiste von XClarity Administrator auf **Jobs**, um eine Übersicht der Jobs anzuzeigen, die ausgeführt werden, abgeschlossen sind oder Fehler aufweisen.



In dieser Pulldown-Liste können Sie auf die folgenden Registerkarten klicken:
- **Fehler**. Zeigt eine Liste aller Jobs an, denen Fehler zugeordnet sind.
- **Warnungen**. Zeigt eine Liste aller Jobs an, denen Warnungen zugeordnet sind.
- **Laufend**. Zeigt eine Liste aller Jobs an, die derzeit ausgeführt werden.
- **Abgeschlossen**. Zeigt eine Liste aller Jobs an, die abgeschlossen sind.

Bewegen Sie den Mauszeiger in der Pulldown-Liste über einen Jobeintrag, um weitere Informationen zum Job zu erhalten, darunter Status, Fortschritt und Benutzer, der den Job erstellt hat.

- Klicken Sie in der Titelleiste von XClarity Administrator auf **Jobs** und klicken Sie anschließend auf den Link **Alle Jobs anzeigen**, um die Seite Jobstatus anzuzeigen.
- Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachen → Jobs** und klicken Sie anschließend auf die Registerkarte **Jobstatus**, um die Seite Jobstatus anzuzeigen.

Nach dieser Aufgabe

Die Seite Jobs wird mit einer Liste aller aktiven Jobs für XClarity Administrator angezeigt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie Jobpläne, indem Sie auf die Registerkarte **Geplante Jobs** klicken (siehe Jobs planen).
- Sie können weitere Informationen zu einem bestimmten Job anzeigen, indem Sie auf die Jobbeschreibung in der Spalte **Jobs** klicken. Ein Dialogfenster wird mit einer Liste von Subtasks (Subjobs) und deren Zielen, einer Zusammenfassung der Subtasks, einschließlich aller erforderlichen Aktionen und Protokolldetails mit Schweregrad und Zeitstempel für jede Nachricht angezeigt. Sie können auswählen, ob Sie die Protokolle für untergeordnete Tasks ausblenden oder anzeigen möchten.
- Bei geplanten Jobs können Sie Informationen zum Zeitplan des Jobs anzeigen, indem Sie auf „diesen“ Link unter der Jobbeschreibung in der Spalte **Jobs** klicken.
- Ändern Sie die Anzahl der Jobs, die pro Seite angezeigt werden. Der Standardwert ist zehn Jobs. Sie können 25, 50 oder alle Jobs anzeigen.
- Grenzen Sie die Liste der angezeigten Jobs ein:
  - Listen Sie nur Jobs von einer bestimmten Quelle auf, indem Sie auf **Jobtypen** klicken und eine der folgenden Optionen auswählen.
    - **Alle Jobtypen**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Fernzugriff**
    - **System-ID**
    - **BS-Images**
    - **BS-Bereitstellung**
    - **BS-Profil-Export**
    - **Custom**
    - **Inventory**
    - **Unknown**
  - Listen Sie nur geplante Jobs auf, die einem bestimmten Zeitplantyp zugeordnet sind, indem Sie auf **Zeitplantypen** klicken und eine der folgenden Optionen auswählen.

  - **Alle Zeitplantypen**
  - **Einmalig**
  - **Wiederkehrend**
  - **Ausgelöst**
- Klicken Sie auf das Symbol **Jobs mit Fehler-/Warnmeldung ausblenden** () um Jobs mit Fehler- oder Warnmeldung anzuzeigen oder auszublenden.
- Klicken Sie auf das Symbol **Laufende Jobs ausblenden** (), um Jobs, die gerade ausgeführt werden, anzuzeigen oder auszublenden.
- Klicken Sie auf das Symbol **Abgeschlossene Jobs ausblenden** (), um abgeschlossene Jobs anzuzeigen oder auszublenden.
- Zeigen Sie nur Jobs an, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
- Wenn auf der Seite ein Filter angewendet wird, entfernen Sie den Filter, indem Sie auf das Symbol **Alle Jobs anzeigen** klicken ().
- Sortieren Sie die Jobs durch Klicken auf eine Spaltenüberschrift spaltenweise.

- Exportieren Sie die Jobliste als CSV-Datei, indem Sie auf das Symbol **Als CSV exportieren** () klicken.

  Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.
- Brechen Sie laufende Jobs oder Subtasks ab, indem Sie einen oder mehrere laufende Jobs auswählen und auf das Symbol **Stoppen** () klicken.

  Anmerkung: Es kann einige Minuten dauern, den Job abzubrechen.
- Löschen Sie abgeschlossenen Jobs oder Subtasks aus dem Jobprotokoll, indem Sie einen oder mehrere abgeschlossene Jobs oder Subtasks auswählen und auf das Symbol **Löschen** () klicken.
- Exportieren Sie Informationen zu bestimmten Jobs, indem Sie die Jobs auswählen und auf das Symbol **Als CSV exportieren** klicken ().
- Aktualisieren Sie das Jobprotokoll durch Klicken auf das Symbol **Aktualisieren** ().

Jobs planen

Sie können Zeitpläne in Lenovo XClarity Administrator erstellen, um bestimmte Tasks zu bestimmten Zeiten auszuführen.

Zu dieser Aufgabe

Sie können die folgenden Jobtypen planen:
- Einfache Tasks, z. B. Ausschalten und Neustarten
- Servicedaten für bestimmte Einheiten sammeln
- Firmwareaktualisierungs- und BS-Einheitentreiber-Kataloge auf der Lenovo Website aktualisieren
- Aktualisierungskatalog von XClarity Administrator auf der Lenovo Website aktualisieren
- Firmware von der Lenovo Website herunterladen
- Firmware und BS-Einheitentreiber auf verwalteten Einheiten aktualisieren
- Daten und Einstellungen von XClarity Administrator sichern
- Switch-Konfigurationsdaten sichern und wiederherstellen

Sie können die folgenden Zeitplantypen für Jobs auswählen:

- nur einmal (sofort oder zu einem späteren Zeitpunkt)
- wiederkehrend
- wenn ein bestimmtes Ereignis auftritt

Vorgehensweise

Gehen Sie wie folgt vor, um einen Job zu erstellen und zu planen.

- Erstellen Sie den Jobplan bei komplexen Tasks, z. B. Aktualisieren von Firmware und Sammeln von Servicedaten, auf der aktuellen Taskseite oder im aktuellen Dialogfenster.
  1. Klicken Sie auf **Zeitplan**, um einen Zeitplan zum Ausführen dieses Tasks zu erstellen. Das Dialogfenster „Neuen Job planen“ wird angezeigt.
  2. Geben Sie einen Namen für den Job ein.
  3. Geben Sie an, wann der Job ausgeführt werden soll. Die verfügbaren Optionen sind vom Jobtyp abhängig. Manche Jobs können nicht wiederkehren oder durch ein Ereignis ausgelöst werden.
     - **Einmalig**. Diese Jobs werden nur einmal ausgeführt. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll.
     - **Wiederkehrend**. Diese Jobs werden mehrmals ausgeführt. Geben Sie an, wann und wie häufig dieser Job ausgeführt werden soll.
     - **Durch Ereignis ausgelöst**. Diese Jobs werden ausgeführt, wenn ein bestimmtes Ereignis auftritt.
       a. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       b. Wählen Sie das Ereignis aus, das den Job auslösen soll.
  4. Klicken Sie auf **Job erstellen**.
- Erstellen Sie den Jobplan bei einfachen Tasks, z. B. Einschalten und Neustarten, auf der Seite „Jobs“.
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachen → Jobs** und klicken Sie anschließend auf die Registerkarte **Geplanter Job**, um die Seite „Geplante Jobs“ anzuzeigen.
  2. Klicken Sie auf das Symbol **Erstellen** ( ), um das Dialogfenster „Neue Jobs planen“ anzuzeigen.
  3. Geben Sie einen Namen für den Job ein.
  4. Geben Sie an, wann der Job ausgeführt werden soll.
     - **Einmalig**. Diese Jobs werden nur einmal ausgeführt.
       a. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       b. Wählen Sie verwaltete Einheiten aus, auf denen der Job ausgeführt werden soll.
     - **Wiederkehrend**. Diese Jobs werden mehrmals ausgeführt.
       a. Geben Sie an, wann und wie häufig dieser Job ausgeführt werden soll.
       b. Wählen Sie verwaltete Einheiten aus, auf denen der Job ausgeführt werden soll**.**
     - **Durch Ereignis ausgelöst**. Diese Jobs werden ausgeführt, wenn ein bestimmtes Ereignis auftritt.
       a. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       b. Wählen Sie verwaltete Einheiten aus, auf denen der Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       c. Wählen Sie das Ereignis aus, das den Job auslösen soll.
  5. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

Die Registerkarte Geplante Jobs wird mit einer Liste aller Jobpläne in XClarity Administrator angezeigt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Sie können Informationen zu allen aktiven und abgeschlossenen Jobs für einen bestimmten Jobplan anzeigen, indem Sie auf den Link in der Spalte **Job** klicken.
  - Sie können die Liste der angezeigten Jobpläne auf einen bestimmten Zeitplantyp beschränken, indem Sie auf **Zeitplantypen** klicken und eine der folgenden Optionen auswählen:
    - **Alle Zeitplantypen**
    - **Einmalig**
    - **Wiederkehrend**
    - **Ausgelöst**
  - Sie können Jobpläne mit einem bestimmten Status ausblenden oder anzeigen, indem Sie auf eines der folgenden Symbole klicken:
    - Alle geplanten Jobs, die aktiv sind, indem Sie auf das Symbol **Aktiv** klicken ( ).
    - Alle geplanten Jobs, die nicht aktiv sind, indem Sie auf das Symbol **Pausiert** klicken ( ).
    - Alle geplanten Jobs, die bereits ausgeführt wurden und die gemäß Planung nicht erneut ausgeführt werden sollen, indem Sie auf das Symbol **Beendet** klicken ( ).
  - Zeigen Sie nur geplante Jobs an, die einen bestimmten Text enthalten, indem Sie Text in das Feld **Filter** eingeben.
  - Sortieren Sie die geplanten Jobs spaltenweise durch Klicken auf eine Spaltenüberschrift.
- Wann der Job zuletzt ausgeführt wurde, wird in der Spalte **Letzte Ausführung** angezeigt. Zeigen Sie den Status des zuletzt ausgeführten Jobs an, indem Sie auf den Link „Jobstatus“ in dieser Spalte klicken.

- Wann der Job zum nächsten Mal ausgeführt wird, wird in der Spalte **Nächste Ausführung** angezeigt. Zeigen Sie eine Liste aller zukünftigen Daten und Uhrzeiten an, indem Sie auf den Link „Mehr“ in dieser Spalte klicken.
- Führen Sie den diesem Zeitplan zugeordneten Job sofort aus, indem Sie auf das Symbol **Ausführen** klicken ().
- Deaktivieren oder aktivieren Sie einen Jobplan, indem Sie auf das Symbol **Pausieren** () oder das Symbol **Aktivieren** () klicken.
- Kopieren und bearbeiten Sie einen Jobplan, indem Sie auf das Symbol **Kopieren** klicken ().
- Bearbeiten Sie einen Jobplan, indem Sie auf das Symbol **Bearbeiten** klicken ().
- Löschen Sie einen oder mehrere ausgewählte Jobpläne, indem Sie auf das Symbol **Löschen** klicken ().
- Exportieren Sie Informationen zu bestimmten Jobplänen, indem Sie die Pläne auswählen und auf das Symbol **Als CSV exportieren** klicken ().
- Aktualisieren Sie die Liste der Jobpläne, indem Sie auf **Alle Aktionen → Aktualisieren** klicken.

Auflösung und Kommentare zu einem Job hinzufügen

Sie können eine Auflösung und Kommentare zu abgeschlossenen Jobs hinzufügen, unabhängig vom Erfolgs- oder Fehlerstatus. Dies kann für einen übergeordneten Job und Subtasks im Job durchgeführt werden.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um eine Auflösung und Kommentare zu einem Job hinzuzufügen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachen → Jobs** und klicken Sie anschließend auf die Registerkarte **Jobstatus**, um die Seite „Jobstatus“ anzuzeigen.

Schritt 2. Klicken Sie auf den Link des Jobs in der Spalte **Job**, um die Jobdetails anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Hinweise** (), um das Dialogfeld „Hinweise“ anzuzeigen.

In diesem Dialogfenster finden Sie einen Verlauf aller Hinweise und Lösungen, die zum Job hinzugefügt wurden. Sie können den Verlauf löschen, indem Sie auf **Alle Datensätze löschen** klicken.

Schritt 4. Wählen Sie eine der folgenden Lösungen aus.
- **Keine Änderungen**
- **Untersuchen**
- **Behoben**
- **Abgebrochen**

Schritt 5. Fügen Sie eine Anmerkung im Feld **Hinweis** hinzu.

Schritt 6. Klicken Sie auf **Übernehmen**.

Die Lösung wird auf der Seite „Jobstatus“ in der **Status**-Spalte für diesen Job angezeigt.

Beziehungen zwischen Jobs und Ereignissen anzeigen

Ein *Flussdiagramm* ist eine grafische Ansicht, die Beziehung zwischen Aktivitäten (einschließlich der Jobs und Ereignisse) anzeigt, die manuell von einem Benutzer eingeleitet oder automatisch von Lenovo XClarity Administrator initiiert werden. Das Flussdiagramm hilft dabei, Probleme zu identifizieren, indem es die

Abfolge von initiierten Aktionen veranschaulicht, sowie von generierten Ereignissen, dem Zeitpunkt ihrer Generierung und ihrer Ursache.

Vorbereitende Schritte

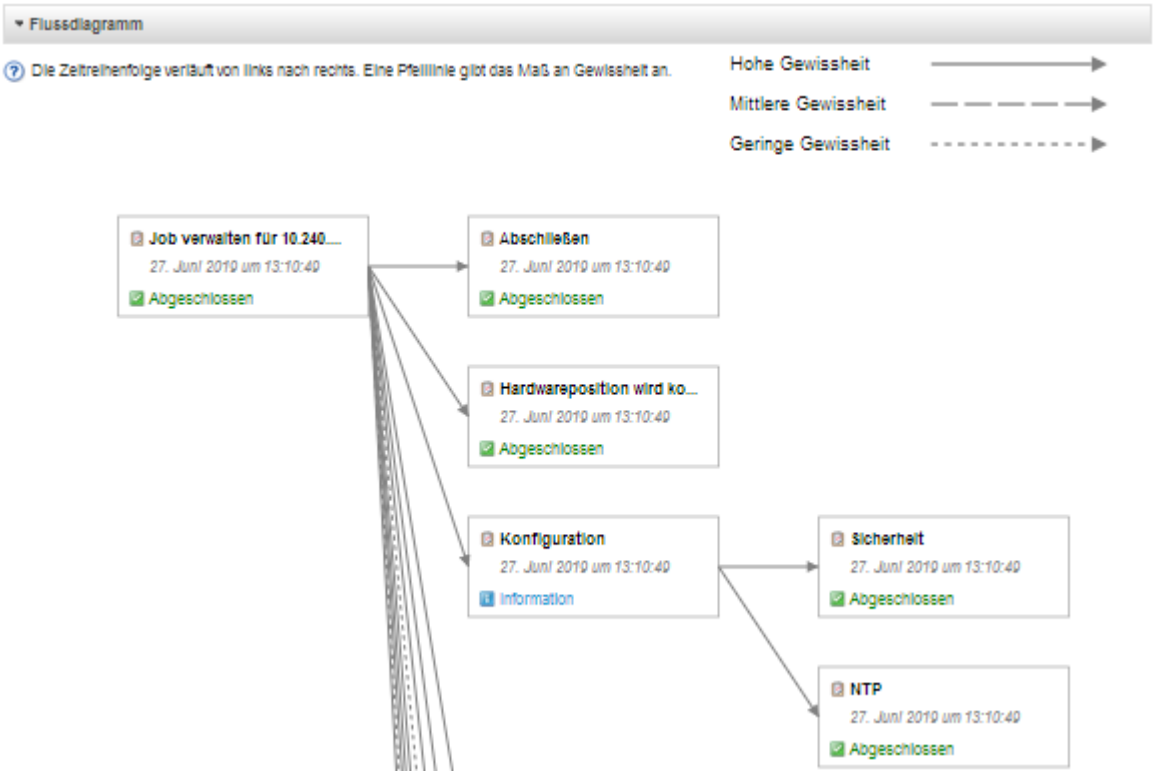
Die Aktivitätsflüsse sind standardmäßig deaktiviert. Sie müssen Aktivitätsflüsse aktivieren, bevor für eine Aktivität Flüsse erzeugt werden können. Sie können Flüsse nur für Aktivitäten anzeigen, die auftreten, wenn der Aktivitätsfluss aktiviert ist.

Achtung: Aktivitätsflüsse erhöhen die Speichernutzung um XClarity Administrator. Es wird empfohlen, Aktivitätsflüsse nicht zu aktivieren, wenn die Speichernutzung von XClarity Administrator bereits hoch ist.

Zu dieser Aufgabe

Das folgende Beispiel zeigt ein Flussdiagramm. Die Abfolge der Ereignisse fließt von links nach rechts. Jeder Knoten im Fluss stellt eine einzelne Aktivität dar und enthält die Beschreibung der Aktivität, das Datum und den Status. Sie können den Cursor über den Knotentitel bewegen, um zusätzliche Informationen über die Aktivität anzuzeigen.

Der Stil der Linien zwischen den Knoten gibt die Sicherheit der Beziehung zwischen Knoten an.
- Durchgezogene Linien repräsentieren eine hohe Sicherheit.
- Langgestrichelte Linien repräsentieren eine mittlere Sicherheit.
- Kurzgestrichelte Linien stellen eine geringe Sicherheit dar.



Vorgehensweise

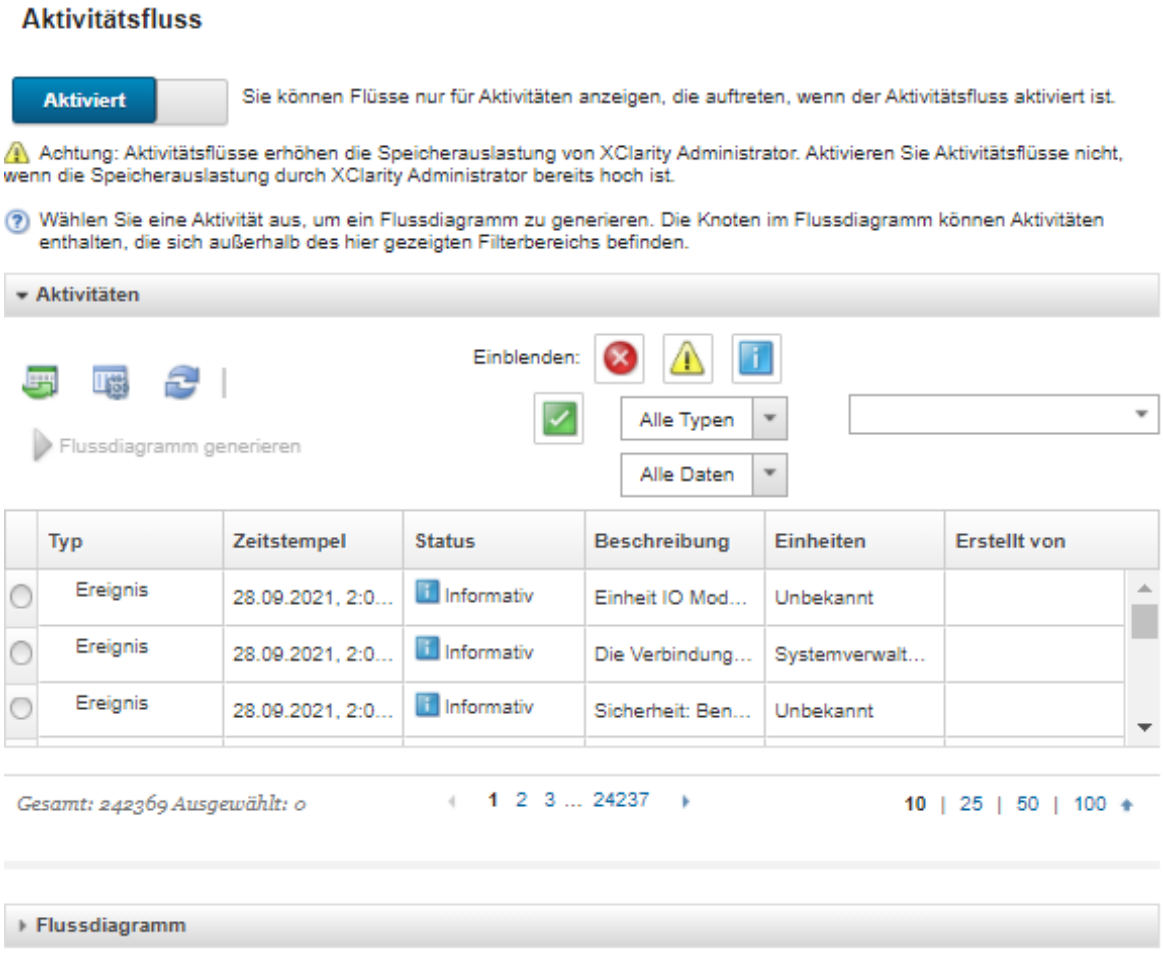
Gehen Sie wie folgt vor, um das Flussdiagramm für eine bestimmte Aktivität anzuzeigen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Überwachung → Aktivitätenfluss**, um die Seite „Aktivitäten“ anzuzeigen.

Schritt 2. Aktivieren Sie Aktivitätsflüsse, indem Sie **Aktivitätsfluss aktivieren** auswählen.

Schritt 3. Wählen Sie im Abschnitt **Aktivitäten** den Job oder das Ereignis aus.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Aktivitäten zu erleichtern. Darüber hinaus können Sie einen Statustyp, einen Aktivitätstyp, ein Datum, einen angepassten Filter oder einen Text (z. B. einen Namen oder eine IP-Adresse) im Feld **Filter** auswählen und nur diejenigen Aktivitäten auflisten, die die ausgewählten Kriterien erfüllen.



Schritt 4. Klicken Sie auf **Flussdiagramm generieren**, um das Flussdiagramm im Abschnitt **Flussdiagramm** anzuzeigen.

Nach dieser Aufgabe

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Weitere Informationen zu jeder Aktivität im Flussdiagramm durch Bewegen des Cursor über den Status anzeigen.
- Den zugehörigen Fluss für die ausgewählten Aktivitäten in eine CSV-Datei durch Klicken auf **Aktionen → In CSV exportieren** exportieren.

Kapitel 4. Verwaltungshinweise

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

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

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

ThinkSystem-, ThinkServer- und System x-Einheiten

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

Flex System-Einheiten

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

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

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

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

Kapitel 5. Ressourcengruppen verwalten

Sie können Ressourcengruppen in Lenovo XClarity Administrator verwenden, um logische Gruppe von verwalteten Einheiten zu erstellen, die Sie gemeinschaftlich anzeigen und verwenden können.

Weitere Informationen: XClarity Administrator: Ressourcengruppen

Zu dieser Aufgabe

Es gibt drei Typen von Ressourcengruppen:

- **Static**. Angepasste Gruppe mit bestimmten Einheiten.
- **Dynamisch**. Regelbasierte Gruppe von Einheiten (z. B. alle Server eines bestimmten Typs). Diese Gruppe enthält eine dynamische Liste der Einheiten basierend auf einer Gruppe von Bestandseigenschaften.

Bei einer Ressourcengruppe können keine Aktionen ausgeführt werden. Sie können jedoch alle Einheiten in einer Gruppe markieren und Aktionen gemeinsam für alle ausgewählten Einheiten durchführen.

Status von Einheiten in einer Ressourcengruppe anzeigen

Sie können den Status aller verwalteten Einheiten in einer Ressourcengruppe anzeigen.

Zu dieser Aufgabe

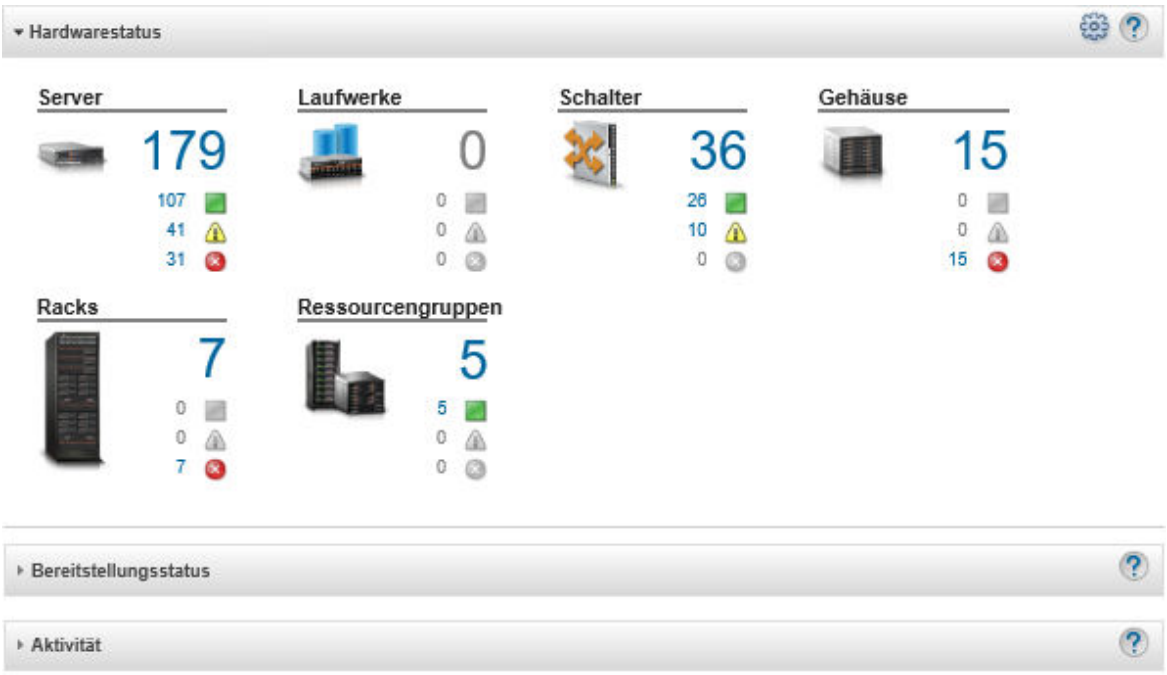
Die folgenden Statussymbole geben den allgemeinen Status aller Einheiten der Ressourcengruppe an. Der allgemeine Status der Gruppe gibt die Einheit mit dem höchsten Schweregrad in der Gruppe an.

- Symbol **Kritisch** ( )
- Symbol **Warnung** ( )
- Symbol **Normal** ( )

Vorgehensweise

Gehen Sie wie folgt vor, um den Status der Einheiten in einer Ressourcengruppe anzuzeigen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Dashboard**. Die Dashboard-Seite wird geöffnet und zeigt eine Übersicht mit dem Status aller verwalteten Einheiten und anderen Ressourcen, einschließlich Ressourcengruppen.



Schritt 2. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Ressourcengruppen**. Die Seite Alle Ressourcengruppen wird angezeigt.

Auf der Seite „Alle Ressourcengruppen“ wird jede Ressourcengruppe mit dem Gruppennamen, der Anzahl der enthaltenen verwalteten Einheiten sowie dem Einheitenstatus mit dem höchsten Schweregrad in der Gruppe aufgelistet.

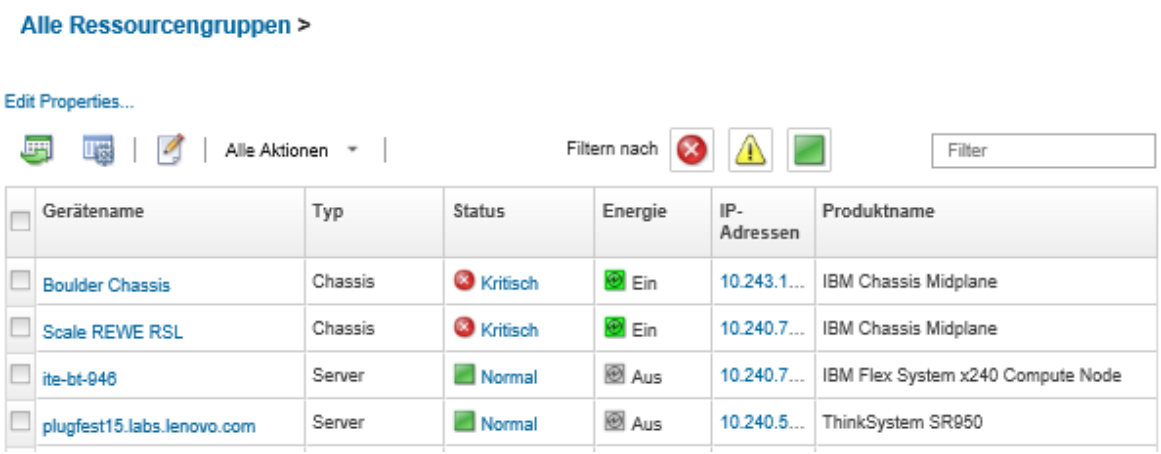
Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie eine neue Ressourcengruppe (siehe Dynamische Ressourcengruppe erstellen und Statische Ressourcengruppe erstellen).
- Bearbeiten Sie die Gruppenzugehörigkeit, indem Sie eine Gruppe auswählen und auf das Symbol **Bearbeiten** klicken ( ).
- Bearbeiten Sie die Gruppeneigenschaften, indem Sie eine Gruppe auswählen und auf **Alle Aktionen → Eigenschaften bearbeiten** klicken.
- Entfernen Sie eine Ressourcengruppe, indem Sie eine Gruppe auswählen und auf das Symbol **Löschen** klicken ( ).

Anmerkung: Das Löschen einer Gruppe löscht nur die Gruppendefinition. Er wirkt sich nicht auf die Einheiten in der Gruppe aus.

- Exportieren Sie ausführliche Informationen über alle Einheiten in einer oder mehreren Ressourcengruppen in eine CSV-Datei. Klicken Sie dazu auf das Symbol **Exportieren** ( ).

Schritt 3. Klicken Sie auf der Seite Alle Ressourcengruppen auf den Namen in der Spalte **Gruppen**, um die Liste der Einheiten in dieser Gruppe anzuzeigen.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Sie können Einheiten zu einer statischen Ressourcengruppe hinzufügen oder daraus entfernen, indem Sie auf das Symbol **Bearbeiten** klicken ( ).
- Sie können ausführliche Informationen zu einer bestimmten Einheit in der Ressourcengruppe anzeigen, indem Sie auf den Einheitenname in der Spalte **Einheitenname** klicken.
- Exportieren Sie ausführliche Informationen über alle Einheiten in einer oder mehreren Ressourcengruppen in eine CSV-Datei. Klicken Sie dazu auf das Symbol **Exportieren** ( ).

Mitglieder einer Ressourcengruppe anzeigen

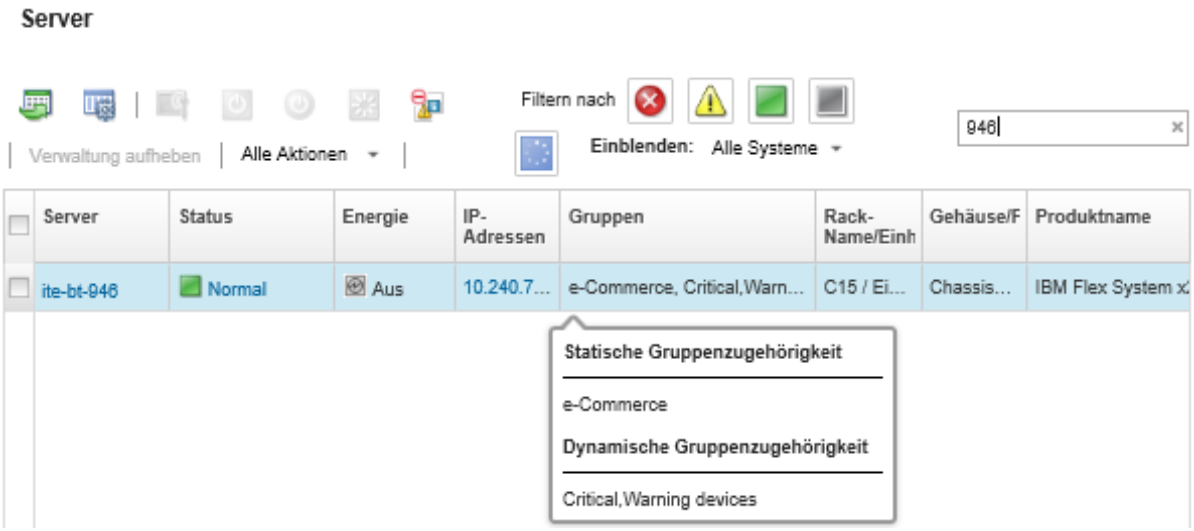
Sie können ausführliche Informationen der Ressourcengruppen anzeigen, einschließlich Gruppenmitglieder.

Vorgehensweise

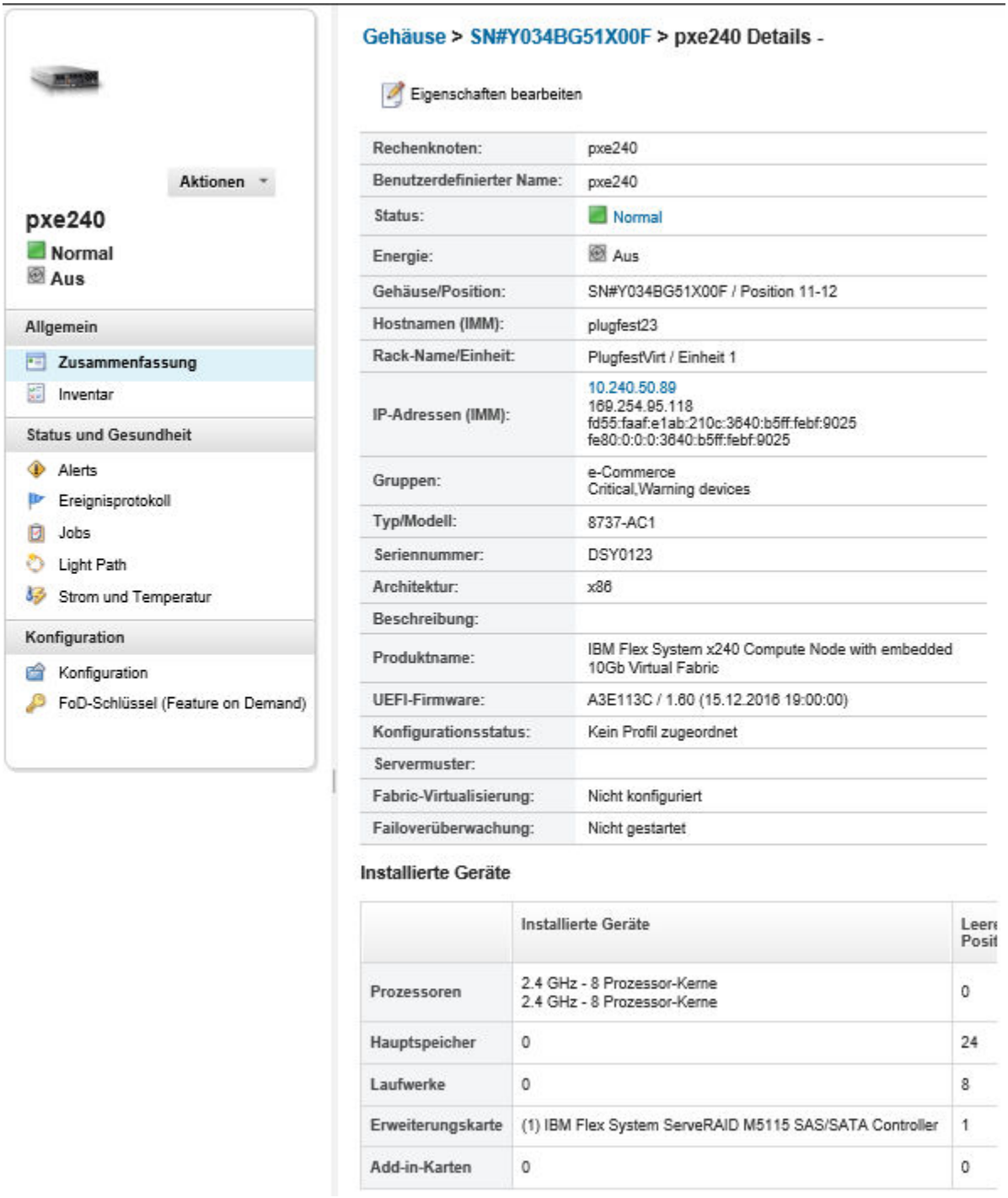
Gehen Sie zum Anzeigen einer Gruppenzugehörigkeit wie folgt vor.

- So zeigen Sie alle Gruppen an, zu denen eine Einheit gehört:
  1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Hardware** und dann auf den Einheitentyp, um die Seite „Alle Einheiten“ zu öffnen.

     Bewegen Sie den Mauszeiger über die Gruppenlisten in der Spalte **Gruppen**, um die Gruppen aufzulisten, denen die Einheit zugeordnet ist.



2. Klicken Sie auf den Link des Einheitennamens in der ersten Spalte. Die Übersichtsseite für diese Einheit wird angezeigt, einschließlich einer Liste der Ressourcengruppen, denen die Einheit zugeordnet ist.

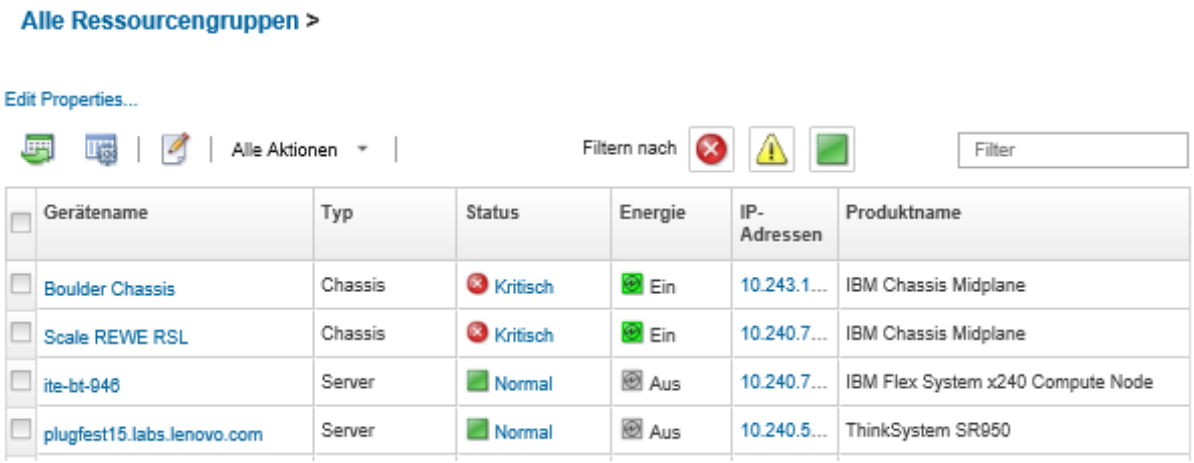


- So zeigen Sie die Mitglieder einer Gruppe an:
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Dashboard**. Die Dashboard-Seite wird geöffnet und zeigt eine Übersicht mit dem Status aller verwalteten Einheiten und anderen Ressourcen, einschließlich Racks.
  2. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Gruppen**. Die Seite „Ressourcengruppen“ wird angezeigt.

     Diese Seite listet die Gesamtzahl der Mitglieder sowie die Anzahl der Mitglieder jedes Einheitentyps in der Gruppe auf.

3. Klicken Sie auf der Seite Alle Ressourcengruppen auf den Namen in der Spalte **Gruppen**, um Details der Ressourcengruppen anzuzeigen.

   Diese Seite listet jede Einheit auf, die Mitglied der Ressourcengruppe ist.



Dynamische Ressourcengruppe erstellen

Sie können eine Ressourcengruppe für einen dynamischen Satz von verwalteten Einheiten basierend auf mehreren Kriterien erstellen.

Zu dieser Aufgabe

Sie können eine dynamische Ressourcengruppe mit einem oder mehreren der folgenden Kriterien für jeden Einheitentyp erstellen:

Kriterien	Gehäuse	Density-Gehäuse	Server	Flex System-Switch	RackSwitch-Switch	Speichereinheit
Name der Add-in-Karte			✓ (außer ThinkServer)			
Kontakt	✓		✓		✓	✓
Beschreibung	✓	✓	✓		✓	✓

Kriterien	Gehäuse	Density-Gehäuse	Server	Flex System-Switch	RackS-witch-Switch	Speicher-einheit
Vollständig qualifizierter Domänenname	✓		✓			
Hostname	✓		✓	✓	✓	
IPv4-Adresse*	✓		✓	✓	✓	✓
IPv6-Adresse	✓		✓	✓	✓	
Position	✓	✓	✓		✓	✓
Maschinentyp	✓		✓	✓	✓	✓
Modell	✓		✓	✓	✓	✓
Gesamt-Integritätsstatus	✓		✓	✓	✓	✓
Prozessorkerne			✓			
Produktname	✓		✓	✓	✓	✓
Rack	✓	✓	✓		✓	✓
Raum	✓	✓	✓		✓	✓
Benutzerdefinierter Name	✓	✓	✓	✓	✓	✓

Anmerkung: Bei IPv4-Adressen können Sie eine einzelne Adresse oder einen Bereich von Adressen angeben, die durch einen Bindestrich getrennt sind oder ein Sternchen als Platzhalter verwenden (z. B. `1.1.1.*` oder `1.1.1.1-1.1.1.255` ohne Leerzeichen).

Vorgehensweise

So erstellen und bestücken Sie eine dynamische Ressourcengruppe

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware** → **Ressourcengruppen**. Die Seite Alle Ressourcengruppen wird angezeigt.

Schritt 2. Klicken Sie auf das Symbol **Erstellen** ( ), um eine leere Gruppe zu erstellen. Das Dialogfenster „Leere Gruppe erstellen“ wird angezeigt.

Schritt 3. Wählen Sie **Dynamische Gruppe** aus, um eine Gruppe von Einheiten zu erstellen, die auf mehreren Kriterien basieren.

Schritt 4. Klicken Sie auf **Erstellen**. Das Dialogfenster „Dynamische Gruppe bearbeiten“ wird angezeigt.

Schritt 5. Fügen Sie Kriterien für diese dynamische Gruppe hinzu.

- Wählen Sie den Bediener für den Gruppensatz aus. Dies kann einer der folgenden Werte sein:
  - **AND**. Mitglieder müssen alle angegebenen Werte erfüllen.
  - **OR**. Mitglieder müssen mindestens einen der angegebenen Werte erfüllen.
- Klicken Sie auf **Kriterien erstellen**, um eine neue Kriterienregel zum Satz hinzuzufügen.
- Klicken Sie auf **Kriteriensatz erstellen**, um eine Untergruppe von Kriterienregeln hinzuzufügen.

Anmerkung: Neue Kriterien und Kriteriensätze werden immer am Ende der Liste hinzugefügt.

Schritt 6. Klicken Sie auf **Übernehmen**, um die Gruppenkriterien zu speichern und die Gruppe zu erstellen, oder auf **Vorschau**, um zu sehen, welche Einheiten bei Verwendung der aktuellen Kriterien zur Gruppe gehören, ohne die Gruppe zu erstellen.

Nach dieser Aufgabe

- In der Spalte **Gruppen** auf den Seiten „Alle Einheiten“ und den Einheiten-Übersichtsseiten können Sie sehen, zu welchen Ressourcengruppen eine Einheit gehört.
- Sie können die Kriterien für die dynamische Gruppe ändern, indem Sie die Ressourcengruppe auswählen und auf das Symbol **Bearbeiten** klicken ( ).
- Sie können die Eigenschaften der Ressourcengruppe ändern, indem Sie auf **Alle Aktionen → Eigenschaften bearbeiten** klicken.

Statische Ressourcengruppe erstellen

Sie können eine Ressourcengruppe erstellen, die eine angepasste Gruppe von verwalteten Einheiten enthält.

Vorgehensweise

Gehen Sie wie folgt vor, um eine statische Ressourcengruppe zu erstellen und zu bestücken.

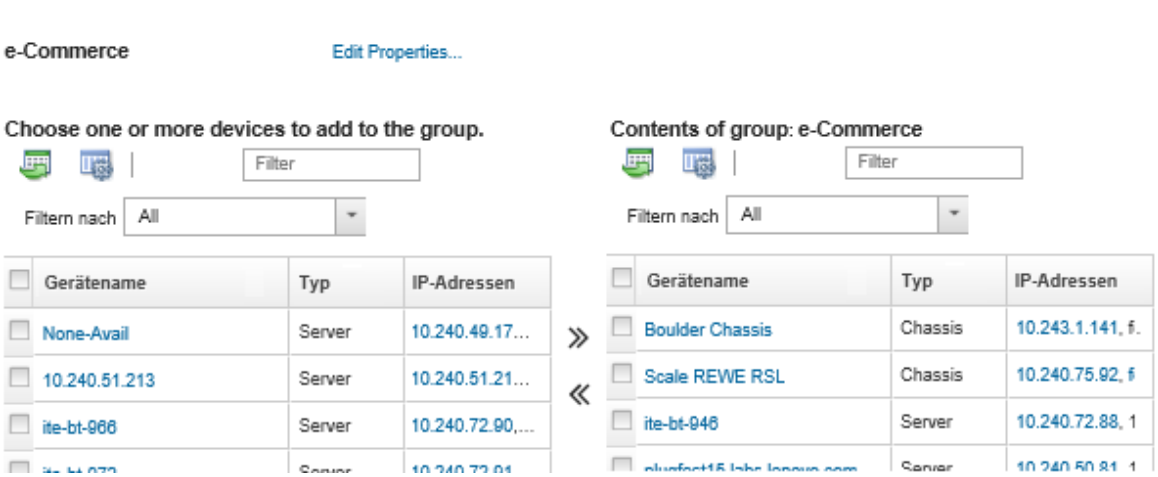
Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Ressourcengruppen**. Die Seite Ressourcengruppen wird angezeigt.

Schritt 2. Klicken Sie auf das Symbol **Erstellen** ( ), um eine leere Gruppe zu erstellen. Das Dialogfenster „Leere Gruppe erstellen“ wird angezeigt.

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

Schritt 4. Wählen Sie **Statische Gruppe** aus, um eine Gruppe mit explizit definierten Einheiten zu erstellen.

Schritt 5. Klicken Sie auf **Erstellen**. Die Seite „Statische Gruppe bearbeiten“ wird angezeigt.



Schritt 6. Wählen Sie in der Liste **Alle verfügbaren Einheiten außerhalb der Gruppe** die Einheiten aus, die Sie zur Gruppe hinzufügen möchten, und klicken Sie auf das Symbol **Hinzufügen** (»), um die ausgewählten Einheiten zur Liste **Inhalte der Gruppe** zu verschieben.

Anmerkungen:

- Sie können die Listen sortieren, um die Suche nach bestimmten Einheiten zu erleichtern. Klicken Sie dazu auf die Spaltenüberschriften. Außerdem können Sie in der Dropdown-Liste **Filtern nach** einen Einheitentyp auswählen, aus der Dropdown-Liste ein Gehäuse auswählen oder im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um nur die Einheiten aufzulisten, die den ausgewählten Kriterien entsprechen.
- Wenn Sie ein Gehäuse in die Gruppe verschieben, werden die Einheiten im Gehäuse nicht automatisch zur Gruppe hinzugefügt. Um alle Gehäusekomponenten zur Gruppe hinzuzufügen, wählen Sie **Gehäuse → <*Gehäusename*>** im Dropdown-Menü **Anzeigen** aus, um alle Komponenten im angegebenen Gehäuse aufzulisten. Aktivieren Sie das Kontrollkästchen neben der Spalte „Einheitenname“, um alle Einheiten auszuwählen, und klicken Sie dann auf das Symbol **Hinzufügen** (»), um die ausgewählten Einheiten zur Liste **Inhalte der Gruppe** zu verschieben.

Nach dieser Aufgabe

- In der Spalte **Gruppen** auf den Seiten „Alle Einheiten“ und den Einheiten-Übersichtsseiten können Sie sehen, zu welchen Ressourcengruppen eine Einheit gehört.
- Sie können eine Einheit auf der den Seiten „Alle Einheiten“ und den Einheiten-Detailseiten zu einer statischen Ressourcengruppe hinzufügen oder daraus entfernen. Klicken Sie dazu auf **Alle Aktionen → Gruppen → Zu Gruppe hinzufügen** oder **Alle Aktionen → Gruppen → Aus Gruppe entfernen**.

  Anmerkung: Sie können Einheiten nur zu statischen Ressourcengruppen hinzufügen bzw. daraus entfernen. Sie können sie nicht aus dynamischen Gruppen entfernen.
- Sie können die Eigenschaften der Ressourcengruppe ändern, indem Sie auf **Alle Aktionen → Eigenschaften bearbeiten** klicken.

Ressourcengruppe entfernen

Sie können eine Ressourcengruppe wieder aus Lenovo XClarity Administrator entfernen.

Zu dieser Aufgabe

Das Löschen einer Gruppe löscht nur die Gruppendefinition. Er wirkt sich nicht auf die Einheiten in dieser Gruppe aus.

Vorgehensweise

Gehen Sie zum Entfernen eine Ressourcengruppe wie folgt vor:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Ressourcengruppen**. Die Seite Alle Ressourcengruppen wird angezeigt.

Auf der Seite „Alle Ressourcengruppen“ wird jede Ressourcengruppe mit dem Gruppennamen, der Anzahl der enthaltenen verwalteten Einheiten sowie dem Einheitenstatus mit dem höchsten Schweregrad in der Gruppe aufgelistet.

Schritt 2. Wählen Sie die zu entfernende Ressourcengruppe aus.

Schritt 3. Klicken Sie auf das Symbol für **Löschen** ( ).

Schritt 4. Klicken Sie auf **Löschen**.

Eigenschaften der Ressourcengruppe ändern

Sie können die Eigenschaften für eine bestimmte Ressourcengruppe ändern.

Vorgehensweise

Gehen Sie wie folgt vor, um die Eigenschaften der Ressourcengruppe zu ändern

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Ressourcengruppen**, um die Seite „Alle Ressourcengruppen“ anzuzeigen.

Schritt 2. Wählen Sie die zu aktualisierende Ressourcengruppe aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Eigenschaften bearbeiten**, um das Dialogfenster Gruppeneigenschaften bearbeiten anzuzeigen.

Schritt 4. Ändern Sie gegebenenfalls die folgenden Daten:
- Gruppenname
- Beschreibung

Schritt 5. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie diese Eigenschaften ändern, kann es einen Moment dauern, bis die Änderungen in der XClarity Administrator-Webschnittstelle angezeigt werden.

Kapitel 6. Racks verwalten

Mithilfe von Racks in Lenovo XClarity Administrator können Sie Ihre verwalteten Einheiten so gruppieren, dass sie der physischen Rack-Konfiguration in Ihrem Rechenzentrum entsprechen.

Vorbereitende Schritte

Nachdem Sie einen Knoten von einem Gehäuse zu einem anderen verschoben haben, warten Sie 5 bis 10 Minuten, bevor Sie versuchen, die Racks in XClarity Administrator zu bearbeiten, der das Gehäuse enthält.

Wenn Sie eine Einheit aus einem Rack verschieben, werden der Rack-Name und die untersten Rack-Einheitenwerte im Einheitenbestand gelöscht. Die Raum- und Positionswerte werden nicht gelöscht.

Zu dieser Aufgabe

In diesem Abschnitt wird beschrieben, wie Sie interaktiv ein Rack mit verwalteten Einheiten und Abdeckblenden erstellen und bestücken.

Wenn Sie viele Einheiten zu Racks hinzufügen oder mehrere Racks bearbeiten müssen, können Sie mithilfe eines Tabellenkalkulations-Arbeitsblatts einen Massenimport ausführen oder ein PowerShell-Script implementieren, um die Task zu automatisieren. Weitere Informationen zum Verwenden des Massenimportverfahrens finden Sie in Gehäuse verwalten und Server verwalten. Informationen zu PowerShell-Scripts erhalten Sie unter PowerShell-Toolkit (LXCAPSTool) in der Onlinedokumentation von XClarity Administrator.

XClarity Administrator erkennt Rack-Eigenschaften, die in einer Einheit definiert sind. Wenn Sie diese Einheit verwalten, legt XClarity Administrator die Systemeigenschaften für diese Einheit fest und aktualisiert die Rack-Ansicht. Falls das Rack nicht in XClarity Administrator vorhanden ist, wird ein neues Rack erstellt und die Einheit wird zum neuen Rack hinzugefügt.

Anmerkungen:

- System x3500 M5-Server, NeXtScale nx360 M5-Server, ThinkServer SD350 Server und Tower-Server werden in der Rack-Ansicht nicht unterstützt.
- Bei skalierbaren komplexen System x3850 X5-Systemen müssen Sie jeden Knoten (Server) einzeln zum Rack hinzufügen.
- Demohardware wird bei einem Neustart von XClarity Administrator nicht weiterhin in Rack-Ansichten angezeigt.

Vorgehensweise

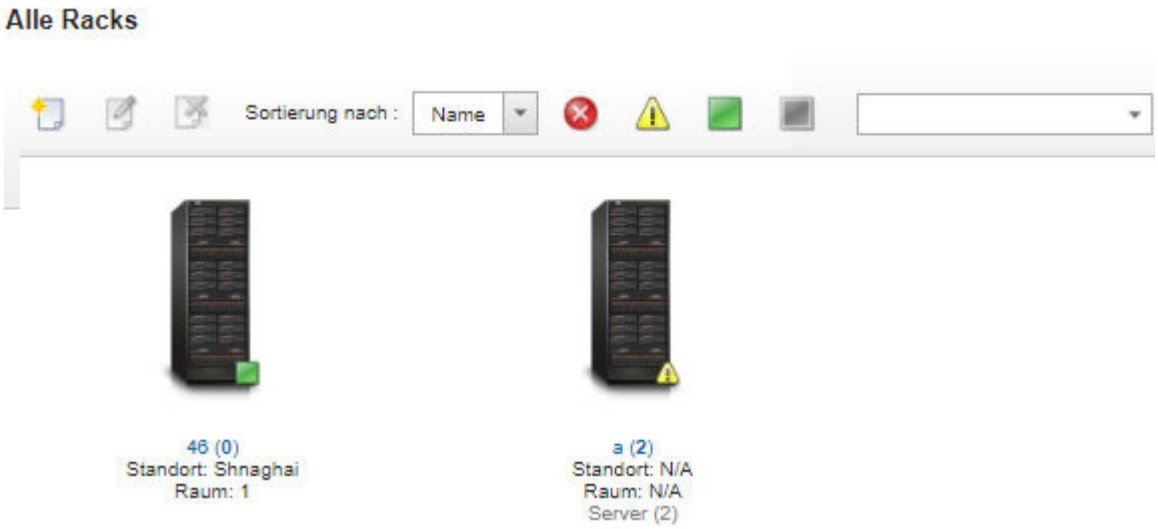
Gehen Sie wie folgt vor, um Racks zu erstellen und zu bestücken.

- Erstellen und bestücken Sie ein einzelnes Rack mit verwalteten Einheiten.
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Racks**. Die Seite Alle Racks wird angezeigt.

     Auf der Seite Alle Racks wird jedes Rack als Miniaturansicht mit dem Rack-Namen, der Anzahl der enthaltenen verwalteten Einheiten sowie dem Einheitenstatus mit dem höchsten Schweregrad angezeigt.

Anmerkungen: Sie können die Racks nach Schweregrad filtern, indem Sie auf die folgenden Symbole in der Symbolleiste klicken. Sie können auch einen Rack-Namen im Feld **Filter** eingeben, um die angezeigten Racks weiter zu filtern.

- Symbol für **Kritische Alerts** ( )
- Symbol für **Warnalerts** ( )
- Symbol für **Normale Alerts** ( )

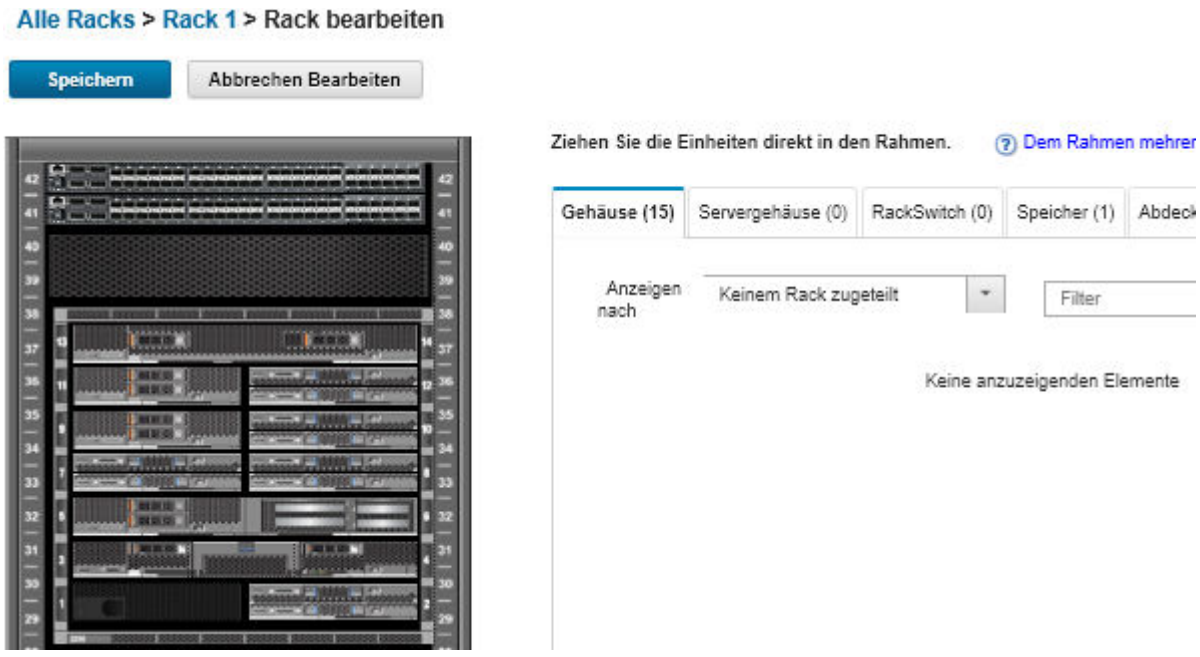


2. Klicken Sie auf das Symbol **Erstellen** ( ), um ein leeres Rack zu erstellen. Das Dialogfenster „Leeres Rack erstellen“ wird angezeigt.
3. Tragen Sie im Dialogfeld die Angaben zu Rack-Name, Höhe, Position und Raum ein.

   Anmerkungen:

   - Rack-Namen müssen nicht eindeutig sein. Sie können Racks mit demselben Namen erstellen, solange sich die Position, der Raum oder beide unterscheiden.
   - Der Rack-Name kann nur Groß- und Kleinbuchstaben, Ziffern und die folgenden Sonderzeichen enthalten: Punkt (.), Bindestrich (-) und Unterstrich (_).
   - Die Position darf maximal 23 Zeichen lang sein.
4. Klicken Sie auf **Erstellen**. Eine Miniaturansicht für das neue Rack wird zur Seite Alle Racks hinzugefügt.
5. Doppelklicken Sie auf die Miniaturansicht für das Rack. Die Seite „Rack-Ansicht“ mit einer Abbildung eines leeren Racks sowie Eigenschaften für dieses Rack wird angezeigt.

6. Klicken Sie auf **Rack bearbeiten**, um die Seite Rack bearbeiten anzuzeigen.



7. Fügen Sie die betreffenden verwalteten Einheiten und Abdeckblenden zur grafischen Ansicht hinzu:

   Anmerkung: Nur verwaltete Einheiten, die den Zustand „Online“ haben, können zum Rack hinzugefügt werden.

   - Klicken Sie auf die Registerkarte **Gehäuse**, um eine Liste mit verwalteten Gehäusen aufzurufen, die noch keinem Rack hinzugefügt wurden. Bewegen Sie ein verwaltetes Gehäuse durch Ziehen und Ablegen an die gewünschte Position im Rack, um das Gehäuse zum Rack hinzuzufügen.
   - Klicken Sie auf die Registerkarte **Servergehäuse**, um eine Liste der verwalteten Rack-Server und der Servergehäuse mit mehreren Knoten anzuzeigen, die noch keinem Rack hinzugefügt wurden. Bewegen Sie einen Rack-Server oder ein Servergehäuse durch Ziehen und Ablegen an die gewünschte Position im Rack, um den Rack-Server bzw. das Servergehäuse zum Rack hinzuzufügen.
   - Klicken Sie auf die Registerkarte **RackSwitch**, um eine Liste mit verwalteten RackSwitch-Switches aufzurufen, die noch keinem Rack hinzugefügt wurden. Bewegen Sie einen RackSwitch-Switch durch Ziehen und Ablegen an die gewünschte Position im Rack, um den Switch zum Rack hinzuzufügen.

- Klicken Sie auf die Registerkarte **Speicher**, um eine Liste mit verschiedenen Speichereinheiten anzuzeigen. Bewegen Sie die betreffende Speichereinheit durch Ziehen und Ablegen an die gewünschte Position im Rack, um die Speichereinheit zum Rack hinzuzufügen.
- Klicken Sie auf die Registerkarte **Abdeckblenden**, um eine Liste mit verschiedenen Abdeckblenden anzuzeigen. Bewegen Sie die jeweilige Abdeckblende durch Ziehen und Ablegen an die gewünschte Position im Rack, um die Abdeckblende zum Rack hinzuzufügen.

  Als *Abdeckblende* wird jede Einheit im Rack bezeichnet, die nicht durch XClarity Administrator verwaltet wird. Folgende Abdeckblenden sind verfügbar:
  - Allgemeine Abdeckblenden
  - Allgemeine Rack-Switches
  - Speichercontroller und Gehäuse
  - Partner-Speicher-Controller und -Gehäuse (z. B. von IBM, NetApp und EMC)

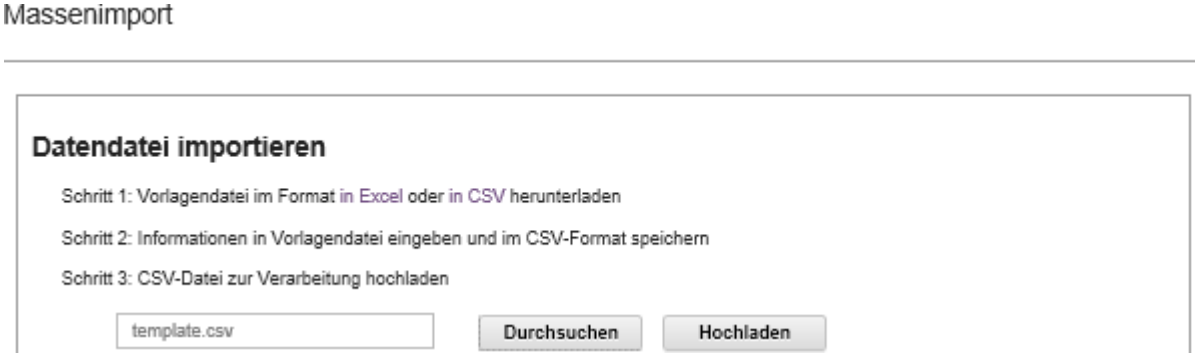
- Wenn Sie Einheiten zu einem Rack hinzufügen oder daraus entfernen, werden die Eigenschaften für Position, Raum, Rack und unterste Rack-Einheit für die Einheit aktualisiert.
- Über die Dropdown-Liste **Anzeigen nach** können Sie die Liste der Einheiten auf jeder Registerkarte sortieren. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Einheiten weiter zu filtern.
- Sie können verwaltete Einheiten und Abdeckblenden aus dem Rack entfernen, indem Sie die betreffenden Objekte durch Ziehen und Ablegen aus dem Rack hinausbewegen.

8. Klicken Sie auf **Speichern**, um die Rack-Konfiguration zu speichern.

   Der Konfigurationsvorgang kann mehrere Minuten in Anspruch nehmen. Während der Konfiguration werden die Rack- und Positionsinformationen zum CMM oder Baseboard Management Controller für die verwalteten Einheiten gesendet.
9. Spezifizieren Sie die Abdeckblenden, die Sie zum Rack hinzugefügt haben, indem Sie auf die Abdeckblende und dann auf **Eigenschaften bearbeiten** klicken. Im Dialogfeld „Eigenschaften bearbeiten“ können Sie einen Namen, die unterste Rack-Einheit sowie eine URL zum Aufrufen der Verwaltungsbenutzeroberfläche für diese Einheit angeben.

   Tipp: Nachdem die Rack-Konfiguration gespeichert wurde, können Sie die Verwaltungsbenutzeroberfläche für eine Abdeckblende aufrufen, indem Sie im Rack auf die Abdeckblende und dann auf den Link **URL starten** klicken.

- Erstellen und bestücken Sie Racks mithilfe einer Massenimportdatei.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.
  2. Klicken Sie auf **Massenimport**. Der Massenimport-Assistent wird angezeigt.

  3. Klicken Sie auf der Seite „Datei importieren“ auf den Link **In Excel** oder **In CSV**, um die Massenimportvorlagendatei im Excel- oder CSV-Format herunterzuladen.

Wichtig: Die Vorlagendatei kann sich von einem Release zum nächsten ändern. Stellen Sie sicher, dass Sie immer die neueste Vorlage verwenden.

4. Füllen Sie das Datenarbeitsblatt in der Vorlagendatei aus und speichern Sie die Datei im CSV-Format.

   Tipp: Die Excel-Vorlagendatei enthält ein Arbeitsblatt namens **Data** und eines namens **Readme**. Verwenden Sie das Arbeitsblatt **Data**, um die Daten zu Ihrer Einheit einzugeben. Das Arbeitsblatt **Readme** enthält Informationen zum Ausfüllen der Felder im Arbeitsblatt **Data**, z. B. die Pflichtfelder und einige Beispiele.

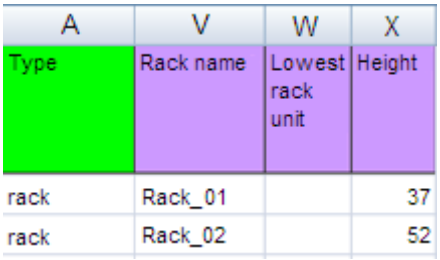
   Wichtig:

   – Die Einheiten werden in der Reihenfolge verwaltet, die in der Massenimportdatei angegeben ist.
   – XClarity Administrator verwendet Informationen zur Rack-Zuordnung, die bei der Verwaltung der Einheit in deren Konfiguration definiert werden. Wenn Sie in die Rack-Zuordnung in XClarity Administrator ändern, aktualisiert XClarity Administrator die Konfiguration für die Einheit. Wenn Sie die Einheitenkonfiguration aktualisieren, nachdem die Einheit verwaltet wurde, werden die Änderungen in XClarity Administrator angezeigt.
   – Es wird empfohlen (dies ist jedoch nicht erforderlich), ein Rack explizit in der Tabelle zu erstellen, bevor Sie das Rack einer Einheit zuordnen. Wenn ein Rack nicht explizit definiert und noch nicht in XClarity Administrator vorhanden ist, werden die Informationen zur Rack-Zuordnung, die für eine Einheit angegeben sind, verwendet, um das Rack mit einer Standardhöhe von 52 U zu erstellen.

     Wenn Sie eine andere Höhe für das Rack wünschen, müssen Sie das Rack explizit in der Tabelle definieren, bevor Sie es einer Einheit zuordnen.

   Um Ihre Racks in der Massenimportdatei zu definieren, füllen die folgenden erforderlichen Spalten.
   – (Spalten A) Geben Sie „Rack“ für den Einheitentyp an.
   – (Spalten V) Geben Sie den Rack-Namen an.
   – (Spalte X) Geben Sie die Höhe des Racks an. Die folgenden Rack-Höhen werden unterstützt: 6 U, 12 U, 18 U, 25 U, 37 U, 42 U, 45 U, 46 U, 48 U, 50 U und 52 U.

   Die folgende Abbildung zeigt ein Beispiel für eine Massenimportdatei mit definierten Racks:



A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

   Anmerkung: Sie können die gleiche Massenimportdatei zum Verwalten von Einheiten und Hinzufügen dieser Einheiten zu einem Rack verwenden (siehe Systeme verwalten in der Onlinedokumentation von Lenovo XClarity Administrator).

5. Geben Sie im Assistenten Massenimport den Namen der CSV-Datei ein, um sie für die Verarbeitung hochzuladen. Sie können auf **Durchsuchen** klicken, um die Datei zu suchen.
6. Klicken Sie auf **Hochladen**, um die Datei hochzuladen und zu überprüfen.
7. Klicken Sie auf **Weiter**, um die Seite mit der Eingabezusammenfassung mit einer Liste der zu verwaltenden Racks und anderen Einheiten anzuzeigen, und überprüfen Sie die Zusammenfassung des Racks und der anderen Einheiten, die Sie verwalten möchten.
8. Klicken Sie auf **Weiter**, um die Seite „Anmeldeinformationen für Einheiten“ anzuzeigen. Klicken Sie auf jede Registerkarte und geben Sie optional die globalen Einstellungen und Anmeldeinformationen an, die für alle Einheiten eines bestimmten Typs verwendet werden sollen. Die Einheiten, die die

globalen Einstellungen und Anmeldeinformationen verwenden, werden auf der rechten Seite jeder Registerkarte aufgelistet.

9. Klicken Sie auf **Verwalten**. Die Seite „Überwachungsergebnisse“ wird mit Informationen zum Verwaltungsstatus der einzelnen Einheiten in der Massenimportdatei angezeigt.

   Für den Verwaltungsprozess wird ein Job erstellt. Wenn Sie den Assistenten für die Massenimportdatei schließen, wird der Verwaltungsprozess im Hintergrund weiterhin ausgeführt. Sie können den Status des Verwaltungsprozesses im Jobprotokoll überwachen. Informationen zum Jobprotokoll finden Sie unter „Jobs überwachen“ auf Seite 184.

Nach dieser Aufgabe

Sie können die bevorzugte Reihenfolge der Rack-Nummerierung ändern (siehe Bestandseinstellungen festlegen).

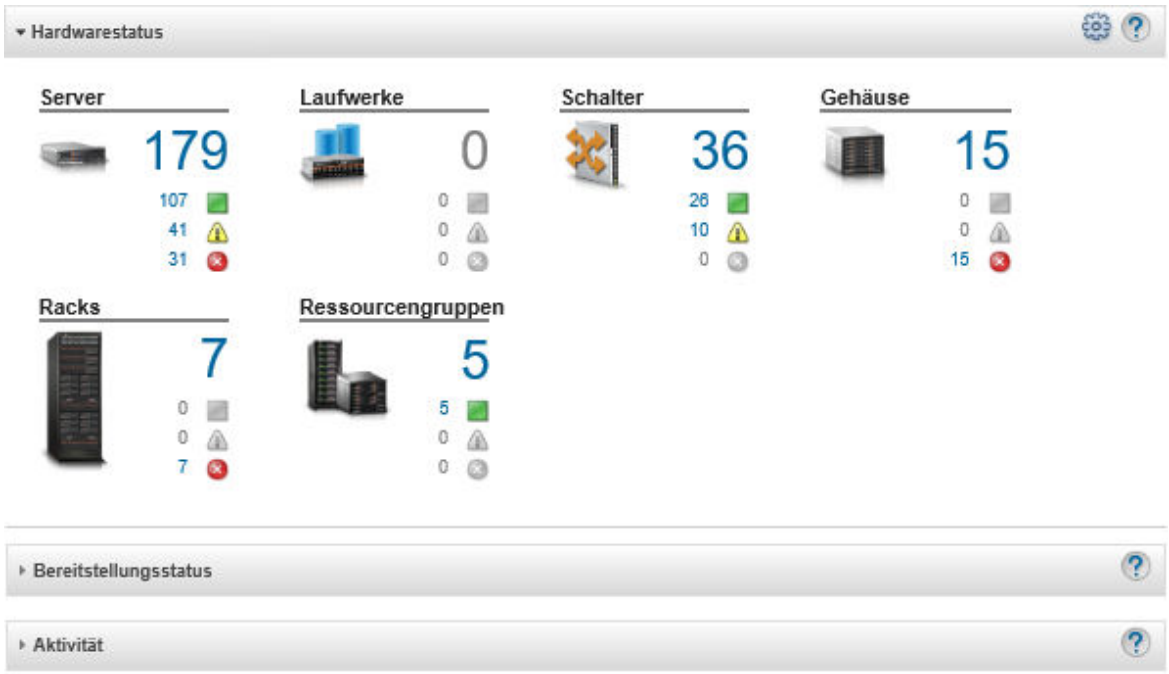
Status von Einheiten in einem Rack anzeigen

Für jedes Rack kann den Status aller verwalteten Rack-Einheiten angezeigt werden.

Vorgehensweise

Führen Sie eine oder mehrere der folgenden Aktionen aus, um den Status aller Einheiten in einem Rack anzuzeigen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Dashboard**. Die Dashboard-Seite wird geöffnet und zeigt eine Übersicht mit dem Status aller verwalteten Einheiten und anderen Ressourcen, einschließlich Racks.

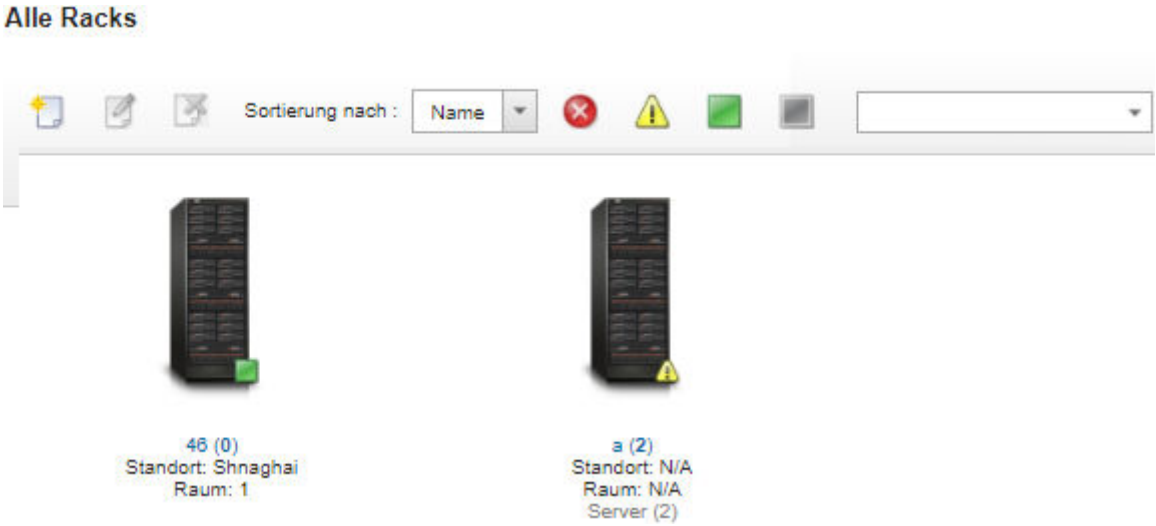


Schritt 2. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Racks**. Die Seite Alle Racks wird angezeigt.

Auf der Seite Alle Racks wird jedes Rack als Miniaturansicht mit dem Rack-Namen, der Anzahl der enthaltenen verwalteten Einheiten sowie dem Einheitenstatus mit dem höchsten Schweregrad angezeigt.

Anmerkungen: Sie können die Liste der Racks nach Rackname, Anzahl der Einheiten im Rack oder Schweregrad sortieren, um bestimmte Racks leichter zu finden. Sortiert wird von links nach rechts und von oben nach unten. Darüber hinaus können Sie die Racks nach Schweregrad filtern, indem Sie auf die folgenden Symbole in der Symbolleiste klicken oder einen Rack-Namen im Feld **Filter** eingeben, um die angezeigten Racks weiter zu filtern.

- Symbol für **Kritische Alerts** ( )
- Symbol für **Warnalerts** ( )
- Symbol für **Normale Alerts** ( )



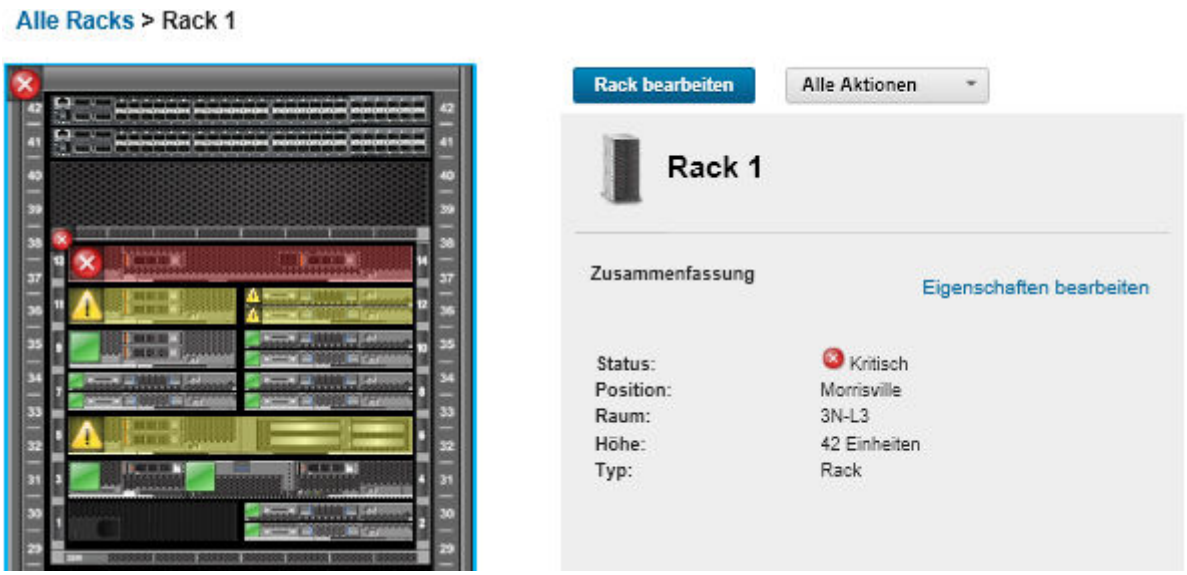
Schritt 3. Klicken Sie auf der Seite Alle Racks auf den Rack-Namen oder doppelklicken Sie auf eine Rack-Miniaturansicht, um die grafische Ansicht und die Eigenschaften für dieses Rack anzuzeigen.

Die *Rack-Ansicht* ist eine grafische Ansicht der Rack-Vorderseite, die alle Einheiten im Rack einschließlich Gehäusen, Rack-Servern, Top-of-Rack-Switches und Abdeckblenden zeigt. Ein Statussymbol an jeder Einheit gibt den aktuellen Status der Einheit an.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Einheiten im Rack hinzufügen oder entfernen, indem Sie auf **Rack bearbeiten** klicken.

  Anmerkung: Wenn Sie die Komponenten im Rack ändern, kann es einen Moment dauern, bis die entsprechenden Änderungen in der XClarity Administrator-Schnittstelle angezeigt werden.
- Ändern Sie Einheiten- und Filtereigenschaften (einschließlich Name, Position und URL zum Starten der Verwaltungswebschnittstelle), indem Sie auf die Einheit oder die Abdeckblende und dann auf **Eigenschaften bearbeiten** im Bereich der Einheitenzusammenfassung klicken.
- Zeigen Sie die Management-Controller-Webschnittstelle für eine Einheit oder eine Abdeckblende an, indem Sie auf die Einheit oder die Abdeckblende und anschließend auf den Link **URL starten** im Bereich Einheitenzusammenfassung klicken.



Schritt 4. Zeigen Sie eine Zusammenfassung oder den detaillierten Status für eine Einheit oder Komponente an:

a. Klicken Sie auf eine Einheit oder Komponente im Rack, um eine Statuszusammenfassung sowie die Eigenschaften und den Status für die Einheit oder Komponente anzuzeigen.

b. Doppelklicken Sie auf eine Einheit, um die Detailseite für diese Einheit anzuzeigen.

Vorgehensweise

Sie können die bevorzugte Reihenfolge der Rack-Nummerierung ändern (siehe Bestandseinstellungen festlegen).

Ein Rack entfernen

Sie können ein Rack auch wieder aus Lenovo XClarity Administrator entfernen.

Vorgehensweise

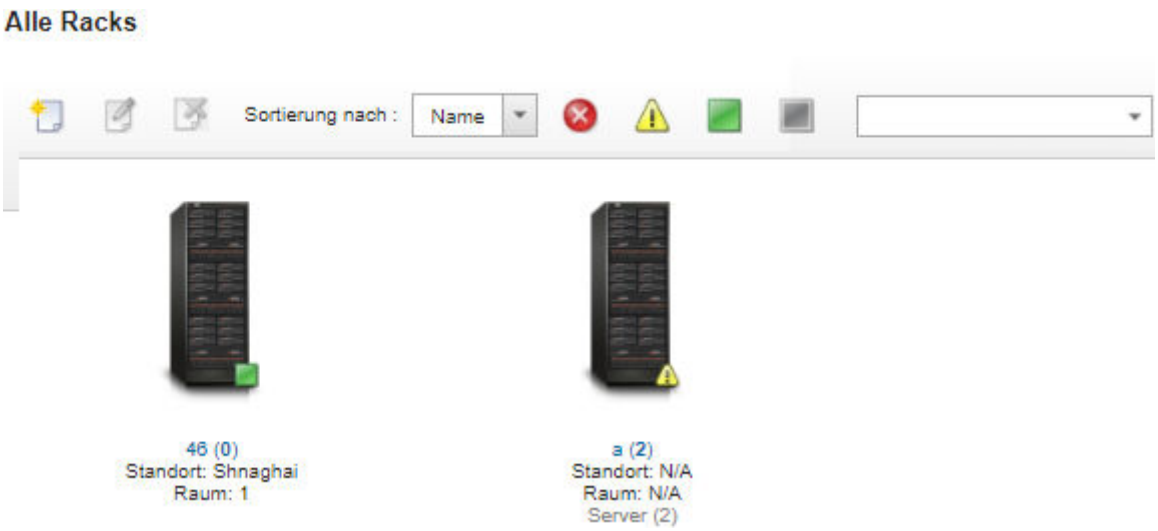
Gehen Sie zum Entfernen eines Racks wie folgt vor:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Racks**. Die Seite Alle Racks wird angezeigt.

Auf der Seite Alle Racks wird jedes Rack als Miniaturansicht mit dem Rack-Namen, der Anzahl der enthaltenen verwalteten Einheiten sowie dem Einheitenstatus mit dem höchsten Schweregrad angezeigt.

Anmerkungen: Sie können die Liste der Racks nach Rackname, Anzahl der Einheiten im Rack oder Schweregrad sortieren, um bestimmte Racks leichter zu finden. Sortiert wird von links nach rechts und von oben nach unten. Darüber hinaus können Sie die Racks nach Schweregrad filtern, indem Sie auf die folgenden Symbole in der Symbolleiste klicken oder einen Rack-Namen im Feld **Filter** eingeben, um die angezeigten Racks weiter zu filtern.

- Symbol für **Kritische Alerts** ( )
- Symbol für **Warnalerts** ( )
- Symbol für **Normale Alerts** ( )



Schritt 2. Wählen Sie die Miniaturansicht für das Rack aus, damit der Gehäuserahmen entfernt werden kann.

Schritt 3. Klicken Sie auf das Symbol **Entfernen** ( ).

Schritt 4. Klicken Sie auf **Entfernen**.

Ergebnisse

Die Miniaturansicht für das Rack wird von der Seite Alle Racks entfernt. Alle Einheiten, die in diesem Rack positioniert waren, stehen nun auf der Seite Racks bearbeiten zum Einfügen in andere Racks zur Verfügung.

Kapitel 7. Gehäuse verwalten

Lenovo XClarity Administrator kann verschiedene Arten von Systemen verwalten, z. B. Flex System-Gehäuse.

Weitere Informationen:  XClarity Administrator: Ermittlung

Vorbereitende Schritte

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

Vor der Verwaltung von Gehäusen sollten Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind:

- Gehen Sie die Verwaltungsaspekte nochmal durch, bevor Sie eine Einheit verwalten. Weitere Informationen finden Sie unter Verwaltungshinweise in der Onlinedokumentation von XClarity Administrator.
- Bestimmte Anschlüsse müssen verfügbar sein, um mit dem CMM für das verwaltete Gehäuse zu kommunizieren. Stellen Sie sicher, dass diese Anschlüsse verfügbar sind, bevor Sie versuchen, ein Gehäuse zu verwalten. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.
- Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jedem Gehäuse installiert ist, das Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.
- Stellen Sie sicher, dass 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 **Mgt Modulverwaltung → 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.
- Um ein Gehäuse zu ermitteln, das sich in einem *anderen* Subnetz als XClarity Administrator befindet, muss eine der folgenden Bedingungen erfüllt sein:
  - Stellen Sie sicher, dass Sie die Multicast-SLP-Weiterleitung für die Top-of-Rack-Switches sowie für die Router in Ihrer Umgebung aktivieren. Lesen Sie die mit dem jeweiligen Switch oder Router bereitgestellte Dokumentation, um herauszufinden, ob die Multicast-SLP-Weiterleitung aktiviert ist und falls nicht, wie Sie sie aktivieren können.
  - Wenn SLP auf dem Endpunkt oder im Netzwerk deaktiviert ist, können die DNS-Ermittlungsmethode stattdessen nutzen, indem Sie manuell einen Servicedatensatz (SRV) auf Ihrem Domain Name Server (DNS) hinzufügen, zum Beispiel für XClarity Administrator.
    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```
    Aktivieren Sie anschließend die DNS-Ermittlung beim CMM über die Verwaltungswebschnittstelle, indem Sie auf **Mgt Modulverwaltung → Netzprotokoll** klicken, danach die Registerkarte **DNS** und zuletzt **DNS zum Ermitteln von Lenovo XClarity Administrator verwenden** auswählen.

    Anmerkungen:

- Das CMM muss mit einer Firmwareversion von Mai 2017 ausgeführt werden, um die automatische Ermittlung mit DNS zu unterstützen.
- Wenn mehrere XClarity Administrator-Instanzen in Ihrer Umgebung vorhanden sind, wird das Gehäuse nur von der Instanz ermittelt, die als erste auf die Ermittlungsanforderung reagiert. Das Gehäuse wird nicht von allen Instanzen ermittelt.

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

Achtung: Wenn Sie beabsichtigen, CMMs mit der Firmwareversion von Flex-Stackversion 1.3.2.1 2PET12K bis 2PET12Q ausführen, die CMMs seit mehr als drei Wochen ausgeführt werden und sie sich in einer Konfiguration mit zwei CMMs befinden, müssen Sie die CMMs vor einer Firmwareaktualisierung mit XClarity Administrator virtuell erneut einsetzen.

Wichtig: Wenn Sie neben Lenovo XClarity Administrator weitere Verwaltungssoftware verwenden möchten, um Ihr Gehäuse zu überwachen, und wenn diese Verwaltungssoftware SNMPv3-Kommunikation nutzt, müssen Sie zuerst eine lokale CMM-Benutzer-ID erstellen, die mit den geeigneten SNMPv3-Informationen konfiguriert ist, und sich dann am CMM mit dieser Benutzer-ID anmelden und das Kennwort ändern. Weitere Informationen hierzu finden Sie unter Verwaltungshinweise in der XClarity Administrator Onlinedokumentation.

Zu dieser Aufgabe

XClarity Administrator kann Gehäuse in Ihrer Umgebung automatisch ermitteln, indem verwaltbare Systeme erkannt werden, die sich im selben IP-Subnetz wie XClarity Administrator befinden. Um Gehäuse zu ermitteln, die sich in anderen Subnetzen befinden, geben Sie eine IP-Adresse oder einen IP-Adressbereich an oder importieren Sie Informationen von einem Arbeitsblatt.

Nachdem die Gehäuse von XClarity Administrator verwaltet werden, fragt XClarity Administrator alle verwalteten Gehäuse regelmäßig ab, um Informationen zu sammeln, z. B. Bestand, elementare Produktdaten und Status. Sie können jedes verwaltete Gehäuse anzeigen und überwachen und Verwaltungsaktionen ausführen (z. B. Systeminformationen, Netzwerkeinstellung und Failover konfigurieren). Bei Gehäusen im Schutzmodus sind die Verwaltungsaktionen deaktiviert.

Gehäuse werden durch Verwendung der verwalteten *XClarity Administrator Authentifizierung verwaltet*.

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

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

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

  Anmerkungen:

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

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

    Anmerkung: Wenn die verwaltete Authentifizierung für ein Gerät aktiviert ist, können Sie mit XClarity Administrator keine gespeicherten Anmeldeinformationen für dieses Gerät bearbeiten.
  - Wenn Sie den lokalen oder externen LDAP-Server als XClarity Administrator-Authentifizierungsserver nutzen, werden auf diesem Authentifizierungsserver definierte Benutzeraccounts für die Anmeldung bei XClarity Administrator, CMMs und BMCs (Baseboard Management Controllern) in der XClarity Administrator-Domäne verwendet. Lokale CMM- und Management-Controller-Benutzeraccounts werden deaktiviert.
  - Bei Verwendung eines SAML 2.0 Identity Provider als XClarity Administrator-Authentifizierungsserver sind SAML-Accounts für verwaltete Einheiten nicht zugänglich. Wenn Sie jedoch einen SAML Identitiy Provider und einen LDAP-Server zusammen verwenden und der Identity Provider Konten nutzt, die sich auf dem LDAP-Server befinden, können LDAP-Benutzeraccounts zur Anmeldung bei den verwalteten Einheiten und gleichzeitig modernere von SAML 2.0 bereitgestellte Authentifizierungsmethoden (z. B. mehrstufige Authentifizierung und Single Sign-on) zur Anmeldung bei XClarity Administrator verwendet werden.
  - Mit Single Sign-On kann sich ein Benutzer, der bereits bei XClarity Administrator angemeldet ist, automatisch beim Baseboard Management Controller anmelden. Single Sign-On ist standardmäßig aktiviert, wenn ein ThinkSystem oder ThinkAgile Server von XClarity Administrator verwaltet wird (es sei denn, der Server wird mit CyberArk-Kennwörtern verwaltet). Sie können global konfigurieren, dass Single Sign-On für alle verwalteten ThinkSystem und ThinkAgile Server aktiviert oder deaktiviert ist. Das Aktivieren von Single Sign-On für einen bestimmten ThinkSystem und ThinkAgile Server überschreibt die globale Einstellung für alle ThinkSystem und ThinkAgile Server (siehe).

    Anmerkung: Single Sign-On ist automatisch deaktiviert, wenn das CyberArk Identitätsverwaltungssystem zur Authentifizierung verwendet wird.
  - Wenn die verwaltete Authentifizierung für ThinkSystem SR635 und SR655 Server aktiviert ist:
    - Die Baseboard Management Controller-Firmware unterstützt bis zu fünf LDAP-Benutzerrollen. XClarity Administrator fügt diese LDAP-Benutzerrollen während der Verwaltung zu den Servern hinzu: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** und **lxc-os-admin**.

      Benutzern muss mindestens eine der angegebenen LDAP-Benutzerrollen zugeordnet werden, damit sie mit den ThinkSystem SR635 und SR655 Servern kommunizieren können.
    - Die Management-Controller-Firmware unterstützt keine LDAP-Benutzer mit demselben Benutzernamen wie der lokale Benutzer des Servers.
  - Für ThinkServer- und System x M4-Server wird der XClarity Administrator-Authentifizierungsserver nicht verwendet. Stattdessen wird ein IPMI-Account in der Einheit mit dem Präfix „LXCA_“ erstellt, auf das eine willkürliche Zeichenfolge folgt. (Die vorhandenen lokalen IPMI-Benutzeraccounts werden nicht

deaktiviert.) Wenn Sie die Verwaltung eines ThinkServer-Servers beenden, wird der Benutzeraccount „LXCA_“ deaktiviert und das Präfix „LXCA_“ wird durch das Präfix „DISABLED_“ ersetzt. Um festzustellen, ob ein ThinkServer-Server durch eine andere Instanz verwaltet wird, sucht XClarity Administrator nach IPMI-Accounts mit dem Präfix „LXCA_“. Wenn Sie sich dazu entschließen, die Verwaltung eines verwalteten ThinkServer-Servers zu erzwingen, werden alle IPMI-Accounts in der Einheit mit dem Präfix „LXCA_“ deaktiviert und umbenannt. IPMI-Konten, die nicht mehr verwendet werden, sollten Sie manuell löschen.

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

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

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

Eine Einheit kann nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie es mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die erste XClarity Administrator-Verwaltung der Speichereinheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten. Falls bei der Verwaltungsaufhebung ein Fehler auftritt, können Sie bei der Verwaltung die Option **Verwaltung erzwingen** auf dem neuen XClarity Administrator auswählen.

Anmerkung: Wenn Sie das Netzwerk nach verwaltbaren Einheiten durchsuchen, weiß XClarity Administrator nicht, ob eine Einheit bereits von einem anderen Manager verwaltet wird, bis er versucht, die Einheit zu verwalten.

Während des Verwaltungsprozesses führt XClarity Administrator die folgenden Aktionen aus:

- Meldet sich am Gehäuse mit den bereitgestellten Anmeldeinformationen an.
- Erfasst den Bestand für alle Komponenten in jedem Gehäuse, z. B. CMM, Rechenknoten, Speichereinheiten und Flex-Switches.

  Anmerkung: Einige Bestandsdaten werden erfasst, nachdem der Verwaltungsprozess abgeschlossen ist. Das Gehäuse befindet sich im Wartestatus, bis alle Bestandsdaten erfasst sind. Sie können bestimmte Tasks auf einer verwalteten Einheit nicht ausführen (z. B. die Implementierung eines Servermusters), bis alle Bestandsdaten für diese Einheit erfasst sind und das Gehäuse sich nicht mehr im Wartestatus befindet.
- Konfiguriert die Einstellungen für den NTP-Server, sodass alle verwalteten Einheiten den NTP-Server von XClarity Administrator verwenden.
- Weist die zuletzt bearbeitete Firmwarekonformitätsrichtlinie dem Gehäuse zu.
- Konfiguriert für Lenovo Flex-Einheiten optional die Firewallregeln der Einheiten, damit eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.
- Tauscht Sicherheitszertifikate mit dem CMM aus, wobei das CMM-Sicherheitszertifikat in den XClarity Administrator-Truststore kopiert wird und das XClarity Administrator-CA-Sicherheitszertifikat an das CMM gesendet wird. Das CMM lädt das Zertifikat in den CMM-Truststore und verteilt es an die Rechenknoten-Serviceprozessoren für die Aufnahme in ihre Truststores.

- Konfiguriert die verwaltete Authentifizierung. Die Einstellungen für den CMM LDAP-Client werden so geändert, dass XClarity Administrator als Authentifizierungsserver verwendet wird, und die globalen Anmeldungseinstellungen im CMM werden in **Nur externer Authentifizierungsserver** geändert. Weitere Informationen zu Authentifizierungsservern finden Sie unter Authentifizierungsserver verwalten.
- Erstellt den Benutzeraccount für die Wiederherstellung (`RECOVERY_ID`). Weitere Informationen über den `RECOVERY_ID` Account finden Sie unter Authentifizierungsserver verwalten.

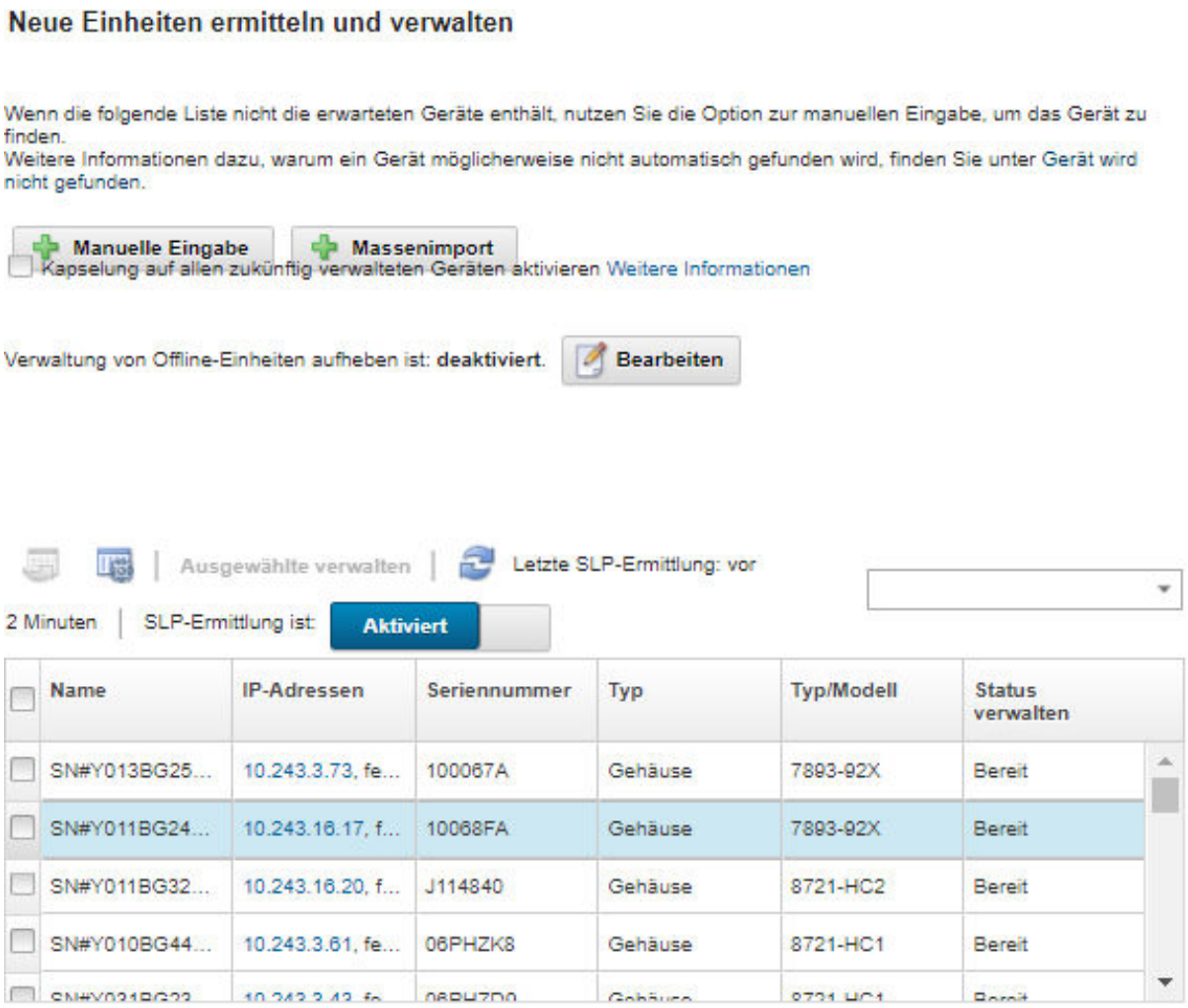
Achtung: Bei der Verwaltung des Gehäuses setzt XClarity Administrator die maximale Anzahl der gleichzeitigen sicheren TCP-Befehlsmodusverbindungen auf 15 und die maximale Anzahl der gleichzeitigen Legacy-TCP-Befehlsmodusverbindungen auf 0. Dadurch werden möglicherweise von Ihnen bereits im CMM festgelegte Einstellungen überschrieben.

Anmerkung: XClarity Administrator ändert die Sicherheitseinstellungen oder die Verschlüsselungseinstellungen (Verschlüsselungsmodus und den für sichere Kommunikation verwendeten Modus) im Verwaltungsprozess nicht. Sie können die Verschlüsselungseinstellungen ändern, nachdem das Gehäuse verwaltet wurde (siehe Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren).

Vorgehensweise

Wählen Sie eine der folgenden Vorgehensweisen, um das Gehäuse mit XClarity Administrator zu ermitteln und zu verwalten.

- Ermitteln und verwalten Sie eine Vielzahl von Gehäusen und anderen Einheiten mithilfe einer Massenimportdatei (siehe Systeme verwalten in der Onlinedokumentation von Lenovo XClarity Administrator).
- Ermitteln und verwalten Sie die Gehäuse, die sich auf demselben IP-Subnetz wie XClarity Administrator befinden.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Neue Einheiten ermitteln und verwalten wird angezeigt.



Sie können die Tabellenspalten sortieren, um das Gehäuse, das Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie Text (z. B. einen Systemnamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Gehäuse weiter zu filtern. Sie können die angezeigten Spalten und die Standard-Sortierreihenfolge ändern, indem Sie auf das Symbol **Spalten anpassen** ( ) klicken.

2. Klicken Sie auf das Symbol **Aktualisieren** ( ), um alle verwaltbaren Einheiten in der XClarity Administrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
3. Aktivieren Sie das Kontrollkästchen **Kapselung für alle zukünftig verwalteten Einheiten aktivieren**, um die Firewallregeln während des Verwaltungsprozesses auf allen Einheiten dahingehend zu ändern, dass eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.

   Die Kapselung kann auf bestimmten Einheiten nach der Verwaltung aktiviert oder deaktiviert werden.

   Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.
4. Wählen Sie ein oder mehrere Gehäuse aus, die Sie verwalten möchten.
5. Klicken Sie auf **Ausgewählte verwalten**.

6. Wählen Sie aus, ob Sie die XClarity Administrator verwaltete Authentifizierung oder die lokale Authentifizierung für diese Einheit verwenden möchten. Die verwaltete Authentifizierung ist standardmäßig ausgewählt. Um die lokale Authentifizierung zu verwenden, deaktivieren sie **Verwaltete Authentifizierung**.

   Anmerkung: Verwaltete und lokale Authentifizierungen werden für ThinkServer- und System x M4-Server nicht unterstützt.

7. Wählen Sie die Art von Anmeldeinformationen aus, die für die Einheit zu verwenden ist, und geben Sie die entsprechenden Anmeldeinformationen an:
   - **Manuell eingegebene Anmeldeinformationen verwenden**
     - Geben Sie die lokale Benutzer-ID und das Kennwert mit **lxc-supervisor**-Berechtigung zur Authentifizierung des CMM an.
     - (Optional) Geben Sie ein neues Kennwort für den CMM-Benutzeraccount an, falls das Kennwort derzeit auf der Einheit abgelaufen ist.
   - **Gespeicherte Anmeldeinformationen verwenden**

     Wählen Sie die gespeicherten Anmeldeinformationen mit **lxc-supervisor**-Berechtigung aus, die für diese verwaltete Einheit verwendet werden sollen. Sie können gespeicherte Anmeldeinformationen durch Klicken auf **Gespeicherte Anmeldeinformationen verwalten** speichern.

     Anmerkung: Wenn Sie sich für die Verwendung der lokalen Authentifizierung entscheiden, müssen Sie gespeicherte Anmeldeinformationen zur Verwaltung der Einheit auswählen.

   Tipp: Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl. Oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).

   Weitere Informationen zu normalen und gespeicherten Anmeldeinformationen finden Sie in Benutzeraccounts verwalten und Gespeicherte Anmeldeinformationen verwalten.

8. Geben Sie das Kennwort für die Wiederherstellung an, falls die verwaltete Authentifizierung ausgewählt ist.

   Ein Account für die Wiederherstellung (`RECOVERY_ID`) wird im CMM erstellt und alle lokalen Benutzeraccounts werden deaktiviert. Wenn ein Problem mit XClarity Administrator auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich *nicht* mehr am CMM mit den normalen Benutzeraccounts anmelden. Jedoch können Sie sich mit dem Account `RECOVERY_ID` anmelden.

   Anmerkung:
   - Das Kennwort für die Wiederherstellung ist erforderlich, falls Sie sich für die Verwendung einer verwalteten Authentifizierung entscheiden und ist nicht zulässig, wenn Sie die lokale Authentifizierung wählen.
   - Sie können auswählen, ob Sie für die Wiederherstellung ein lokales Account oder gespeicherte Anmeldeinformationen verwenden möchten. In beiden Fällen lautet der Benutzername immer `RECOVERY_ID`.
   - Stellen Sie sicher, dass das Kennwort den Sicherheits- und Kennwortrichtlinien der Einheit entspricht. Sicherheits- und Kennwortrichtlinien können variieren.
   - Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.

   Weitere Informationen über die Wiederherstellungs-ID finden Sie unter Authentifizierungsserver verwalten.

9. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

   Anmerkungen:

   – Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.

   – Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.

10. Klicken Sie auf **Verwalten**.

    Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

    Wenn der Prozess abgeschlossen ist, zeigt der Dialog die Anzahl der Einheiten im Gehäuse und den Gehäusestatus an.

    Anmerkung: Einige Bestandsdaten werden erfasst, nachdem der Verwaltungsprozess abgeschlossen ist. Das Gehäuse befindet sich im Wartestatus, bis alle Bestandsdaten erfasst sind. Sie können bestimmte Tasks auf einer verwalteten Einheit nicht ausführen (z. B. die Implementierung eines Servermusters), bis alle Bestandsdaten für diese Einheit erfasst sind und das Gehäuse sich nicht mehr im Wartestatus befindet.

11. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

    Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

    – Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

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

    – Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.

    – Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

    Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

12. Wenn es sich um ein neues Gehäuse handelt, klicken Sie auf **Mit Gehäusekonfiguration fortfahren**, um die Verwaltungsnetzwerkeinstellungen für das gesamte Gehäuse zu überprüfen und zu ändern (einschließlich Rechenknoten und Flex-Switches) und die Rechenknoteninformationen, den lokalen Speicher, den E/A-Adapter, die Bootziele und Firmwareeinstellungen zu konfigurieren, indem Sie Servermuster erstellen und implementieren. Weitere Informationen finden Sie in den Abschnitten IP-Verwaltungseinstellungen für ein Gehäuse ändern und Server mithilfe von Konfigurationsmustern konfigurieren.

- Ermitteln und verwalten Sie Gehäuse, die sich nicht im selben IP-Subnetz wie XClarity Administrator befinden, indem Sie manuell IP-Adressen angeben.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen **Kapselung für alle zukünftig verwalteten Einheiten aktivieren**, um die Firewallregeln während des Verwaltungsprozesses auf allen Einheiten dahingehend zu ändern, dass eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.

   Die Kapselung kann auf bestimmten Einheiten nach der Verwaltung aktiviert oder deaktiviert werden.

   Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.
3. Wählen Sie **Manuelle Eingabe**.
4. Geben Sie die Netzwerkadressen des Gehäuses an, das Sie verwalten möchten:
   - Klicken Sie auf **Einzelsystem** und geben Sie einen einzelnen IP-Adress-Domänennamen oder einen vollständig qualifizierten Domänennamen (FQDN) ein.

     Anmerkung: Stellen Sie bei der Angabe eines FQDN sicher, dass ein gültiger Domänenname auf der Seite Netzwerkzugriff angegeben wird (siehe Netzwerkzugriff konfigurieren).
   - Klicken Sie auf **Mehrere Systeme** und geben Sie einen Bereich von IP-Adressen ein. Um einen weiteren Bereich hinzuzufügen, klicken Sie auf das Symbol **Hinzufügen** (). Um einen Bereich zu entfernen, klicken Sie auf das Symbol **Entfernen** ().
5. Klicken Sie auf **OK**.
6. Wählen Sie aus, ob Sie die XClarity Administrator verwaltete Authentifizierung oder die lokale Authentifizierung für diese Einheit verwenden möchten. Die verwaltete Authentifizierung ist standardmäßig ausgewählt. Um die lokale Authentifizierung zu verwenden, deaktivieren sie **Verwaltete Authentifizierung**.

   Anmerkung: Verwaltete und lokale Authentifizierungen werden für ThinkServer- und System x M4-Server nicht unterstützt.
7. Wählen Sie die Art von Anmeldeinformationen aus, die für die Einheit zu verwenden ist, und geben Sie die entsprechenden Anmeldeinformationen an:
   - **Manuell eingegebene Anmeldeinformationen verwenden**
     - Geben Sie die lokale Benutzer-ID und das Kennwert mit **lxc-supervisor**-Berechtigung zur Authentifizierung des CMM an.
     - (Optional) Geben Sie ein neues Kennwort für den CMM-Benutzeraccount an, falls das Kennwort derzeit auf der Einheit abgelaufen ist.
   - **Gespeicherte Anmeldeinformationen verwenden**

     Wählen Sie die gespeicherten Anmeldeinformationen mit **lxc-supervisor**-Berechtigung aus, die für diese verwaltete Einheit verwendet werden sollen. Sie können gespeicherte Anmeldeinformationen durch Klicken auf **Gespeicherte Anmeldeinformationen verwalten** speichern.

     Anmerkung: Wenn Sie sich für die Verwendung der lokalen Authentifizierung entscheiden, müssen Sie gespeicherte Anmeldeinformationen zur Verwaltung der Einheit auswählen.

   Tipp: Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl. Oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).

Weitere Informationen zu normalen und gespeicherten Anmeldeinformationen finden Sie in Benutzeraccounts verwalten und Gespeicherte Anmeldeinformationen verwalten.

8. Geben Sie das Kennwort für die Wiederherstellung an, falls die verwaltete Authentifizierung ausgewählt ist.

   Ein Account für die Wiederherstellung (`RECOVERY_ID`) wird im CMM erstellt und alle lokalen Benutzeraccounts werden deaktiviert. Wenn ein Problem mit XClarity Administrator auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich *nicht* mehr am CMM mit den normalen Benutzeraccounts anmelden. Jedoch können Sie sich mit dem Account `RECOVERY_ID` anmelden.

   Anmerkung:

   – Das Kennwort für die Wiederherstellung ist erforderlich, falls Sie sich für die Verwendung einer verwalteten Authentifizierung entscheiden und ist nicht zulässig, wenn Sie die lokale Authentifizierung wählen.
   – Sie können auswählen, ob Sie für die Wiederherstellung ein lokales Account oder gespeicherte Anmeldeinformationen verwenden möchten. In beiden Fällen lautet der Benutzername immer `RECOVERY_ID`.
   – Stellen Sie sicher, dass das Kennwort den Sicherheits- und Kennwortrichtlinien der Einheit entspricht. Sicherheits- und Kennwortrichtlinien können variieren.
   – Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.

   Weitere Informationen über die Wiederherstellungs-ID finden Sie unter Authentifizierungsserver verwalten.

9. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

   Anmerkungen:

   – Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
   – Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.

10. Klicken Sie auf **Verwalten**.

    Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

    Wenn der Prozess abgeschlossen ist, zeigt der Dialog die Anzahl der Einheiten im Gehäuse und den Gehäusestatus an.

    Anmerkung: Einige Bestandsdaten werden erfasst, nachdem der Verwaltungsprozess abgeschlossen ist. Das Gehäuse befindet sich im Wartestatus, bis alle Bestandsdaten erfasst sind. Sie können bestimmte Tasks auf einer verwalteten Einheit nicht ausführen (z. B. die Implementierung eines Servermusters), bis alle Bestandsdaten für diese Einheit erfasst sind und das Gehäuse sich nicht mehr im Wartestatus befindet.

11. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

    Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

    – Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

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

- Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

12. Wenn es sich um ein neues Gehäuse handelt, klicken Sie auf **Mit Gehäusekonfiguration fortfahren**, um die Verwaltungsnetzwerkeinstellungen für das gesamte Gehäuse zu überprüfen und zu ändern (einschließlich Rechenknoten und Flex-Switches) und die Rechenknoteninformationen, den lokalen Speicher, den E/A-Adapter, die Bootziele und Firmwareeinstellungen zu konfigurieren, indem Sie Servermuster erstellen und implementieren. Weitere Informationen finden Sie in den Abschnitten IP-Verwaltungseinstellungen für ein Gehäuse ändern und Server mithilfe von Konfigurationsmustern konfigurieren.

Nach dieser Aufgabe

- Ermitteln und verwalten Sie weitere Einheiten.
- Implementieren Sie Betriebssystem-Images auf den Servern, auf denen noch kein Betriebssystem installiert ist. Siehe Betriebssysteme auf Bare-Metal-Servern installieren für weitere Informationen.
- Aktualisieren Sie die Firmware auf Einheiten, die nicht den aktuellen Richtlinien entsprechen (siehe Firmware auf verwalteten Einheiten aktualisieren).
- Fügen Sie die neu verwalteten Einheiten zum entsprechenden Rack hinzu, um die physische Umgebung widerzuspiegeln (siehe Racks verwalten).
- Überwachen Sie den Hardwarestatus und die Details (siehe Den Status eines verwalteten Servers anzeigen).
- Überwachen Sie Ereignisse und Alerts (siehe Ereignisse handhaben und Mit Alerts arbeiten).

Den Status eines verwalteten Gehäuses anzeigen

Sie können eine Zusammenfassung und den detaillierten Status für das verwaltete Gehäuse und die zugehörigen installierten Komponenten über Lenovo XClarity Administrator anzeigen.

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

Zu dieser Aufgabe

Die folgenden Statussymbole geben den allgemeinen Status der Einheit an. Wenn die Zertifikate nicht übereinstimmen, wird „(nicht vertrauenswürdig)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (nicht vertrauenswürdig)“. Wenn ein Verbindungsproblem besteht oder eine Verbindung zur Einheit nicht vertrauenswürdig ist, wird „(Verbindung)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (Verbindung)“.

- () Kritisch
- () Warnung
- () Ausstehend
- () Information
- () Normal
- () Offline
- () Nicht bekannt

Vorgehensweise

Gehen Sie wie folgt vor, um den Status für ein verwaltetes Gehäuse anzuzeigen.

- Sie können ausführliche Informationen über das Gehäuse anzeigen, indem Sie auf den Link **Details** oder auf **Aktionen → Anzeigen → Details** klicken.
- Sie können die CMM-Webschnittstelle für das Gehäuse starten, indem Sie auf den Link **IP-Adresse** klicken (siehe Die CMM-Webschnittstelle für ein Gehäuse starten).
- Sie können Informationen (z. B. Support-Kontakt, Position und Beschreibung) ändern, indem Sie auf **Aktionen → Bestand → Eigenschaften bearbeiten**klicken.
- Sie können die IP-Verwaltungseinstellungen für das ganze Gehäuse (einschließlich Rechenknoten und Flex-Switches) ändern, indem Sie auf **Aktionen → Bestand → IP-Verwaltungsadressen bearbeiten** klicken.
- Sie können ausführliche Informationen zu einem oder mehreren Gehäusen in eine CSV-Datei exportieren, indem Sie das Gehäuse auswählen und auf **Aktionen → Bestand → Bestand exportieren** klicken.

  Anmerkung: Sie können Bestandsdaten für maximal 60 Einheiten gleichzeitig exportieren.

  Tipp: Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Sie können mögliche Probleme zwischen dem Sicherheitszertifikat von Lenovo XClarity Administrator und dem Sicherheitszertifikat des CMM im Gehäuse beheben, indem Sie ein Gehäuse auswählen und auf **Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen** klicken.

Die Details eines verwalteten Gehäuses anzeigen

Sie können über Lenovo XClarity Administrator ausführliche Informationen zum verwalteten Gehäuse anzeigen. Dazu gehören die Firmwareversionen, IP-Adressen und UUID (Universally Unique Identifier).

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

Zu dieser Aufgabe

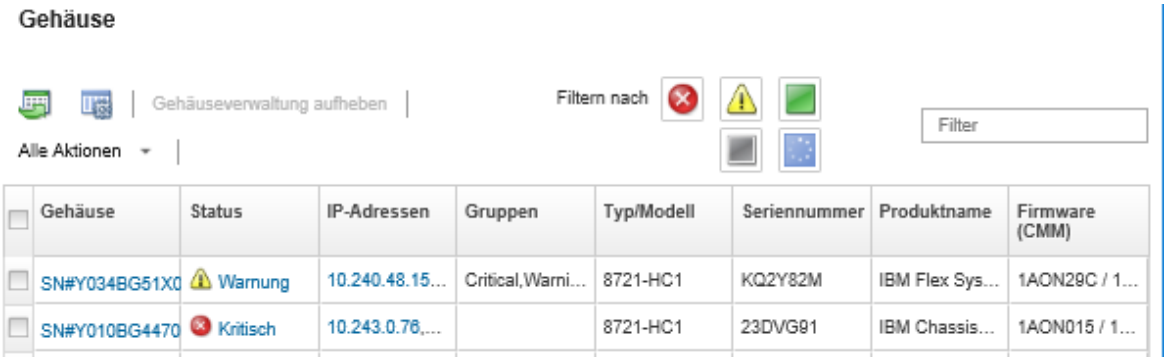
Die Lufttemperatur auf Systemebene wird von einem physischen Sensor an der Vorderseite des Servers gemessen. Diese Temperatur gibt die Lufteintrittstemperatur für den Server an. Beachten Sie, dass die vom XClarity Administrator und die vom CMM gemeldete Lufttemperatur abweichen kann, falls die Temperatur zu verschiedenen Zeitpunkten erfasst wird.

Vorgehensweise

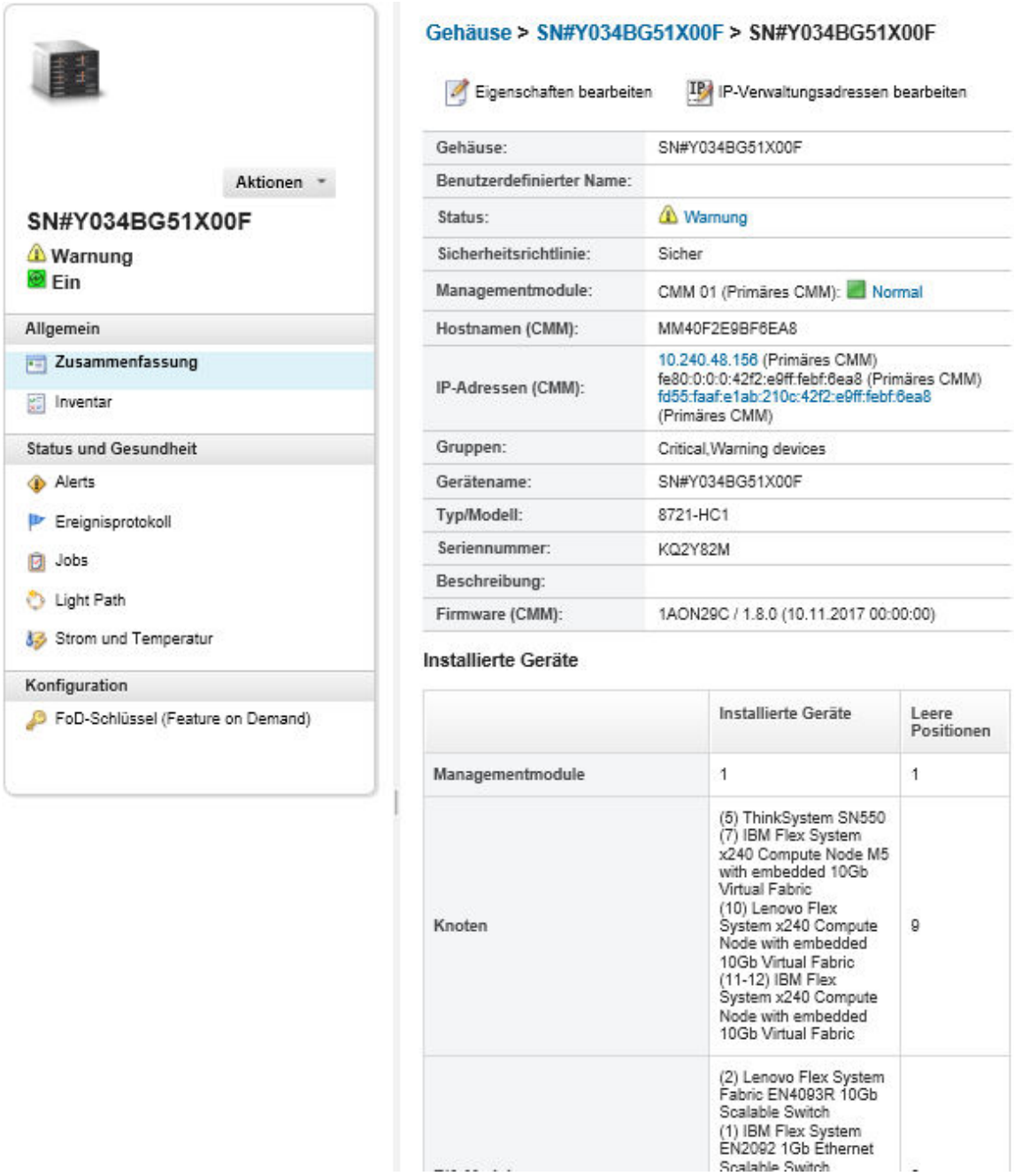
Gehen Sie wie folgt vor, um die Details für ein verwaltetes Gehäuse anzuzeigen:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Gehäuse**. Die Seite Gehäuse wird mit einer Tabellenansicht aller verwalteten Gehäuse angezeigt.

Sie können die Tabellenspalten sortieren, um das Gehäuse, das Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie Text (z. B. einen Gehäusenamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Gehäuse weiter zu filtern.



Schritt 2. Klicken Sie auf den Gehäusenamen in der Spalte **Gehäuse**. Die Statusübersichtsseite für das Gehäuse mit den Gehäuseeigenschaften und den im Gehäuse installierten Komponenten wird angezeigt.



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

- Klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung des Gehäuses, einschließlich Systeminformationen und installierten Komponenten anzuzeigen (siehe Den Status eines verwalteten Gehäuses anzeigen).
- Klicken Sie auf **Inventardetails**, um Details zu den Gehäusekomponenten anzuzeigen. Dazu gehören:
  - Firmwareversionen für alle Gehäusekomponenten.
  - Details des CMM, z. B. Hostname, IPv4-Adresse, IPv6-Adresse und MAC-Adressen.
  - Asset-Details des Gehäuses und im Gehäuse installiertes CMM, einschließlich Name, UUID (Universally Unique Identifier) und Position.

- Klicken Sie auf **Alerts**, um die Liste der aktuellen Alerts für dieses Gehäuse anzuzeigen (siehe Mit Alerts arbeiten).
- Klicken Sie auf **Ereignisprotokoll**, um die Liste der Ereignisse für dieses Gehäuse anzuzeigen (siehe Ereignisse im Ereignisprotokoll überwachen).
- Klicken Sie auf **Jobs**, um eine Liste der diesem Gehäuse zugeordneten Jobs anzuzeigen (siehe Jobs überwachen).
- Klicken Sie auf **Light Path**, um den aktuellen Status der Gehäuse-LEDs anzuzeigen (z. B. Position, Fehler und Informationen). Dies entspricht der Betrachtung des Gehäusebedienfelds.
- Klicken Sie auf **Strom und Temperatur**, um Details zu Strom und Luftstrom anzuzeigen.

  Tipp: Verwenden Sie die Aktualisierungsschaltfläche des Webbrowsers, um die neuesten Strom- und Temperaturdaten zu erfassen. Die Datenerfassung kann mehrere Minuten in Anspruch nehmen.
- Klicken Sie auf **FoD-Schlüssel** um auf die für die Bestellung eines FoD-Schlüssels benötigten Informationen und andere agentenlose Informationen zuzugreifen (siehe Features on Demand-Schlüssel anzeigen).

Nach dieser Aufgabe

Außer der Anzeige von Übersichts- und Detailinformationen zu einem Gehäuse können Sie die folgenden Aktionen durchführen:

- Sie können ein Gehäuse in einer grafischen Rack- oder Gehäuseansicht anzeigen, indem Sie auf **Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Aktionen → anzeigen → In der Gehäuseansicht anzeigen** klicken.
- Sie können die CMM-Webschnittstelle starten, indem Sie auf den Link **IP-Adresse** klicken (siehe Die CMM-Webschnittstelle für ein Gehäuse starten).
- Sie können Informationen (z. B. Support-Kontakt, Position und Beschreibung) ändern, indem Sie auf **Eigenschaften bearbeiten** klicken (siehe Systemeigenschaften für ein Gehäuse ändern).
- Sie können die IP-Verwaltungseinstellungen für das ganze Gehäuse ändern, z. B. Rechenknoten und Flex-Switches, indem Sie auf **Alle Aktionen → Bestand → IP-Verwaltungsadressen bearbeiten** klicken (siehe IP-Verwaltungseinstellungen für ein Gehäuse ändern).
- Sie können ausführliche Informationen über das Gehäuse in eine CSV-Datei exportieren, indem Sie auf **Aktionen → Bestand → Bestand exportieren**.

  Anmerkungen:

  – Weitere Informationen zu Bestandsdaten in der CSV-Datei finden Sie unter GET /chassis/<*UUID_list*> in der Onlinedokumentation zu XClarity Administrator.

  – Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Sie können die Verwaltung eines Gehäuses aufheben (siehe Verwaltung eines Gehäuses aufheben).
- Sie können Änderungen der Firewallregeln in einem Gehäuse aktivieren oder deaktivieren, die eingehende Anforderungen nur auf solche von XClarity Administrator begrenzen, indem Sie das Gehäuse auswählen und auf **Aktionen → Sicherheit → Kapselung aktivieren** oder **Aktionen → Sicherheit → Kapselung deaktivieren** klicken.

  Die globale Kapselungseinstellung 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.

Die globale Kapselungseinstellung 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 die globale Kapselungseinstellung aktiviert ist und die Einheit Kapselung unterstützt, kommuniziert XClarity Administrator 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 von XClarity Administrator akzeptiert werden.

Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.

- Sie können mögliche Probleme zwischen dem Sicherheitszertifikat von XClarity Administrator und dem Sicherheitszertifikat des CMM im Gehäuse beheben, indem Sie ein Gehäuse auswählen und auf **Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen** klicken (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).

CMM-Konfigurationsdaten sichern und wiederherstellen

Lenovo XClarity Administrator enthält keine integrierten Sicherungsfunktionen für CMM-Konfigurationsdaten. Verwenden Sie stattdessen die Sicherungsfunktionen, die für Ihr verwaltetes CMM verfügbar sind.

Verwenden Sie die Verwaltungswebschnittstelle oder die Befehlszeilenschnittstelle (CLI), um das CMM zu sichern und wiederherzustellen.

- CMM-Konfigurationsdaten sichern
  - Klicken Sie in der Verwaltungswebschnittstelle auf **Mgt Modulverwaltung → Konfiguration → Sicherungskonfiguration**. Siehe CMM-Konfiguration über die Webschnittstelle speichern in der Flex Systems-Onlinedokumentation für weitere Informationen.
  - Verwenden Sie in der CLI den Befehl `write`. Weitere Informationen hierzu finden Sie im Abschnitt CMM-Befehl „write“ in der Flex Systems- Onlinedokumentation
- CMM-Konfigurationsdaten wiederherstellen
  - Klicken Sie in der Verwaltungswebschnittstelle auf **Mgt Modulverwaltung → Konfiguration → Konfiguration aus Datei wiederherstellen**. Siehe CMM-Konfiguration über die Webschnittstelle wiederherstellen in der Flex Systems-Onlinedokumentation für weitere Informationen.
  - Verwenden Sie in der CLI den Befehl `read`. Siehe CMM-Befehl „read“ in der Flex Systems-Onlinedokumentation für weitere Informationen.

Anmerkung: Tipp: Zusätzliche Informationen zum Sichern und Wiederherstellen von Gehäusekomponenten finden Sie im Best Practices-Handbuch zum Sichern und Wiederherstellen von PureFlex und Flex System.

Die CMM-Webschnittstelle für ein Gehäuse starten

Sie können die CMM-Webschnittstelle für ein bestimmtes Gehäuse über Lenovo XClarity Administrator starten.

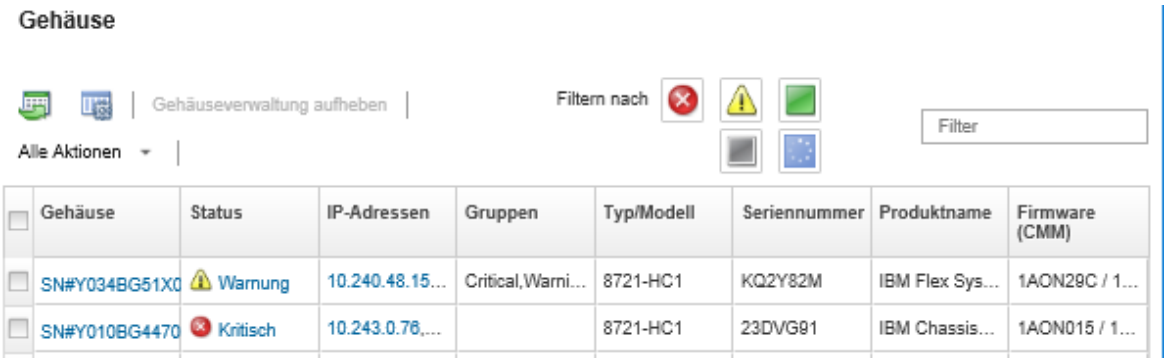
Vorgehensweise

Gehen Sie wie folgt vor, um die CMM-Webschnittstelle zu starten:

Anmerkung: Das Starten der CMM-Webschnittstelle von XClarity Administrator unter Verwendung des Safari-Webbrowsers wird nicht unterstützt.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Gehäuse**, um die Seite Gehäuse anzuzeigen.

Sie können die Tabellenspalten sortieren, um das Gehäuse, das Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie Text (z. B. einen Gehäusenamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Gehäuse weiter zu filtern.



Schritt 2. Klicken Sie auf den Link für das Gehäuse in der Spalte **Gehäuse**. Die Statusübersichtsseite für das Gehäuse wird angezeigt.

Schritt 3. Klicken Sie auf **Alle Aktionen → Starten → Verwaltungswebschnittstelle**. Die CMM-Webschnittstelle wird gestartet.

Tipp: Sie können auch auf die IP-Adresse klicken, um das CMM zu starten.

Schritt 4. Melden Sie sich an der CMM-Webschnittstelle mit Ihren Benutzeranmeldeinformationen von XClarity Administrator an.

Systemeigenschaften für ein Gehäuse ändern

Sie können die Systemeigenschaften für ein bestimmtes Gehäuse ändern.

Vorgehensweise

Gehen Sie wie folgt vor, um die Systemeigenschaften zu ändern:

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Gehäuse**, um die Seite Gehäuse anzuzeigen.

Schritt 2. Wählen Sie das zu aktualisierende Gehäuse aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**, um den Dialog Bearbeiten anzuzeigen.

Schritt 4. Ändern Sie gegebenenfalls die folgenden Daten:
- Servername
- Wenden Sie sich an den Support
- Beschreibung

Anmerkung: Die Eigenschaften für Position, Raum, Rack und unterste Rackeinheit werden von XClarity Administrator aktualisiert, wenn Sie Einheiten in der Webschnittstelle zu einem Rack hinzufügen oder daraus entfernen (siehe Racks verwalten).

Schritt 5. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie diese Eigenschaften ändern, kann es einen Moment dauern, bis die Änderungen in der XClarity Administrator-Webschnittstelle angezeigt werden.

IP-Verwaltungseinstellungen für ein Gehäuse ändern

Sie können die IP-Verwaltungseinstellungen für das gesamte Gehäuse, einschließlich Rechenknoten, Speichereinheiten und Flex-Switches ändern.

Vorgehensweise

Gehen Sie wie folgt vor, um die IP-Verwaltungseinstellungen zu ändern.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Gehäuse**, um die Seite Gehäuse anzuzeigen.

Schritt 2. Wählen Sie das Gehäuse aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Bestand → IP-Verwaltungsadressen bearbeiten**, um die Seite für die Gehäuse- und Komponenten-IP-Einstellungen anzuzeigen.

Schritt 4. Ändern Sie gegebenenfalls die folgenden globalen Einstellungen:

- Aktivieren oder deaktivieren Sie IPv4-Adressen.

  Wenn Sie IPv4-Adressen aktivieren, legen Sie die folgenden Einstellungen fest. Globale IPv4-Einstellungen werden für eine Komponente übernommen, wenn ihre IPv4-Adresse aktualisiert wird.
  - (Optional) Erhalten Sie IP-Adressen über statisch zugeordnete IP-Adressen.
  - Geben Sie die Subnetzmaske und Gateway-Adresse an.
- Legen Sie die folgenden Einstellungen für IPv6-Adressen fest. Globale IPv6-Einstellungen werden für eine Komponente übernommen, wenn ihre IPv6-Adresse aktualisiert wird.
  - (Optional) Erhalten Sie IP-Adressen über statisch zugeordnete IP-Adressen.

    Wenn statische IP-Adressen verwendet werden, können Sie auch die statusunabhängige automatische IP-Adresskonfiguration und die statusabhängige IP-Adresskonfiguration verwenden.
  - Geben Sie die Präfixlänge und Gateway-Adresse an.
- Aktivieren oder deaktivieren Sie DNS-Server.

  Wenn Sie DNS-Server aktivieren:
  - Wählen Sie die DNS-Server-Sucheinstellung aus.
  - Geben Sie die IP-Adressen ein, die für die DNS-Suchreihenfolge verwendet werden sollen.
  - Geben Sie den Domänennamen ein.

Schritt 5. Ändern Sie die folgenden CMM-IP-Einstellungen.

- Geben Sie den Hostnamen und die IP-Adresse für das CMM ein.
- Klicken Sie auf **IP-Adressen automatisch generieren**, um IP-Adressen für die Rechenknoten, Speichereinheiten und Flex-Switches mit der CMM-IP-Adresse als Startpunkt zu erstellen.

Schritt 6. Geben Sie den Hostnamen und die IP-Adressen für jeden Rechenknoten im Gehäuse ein.

Schritt 7. Geben Sie den Hostnamen und die IP-Adressen für jede Speichereinheit im Gehäuse ein.

Schritt 8. Geben Sie die IP-Adressen für jeden Flex-Switch im Gehäuse ein.

Schritt 9. Klicken Sie auf **Speichern**. Ein Dialogfenster mit der Zusammenfassung der Netzwerkeinstellungen wird angezeigt.

Schritt 10. Klicken Sie auf **Übernehmen**.

Alle vorhandenen Komponenten im Gehäuse werden den angegebenen globalen Einstellungen entsprechend aktualisiert. Wenn die Aktualisierung abgeschlossen ist, werden im Dialogfenster die geänderten Einstellungen angezeigt.

Anmerkung: Wenn Sie diese Informationen ändern, kann es einen Moment dauern, bis die Änderungen in der Lenovo XClarity Administrator-Schnittstelle angezeigt werden.

Schritt 11. Klicken Sie auf **Schließen**.

CMM-Failover konfigurieren

Wenn Sie ein zweites CMM in einem Gehäuse installieren, wird das zweite CMM standardmäßig automatisch als Standby-CMM konfiguriert. Wenn das primäre CMM ausfällt, nutzt das Standby-CMM dieselbe IP-Adresse, die für das primäre CMM verwendet wurde, und das Standby-CMM übernimmt die Verwaltung des Gehäuses. Sie können jedoch eine erweitertere Failoverkonfiguration über die Management-Controller-Webschnittstelle für das Gehäuse durchführen.

Zu dieser Aufgabe

Beispielsweise können Sie Folgendes auswählen:

- Die Netzwerkschnittstelle für das Standby-CMM deaktivieren, um ein Failover zu vermeiden.
- Die Netzwerkschnittstelle für das Standby-CMM aktivieren und den Austausch der IP-Adressen zwischen den beiden CMMs beim Failover zulassen.
- Die Netzwerkschnittstelle für das Standby-CMM aktivieren und den Austausch der IP-Adressen zwischen den beiden CMMs beim Failover verhindern.

Weitere Informationen zu den erweiterten CMM-Failover-Funktionen finden Sie unter Befehl „advfailover“ in der CMM-Onlinedokumentation.

Vorgehensweise

Führen Sie folgende Schritte aus, um eine austauschbare IP-Adresse für das primäre CMM und das Standby-CMM zu aktivieren:

Schritt 1. Klicken Sie in der Management-Controller-Webschnittstelle für das Gehäuse auf **Mgt Modulverwaltung → Netzwerk → Ethernet**, um die Ethernet-Konfigurationsseite anzuzeigen.

Schritt 2. Wählen Sie entweder **IPv4** oder **IPv6** für Ihr System.

Schritt 3. Wählen Sie unter **IP-Adresse konfigurieren** die Option zur Verwendung einer statischen IP-Adresse. Wiederholen Sie dies für das andere Protokoll.

Schritt 4. Klicken Sie auf **Mgt Modulverwaltung → Eigenschaften → Erweitertes Failover** und aktivieren Sie die Option für erweitertes Failover.

Schritt 5. Wählen Sie **Verwaltungsmodul-IP-Adresse austauschen**.

Schritt 6. Führen Sie Testszenarien durch, um zu überprüfen, ob das Failover ordnungsgemäß funktioniert und Lenovo XClarity Administrator eine Verbindung mit primären und Backup-CMMs herstellen kann.

Ein CMM neu starten

Sie können ein Chassis Management Module (CMM) über Lenovo XClarity Administrator neu starten.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Gehäuse neu zu starten.

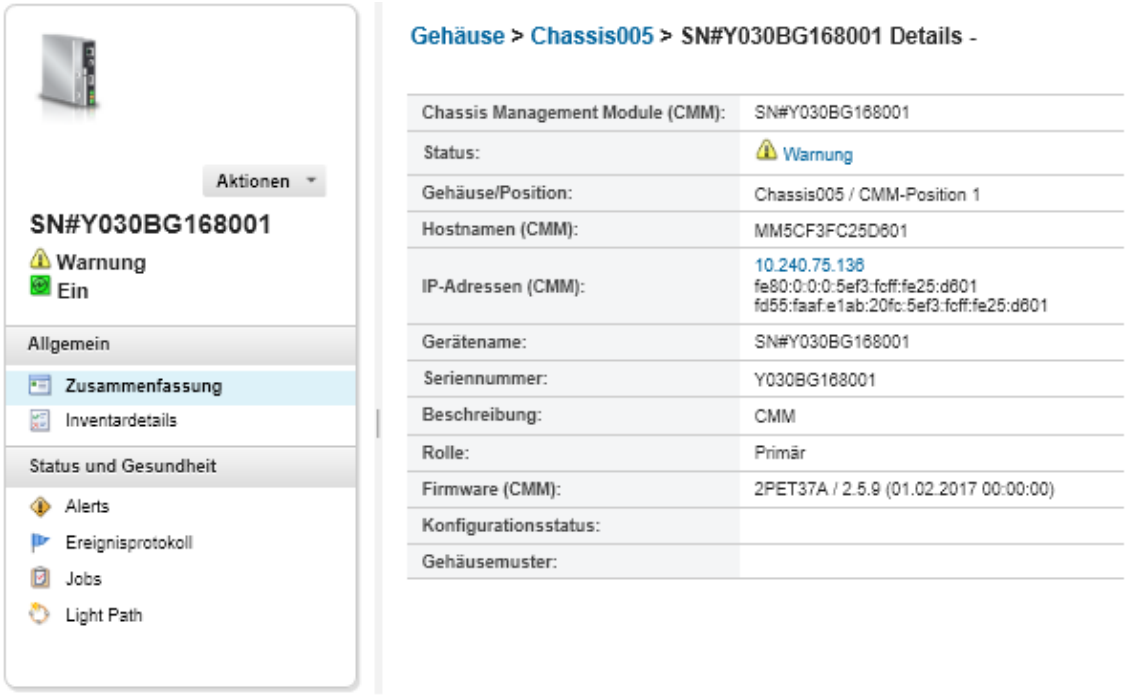
Anmerkung: Wenn das CMM neu gestartet wird, werden alle bestehenden Netzwerkverbindungen zum CMM vorübergehend getrennt.

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Gehäuse**. Die Seite Gehäuse wird mit einer Tabellenansicht aller verwalteten Gehäuse angezeigt.

Schritt 2. Klicken Sie in der Spalte **Gehäuse** auf den Gehäusenamen, um die grafische Gehäuseansicht anzuzeigen.

Schritt 3. Klicken Sie auf die CMM-Grafik, um die Seite „CMM-Zusammenfassung“ anzuzeigen.

Tipp: Sie können auch auf **Tabellenansicht** und dann auf den CMM-Namen in der Spalte **Name** klicken, um die Seite „CMM-Zusammenfassung“ anzuzeigen.



Schritt 4. Klicken Sie auf **Aktionen → Stromversorgungsaktionen → Neu starten**.

Schritt 5. Klicken Sie auf **Sofort neu starten**.

Dieser Vorgang kann einige Minuten dauern. Möglicherweise müssen Sie die Seite aktualisieren, um die Ergebnisse zu sehen.

Ein CMM virtuell neu einsetzen

Sie können das Entfernen und Wiedereinsetzen eines Chassis Management Module (CMM) in einem Gehäuse simulieren.

Zu dieser Aufgabe

Beim virtuellen erneuten Einsetzen gehen alle bestehenden Netzwerkverbindungen zum CMM verloren und der Stromversorgungsstatus des CMM ändert sich.

Achtung: Stellen Sie vor einem virtuellen Neueinsetzen sicher, dass Sie alle Benutzerdaten auf dem CMM gespeichert haben.

Vorgehensweise

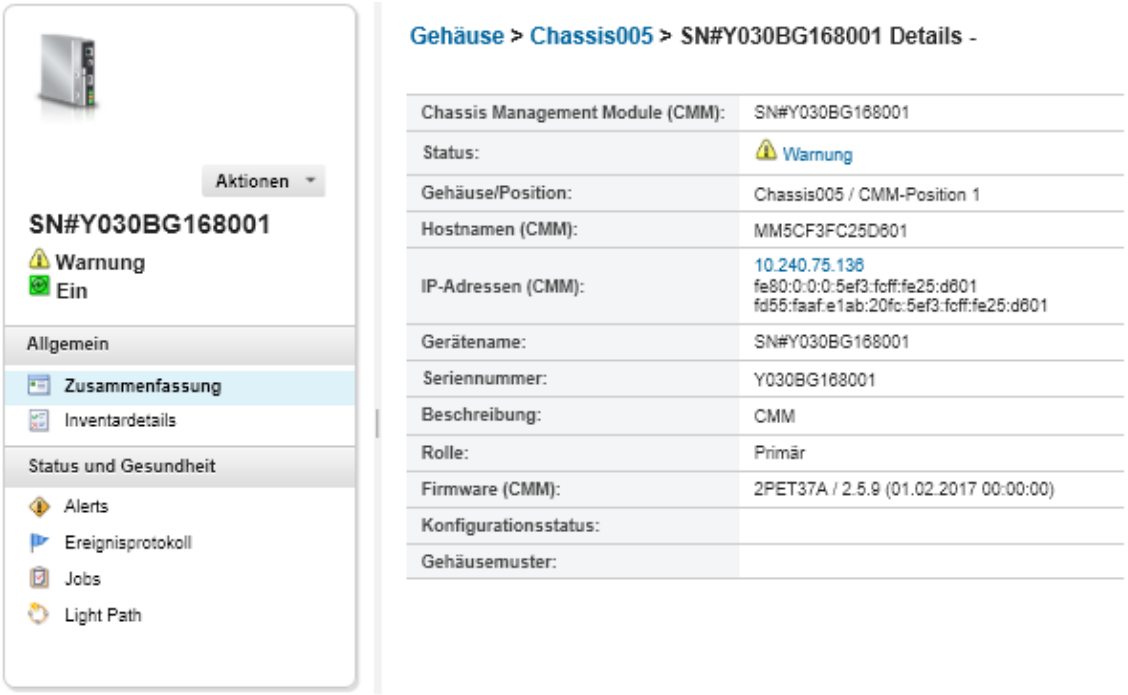
Führen Sie die folgenden Schritte aus, um ein CMM virtuell neu einzusetzen.

Schritt 1. Klicken Sie im Lenovo XClarity Administrator-Menü auf **Hardware → Gehäuse**. Die Seite Gehäuse wird mit einer Tabellenansicht aller verwalteten Gehäuse angezeigt.

Schritt 2. Klicken Sie in der Spalte **Gehäuse** auf den Gehäusenamen, um die grafische Gehäuseansicht anzuzeigen.

Schritt 3. Klicken Sie auf die CMM-Grafik, um die Seite „CMM-Zusammenfassung“ anzuzeigen.

Tipp: Sie können auch auf **Tabellenansicht** und dann auf den CMM-Namen in der Spalte **Name** klicken, um die Seite „CMM-Zusammenfassung“ anzuzeigen.



Schritt 4. Klicken Sie auf **Aktionen → Service → Virtuell erneut einsetzen**.

Schritt 5. Klicken Sie auf **Virtuell erneut einsetzen**.

Abgelaufene oder ungültige gespeicherte Anmeldeinformationen für ein Gehäuse auflösen

Wenn gespeicherte Anmeldeinformationen auf einer Einheit ablaufen oder nicht mehr funktionsfähig sind, wird der Status für diese Einheit mit „Offline“ angezeigt.

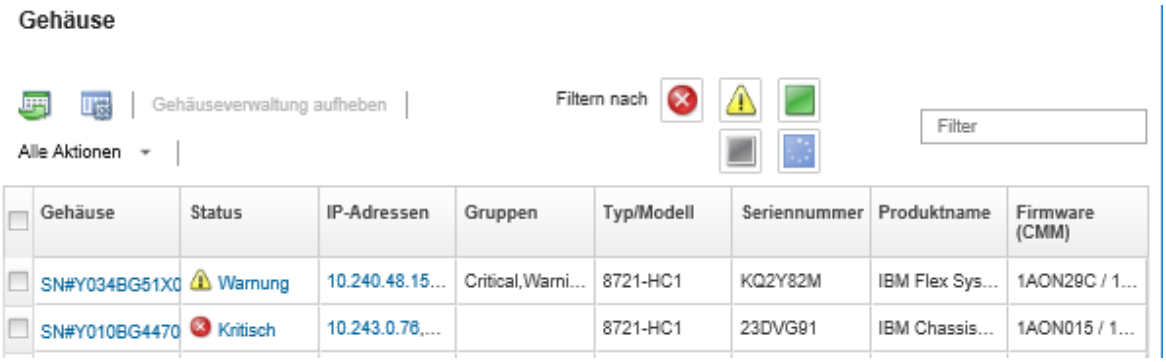
Vorgehensweise

Zum Auflösen abgelaufener oder ungültiger gespeicherter Anmeldeinformationen für ein Gehäuse.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Gehäuse**. Die Seite Gehäuse wird mit einer Tabellenansicht aller verwalteten Gehäuse angezeigt.

Schritt 2. Klicken Sie auf die Spaltenüberschrift der Tabelle **Power**, um alle Offline-Gehäuse oben in der Tabelle zu gruppieren.

Sie können die Tabellenspalten sortieren, um das Gehäuse, das Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie Text (z. B. einen Gehäusenamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Gehäuse weiter zu filtern.



Schritt 3. Wählen Sie das aufzulösende Gehäuse aus.

Schritt 4. Klicken Sie auf **Alle Aktionen → Sicherheit → Gespeicherte Anmeldeinformationen bearbeiten**.

Schritt 5. Ändern Sie das Kennwort für gespeicherte Anmeldeinformationen oder wählen Sie andere gespeicherte Anmeldeinformationen aus, um diese für die verwaltete Einheit zu verwenden.

Anmerkung: Wenn Sie mehr als eine Einheit mit denselben gespeicherten Anmeldeinformationen verwaltet haben und das Kennwort für die gespeicherten Anmeldeinformationen ändern, betrifft die Änderung des Kennworts alle Einheiten, die derzeit die gespeicherten Anmeldeinformationen verwenden.

Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen

Wenn ein Gehäuse von Lenovo XClarity Administrator verwaltet wird und XClarity Administrator ausfällt, können Sie die Verwaltungsfunktionen und die lokalen Benutzeraccounts für ein CMM wiederherstellen, bis der Verwaltungsknoten wiederhergestellt oder ersetzt wurde.

Vorgehensweise

Wählen Sie eine der folgenden Vorgehensweisen, um die Verwaltung auf einem CMM wiederherzustellen.

- Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, verwalten Sie das Gehäuse mit dem RECOVERY_ID-Account und -Kennwort und der Option **Verwaltung erzwingen** (siehe Gehäuse verwalten).
- Setzen Sie das CMM auf die werkseitigen Voreinstellungen zurück, indem Sie im Stiftloch den Grundstellungsknopf am CMM mit einer Büroklammer mindestens 10 Sekunden gedrückt halten. Weitere Informationen zum Zurücksetzen des CMM und wichtige Hinweise finden Sie unter CMM zurücksetzen in der Flex Systems-Onlinedokumentation.
- Führen Sie folgende Schritte aus, um die CMM-Konfiguration zurückzusetzen:
  1. Öffnen Sie über eine SSH-Sitzung eine Verwaltungsbefehlszeilenschnittstelle für das Gehäuse und melden Sie sich mit dem `RECOVERY_ID`-Account an.

     Anmerkung: Das Kennwort für das `RECOVERY_ID`-Account wurde festgelegt, als Sie das Gehäuse für die Verwaltung auf der Seite für die Verwaltungsdomäne ausgewählt haben. Weitere Informationen zur zentralen Kontenverwaltung finden Sie unter Gehäuse verwalten.

     Wenn Sie das `RECOVERY_ID`-Account zum ersten Mal zur Anmeldung bei CMM verwenden, müssen Sie das Kennwort ändern.
  2. Geben Sie das neue Kennwort für das `RECOVERY_ID`-Account ein, wenn Sie dazu aufgefordert werden.
  3. Stellen Sie die CMM-Konfiguration wieder her, indem Sie einen der folgenden Schritte ausführen:

– Wenn Sie das Release der CMM-Firmware von Juni 2015 oder später verwenden, führen Sie den folgenden Befehl aus:
  `read -f unmanage -T mm[p]`
  Weitere Informationen finden Sie unter Befehl „read“ in der CMM-Onlinedokumentation.
– Wenn Sie ein älteres Release der CMM-Firmware als Juni 2015 verwenden, führen Sie die folgenden Befehle in der angezeigten Reihenfolge aus:
  a. `env -T mm[p]`
  b. `sslcfg -client disabled -tc1 remove`
  c. `accseccfg -am local`
  d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
  e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
  f. `cimsub -clear all`
  g. `fsmcm -off`

     Der Befehl `fsmcm` deaktiviert die XClarity Administrator-Benutzeraccountverwaltung und ermöglicht die Verwendung lokaler CMM-Benutzeraccounts für die Authentifizierung bei CMM und bei allen im Gehäuse installierten Verwaltungsprozessoren.

     Nach der Ausführung des Befehls `fsmcm -off` wird das `RECOVERY_ID`-Account aus der CMM-Benutzerregistry entfernt. Wenn Sie den Befehl `fsmcm -off` ausführen, wird die CMM-CLI-Sitzung beendet. Sie können sich nun bei CMM und anderen Gehäusekomponenten authentifizieren, indem Sie lokale CMM-Anmeldeinformationen verwenden und lokale CMM-Anmeldeinformationen zum Zugriff auf die CMM-Webschnittstelle oder CLI für das Gehäuse nutzen, bis die Benutzerverwaltung von XClarity Administrator wiederhergestellt ist.

     Weitere Informationen finden Sie unter Befehl „fsmcm“ in der CMM-Onlinedokumentation.

Nachdem XClarity Administrator wiederhergestellt oder ausgetauscht wurde, können Sie das Gehäuse wieder verwalten (siehe Gehäuse verwalten). Alle Informationen zum Gehäuse (z. B. Netzwerkeinstellungen) werden beibehalten.

Verwaltung eines Gehäuses aufheben

Sie können die Verwaltung eines Gehäuses durch Lenovo XClarity Administrator beenden. Dieser Vorgang wird als *Aufheben der Verwaltung* bezeichnet. Nachdem die Verwaltung des Gehäuses aufgehoben wurde, können Sie sich am CMM für das Gehäuse anmelden, indem Sie die lokalen CMM-Benutzeraccounts verwenden.

Vorbereitende Schritte

Sie können XClarity Administrator so konfigurieren, dass die Verwaltung von Einheiten, die für einen bestimmten Zeitraum offline sind, automatisch aufgehoben wird. Dies ist standardmäßig deaktiviert. Um die automatische Aufhebung der Verwaltung von Offline-Einheiten zu aktivieren, klicken Sie im Menü von XClarity Administrator auf **Hardware → Neue Einheiten ermitteln und verwalten** und klicken Sie dann auf **Bearbeiten** neben **Aufheben der Verwaltung von Offline-Einheiten ist deaktiviert**. Wählen Sie anschließend **Aufheben der Verwaltung von Offline-Einheiten aktivieren** aus und legen Sie das Zeitintervall fest. Standardmäßig wird die Verwaltung von Einheiten aufgehoben, nachdem sie 24 Stunden offline waren.

Bevor Sie die Verwaltung für ein Gehäuse aufheben, müssen Sie sicherstellen, dass keine aktiven Jobs für die Einheiten existieren, die im Gehäuse installiert sind.

Wenn Call-Home-Funktion in XClarity Administrator aktiviert ist, wird Call-Home-Funktion auf allen verwalteten Gehäusen und Servern deaktiviert, damit keine doppelten Problemdatensätze generiert werden.

Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren - anstatt Call-Home-Funktion später auf jeder einzelnen Einheit zu aktivieren (siehe Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren in der Onlinedokumentation von XClarity Administrator).

Zu dieser Aufgabe

Wenn Sie die Verwaltung für ein Gehäuse aufheben, führt XClarity Administrator die folgenden Aktionen aus:

- Löscht die Konfiguration, die für die zentrale Benutzerverwaltung verwendet wird.
- Entfernt das CMM-Sicherheitszertifikat aus dem XClarity Administrator-Truststore.
- Setzt die Firewallregeln für die Einheit auf die vor der Verwaltung der Einheit festgelegten Einstellungen, wenn Encapsulation auf der Einheit aktiviert ist.
- Entfernt den Zugriff auf den NTP-Server über das CMM.
- Entfernt die CIM-Abonnements für das CMM aus der XClarity Administrator-Konfiguration, sodass XClarity Administrator keine Ereignisse mehr aus dem Gehäuse empfängt.

Wenn Sie die Verwaltung für ein Gehäuse aufgehoben haben, behält XClarity Administrator bestimmte Informationen über das Gehäuse. Diese Informationen werden erneut angewendet, wenn Sie dasselbe Gehäuse wieder verwalten.

Wenn Sie die Verwaltung für ein Gehäuse aufheben, werden von den Gehäusekomponenten gesendete Ereignisse gelöscht. Sie können diese Ereignisse behalten, indem Sie die Ereignisse an ein externes Repository wie syslog weiterleiten (siehe Ereignisse weiterleiten).

Tipp: Alle Demo-Einheiten, die während der Erstkonfiguration optional hinzugefügt werden, sind Knoten in einem Gehäuse. Um die Verwaltung der Demo-Einheiten aufzuheben, müssen Sie die Gehäuseverwaltung mit der Option **Aufheben der Verwaltung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aufheben.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verwaltung für ein Gehäuse aufzuheben.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Gehäuse**, um die Seite Gehäuse anzuzeigen.

Schritt 2. Wählen Sie ein oder mehrere Gehäuse aus der Liste der verwalteten Gehäuse aus.

Schritt 3. Klicken Sie auf **Gehäuseverwaltung aufheben**. Der Dialog „Verwaltung aufheben“ wird angezeigt.

Schritt 4. **Optional:** Wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn das Gerät nicht erreichbar ist**.

Wichtig: Wenn Sie die Verwaltung für Demo-Hardware aufheben, müssen Sie diese Option auswählen.

Schritt 5. Klicken Sie auf **Verwaltung aufheben**.Der Dialog „Verwaltung aufheben“ zeigt den Status jedes Schritts im Verwaltungsaufhebungsprozess an.

Schritt 6. Wenn der Verwaltungsaufhebungsprozess abgeschlossen ist, klicken Sie auf **OK**.

Nach dieser Aufgabe

Nachdem der Verwaltungsaufhebungsprozess abgeschlossen ist, können Sie sich am CMM mit den lokalen CMM-Benutzeraccounts anmelden. Wenn Sie die Benutzernamen oder Kennwörter für die lokalen CMM-Benutzeraccounts vergessen haben, setzen Sie das CMM auf die werkseitigen Voreinstellungen zurück, um sich am CMM anzumelden. Weitere Informationen zum Zurücksetzen des CMM auf die werkseitigen

Voreinstellungen finden Sie unter CMM zurücksetzen in der Flex Systems-Onlinedokumentation in der CMM-Produktdokumentation.

Gehäuse wiederherstellen, für das die Verwaltung nicht ordnungsgemäß aufgehoben wurde

Wenn für ein Gehäuse die Verwaltung nicht korrekt aufgehoben wurde, müssen Sie das Gehäuse wiederherstellen, bevor Sie es erneut verwalten können.

Vorgehensweise

Wählen Sie eine der folgenden Vorgehensweisen, um die Verwaltung auf einem CMM wiederherzustellen.

- Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, verwalten Sie das Gehäuse mit dem RECOVERY_ID-Account und -Kennwort und der Option **Verwaltung erzwingen** (siehe Gehäuse verwalten).
- Setzen Sie das CMM auf die werkseitigen Voreinstellungen zurück, indem Sie im Stiftloch den Grundstellungsknopf am CMM mit einer Büroklammer mindestens 10 Sekunden gedrückt halten. Weitere Informationen zum Zurücksetzen des CMM und wichtige Hinweise finden Sie unter CMM zurücksetzen in der Flex Systems-Onlinedokumentation.
- Führen Sie folgende Schritte aus, um die CMM-Konfiguration zurückzusetzen:
  1. Öffnen Sie über eine SSH-Sitzung eine Verwaltungsbefehlszeilenschnittstelle für das Gehäuse und melden Sie sich mit dem `RECOVERY_ID`-Account an.

     Anmerkung: Das Kennwort für das `RECOVERY_ID`-Account wurde festgelegt, als Sie das Gehäuse für die Verwaltung auf der Seite für die Verwaltungsdomäne ausgewählt haben. Weitere Informationen zur zentralen Kontenverwaltung finden Sie unter Gehäuse verwalten.

     Wenn Sie das `RECOVERY_ID`-Account zum ersten Mal zur Anmeldung bei CMM verwenden, müssen Sie das Kennwort ändern.
  2. Geben Sie das neue Kennwort für das `RECOVERY_ID`-Account ein, wenn Sie dazu aufgefordert werden.
  3. Stellen Sie die CMM-Konfiguration wieder her, indem Sie einen der folgenden Schritte ausführen:
     - Wenn Sie das Release der CMM-Firmware von Juni 2015 oder später verwenden, führen Sie den folgenden Befehl aus:
       `read -f unmanage -T mm[p]`
       Weitere Informationen finden Sie unter Befehl „read“ in der CMM-Onlinedokumentation.
     - Wenn Sie ein älteres Release der CMM-Firmware als Juni 2015 verwenden, führen Sie die folgenden Befehle in der angezeigten Reihenfolge aus:
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

          Der Befehl `fsmcm` deaktiviert die XClarity Administrator-Benutzeraccountverwaltung und ermöglicht die Verwendung lokaler CMM-Benutzeraccounts für die Authentifizierung bei CMM und bei allen im Gehäuse installierten Verwaltungsprozessoren.

          Nach der Ausführung des Befehls `fsmcm -off` wird das `RECOVERY_ID`-Account aus der CMM-Benutzerregistry entfernt. Wenn Sie den Befehl `fsmcm -off` ausführen, wird die CMM-CLI-

Sitzung beendet. Sie können sich nun bei CMM und anderen Gehäusekomponenten authentifizieren, indem Sie lokale CMM-Anmeldeinformationen verwenden und lokale CMM-Anmeldeinformationen zum Zugriff auf die CMM-Webschnittstelle oder CLI für das Gehäuse nutzen, bis die Benutzerverwaltung von XClarity Administrator wiederhergestellt ist.

Weitere Informationen finden Sie unter Befehl „fsmcm“ in der CMM-Onlinedokumentation.

Nachdem XClarity Administrator wiederhergestellt oder ausgetauscht wurde, können Sie das Gehäuse wieder verwalten (siehe Gehäuse verwalten). Alle Informationen zum Gehäuse (z. B. Netzwerkeinstellungen) werden beibehalten.

Kapitel 8. Server verwalten

Lenovo XClarity Administrator kann zahlreiche Systemtypen verwalten, darunter ThinkAgile-, ThinkSystem-, Converged-, Flex System-, NeXtScale-, System x®- und ThinkServer®-Server.

Weitere Informationen:  XClarity Administrator: Ermittlung

Vorbereitende Schritte

Anmerkung: Flex-Rechenknoten werden automatisch ermittelt und verwaltet, wenn das Gehäuse, in dem sie enthalten sind, verwaltet wird. Flex-Rechenknoten können nicht unabhängig vom Gehäuse ermittelt und verwaltet werden.

Vor der Verwaltung von Servern sollten Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind:

- Gehen Sie die Verwaltungsaspekte nochmal durch, bevor Sie eine Einheit verwalten. Weitere Informationen finden Sie unter Verwaltungshinweise in der Onlinedokumentation von XClarity Administrator.
- 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. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.
- Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jedem Server installiert ist, den Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.
- Stellen Sie sicher, dass CIM over HTTPS auf der Einheit aktiviert ist.
  1. Melden Sie sich bei der Verwaltungswebschnittstelle für den Server mit dem Benutzeraccount `RECOVERY_ID` an.
  2. Klicken Sie auf **IMM-Verwaltung → Sicherheit**.
  3. Klicken Sie auf die Registerkarte **CIM Over HTTPS** und stellen Sie sicher, dass **CIM Over HTTPS aktivieren** ausgewählt ist.
- Für 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 Administrator 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 mithilfe von TSM zu aktivieren, klicken Sie auf **Einstellungen → IPMI-Konfiguration**. Möglicherweise müssen Sie den Server neu starten, damit die Änderung übernommen wird.
- Wenn das Serverzertifikat der Einheit von einer externen Zertifizierungsstelle signiert ist, müssen Sie sicherstellen, dass das Zertifizierungsstellen und alle Zwischenzertifikate in den Angepasste Serverzertifikate in verwaltete Einheiten implementieren-Truststore importiert werden (siehe XClarity Administrator).
- Um einen Server zu ermitteln, der sich in einem *anderen* Subnetz als XClarity Administrator befindet, muss eine der folgenden Bedingungen erfüllt sein:

  - Stellen Sie sicher, dass Sie die Multicast-SLP-Weiterleitung für die Top-of-Rack-Switches sowie für die Router in Ihrer Umgebung aktivieren. Lesen Sie die mit dem jeweiligen Switch oder Router bereitgestellte Dokumentation, um herauszufinden, ob die Multicast-SLP-Weiterleitung aktiviert ist und falls nicht, wie Sie sie aktivieren können.
  - Wenn SLP auf dem Endpunkt 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, zum Beispiel für XClarity Administrator.
    ```
    _lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```

    Aktivieren Sie anschließend die DNS-Ermittlung bei der BMC über die Verwaltungswebschnittstelle, indem Sie auf **IMM-Verwaltung → Netzprotokoll** klicken, danach die Registerkarte **DNS** und zuletzt **DNS zum Ermitteln von Lenovo XClarity Administrator verwenden** auswählen.

    Anmerkungen:

    - Der Management-Controller muss mit einer Firmwareversion von Mai 2017 oder höher ausgeführt werden, um die automatische Ermittlung mit DNS zu unterstützen.
    - Wenn mehrere XClarity Administrator-Instanzen in Ihrer Umgebung vorhanden sind, wird der Server nur von der Instanz ermittelt, die als erste auf die Ermittlungsanforderung reagiert. Der Server wird nicht von allen Instanzen ermittelt.
- Stellen Sie für die Ermittlung und Verwaltung von ThinkServer-Servern sicher, dass die folgenden Anforderungen erfüllt sind. Weitere Informationen finden Sie unter Einheit kann nicht erkannt werden und Einheit kann nicht verwaltet werden in der Onlinedokumentation von XClarity Administrator.
  - Wenn Sie möchten, dass XClarity Administrator die Server automatisch ermittelt, muss der Hostname des Servers mit einem gültigen Hostnamen oder einer gültigen IP-Adresse konfiguriert sein.
  - Die Netzwerkkonfiguration muss den SLP-Datenverkehr zwischen XClarity Administrator und dem Server zulassen.
  - Unicast-SLP ist erforderlich.
  - Sollen die ThinkServer-Server automatisch von XClarity Administrator ermittelt werden, 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 Administrator, muss das Netzwerk so konfiguriert sein, dass eingehender UDP-Datenverkehr über Port 162 zulässig ist, damit XClarity Administrator Ereignisse zu diesen Einheiten erhalten kann.
- Für ThinkAgile, ThinkSystem, Converged, Flex System. Falls Sie bei NeXtScale- und System x-Servern einen Adapter im Server ersetzen oder konfigurieren oder aus dem Server entfernen, muss der Server mindestens einmal neu gestartet werden, um die Adapterinformationen im Baseboard Management Controller und in den XClarity Administrator-Berichten zu aktualisieren (Einen Server ein- und ausschalten).
- 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. (Sie können die BIOS/UEFI-Konfiguration über die Seite „Server“ in XClarity Administrator starten. Klicken Sie dazu auf **Alle Aktionen → Stromversorgungsaktionen → Über BIOS/UEFI-Konfiguration neu starten**.) 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 `<F1> Setup` angezeigt wird, drücken Sie `F1`, um „Setup Utility“ zu starten. Navigieren Sie zu **System Settings → Devices and I/O Ports → Enable/Disable Adapter Option ROM Support** und suchen Sie den Bereich **Enable/Disable UEFI Option ROM(s)**. Stellen Sie dort sicher, dass die Einstellungen aktiviert sind.

Anmerkung: Diese Einstellungen können Sie auch mithilfe der Remote-Konsole (sofern diese Funktion unterstützt wird) in der Baseboard Management Controller-Schnittstelle remote prüfen und ändern.

- System x3950 X6-Server müssen als zwei 4U-Gehäuse mit jeweils einem eigenen Baseboard Management Controller verwaltet werden.

Zu dieser Aufgabe

XClarity Administrator kann Rack- und Tower-Server in der Umgebung automatisch ermitteln. Dabei wird nach verwaltbaren Einheiten gesucht, die im gleichen IP-Subnetz sind wie XClarity Administrator. Um Rack- und Tower-Server zu ermitteln, die sich in anderen Subnetzen befinden, geben Sie eine IP-Adresse oder einen IP-Adressbereich an oder importieren Sie Informationen von einem Arbeitsblatt.

Wichtig: Bei System x3850- und x3950 X6-Servern müssen Sie jeden Server in der skalierbaren Rack-Umgebung verwalten.

Nachdem die Server von XClarity Administrator verwaltet werden, fragt Lenovo XClarity Administrator jeden verwalteten Server regelmäßig ab, um Informationen zu sammeln, z. B. Bestand, elementare Produktdaten und Status. Sie können jeden verwalteten Server anzeigen und überwachen sowie Verwaltungsaktionen ausführen (z. B. Systemeinstellungen konfigurieren, Betriebssystem-Images bereitstellen, ein- und ausschalten).

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

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

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

  Anmerkungen:

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

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

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

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

- Wenn Sie den lokalen oder externen LDAP-Server als XClarity Administrator-Authentifizierungsserver nutzen, werden auf diesem Authentifizierungsserver definierte Benutzeraccounts für die Anmeldung bei XClarity Administrator, CMMs und BMCs (Baseboard Management Controllern) in der XClarity Administrator-Domäne verwendet. Lokale CMM- und Management-Controller-Benutzeraccounts werden deaktiviert.
- Bei Verwendung eines SAML 2.0 Identity Provider als XClarity Administrator-Authentifizierungsserver sind SAML-Accounts für verwaltete Einheiten nicht zugänglich. Wenn Sie jedoch einen SAML Identitiy Provider und einen LDAP-Server zusammen verwenden und der Identity Provider Konten nutzt, die sich auf dem LDAP-Server befinden, können LDAP-Benutzeraccounts zur Anmeldung bei den verwalteten Einheiten und gleichzeitig modernere von SAML 2.0 bereitgestellte Authentifizierungsmethoden (z. B. mehrstufige Authentifizierung und Single Sign-on) zur Anmeldung bei XClarity Administrator verwendet werden.
- Mit Single Sign-On kann sich ein Benutzer, der bereits bei XClarity Administrator angemeldet ist, automatisch beim Baseboard Management Controller anmelden. Single Sign-On ist standardmäßig aktiviert, wenn ein ThinkSystem oder ThinkAgile Server von XClarity Administrator verwaltet wird (es sei denn, der Server wird mit CyberArk-Kennwörtern verwaltet). Sie können global konfigurieren, dass Single Sign-On für alle verwalteten ThinkSystem und ThinkAgile Server aktiviert oder deaktiviert ist. Das Aktivieren von Single Sign-On für einen bestimmten ThinkSystem und ThinkAgile Server überschreibt die globale Einstellung für alle ThinkSystem und ThinkAgile Server (siehe).

  Anmerkung: Single Sign-On ist automatisch deaktiviert, wenn das CyberArk Identitätsverwaltungssystem zur Authentifizierung verwendet wird.
- Wenn die verwaltete Authentifizierung für ThinkSystem SR635 und SR655 Server aktiviert ist:
  - Die Baseboard Management Controller-Firmware unterstützt bis zu fünf LDAP-Benutzerrollen. XClarity Administrator fügt diese LDAP-Benutzerrollen während der Verwaltung zu den Servern hinzu: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** und **lxc-os-admin**.

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

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

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

  - Jedes Mal, wenn Sie ein Gerät mit manuell eingegebenen Anmeldeinformationen verwalten, werden auch dann neue gespeicherte Anmeldeinformationen für dieses Gerät erstellt, wenn bei einem vorherigen Verwaltungsprozess andere gespeicherte Anmeldeinformationen für dieses Gerät erstellt wurden.

– Wenn Sie die Verwaltung eines Geräts aufheben, löscht XClarity Administrator keine gespeicherten Anmeldeinformationen, die während des Verwaltungsprozesses automatisch für dieses Gerät erstellt wurden.

Eine Einheit kann nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie es mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die erste XClarity Administrator-Verwaltung der Speichereinheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten. Falls bei der Verwaltungsaufhebung ein Fehler auftritt, können Sie bei der Verwaltung die Option **Verwaltung erzwingen** auf dem neuen XClarity Administrator auswählen.

Anmerkung: Wenn Sie das Netzwerk nach verwaltbaren Einheiten durchsuchen, weiß XClarity Administrator nicht, ob eine Einheit bereits von einem anderen Manager verwaltet wird, bis er versucht, die Einheit zu verwalten.

Anmerkung: Wenn das Netzwerk nach verwaltbaren Einheiten durchsucht wird, weiß XClarity Administrator nicht, ob eine ThinkServer-Einheit bereits verwaltet wird. Daher können verwaltete ThinkServer-Einheiten in der Liste der verwaltbaren Einheiten aufgeführt werden.

Während des Verwaltungsprozesses führt XClarity Administrator die folgenden Aktionen aus:

- Meldet sich am Server mit den bereitgestellten Anmeldeinformationen an.
- Erfasst den Bestand für die einzelnen Server.

  Anmerkung: Einige Bestandsdaten werden erfasst, nachdem der Verwaltungsprozess abgeschlossen ist. Sie können bestimmte Aufgaben auf einem verwalteten Server nicht ausführen (z. B. die Implementierung eines Servermusters), bis alle Bestandsdaten für diesen Server erfasst sind und der Server sich nicht mehr im Wartestatus befindet.
- Konfiguriert die Einstellungen für den NTP-Server, sodass alle verwalteten Einheiten dieselbe NTP-Serverkonfiguration verwenden, die auf XClarity Administrator konfiguriert ist.
- (Nur System x- und NeXtScale-Server) Weist die zuletzt bearbeitete Firmwarekonformitätsrichtlinie dem Server zu.
- (Nur Lenovo System x- und NeXtScale-Server) Konfiguriert optional die Firewallregeln der Einheiten, damit eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.
- (Nur System x- und NeXtScale-Server) Tauscht Sicherheitszertifikate mit dem Management-Controller aus, kopiert das CIM-Serverzertifikat und das LDAP-Clientzertifikat vom Management-Controller in den XClarity Administrator-Truststore und übermittelt das CA-Sicherheitszertifikat von XClarity Administrator sowie die vertrauenswürdigen LDAP-Zertifikate an den Management-Controller. Der Management-Controller lädt die Zertifikate in den eigenen Truststore, sodass er den Verbindungen zu den LDAP- und CIM-Servern von XClarity Administrator vertrauen kann.

  Anmerkung: Falls kein CIM-Serverzertifikat oder LDAP-Clientzertifikat vorhanden sein sollte, wird dieses im Verwaltungsprozess erstellt.
- Konfiguriert bei Bedarf die verwaltete Authentifizierung. Weitere Informationen zur verwalteten Authentifizierung finden Sie unter Authentifizierungsserver verwalten.
- Erstellt bei Bedarf den Benutzeraccount für die Wiederherstellung (`RECOVERY_ID`). Weitere Informationen zum Account `RECOVERY_ID` finden Sie unter Authentifizierungsserver verwalten.

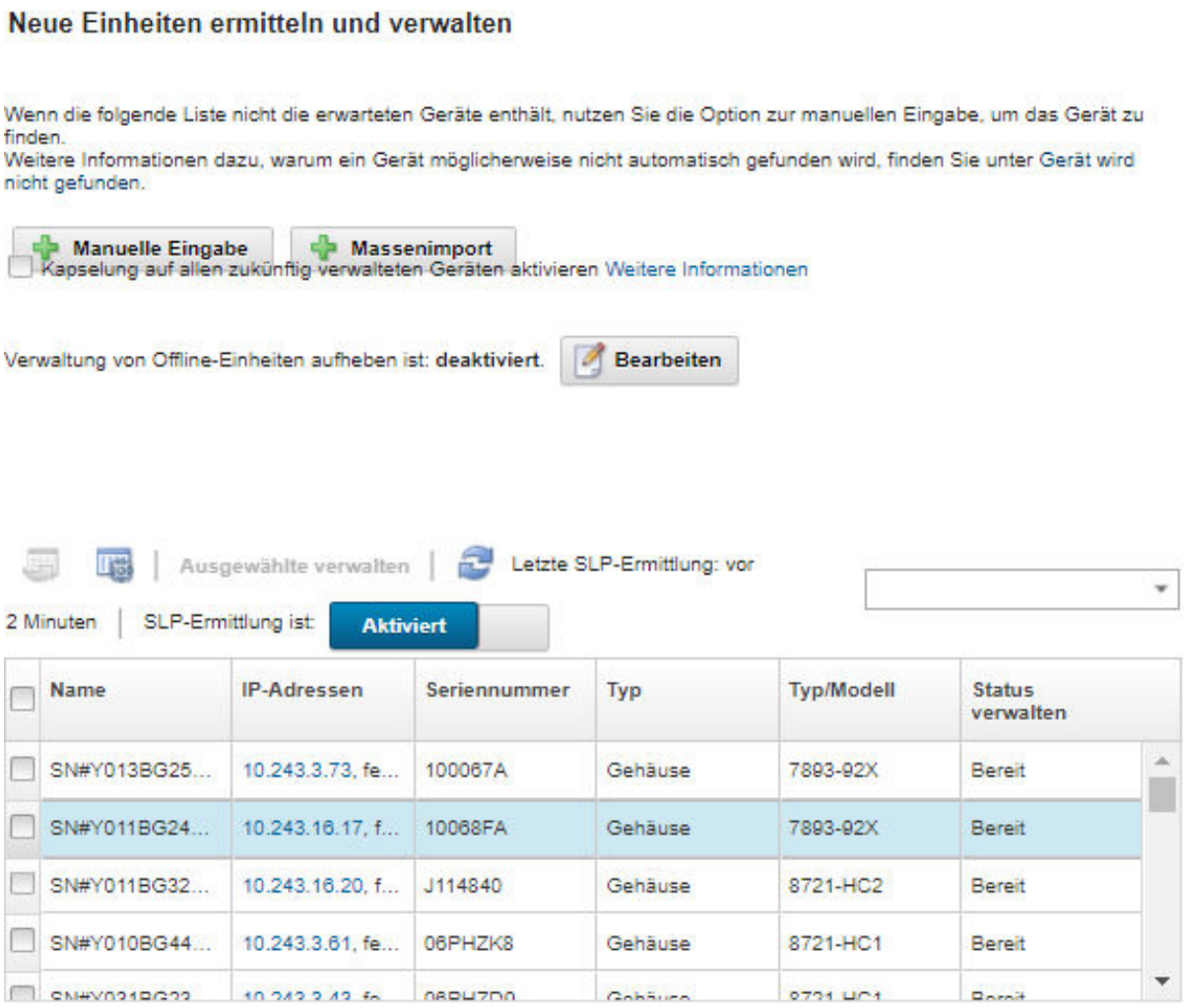
Anmerkung: XClarity Administrator ändert die Sicherheitseinstellungen oder die Verschlüsselungseinstellungen (Verschlüsselungsmodus und den für sichere Kommunikation verwendeten Modus) im Verwaltungsprozess nicht. Sie können die Verschlüsselungseinstellungen ändern, nachdem der Server verwaltet wird (siehe Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren).

Wichtig: Wenn Sie die IP-Adresse eines Server ändern, nachdem dieser von XClarity Administrator verwaltet wird, erkennt XClarity Administrator die neue IP-Adresse und verwaltet den Server weiterhin. Allerdings wird die IP-Adressänderung für einige Server von XClarity Administrator nicht erkannt. Falls XClarity Administrator anzeigt, dass der Server nach der IP-Adressänderung offline ist, können Sie den Server mit der Option **Verwaltung erzwingen** wieder verwalten.

Vorgehensweise

Wählen Sie eine der folgenden Vorgehensweisen, um die Rack- und Tower-Server mit XClarity Administrator zu verwalten.

- Ermitteln und verwalten Sie eine Vielzahl von Tower- und Rack-Servern und anderen Einheiten mithilfe einer Massenimportdatei (siehe Systeme verwalten in der Onlinedokumentation von XClarity Administrator).
- Ermitteln und verwalten Sie Rack- und Tower-Server, die im gleichen IP-Subnetz sind wie XClarity Administrator.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Neue Einheiten ermitteln und verwalten wird angezeigt.



Sie können die Tabellenspalten sortieren, um die zu verwaltenden Server schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die

angezeigten Server weiter zu filtern. Sie können die angezeigten Spalten und die Standard-Sortierreihenfolge ändern, indem Sie auf das Symbol **Spalten anpassen** () klicken.

2. Klicken Sie auf das Symbol **Aktualisieren** (), um alle verwaltbaren Einheiten in der XClarity Administrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
3. Aktivieren Sie das Kontrollkästchen **Kapselung für alle zukünftig verwalteten Einheiten aktivieren**, um die Firewallregeln während des Verwaltungsprozesses auf allen Einheiten dahingehend zu ändern, dass eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.

   Die Kapselung kann auf bestimmten Einheiten nach der Verwaltung aktiviert oder deaktiviert werden.

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

   Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.
4. Wählen Sie einen oder mehrere zu verwaltende Server aus.
5. Klicken Sie auf **Ausgewählte verwalten**. Das Dialogfenster „Verwalten“ wird angezeigt.
6. Wählen Sie aus, ob Sie die XClarity Administrator verwaltete Authentifizierung oder die lokale Authentifizierung für diese Einheit verwenden möchten. Die verwaltete Authentifizierung ist standardmäßig ausgewählt. Um die lokale Authentifizierung zu verwenden, deaktivieren sie **Verwaltete Authentifizierung**.
7. Wählen Sie die Art von Anmeldeinformationen aus, die zum Authentifizieren der Einheit zu verwenden ist, und geben Sie die entsprechenden Anmeldeinformationen an:
   - **Manuell eingegebene Anmeldeinformationen verwenden**
     - Geben Sie Benutzer-ID und Kennwort für die Authentifizierung am Server an.
     - (Optional) Legen Sie ein neues Kennwort für den angegebenen Benutzernamen fest, falls das Kennwort auf der Einheit derzeit abgelaufen ist.

     Anmerkung: Um manuell eingegebene Anmeldeinformationen zu verwenden, müssen Sie die verwaltete XClarity Administrator-Authentifizierung auswählen.
   - **Gespeicherte Anmeldeinformationen verwenden**

     Wählen Sie die gespeicherten Anmeldeinformationen aus, um diese für die verwaltete Einheit zu verwenden. Sie können neue gespeicherte Anmeldeinformationen durch Klicken auf **Neue erstellen** erzeugen.
   - **Identitätsverwaltungssystem verwenden**

     Wählen Sie das Identitätsverwaltungssystem aus, das für diese verwaltete Einheit verwendet werden soll. Geben Sie dann die verbleibenden Felder ein, einschließlich IP-Adresse oder Hostname des verwalteten Servers, Benutzername und optional Anwendungs-ID, Safe und Ordner.

     Wenn Sie die Anwendungs-ID angeben, müssen Sie ggf. auch den Safe und den Ordner angeben.

     Wenn Sie die Anwendungs-ID nicht angeben, verwendet XClarity Administrator die Pfade, die bei der Einrichtung von CyberArk definiert wurden, um die integrierten Accounts in CyberArk zu identifizieren.

Anmerkung: Es werden nur ThinkSystem oder ThinkAgile Server unterstützt. Das Identitätsverwaltungssystem muss in XClarity Administrator konfiguriert sein und der Lenovo XClarity Controller für die verwalteten ThinkSystem oder ThinkAgile Server muss in CyberArk integriert sein.

Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl. Oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).

Weitere Informationen zu normalen und gespeicherten Anmeldeinformationen finden Sie in Benutzeraccounts verwalten und Gespeicherte Anmeldeinformationen verwalten.

8. Geben Sie das Kennwort für die Wiederherstellung an, falls die verwaltete Authentifizierung ausgewählt ist.

   Bei Angabe eines Kennworts wird der Account zur Wiederherstellung (`RECOVERY_ID`) auf dem Server erstellt und alle lokalen Benutzeraccounts werden deaktiviert. Wenn ein Problem mit XClarity Administrator auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich auch *nicht* mehr am Management-Controller mit den normalen Benutzeraccounts anmelden. Jedoch können Sie sich über das Account zur Wiederherstellung anmelden.

   Anmerkungen:

   - Das Kennwort für die Wiederherstellung ist optional, falls Sie sich für die Verwendung einer verwalteten Authentifizierung entscheiden und ist nicht zulässig, wenn Sie die lokale Authentifizierung wählen.
   - Sie können auswählen, ob Sie für die Wiederherstellung ein lokales Account oder gespeicherte Anmeldeinformationen verwenden möchten. In beiden Fällen lautet der Benutzername immer `RECOVERY_ID`.
   - Stellen Sie sicher, dass das Kennwort den Sicherheits- und Kennwortrichtlinien der Einheit entspricht. Sicherheits- und Kennwortrichtlinien können variieren.
   - Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.
   - Der Wiederherstellungsaccount wird für ThinkServer- und System x M4-Server nicht unterstützt.

   Weitere Informationen zur Recovery-ID finden Sie unter Authentifizierungsserver verwalten.

9. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

   Anmerkungen:

   - Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
   - Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.

10. Klicken Sie auf **Verwalten**.

    Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

11. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

    Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

- Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

  Anmerkung: Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.
- Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

- Ermitteln und verwalten Sie Rack- und Tower-Server, die nicht im gleichen IP-Subnetz sind wie XClarity Administrator, indem Sie die IP-Adressen manuell angeben.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.
  2. Aktivieren Sie das Kontrollkästchen **Kapselung für alle zukünftig verwalteten Einheiten aktivieren**, um die Firewallregeln während des Verwaltungsprozesses auf allen Einheiten dahingehend zu ändern, dass eingehende Anforderungen nur von XClarity Administrator akzeptiert werden.

     Die Kapselung kann auf bestimmten Einheiten nach der Verwaltung aktiviert oder deaktiviert werden.

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

     Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.
  3. Wählen Sie **Manuelle Eingabe**.
  4. Geben Sie die Netzwerkadressen der Server an, die verwaltet werden sollen:
     - Klicken Sie auf **Einzelsystem** und geben Sie einen einzelnen IP-Adress-Domänennamen oder einen vollständig qualifizierten Domänennamen (FQDN) ein.

       Anmerkung: Stellen Sie bei der Angabe eines FQDN sicher, dass ein gültiger Domänenname auf der Seite Netzwerkzugriff angegeben wird (siehe Netzwerkzugriff konfigurieren).
     - Klicken Sie auf **Mehrere Systeme** und geben Sie einen Bereich von IP-Adressen ein. Um einen weiteren Bereich hinzuzufügen, klicken Sie auf das Symbol **Hinzufügen** (). Um einen Bereich zu entfernen, klicken Sie auf das Symbol **Entfernen** ().
  5. Klicken Sie auf **OK**. Das Dialogfenster „Verwalten“ wird angezeigt.
  6. Wählen Sie aus, ob Sie die XClarity Administrator verwaltete Authentifizierung oder die lokale Authentifizierung für diese Einheit verwenden möchten. Die verwaltete Authentifizierung ist

standardmäßig ausgewählt. Um die lokale Authentifizierung zu verwenden, deaktivieren sie **Verwaltete Authentifizierung**.

7. Wählen Sie die Art von Anmeldeinformationen aus, die zum Authentifizieren der Einheit zu verwenden ist, und geben Sie die entsprechenden Anmeldeinformationen an:

   - **Manuell eingegebene Anmeldeinformationen verwenden**

     - Geben Sie Benutzer-ID und Kennwort für die Authentifizierung am Server an.
     - (Optional) Legen Sie ein neues Kennwort für den angegebenen Benutzernamen fest, falls das Kennwort auf der Einheit derzeit abgelaufen ist.

     Anmerkung: Um manuell eingegebene Anmeldeinformationen zu verwenden, müssen Sie die verwaltete XClarity Administrator-Authentifizierung auswählen.

   - **Gespeicherte Anmeldeinformationen verwenden**

     Wählen Sie die gespeicherten Anmeldeinformationen aus, um diese für die verwaltete Einheit zu verwenden. Sie können neue gespeicherte Anmeldeinformationen durch Klicken auf **Neue erstellen** erzeugen.

   - **Identitätsverwaltungssystem verwenden**

     Wählen Sie das Identitätsverwaltungssystem aus, das für diese verwaltete Einheit verwendet werden soll. Geben Sie dann die verbleibenden Felder ein, einschließlich IP-Adresse oder Hostname des verwalteten Servers, Benutzername und optional Anwendungs-ID, Safe und Ordner.

     Wenn Sie die Anwendungs-ID angeben, müssen Sie ggf. auch den Safe und den Ordner angeben.

     Wenn Sie die Anwendungs-ID nicht angeben, verwendet XClarity Administrator die Pfade, die bei der Einrichtung von CyberArk definiert wurden, um die integrierten Accounts in CyberArk zu identifizieren.

     Anmerkung: Es werden nur ThinkSystem oder ThinkAgile Server unterstützt. Das Identitätsverwaltungssystem muss in XClarity Administrator konfiguriert sein und der Lenovo XClarity Controller für die verwalteten ThinkSystem oder ThinkAgile Server muss in CyberArk integriert sein.

   Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl. Oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).

   Weitere Informationen zu normalen und gespeicherten Anmeldeinformationen finden Sie in Benutzeraccounts verwalten und Gespeicherte Anmeldeinformationen verwalten.

8. Geben Sie das Kennwort für die Wiederherstellung an, falls die verwaltete Authentifizierung ausgewählt ist.

   Bei Angabe eines Kennworts wird der Account zur Wiederherstellung (`RECOVERY_ID`) auf dem Server erstellt und alle lokalen Benutzeraccounts werden deaktiviert. Wenn ein Problem mit XClarity Administrator auftritt und er aus irgendeinem Grund nicht mehr funktioniert, können Sie sich auch *nicht* mehr am Management-Controller mit den normalen Benutzeraccounts anmelden. Jedoch können Sie sich über das Account zur Wiederherstellung anmelden.

   Anmerkungen:

   - Das Kennwort für die Wiederherstellung ist optional, falls Sie sich für die Verwendung einer verwalteten Authentifizierung entscheiden und ist nicht zulässig, wenn Sie die lokale Authentifizierung wählen.

- Sie können auswählen, ob Sie für die Wiederherstellung ein lokales Account oder gespeicherte Anmeldeinformationen verwenden möchten. In beiden Fällen lautet der Benutzername immer `RECOVERY_ID`.
- Stellen Sie sicher, dass das Kennwort den Sicherheits- und Kennwortrichtlinien der Einheit entspricht. Sicherheits- und Kennwortrichtlinien können variieren.
- Notieren Sie sich das Kennwort für die Wiederherstellung für die spätere Verwendung.
- Der Wiederherstellungsaccount wird für ThinkServer- und System x M4-Server nicht unterstützt.

Weitere Informationen zur Recovery-ID finden Sie unter Authentifizierungsserver verwalten.

9. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

   Anmerkungen:

   - Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
   - Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.

10. Klicken Sie auf **Verwalten**.

    Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

11. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

    Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

    - Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

      Anmerkung: Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.
    - Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
    - Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

    Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

Nach dieser Aufgabe

- Ermitteln und verwalten Sie weitere Einheiten.
- Konfigurieren Sie Systeminformationen, lokalen Speicher, E/A-Adapter, Boot-Themen und Firmwareeinstellungen, indem Sie Servermuster erstellen und implementieren (siehe Server mithilfe von Konfigurationsmustern konfigurieren).

- Implementieren Sie Betriebssystem-Images auf Servern, auf denen noch kein Betriebssystem installiert ist (siehe Betriebssysteme auf Bare-Metal-Servern installieren).
- Aktualisieren Sie die Firmware auf Einheiten, die nicht den aktuellen Richtlinien entsprechen (siehe Firmware auf verwalteten Einheiten aktualisieren).
- Fügen Sie die Einheiten zum entsprechenden Rack hinzu, um die physische Umgebung widerzuspiegeln (siehe Racks verwalten).
- Überwachen Sie den Hardwarestatus und die Details (siehe Den Status eines verwalteten Servers anzeigen).
- Überwachen Sie Ereignisse und Alerts (siehe Ereignisse handhaben und Mit Alerts arbeiten).
- Löschen Sie das SEL-Protokoll eines Servers, indem Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server** klicken, den Server auswählen und dann auf **Alle Aktionen → Sicherheit → SEL-Protokoll löschen** klicken.Diese Aktion wird nur für ThinkSystem und ThinkAgile Server unterstützt.
- Lösen Sie gespeicherte Anmeldeinformationen auf, die abgelaufen oder ungültig sind (siehe Gespeicherte Anmeldeinformationen verwalten).
- Aktivieren oder deaktivieren Sie Single Sign-On für alle verwalteten ThinkSystem und ThinkAgile Server. Klicken Sie dazu in der Menüleiste von XClarity Administrator auf **Verwaltung → Sicherheit**, wählen Sie dann **Aktive Sitzungen** aus und aktivieren oder deaktivieren Sie **Single Sign-On**.
- Aktivieren oder deaktivieren Sie Single Sign-On für verwaltete ThinkSystem und ThinkAgile Server.
  - Klicken Sie für alle verwalteten ThinkSystem und ThinkAgile Server (global) in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**, wählen Sie dann **Aktive Sitzungen** aus und aktivieren oder deaktivieren Sie **Single Sign-On**.
  - Klicken Sie für einen bestimmten ThinkSystem und ThinkAgile Server in der XClarity Administrator-Menüleiste auf **Hardware → Server** und wählen Sie dann **Alle Aktionen → Sicherheit → Single Sign-On aktivieren** oder **Alle Aktionen → Sicherheit → Single Sign-On deaktivieren** aus.

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

Den Status eines verwalteten Servers anzeigen

Sie können eine Zusammenfassung und den detaillierten Status für verwaltete Server und die zugehörigen installierten Komponenten über Lenovo XClarity Administrator anzeigen.

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

Zu dieser Aufgabe

Die folgenden Statussymbole geben den allgemeinen Status der Einheit an. Wenn die Zertifikate nicht übereinstimmen, wird „(nicht vertrauenswürdig)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (nicht vertrauenswürdig)“. Wenn ein Verbindungsproblem besteht oder eine Verbindung zur Einheit nicht vertrauenswürdig ist, wird „(Verbindung)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (Verbindung)“.

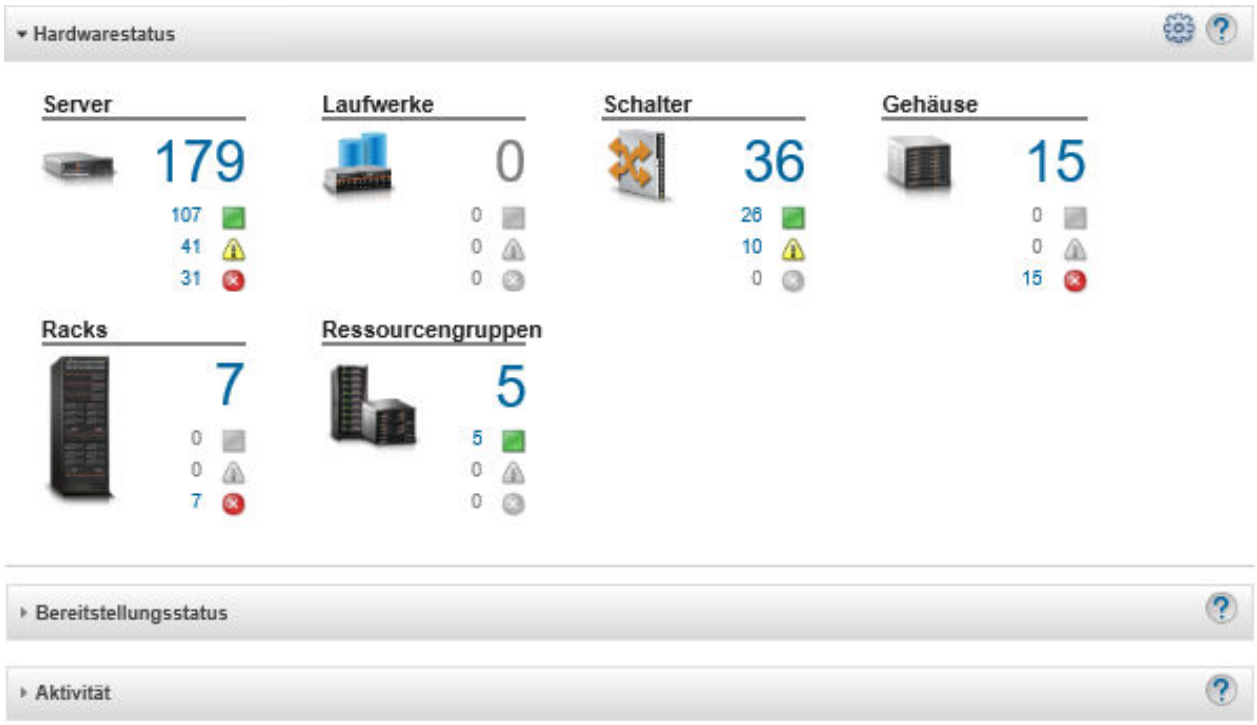
- ( ) Kritisch
- ( ) Warnung
- ( ) Ausstehend
- ( ) Information
- ( ) Normal
- ( ) Offline
- ( ) Nicht bekannt

Eine Einheit kann einen der folgenden Stromversorgungsstatus aufweisen:
- Ein
- Aus
- Wird heruntergefahren
- Standby
- Hibernation
- Unbekannt

Vorgehensweise

Führen Sie eine oder mehrere der folgenden Aktionen aus, um den Status für einen verwalteten Server anzuzeigen.

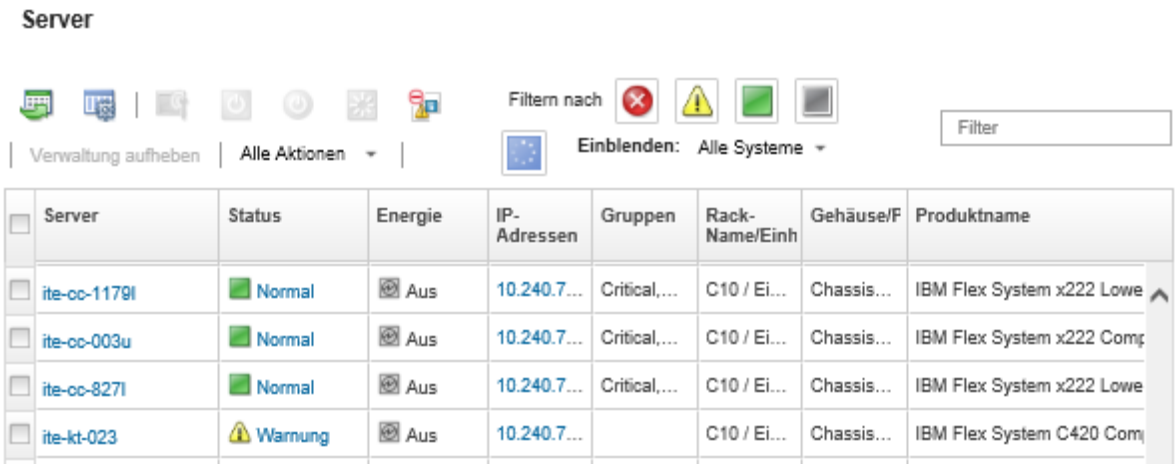
- Klicken Sie in der Menüleiste von XClarity Administrator auf **Dashboard**. Die Dashboard-Seite wird mit einer Übersicht und dem Status aller verwalteten Einheiten und anderen Ressourcen angezeigt.



- Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite Server wird mit einer Tabellenansicht aller verwalteten Server (Rack- und Tower-Server sowie Rechenknoten) geöffnet.

  Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdown-Liste **Alle Systeme** einen Systemtyp auswählen und im Feld

Filter einen Text eingeben (beispielsweise den Namen oder die IP-Adresse) und anschließend auf die Statussymbole klicken, um nur die Server aufzulisten, die den ausgewählten Kriterien entsprechen.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Sie können ausführliche Informationen zum Server und den zugehörigen Komponenten anzeigen (siehe Die Details eines verwalteten Servers anzeigen).
- Zeigen Sie einen Server in einer grafischen Rack- oder Gehäuseansicht an. Klicken Sie dazu auf **Alle Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Alle Aktionen → Anzeigen → In der Gehäuseansicht anzeigen**.
- Starten Sie die Management-Controller-Webschnittstelle für den Server. Klicken Sie dazu auf die Verknüpfung **IP-Adresse** (siehe Management-Controller-Webschnittstelle für einen Server starten).
- Verwalten Sie den Server remote (siehe Verwenden der Fernsteuerung zur Verwaltung von Converged-, Flex System-, NeXtScale- und System x-Servern).
- Schalten Sie den Server ein oder aus (siehe Einen Server ein- und ausschalten).
- Ändern Sie die Systeminformationen. Markieren Sie dazu einen Server und klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**.
- Aktualisieren Sie den Bestand. Markieren Sie dazu einen Server und klicken Sie auf **Alle Aktionen → Bestand → Bestand aktualisieren**.
- Exportieren Sie ausführliche Informationen über einen oder mehrere Server in eine CSV-Datei. Markieren Sie dazu die Server und klicken Sie auf **Alle Aktionen → Bestand → Bestand exportieren**.

  Anmerkung: Sie können Bestandsdaten für maximal 60 Einheiten gleichzeitig exportieren.

  Tipp: Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Heben Sie die Verwaltung eines Servers auf (siehe Verwaltung eines Rack- oder Tower-Servers aufheben).
- Setzen Sie die lokalen Speicheradapter auf ihre werkseitigen Standardeinstellungen zurück. Klicken Sie dazu auf **Alle Aktionen → Service → Lokalen Speicher auf Standardwerte zurücksetzen**.
- Ändern Sie den LED-Standortstatus eines Servers in ein, aus oder blinkend. Markieren Sie dazu einen Server und klicken Sie auf **Alle Aktionen → Service → LED-Standortstatus ein-/ausschalten**. Wählen Sie den Status aus und klicken Sie auf **Übernehmen**.
  - Das Umschalten der Positionsanzeige für ThinkSystem SR635 und SR655 Server wird nicht unterstützt.

  - Die Positionsanzeige auf ThinkServer-Servern kann ein- oder ausgeschaltet sein. Das Blinken wird nicht unterstützt.
- Setzen Sie den Server virtuell neu ein (siehe Server in einem Flex System-Gehäuse virtuell neu einsetzen).
- Schließen Sie belanglose Ereignisse auf allen Seiten aus, auf denen Ereignisse angezeigt werden.

  Klicken Sie dazu auf das Symbol **Ereignisse ausschließen** () (siehe Ereignisse ausschließen).
- Starten Sie den Server mit einem NMI (Non-Maskable Interrupt) neu, indem Sie auf **Alle Aktionen → Service → NMI auslösen** klicken.
- Aktivieren oder deaktivieren Sie Änderungen der Firewallregeln auf einem Server, mit denen eingehende Anforderungen auf XClarity Administrator begrenzt werden. Markieren Sie dazu den Server und klicken Sie auf **Alle Aktionen → Sicherheit → Encapsulation aktivieren** oder **Alle Aktionen → Sicherheit → Encapsulation deaktivieren**.Die globale Kapselungseinstellung 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 die globale Kapselungseinstellung aktiviert ist und die Einheit Kapselung unterstützt, kommuniziert XClarity Administrator 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 von XClarity Administrator akzeptiert werden.

  Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.
- (Nur Converged-, Flex System-, NeXtScale-, System x- und ThinkSystem-Server) Beheben Sie mögliche Probleme zwischen dem XClarity Administrator-Sicherheitszertifikat und dem Sicherheitszertifikat vom Baseboard Management Controller im Server. Markieren Sie dazu einen Server und klicken Sie auf **Alle Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen** (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).
- Lösen Sie abgelaufene oder ungültige gespeicherte Anmeldeinformationen für eine Einheit in der Gruppe auf (siehe Abgelaufene oder ungültige gespeicherte Anmeldeinformationen für einen Server auflösen).
- Sie können einen Server zu einer statischen Ressourcengruppe hinzufügen oder daraus entfernen. Klicken Sie dazu auf **Alle Aktionen → Gruppen → Zu Gruppe hinzufügen** oder **Alle Aktionen → Gruppen → Aus Gruppe entfernen**.

Die Details eines verwalteten Servers anzeigen

Sie können über Lenovo XClarity Administrator ausführliche Informationen über verwaltete Server anzeigen, z. B. Firmwareversionen, Servername und UUID (Universally Unique Identifier).

Weitere Informationen:

-  XClarity Administrator: Bestand
-  XClarity Administrator: Überwachung

Zu dieser Aufgabe

Die CPU-Auslastung ist ein Messwert für den aggregierten C-State. Dies wird als Prozentsatz des verwendeten und maximalen C0-State-Werts pro Sekunde gemessen.

Die Speicherauslastung ist der Messwert für die aggregierten Lese-/Schreibvolumes aller Speicherkanäle. Dies wird als Prozentsatz der verwendeten und maximal verfügbaren Speicherbandbreite pro Sekunde berechnet.

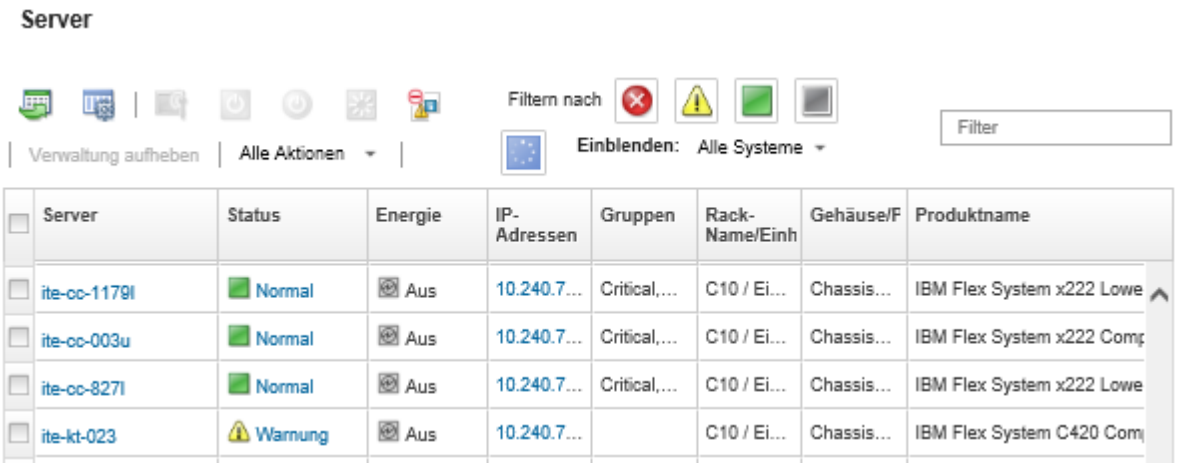
Die Lufttemperatur auf Systemebene wird von einem physischen Sensor an der Vorderseite des Servers gemessen. Diese Temperatur gibt die Lufteintrittstemperatur für den Server an. Beachten Sie, dass die vom XClarity Administrator und die vom CMM gemeldete Lufttemperatur abweichen kann, falls die Temperatur zu verschiedenen Zeitpunkten erfasst wird.

Vorgehensweise

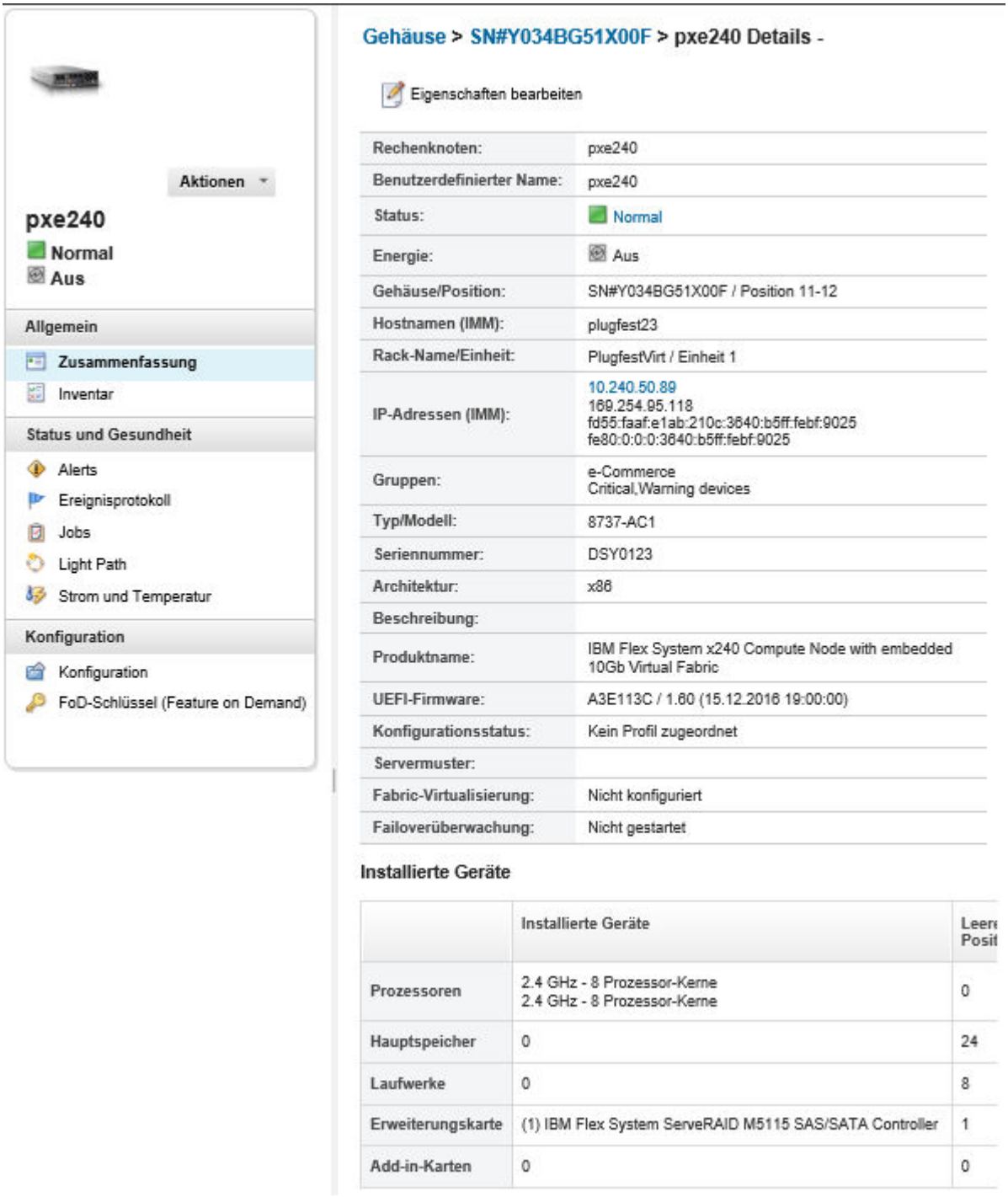
Gehen Sie wie folgt vor, um die Details für einen verwalteten Server anzuzeigen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rack-Server und Rechenknoten).

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdown-Liste **Alle Systeme** einen Systemtyp auswählen und im Feld **Filter** Text (beispielsweise einen Systemnamen oder eine IP-Adresse) eingeben, um die angezeigten Server weiter zu filtern.



Schritt 2. Klicken Sie in der Spalte **Server** auf die Verknüpfung zum Server. Die Statusübersichtsseite für den Server mit den Servereigenschaften und den auf dem Server installierten Komponenten wird angezeigt.



Anmerkung: Bei System x- und NeXtScale-Servern wird die LAN-over-USB-Adresse auf dieser Seite angegeben. Diese Adresse kann mit XClarity Administrator nicht geändert werden. Stattdessen müssen Sie die BMC-Schnittstelle (BMC - Baseboard Management Controller) des Servers verwenden. Weitere Informationen finden Sie unter „Zugriff auf das IMM2 über die Schnittstelle LAN over USB“ in der Produktdokumentation zum Server. Die Produktdokumentation für Ihren Server finden Sie in der Onlinedokumentation für BladeCenter.

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

- Klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung für den Server mit Systeminformationen und installierten Komponenten anzuzeigen (siehe Den Status eines verwalteten Servers anzeigen).
- Klicken Sie auf **Inventardetails**, um Details zu den Serverkomponenten anzuzeigen. Dazu gehören:
  - Firmwareversionen für den Server und den Management-Controller
  - Netzwerkdetails für das Verwaltungsmodul, z. B. Hostname, IPv4-Adresse, IPv6-Adresse und MAC-Adressen
  - Anlagendetails mit Servername, UUID (Universally Unique Identifier) und Standort
  - Komponentendetails mit CPUs, Speicher, Laufwerken und Erweiterungskarten

  Anmerkungen:

  - Es werden alle IP-Adressen für den Server aufgelistet. Die IP-Adresse des Management-Controller-Ports wird als erstes aufgeführt. Wenn die IP-Adresse des Management-Controllers verfügbar ist, wird sie für die Verbindung mit dem Server verwendet.
  - Falls für einen bestimmten Adapter keine Daten verfügbar sind, bleiben einige Adapterfelder (z. B. der Produktname) leer.
  - Wenn ein neuer Adapter im Server installiert wurde, muss der Server erneut gestartet werden, damit der Adapter im Bestand angezeigt wird.
  - Bei einigen Add-In-Karten wird die Feature on Demand-Information (FoD) unter dem Einheitennamen angezeigt.
  - Sie können den Mauszeiger über die Spalte „Typ“ bewegen, um weitere Informationen zu bestimmten Komponenten aufzurufen, z. B. Intel Optain DCPMM-Speicher.
- Klicken Sie auf **Alerts**, um die Liste der aktuellen Alerts für diesen Server anzuzeigen (siehe Mit Alerts arbeiten).

  Anmerkung: Sie können Schwellenwerteinstellungen für das Auslösen von Alerts und Ereignissen festlegen, wenn ein bestimmter Wert wie die Lebensdauer einer SSD in einem ThinkSystem- oder ThinkServer-Server eine Warnung oder einen kritischen Wert überschreitet (siehe Schwellenwerteinstellungen für die Generierung von Alerts und Ereignissen festlegen).
- Klicken Sie auf **Ereignisprotokoll**, um die Liste der Ereignisse für diesen Server anzuzeigen (siehe Ereignisse im Ereignisprotokoll überwachen).
- Klicken Sie auf **Jobs**, um eine Liste der diesem Server zugeordneten Jobs anzuzeigen (siehe Jobs überwachen).
- Klicken Sie auf **Light Path**, um den aktuellen Status der Server-LEDs anzuzeigen (z. B. Position, Fehler und Informationen). Dies entspricht der Betrachtung des Serverbedienfelds.
- Klicken Sie auf **Strom und Temperatur**, um Details zum Stromverbrauch und zur Lufttemperatur anzuzeigen.

  Tipp: Verwenden Sie die Aktualisierungsschaltfläche des Webbrowsers, um die neuesten Strom- und Temperaturdaten zu erfassen. Die Datenerfassung kann mehrere Minuten in Anspruch nehmen.
- Klicken Sie auf **Konfiguration**, um die aktuellen Konfigurationsinformationen für den Server (inkl. lokalem Speicher, E/A-Adaptern, SAN-Booteinstellungen und Firmwareeinstellungen) und dessen Konformität mit dem zugewiesenen Konfigurationsmuster anzuzeigen (siehe Server mithilfe von Konfigurationsmustern konfigurieren).
- Klicken Sie auf **FoD-Schlüssel (Feature on Demand)**, um eine Liste der aktuell für den verwalteten Server installierten FoD-Schlüssel (Feature on Demand) anzuzeigen (siehe Features on Demand-Schlüssel anzeigen).

Nach dieser Aufgabe

Außer der Anzeige von Übersichts- und Detailinformationen zu einem Server können Sie die folgenden Aktionen durchführen:

- Zeigen Sie das Rack oder das Gehäuse des Servers an, indem Sie auf der Seite „Zusammenfassung“ auf den Rack- oder Gehäusenamen klicken.
- Zeigen Sie einen ausgewählten Server in einer grafischen Rack- oder Gehäuseansicht an. Klicken Sie dazu auf **Alle Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Alle Aktionen → Anzeigen → In der Gehäuseansicht anzeigen**.
- Starten Sie die Management-Controller-Webschnittstelle für einen ausgewählten Server. Klicken Sie dazu auf die Verknüpfung **IP-Adresse** (siehe Management-Controller-Webschnittstelle für einen Server starten).
- Greifen Sie per Fernzugriff auf einen Server zu (siehe Verwenden der Fernsteuerung zur Verwaltung von Converged-, Flex System-, NeXtScale- und System x-Servern).
- Schalten Sie einen ausgewählten Server ein oder aus (siehe Einen Server ein- und ausschalten).
- Ändern Sie die Systeminformationen eines ausgewählten Servers, indem Sie auf **Eigenschaften bearbeiten** klicken.
- Aktualisieren Sie den Bestand eines ausgewählten Servers, indem Sie auf **Aktionen → Bestand → Bestand aktualisieren** klicken.
- Exportieren Sie ausführliche Informationen über die Server in eine CSV-Datei. Klicken Sie dazu auf **Aktionen → Bestand → Bestand exportieren**.

  Anmerkungen:

  – Weitere Informationen zu Bestandsdaten in der CSV-Datei finden Sie unter GET /nodes/<*UUID_list*> in der Onlinedokumentation zu XClarity Administrator.

  – Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Schließen Sie belanglose Ereignisse auf allen Seiten aus, auf denen Ereignisse angezeigt werden. Klicken Sie dazu auf **Aktionen → Servicerücksetzung → Ereignisse ausschließen** (siehe Ereignisse ausschließen).
- Starten Sie einen ausgewählten Server mit einem NMI (Non-Maskable Interrupt) neu, indem Sie auf **Aktionen → Service → NMI auslösen** klicken.
- Ändern Sie den LED-Standortstatus eines ausgewählten Servers in „ein“, „aus“ oder „blinkend“. Markieren Sie dazu den Server und klicken Sie auf **Aktionen → Service → LED-Standortstatus ein-/ausschalten**. Wählen Sie den Status aus und klicken Sie auf **Übernehmen**.

  Anmerkungen:
  – Das Umschalten der Positionsanzeige für ThinkSystem SR635 und SR655 Server wird nicht unterstützt.
  – Die Positionsanzeige auf ThinkServer-Servern kann ein- oder ausgeschaltet sein. Das Blinken wird nicht unterstützt.
- Aktivieren oder deaktivieren Sie Single Sign-On für einen ausgewählten ThinkSystem und ThinkAgile Server. Klicken Sie dazu auf **Alle Aktionen → Sicherheit → Single Sign-On aktivieren** oder **Alle Aktionen → Sicherheit → Single Sign-On deaktivieren**.

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

Aktivieren von Single Sign-On für einen bestimmten ThinkSystem und ThinkAgile Server überschreibt die globale Einstellung für alle ThinkSystem und ThinkAgile Server.

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

- Aktivieren oder deaktivieren Sie Änderungen der Firewallregeln auf einem ausgewählten Server, mit denen eingehende Anforderungen auf XClarity Administrator begrenzt werden. Markieren Sie dazu den Server und klicken Sie auf **Aktionen → Sicherheit → Kapselung aktivieren** oder **Aktionen → Sicherheit → Kapselung deaktivieren**. Die globale Kapselungseinstellung 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 die globale Kapselungseinstellung aktiviert ist und die Einheit Kapselung unterstützt, kommuniziert XClarity Administrator 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 von XClarity Administrator akzeptiert werden.

  Achtung: Wenn Kapselung aktiviert ist und XClarity Administrator nicht mehr verfügbar ist, bevor die Verwaltung einer Einheit aufgehoben wird, müssen die erforderlichen Schritte zur Deaktivierung der Kapselung ausgeführt werden, um die Kommunikation mit der Einheit herzustellen. Informationen zu Wiederherstellungsprozeduren finden Sie unter Datei „lenovoMgrAlert.mib“ und Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.
- (Nur ThinkServer-fremde Server) Beheben Sie mögliche Probleme zwischen dem Lenovo XClarity Administrator-Sicherheitszertifikat und dem Management-Controller-Sicherheitszertifikat im ausgewählten Server. Markieren Sie dazu den Server und klicken Sie auf **Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen** (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).

Serverkonfigurationsdaten sichern und wiederherstellen

Lenovo XClarity Administrator enthält keine integrierten Sicherungsfunktionen für Serverkonfigurationsdaten. Verwenden Sie stattdessen die Sicherungsfunktionen, die für Ihren verwalteten Server verfügbar sind.

- **Converged-, Flex System-, System x-, ThinkSystem- und NeXtScale-Server**
  - Serverkonfigurationsdaten sichern

    Verwenden Sie die Verwaltungswebschnittstelle oder Befehlszeilenschnittstelle, um die Firmware zu sichern.

    - Klicken Sie in der IMM-Webschnittstelle auf **IMM-Verwaltung → IMM-Konfiguration**.
    - Verwenden Sie in der CLI den Befehl `backup`.

    Weitere Informationen über das Sichern von Servern mit IMM finden Sie in der Onlinedokumentation für Integrated Management Module II.

    Verwenden Sie zum Sichern von Anwendungen, die auf dem Server ausgeführt werden, Tools, die vom Betriebssystem bereitgestellt werden. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Betriebssystem.

    Stellen Sie für Flex System-Recheneinheiten sicher, dass Sie die Einstellungen für Optionen sichern, die auf den Rechenknoten installiert sind. Sie können alle Rechenknoteneinstellungen, einschließlich der Optionseinstellungen, mit dem erweiterten Konfigurationsdienstprogramm (Advanced Setup Utility, ASU) sichern. Informationen zum ASU finden Sie auf der Website Website zum Advanced Settings Utility (ASU).
  - Serverkonfigurationsdaten wiederherstellen

Verwenden Sie die Verwaltungswebschnittstelle oder die Befehlszeilenschnittstelle, um die Firmware wiederherzustellen. Weitere Informationen über das Wiederherstellen von Servern über BMC finden Sie in der Onlinedokumentation für Integrated Management Module II.

Verwenden Sie die Dokumentation, die mit dem Betriebssystem und jeglichen Anwendungen, die auf dem Server ausgeführt werden, bereitgestellt wird, um die Software wiederherzustellen, die auf dem Server installiert ist.

- Klicken Sie in der IMM-Webschnittstelle auf **IMM-Verwaltung → IMM-Konfiguration**.
- Verwenden Sie in der CLI den Befehl `restore`.

Anmerkung: Tipp: Zusätzliche Informationen zum Sichern und Wiederherstellen von Gehäusekomponenten finden Sie im Best Practices-Handbuch zum Sichern und Wiederherstellen von PureFlex und Flex System.

- **ThinkServer-Server**Die Wiederherstellungsverfahren variieren je nach ThinkServer-Server. Informationen zur Wiederherstellung der Einheit finden Sie in der Produktdokumentation, die mit Ihrem Server geliefert wird.

Systemschutz aktivieren

Systemschutz überwacht den Hardwarebestand für ThinkSystem Server mit XCC2.

Zu dieser Aufgabe

Der überwachte Bestand umfasst Prozessoren, Speicher, PCI-Adapter, Laufwerke, Systemplatine und Adapterkarten. Änderungen bei Firmwareversionen und Konfigurationseinstellungen werden nicht erkannt.

Wenn der Systemschutz aktiviert ist, wird eine Momentaufnahme des Hardwarebestands als vertrauenswürdige Referenz für jede ausgewählte Einheit erstellt. Wenn eine Einheit neu gestartet wird, erfasst der Baseboard Management Controller in der Einheit die aktuelle Systemkonfiguration und vergleicht sie mit der Momentaufnahme. Wenn eine Abweichung bei mindestens einer Komponente erkannt wird, löst der Systemschutz ein Ereignis aus. Wenn eine Abweichung bei einem Prozessor oder Speicher festgestellt wird, löst der Systemschutz ein Ereignis aus und kann optional verhindern, dass der Server zum Betriebssystem bootet.

Vorgehensweise

Gehen Sie wie folgt vor, um den Systemschutz für einen weiteren Server mit XCC2 zu aktivieren.

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Server**. Die Seite Server wird aufgerufen, die eine Tabellenansicht aller verwalteten Server enthält.

Schritt 2. Wählen Sie mindestens einen Server mit XCC2 aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Sicherheit → Systemschutz aktivieren**, um das Dialogfenster Systemschutz aktivieren anzuzeigen.

Schritt 4. Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn der Systemschutz aktiviert ist, eine Bestandsänderung erkannt wird und der Server nicht mehr konform ist.

- **Aktivieren, Standardverhalten des Systems beibehalten**. Das aktuelle Verhalten wird verwendet. . Das Standardverhalten ist die Generierung eines Ereignisses.
- **Aktivieren, BS-Start verhindern bei fehlender Konformität**. Ein Ereignis wird ausgelöst. Wenn Sie versuchen, in das BS zu booten, werden Sie gewarnt, wenn der Systemschutz Konfigurationsänderungen bei Prozessoren oder Speicher erkennt. In diesem Fall werden Sie aufgefordert, sich beim Baseboard Management Controller anzumelden, falls die Änderungen unerwartet sind. Andernfalls können Sie das Booten oder Herunterfahren fortsetzen. Wenn Sie nicht innerhalb von 5 Minuten reagieren, wird der Server standardmäßig heruntergefahren.

- **Aktivieren, Ereignis generieren bei fehlender Konformität**. Es wird ein Ereignis ausgelöst, aber keine andere Aktion ausgeführt.

Schritt 5. Klicken Sie auf **Übernehmen**.

Es wird ein Job erstellt, um Momentaufnahmen vom Bestand für den ausgewählten Server zu erstellen. Sie können den Jobfortschritt im Jobprotokoll überwachen. Klicken Sie im XClarity Administrator-Menü auf **Überwachung → Jobs**. Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

Nach dieser Aufgabe

Um den Systemschutz auf ausgewählten Servern zu deaktivieren, klicken Sie auf **Alle Aktionen → Sicherheit → Systemschutz deaktivieren** und anschließend auf **Übernehmen**.

Laufwerkdaten sicher löschen

Lenovo XClarity Administrator kann Daten auf allen Laufwerken in ausgewählten ThinkSystem und ThinkAgile Servern mit Version 22B und höher sicher löschen. Durch diesen Vorgang wird jedes Laufwerk dauerhaft neu beschrieben, indem das gesamte Laufwerk mit einer binären Null, binären Eins oder Zufallsdaten gefüllt wird. Dies erschwert es, die ursprünglich gespeicherten Daten auf dem Laufwerk zu ermitteln.

Achtung:

- Bei diesem Vorgang werden alle Daten auf den Laufwerken *dauerhaft* und *unwiederbringlich* gelöscht.
- Sobald der Job übermittelt wurde, gibt es keine Möglichkeit mehr, den Vorgang abzubrechen.

Vorbereitende Schritte

Sie müssen die Berechtigung **lxc-supervisor** haben, um Laufwerkdaten löschen zu können.

Stellen Sie sicher, dass das UEFI-Administratorkennwort nicht auf den verwalteten Servern festgelegt ist, die gelöscht werden sollen. Wenn das UEFI-Administratorkennwort für einen Server festgelegt wurde, werden die Laufwerke auf diesem Server nicht gelöscht.

Standardmäßig können Sie Laufwerkdaten für bis zu drei Server gleichzeitig sicher löschen. Sie können die Anzahl der gleichzeitig zulässigen Server konfigurieren. Navigieren Sie dazu zu **Verwaltung → Bestandseinstellungen** und legen Sie den gewünschten Wert unter **Maximale Anzahl von Servern, die in einem Batch gelöscht werden können** fest. Sie können eine Zahl von `3 - 100` Servern auswählen.

Es ist jeweils nur ein sicherer Löschjob erlaubt. Sie müssen warten, bis der aktuelle Job abgeschlossen ist, bevor Sie einen weiteren sicheren Löschjob starten.

Das Löschen sehr großer Laufwerke kann einige Stunden dauern.

Sie können keine SATA-SDD-Datenträger sicher löschen, die mit Marvell RAID-Controllern verbunden sind. Ziehen Sie stattdessen die folgenden Empfehlungen in Betracht.

- Für 7mm-SATA-SSDs verbinden Sie diese mit Broadcom RAID-Controllern, um ein sicheres Löschen durchzuführen.
- Verbinden Sie M.2 SATA SSDs mit Marvell Nicht-RAID-Controllern (z. B. ThinkSystem M.2 SATA/NVMe Einrichtungssatz für zwei Positionen), um eine sichere Löschung durchzuführen.

Zu dieser Aufgabe

Sie können die Daten auf den folgenden Laufwerken löschen.

- NVMe
- SAS
- SAS HBA
- SAS RAID
- SATA
- Extern verbundene Speichereinheiten
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

Der Vorgang des sicheren Löschens erzeugt einen Eintrag im Audit-Protokoll. Sie können diese Ereignisse über die Ereignisweiterleitungsfunktion weiterleiten (siehe Ereignisse an syslog, Remote-SNMP-Manager, E-Mail und andere Ereignisservices weiterleiten).

Um Probleme mit dem sicheren Löschen zu beheben, siehe Daten auf blockierten Laufwerken können nicht sicher gelöscht werden und SATA-SDD-Datenträger können nicht sicher gelöscht werden, wenn sie mit Marvell RAID verbunden sind in der XClarity Administrator Onlinedokumentation.

Vorgehensweise

Gehen Sie wie folgt vor, um alle Laufwerke auf bestimmten verwalteten Servern sicher zu löschen.

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Server**. Die Seite Server wird aufgerufen, die eine Tabellenansicht aller verwalteten Server enthält.

Schritt 2. Wählen Sie den Server aus.

Schritt 3. Navigieren Sie zu **Alle Aktionen → Service → Laufwerk sicher löschen (HDD/SDD)**.

Schritt 4. Geben Sie Ihr Administratorkennwort ein, um zu bestätigen, dass Sie alle Laufwerke auf den ausgewählten Servern löschen möchten.

Schritt 5. Klicken Sie auf **Löschen**.

Wenn Sie Laufwerke auf mehr als drei Servern auf einmal löschen möchten, werden Sie dazu aufgefordert, Ihre Benutzer-ID und Ihr Kennwort einzugeben. Geben Sie dieselben Anmeldeinformationen ein, die Sie für die Anmeldung bei XClarity Administrator verwendet haben.

Für diesen Vorgang muss ein Job erstellt werden. Sie können den Fortschritt auf der Seite „Jobs“ überwachen. Navigieren Sie dazu im Menü von XClarity Administrator zu **Überwachung → Jobs**. Wenn der Job nicht erfolgreich abgeschlossen wurde, klicken Sie auf den Job-Link, um Details zum Job anzuzeigen (siehe Jobs überwachen).

Fernsteuerung verwenden

Über die Lenovo XClarity Administrator-Webschnittstelle können Sie eine Fernsteuerungssitzung für einen verwalteten Server öffnen, als würden Sie sich an der lokalen Konsole befinden. Sie können die Fernsteuerungssitzung verwenden, um Vorgänge, wie das Ein- und Ausschalten des Servers, und das logische Anhängen eines lokalen oder Remote-Laufwerks durchzuführen.

Zum Starten einer Fernsteuerungssitzung für ein Gerät müssen Sie über die folgenden Berechtigungen verfügen: **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** oder **lxc-hw-manager**.

Fernsteuerung zur Verwaltung von ThinkSystem- oder ThinkAgile-Servern verwenden

Über die Lenovo XClarity Administrator-Webschnittstelle können Sie eine Fernsteuerungssitzung für einen verwalteten ThinkSystem- oder ThinkAgile-Server öffnen, als würden Sie sich an der lokalen Konsole befinden. Sie können die Fernsteuerungssitzung verwenden, um Stromversorgungsoption durchzuführen und ein lokales oder Remote-Laufwerks logisch anzuhängen.

Vorbereitende Schritte

Auf dem Server muss die Kapselung deaktiviert sein.

Um eine Fernsteuerungssitzung zu einem Server zu öffnen, muss sich der Server im Status „Online“ oder „Normal“ befinden. Wenn der Server einen anderen Zugriffsstatus hat, kann die Fernsteuerungssitzung keine Verbindung zum Server aufbauen. Weitere Informationen zum Anzeigen des Serverstatus finden Sie unter Die Details eines verwalteten Servers 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 über eine Fernsteuerungssitzung zu einem einzelnen ThinkSystem- oder ThinkAgile-Server aus XClarity Administrator 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

So öffnen Sie eine Fernsteuerungssitzung zu einem bestimmten Server:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rackserver und Rechenknoten).

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdownliste **Alle Systeme** einen Systemtyp auswählen und im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um die anzuzeigenden Server auszuwählen.

Schritt 2. Wählen Sie den Server aus, zu dem Sie eine Fernsteuerungssitzung öffnen möchten.

Schritt 3. Klicken Sie auf das Symbol **Fernsteuerung** ( ).

Schritt 4. Akzeptieren Sie die Sicherheitswarnungen Ihres Webbrowsers.

Nach dieser Aufgabe

Wenn sich die Fernsteuerungssitzung nicht erfolgreich öffnet, finden Sie unter Fernsteuerungsprobleme in der XClarity Administrator-Onlinedokumentation weitere Informationen.

Fernsteuerung zur Verwaltung von ThinkServer- und NeXtScale sd350 M5-Servern verwenden

Über die Lenovo XClarity Administrator-Webschnittstelle können Sie eine Fernsteuerungssitzung für verwaltete ThinkServer- und NeXtScale sd350 M5-Server öffnen. Diese arbeitet so, als würden Sie sich an der entsprechenden lokalen Konsole befinden. Sie können die Fernsteuerungssitzung verwenden, um den Server an- und auszuschalten, einen Reset auszulösen, ein lokales Laufwerk oder ein Netzwerklaufwerk auf dem Server anzuhängen und Screenshots und Videos aufzunehmen.

Vorbereitende Schritte

- Die Fernsteuerung für diese Server erfordert eine Java Runtime Environment (JRE) mit Java WebStart-Unterstützung, die beim Client installiert ist. Ein Open-Source-JDK wird dringend empfohlen. Wenn Sie ein JRE oder JDK eines Anbieters verwenden, stellen Sie sicher, dass es ordnungsgemäß für die kommerzielle Nutzung lizenziert ist. Die folgenden JREs werden unterstützt.
  - Oracle JRE 7 (siehe Website zum Herunterladen von Oracle Java)

    Achtung:
    - Java 7 erfordert mindestens die Unterstützung von TLSv1.2 (siehe Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren).
    - Java 7 wird künftig nicht mehr unterstützt.
  - Oracle JRE 8, für das eine kostenpflichtige Lizenz erforderlich ist (siehe Website zum Herunterladen von Oracle Java)
  - Adoptium OpenJDK 8 mit dem IcedTea-Web v1.8-Plug-In (siehe Adoptium OpenJDK-Website)
  - Amazon Corretto 8 (siehe Website zum Herunterladen von Amazon Corretto 8)

  Java WebStart ist nicht in OpenJDK- oder Coretto-Installationspaketen enthalten und muss separat installiert werden. IcedTea-Web oder OpenWebStart können mit der GNU GPLV2-Lizenz verwendet werden (siehe Website zum Herunterladen von IcedTea OpenJDK und OpenWebStart-Website).
- Für die Fernsteuerung ist es erforderlich, dass ein Features on Demand-Schlüssel für ThinkServer System Manager Premium Upgrade auf den ThinkServer-Servern installiert ist. Weitere Informationen zu den auf Ihren Servern installierten FoD-Schlüsseln finden Sie unter Features on Demand-Schlüssel anzeigen .

Zu dieser Aufgabe

Sie können über XClarity Administrator eine Fernsteuerungssitzung zu einem einzelnen ThinkServer-Server starten.

Um eine Fernsteuerungssitzung zu einem Server zu öffnen, muss sich der Server im Status „Online“ oder „Normal“ befinden. Wenn der Server einen anderen Zugriffsstatus hat, kann die Fernsteuerungssitzung keine Verbindung zum Server aufbauen. Weitere Informationen zum Anzeigen des Serverstatus finden Sie unter Die Details eines verwalteten Servers anzeigen.

Weitere Informationen zur Verwendung der ThinkServer-Fernsteuerung und der Medien-Features finden Sie in der ThinkServer-Serverdokumentation.

Vorgehensweise

So öffnen Sie eine Fernsteuerungssitzung zu einem bestimmten Server:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rackserver und Rechenknoten).

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdownliste **Alle Systeme** einen Systemtyp auswählen und im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um die anzuzeigenden Server auszuwählen.

Schritt 2. Wählen Sie den Server aus, zu dem Sie eine Fernsteuerungssitzung öffnen möchten.

Schritt 3. Klicken Sie auf das Symbol **Fernsteuerung** ().

Schritt 4. Akzeptieren Sie die Sicherheitswarnungen Ihres Webbrowsers.

Nach dieser Aufgabe

Wenn sich die Fernsteuerungssitzung nicht erfolgreich öffnet, finden Sie unter Fernsteuerungsprobleme in der XClarity Administrator-Onlinedokumentation weitere Informationen.

Verwenden der Fernsteuerung zur Verwaltung von Converged-, Flex System-, NeXtScale- und System x-Servern

Über die Lenovo XClarity Administrator-Webschnittstelle können Sie eine Fernsteuerungssitzung zur Verwaltung von Converged-, Flex System-, NeXtScale- und System x-Servern öffnen. Diese arbeitet so, als würden Sie sich an der entsprechenden lokalen Konsole befinden.

Vorbereitende Schritte

Weitere Informationen:  XClarity Administrator: Fernsteuerung

- Die Fernsteuerung für diese Server erfordert eine Java Runtime Environment (JRE) mit Java WebStart-Unterstützung, die beim Client installiert ist. Ein Open-Source-JDK wird dringend empfohlen. Wenn Sie ein JRE oder JDK eines Anbieters verwenden, stellen Sie sicher, dass es ordnungsgemäß für die kommerzielle Nutzung lizenziert ist. Die folgenden JREs werden unterstützt.
  - Oracle JRE 7 (siehe Website zum Herunterladen von Oracle Java)

    Achtung:
    - Java 7 erfordert mindestens die Unterstützung von TLSv1.2 (siehe Verschlüsselungseinstellungen auf dem Verwaltungsserver konfigurieren).
    - Java 7 wird künftig nicht mehr unterstützt.
  - Oracle JRE 8, für das eine kostenpflichtige Lizenz erforderlich ist (siehe Website zum Herunterladen von Oracle Java)
  - Adoptium OpenJDK 8 mit dem IcedTea-Web v1.8-Plug-In (siehe Adoptium OpenJDK-Website)
  - Amazon Corretto 8 (siehe Website zum Herunterladen von Amazon Corretto 8)

  Java WebStart ist nicht in OpenJDK- oder Coretto-Installationspaketen enthalten und muss separat installiert werden. IcedTea-Web oder OpenWebStart können mit der GNU GPLV2-Lizenz verwendet werden (siehe Website zum Herunterladen von IcedTea OpenJDK und OpenWebStart-Website).
- Die Fernsteuerungssitzung wird für Server mit den folgenden Betriebssystemen (mit 32 Bit oder 64 Bit) unterstützt:
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- Für die Fernsteuerung muss ein Features on Demand-Schlüssel für die Fernpräsenz auf Converged-, NeXtScale- und System x-Servern installiert sein. Wenn der FoD-Schlüssel auf einem Server nicht erkannt wird, zeigt die Fernsteuerungssitzung in der Liste der verfügbaren Server für den entsprechenden Server die Meldung `Fehlender Aktivierungsschlüssel` an. Auf der Seite „Server“ sehen Sie, ob die Fernpräsenz-Funktion auf einem Server aktiviert, deaktiviert oder nicht installiert ist (siehe Den Status eines verwalteten Servers anzeigen). Weitere Informationen zu den auf Ihren Servern installierten FoD-Schlüsseln finden Sie unter Features on Demand-Schlüssel anzeigen.
- Der Benutzeraccount, der zum Starten der Fernsteuerungssitzung verwendet wird, muss gültig und auf dem XClarity Administrator-Authentifizierungsserver definiert sein. Außerdem muss der Benutzeraccount über hinreichende Benutzerberechtigungen für den Zugriff auf einen Server und seine Verwaltung verfügen.

- Berücksichtigen Sie die Aspekte zur Sicherheit, Leistung und Tastatureingabe, bevor Sie eine Fernsteuerungssitzung öffnen. Weitere Informationen zu diesen Aspekten finden Sie unter Fernsteuerungshinweise.
- Der Fernsteuerungsdialog verwendet die Ländereinstellungs- und Anzeigensprachеneinstellungen, die für das Betriebssystem auf Ihrem lokalen System definiert wurden.Wenn Ihr lokales System unter Windows ausgeführt wird, finden Sie unter Java-Website Informationen zur Änderung der Ländereinstellungen. Um die Anzeigensprache zu ändern, installieren Sie eine lokalisierte Windows-Version oder ein Sprachpaket über das Windows-Website.

Zu dieser Aufgabe

Sie können über Lenovo XClarity Administrator mehrere Fernsteuerungssitzungen starten. Jede Sitzung kann mehrere Server verwalten.

Um eine Fernsteuerungssitzung zu einem Server zu öffnen, muss sich der Server im Status „Online“ oder „Normal“ befinden. Wenn der Server einen anderen Zugriffsstatus hat, kann die Fernsteuerungssitzung keine Verbindung zum Server aufbauen. Weitere Informationen zum Anzeigen des Serverstatus finden Sie unter Die Details eines verwalteten Servers anzeigen.

Sie können eine nicht zielgerichtete Fernsteuerungssitzung öffnen, indem Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Fernsteuerung** klicken. Akzeptieren Sie dann die Sicherheitswarnungen Ihres Webbrowsers.

Anmerkung: Bei Flex System x280, x480 und x880-Rechenknoten 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 zu einem bestimmten NeXtScale-, Flex System- und System x-Server zu öffnen:

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rackserver und Rechenknoten).

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdownliste **Alle Systeme** einen Systemtyp auswählen und im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um die anzuzeigenden Server auszuwählen.

Schritt 2. Wählen Sie den Server aus, zu dem Sie eine Fernsteuerungssitzung öffnen möchten.

Schritt 3. Klicken Sie auf das Symbol **Fernsteuerung** ().

Schritt 4. Akzeptieren Sie die Sicherheitswarnungen Ihres Webbrowsers.

Schritt 5. Wählen Sie optional das zu speichernde Fernsteuerungssymbol auf Ihrem Desktop aus. Über dieses Symbol können Sie eine Fernsteuerungssitzung starten, ohne sich an der XClarity Administrator-Webschnittstelle anzumelden.

Schritt 6. 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 Administrator unterstützt bis zu sechs gleichzeitige Fernsteuerungssitzungen zu einem Server.

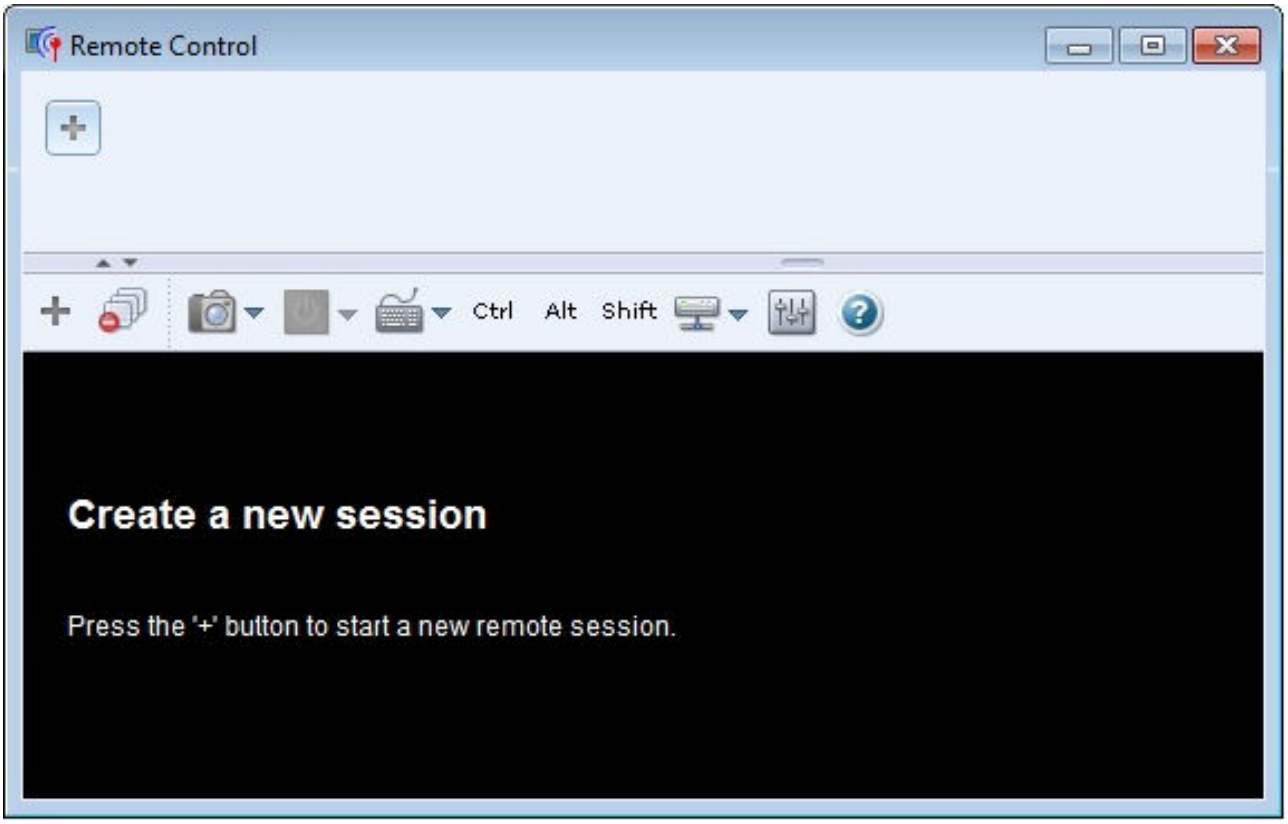
Schritt 7. Wenn Sie dazu aufgefordert werden, wählen Sie aus, ob eine Verknüpfung für die Fernsteuerungssitzung auf Ihrem lokalen System gespeichert werden soll.

Wenn Sie die Verknüpfung speichern, können Sie diese zum Öffnen der Fernsteuerungssitzung zum angegebenen Server nutzen, ohne die XClarity Administrator-Webschnittstelle zu öffnen. Ihr lokales System muss allerdings Zugriff auf XClarity Administrator haben, um das Benutzeraccount über den XClarity Administrator-Authentifizierungsserver zu überprüfen.

Die Verknüpfung enthält einen Link, der eine leere Fernsteuerungssitzung öffnet. Über diese können Sie die Rechenknoten manuell hinzufügen.

Ergebnisse

Das Fenster Fernsteuerung wird angezeigt.



Der Miniaturansichtsbereich zeigt alle Serversitzungen an, die momentan über die Fernsteuerungssitzung verwaltet werden.

Sie können mehrere Serversitzungen anzeigen und zwischen den Serversitzungen wechseln, indem Sie auf eine Miniaturansicht klicken, das die Serverkonsole im Videositzungsbereich darstellt. Wenn Sie auf mehre Server zugreifen, als im Miniaturansichtsbereich angezeigt werden können, klicken Sie auf das **Nach rechts blättern**- ( ) und das **Nach links blättern**-Symbol ( ), um zu den zusätzlichen Servern zu blättern. Klicken Sie auf das Symbol **Alle Sitzungen** ( ), um eine Liste aller offenen Serversitzungen anzuzeigen.

Klicken Sie im Miniaturansichtsbereich auf das **Server hinzufügen**-Symbol (), um einen neuen Server zur Liste der verwalteten Server hinzuzufügen. Weitere Informationen zum Hinzufügen einer Sitzung finden Sie unter Eine Serverkonsole zu einer Fernsteuerungssitzung hinzufügen. Sie können steuern, ob der Miniaturansichtsbereich angezeigt wird und wie oft die Piktogramme auf der Seite „Miniaturansicht“ aktualisiert werden. Weitere Informationen zu den Miniaturansichtseinstellungen finden Sie unter Fernbedienungseinstellungen festlegen.

Nach dieser Aufgabe

Wenn sich die Fernsteuerungssitzung nicht erfolgreich öffnet, finden Sie unter Fernsteuerungsprobleme in der XClarity Administrator-Onlinedokumentation weitere Informationen.

Im Dialog „Fernsteuerung“ können Sie die folgenden Aktionen ausführen:

- Hinzufügen einer Sitzung zu anderen Servern zur aktuellen Fernsteuerungssitzung (siehe Eine Serverkonsole zu einer Fernsteuerungssitzung hinzufügen).
- Ausblenden oder Anzeigen eines Miniaturansichtsbereiches über das **Miniaturansichten ein-/ausschalten**-Symbol ().
- Anzeigen der Fernsteuerungssitzung als Fenster oder als Vollbild über das **Bildschirm**-Symbol () und die Option **Vollbild einschalten** oder **Vollbild ausschalten**.
- Verwenden der Tasten STRG, ALT und UMSCHALT in einer Fernsteuerungssitzung (siehe Verwenden der Tasten STRG, ALT und UMSCHALT).
- Definieren von benutzerdefinierten Tastenfolgen (auch Programmfunktionssymbole genannt, siehe Programmfunktionssymbole definieren).
- Erstellen von Anzeigeerfassungen der aktuell ausgewählten Serversitzung und Speichern der Anzeigeerfassung in verschiedenen Formaten über das **Bildschirm**-Symbol () und die Option **Screenshot**.
- Anhängen ferner Medien (wie CD-, DVD- oder USB-Einheiten, Festplattenimages oder CD-Image (ISO)) für den ausgewählten Server oder Verschieben einer angehängten Einheit auf einen anderen Server (siehe Remote-Medien einbauen oder transportieren).
- Hochladen von Images von fernen Medien auf einen Server (siehe Ein Image zum Server hochladen).
- Ein- und Ausschalten des Servers über eine ferne Konsole (siehe Einen Server per Fernsteuerungssitzung ein- und ausschalten).
- Ändern von Fernbedienungseinstellungen (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 Administrator-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.

   Tipp: Weitere Informationen zur FIPS-140-Konformität finden Sie auf der Website zum FIPS 140-kompatiblen Modus für SunJSSE.
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.

Eine Serverkonsole zu einer Fernsteuerungssitzung hinzufügen

Sie können zur aktuellen Fernsteuerungssitzung eine oder mehrere Serverkonsolen hinzufügen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine oder mehrere Serverkonsolen zur aktuellen Fernsteuerungssitzung hinzuzufügen.

Schritt 1. Klicken Sie im Fenster „Fernsteuerung“ auf das Symbol **Neue Sitzung** ().

Ein Dialogfenster mit einer Liste der verfügbaren Gehäuse und Rack-Server wird angezeigt, die durch Lenovo XClarity Administrator verwaltet werden und für die Ihr Benutzeraccount eine Verwaltungsberechtigung besitzt.

Tipp: Wenn keine Server in der Liste angezeigt werden, finden Sie unter Fernsteuerungsprobleme in der Onlinedokumentation von XClarity Administrator mögliche Vorgehensweisen zur Behebung des Problems.

Schritt 2. Wählen Sie mindestens einen Server aus, zu dem eine Verbindung hergestellt werden soll.

Sie können die angezeigten Server filtern, indem Sie in der Dropdown-Liste **Typ** einen Systemtyp auswählen und im Feld **Filter** Text eingeben (z. B. den Systemnamen oder einen Gehäusenamen).

Mit **Alle auswählen** können Sie alle Server in der Liste auswählen.

Schritt 3. **Optional:** Wählen Sie **Einzelbenutzermodus** aus, um eine exklusive Sitzung für jeden ausgewählten Server zu öffnen.

Wenn Sie diese Option auswählen, werden alle anderen Fernsteuerungssitzungen mit den ausgewählten Servern blockiert, bis Sie die Verbindung zu den ausgewählten Servern trennen. Diese Option ist nur verfügbar, wenn keine anderen Fernsteuerungssitzungen mit den ausgewählten Servern aktiv sind.

Wenn Sie diese Option nicht auswählen, wird standardmäßig der Mehrbenutzermodus verwendet.

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

Einen Server per Fernsteuerungssitzung ein- und ausschalten

Ein Server kann über eine Fernsteuerungssitzung ein- und ausgeschaltet werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Server ein-oder auszuschalten.

Schritt 1. Klicken Sie im Fenster Fernsteuerung auf die Miniaturansicht für den Server, den Sie ein- oder ausschalten möchten.

Schritt 2. Klicken Sie auf das Symbol **Strom** () und dann auf eine der folgenden Stromversorgungsaktionen:
- **Einschalten**

- **Normal ausschalten**
- **Sofort ausschalten**
- **Normal neu starten**
- **Sofort neu starten**
- **NMI auslösen**
- **Systemkonfiguration neu starten** (Nur Lenovo Converged-, Flex System-, NeXtScale- und System x-Server)

Tipp: Das Symbol **Strom** ist grün, wenn der Server aktuell eingeschaltet ist.

Programmfunktionssymbole definieren

Sie können für die aktuelle Fernsteuerungssitzung eigene benutzerdefinierte Tastenkombinationen definieren, sogenannte *Programmierfunktionssymbole.*

Vorbereitende Schritte

Um eine aktuelle Liste der Programmierfunktionssymbole anzuzeigen, klicken Sie auf das Symbol **Tastatur** ().

Die Definitionen von Programmierfunktionssymbolen 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 Programmierfunktionssymbole erneut definieren.

Auf Wunsch können Sie die Benutzereinstellungen (einschließlich Programmierfunktionssymbole) über die Registerkarte **Benutzereinstellungen** im Dialogfenster Einstellungen exportieren. Siehe Benutzereinstellungen importieren oder exportieren für weitere Informationen.

Anmerkung: Wenn Sie eine internationale Tastatur verwenden und Programmierfunktionssymbole definieren, die die AltGr-Taste erfordern, stellen Sie sicher, dass die Workstation, auf der Sie die Fernsteuerungsanwendung aufrufen, denselben Betriebssystemtyp nutzt wie der Server, auf den Sie per Fernsteuerung zugreifen. Wenn der Server z. B. unter Linux läuft, muss die Fernsteuerungssitzung auf einer Workstation aufgerufen werden, die ebenfalls unter Linux ausgeführt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Programmierfunktionssymbol hinzuzufügen.

Schritt 1. Klicken Sie im Fenster Fernsteuerung auf das Symbol **Tastatur** () und dann auf **Programmierfunktionssymbol hinzufügen**. Die Registerkarte **Programmierfunktion für Programmierfunktionssymbole** im Dialogfeld Einstellungen wird angezeigt.

Schritt 2. Klicken Sie auf **Neu**.

Schritt 3. Geben Sie die Tastenkombination ein, die Sie definieren möchten.

Schritt 4. Klicken Sie auf **OK**. Das neue Programmierfunktionssymbol wird zur Liste der Programmierfunktionssymbole hinzugefügt.

Verwenden der Tasten STRG, ALT und UMSCHALT

Einige Betriebssysteme fangen bestimmte Tasten ab, anstatt sie an den fernen Server zu übertragen. Mithilfe der Einrastfunktion können Sie Tastatureingaben direkt an den von Ihnen verwalteten Server senden.

Vorgehensweise

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.

Wenn Sie beispielsweise die Tastenkombination Strg+Alt+Entf senden möchten, gehen Sie wie folgt vor:
1. Klicken Sie auf **STRG** in der Symbolleiste.
2. Klicken Sie auf **ALT** in der Symbolleiste.
3. Klicken Sie mit der linken Maustaste an einer beliebigen Stelle im Videositzungsbereich.
4. Drücken Sie die Entf-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).

Wenn Sie in der Symbolleiste auf die Schaltfläche **Strg**, **Alt** oder **Umschalt** klicken, um die Taste zu aktivieren, bleiben die Schaltflächen so lange aktiv, bis Sie eine Taste auf der Tastatur drücken oder erneut auf die Schaltfläche klicken.

Remote-Medien einbauen oder transportieren

Mit der Funktion für ferne Medien können Sie Medien auf dem lokalen System, z. B. eine CD-, DVD- oder USB-Einheit bzw. ein Platten- oder CD-Image (ISO-Image), an den ausgewählten Server anhängen. Sie können auch ein Image in den lokalen Speicher auf dem Baseboard Management Controller (BMC) hochladen.

Vorbereitende Schritte

Gleichzeitig kann immer nur ein Benutzer Medien anhängen oder Daten in den lokalen Speicher auf dem Management-Controller hochladen. Während des Anhängens oder des Hochladens von Daten in den lokalen Speicher können keine anderen Benutzer auf den lokalen Speicher auf dem Management-Controller zugreifen.

Auf einem Server, auf dem das Betriebssystem Linux ausgeführt wird, wird das Anhängen mehrerer ISO-Images nicht unterstützt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ferne Medien anzuhängen oder zu verschieben.

Schritt 1. Klicken Sie im Fenster Fernsteuerung auf das Symbol **Ferne Medien** ().

Schritt 2. Klicken Sie auf eine der folgenden Aktionen:

- **Ferne Medien anhängen**

  Diese Aktion macht lokale Medienressourcen für den aktuell ausgewählten Server verfügbar. Eine Medienressource kann innerhalb einer Fernsteuerungssitzung nur an einen einzigen Server angehängt werden.

  Wenn Sie auf **Ferne Medien anhängen** klicken, haben Sie folgende Möglichkeiten:

  – **Anzuhängendes Image auswählen**. Das Image ist für den aktuell ausgewählten Server verfügbar, bis Sie die Einheit abhängen oder die Fernsteuerungssitzung schließen. An einen einzelnen Server können mehrere Images angehängt werden und jedes Image kann an mehrere Server angehängt werden.

  – **Anzuhängendes Laufwerk (CD-, DVD- oder USB-Einheit) auswählen**. Die Einheit ist für den aktuell ausgewählten Server verfügbar, bis Sie das Laufwerk abhängen oder die

Fernsteuerungssitzung schließen. An einen einzelnen Server können mehrere Einheiten angehängt werden, jede Einheit kann jedoch nur an einen Server angehängt werden.

Anmerkung: Achten Sie beim Auswählen eines Laufwerks darauf, dass Sie das Laufwerk abhängen, bevor Sie Datenträger von diesem Laufwerk entfernen.

- **Image auf IMM hochladen**. Verwenden Sie diese Option, um ein Image im lokalen Speicher auf dem Management-Controller des ausgewählten Servers zu speichern. Das Image verbleibt auf dem Management-Controller, auch wenn Sie die Fernsteuerungssitzung beenden oder der Server neu gestartet wird.

  Auf dem Management-Controller können ca. 50 MB an Daten gespeichert werden.

  Sie können mehrere Images auf den Management-Controller hochladen, solange der Gesamtspeicherplatz für alle Images kleiner ist als 50 MB.

  Jedes auf den Management-Controller hochgeladene Image wird automatisch an den Server angehängt. Nachdem Sie eine Image an den Management-Controller angehängt haben, können Sie das hochgeladene Image auch zum Management-Controller eines anderen Servers verschieben. Beim Verschieben wird das hochgeladene Image vom aktuellen Server entfernt und auf einen ausgewählten Server hochgeladen.

- **Ferne Medien verschieben**

  Diese Aktion verschiebt eine zuvor angehängte Medienressource zu einem anderen Server.

  Führen Sie die folgenden Schritte aus, um eine Ressource für einen Server verfügbar zu machen:

  1. Wählen Sie mindestens eine Ressource aus.
  2. Klicken Sie auf **Hinzufügen**, um die Ressourcen zur Liste **Ausgewählte Ressourcen** zu verschieben.
  3. Klicken Sie auf **Anhängen**, um die Ressourcen für die Verwendung durch den Server anzuhängen. Die Fernsteuerungssitzung definiert eine Einheit für die Ressource und ordnet diese Einheit einem Mountpunkt für den aktuell ausgewählten Server zu. Sie haben die Möglichkeit, den Schreibschutz für die angehängten Medien zu aktivieren.

Ein Image zum Server hochladen

Sie können ein Image in den lokalen Speicher auf dem Baseboard Management Controller (BMC) für den ausgewählten Server hochladen.

Zu dieser Aufgabe

Das Image verbleibt auf dem Management-Controller, auch wenn Sie die Fernsteuerungssitzung beenden oder der Server neu gestartet wird.

Auf dem Management-Controller können ca. 50 MB an Daten gespeichert werden.

Sie können mehrere Images auf den Management-Controller hochladen, solange der Gesamtspeicherplatz für alle Images kleiner ist als 50 MB.

Jedes auf den Management-Controller hochgeladene Image wird automatisch an den Server angehängt. Nachdem Sie eine Image an den Management-Controller angehängt haben, können Sie das hochgeladene Image auch zum Management-Controller eines anderen Servers verschieben. Beim Verschieben wird das hochgeladene Image vom aktuellen Server entfernt und auf einen ausgewählten Server hochgeladen.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Image an den Server hochzuladen:

Schritt 1. Klicken Sie im Fenster Fernsteuerung auf das Symbol **Ferne Medien** ().

Schritt 2. Klicken Sie auf **Fernen Medien anhängen**.

Schritt 3. Klicken Sie auf **Image auf IMM hochladen**.

Benutzereinstellungen importieren oder exportieren

Sie können Benutzereinstellungen für die aktuelle Fernsteuerungssitzung importieren oder exportieren.

Zu dieser Aufgabe

Beim Exportieren von Benutzereinstellungen werden alle Benutzereinstellungen für die aktuelle Fernsteuerungssitzung in einer Eigenschaftendatei auf Ihrem lokalen System gespeichert. Die Eigenschaftendatei können Sie auf ein anderes System kopieren und die darin gespeicherten Einstellungen in die Fernsteuerungsanwendung importieren, um sie dort zu verwenden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Benutzereinstellungen für die aktuelle Fernsteuerungssitzung zu importieren oder zu exportieren.

Schritt 1. Klicken Sie im Fenster Fernsteuerung auf das Symbol **Einstellungen** ().

Schritt 2. Klicken Sie auf die Registerkarte **Benutzereinstellungen**.

Schritt 3. Klicken Sie auf **Importieren**, um Einstellungen aus einer exportierten Datei zu importieren, oder klicken Sie auf **Exportieren**, um alle aktuellen Benutzereinstellungen in einer Eigenschaftendatei auf dem lokalen System zu speichern.

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 Administrator 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. Weitere Informationen zu den Positionen der Protokolldateien finden Sie unter Protokolle und Traces der Fernbedienung anzeigen.
  - **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.

Protokolle und Traces der Fernbedienung anzeigen

Für jede Fernsteuerungssitzung werden Protokolldateien erstellt. Welche Ereignistypen in diesen Dateien protokolliert werden, hängt vom Debugmodus ab, der auf der Registerkarte **Allgemein** im Dialogfeld Einstellungen festgelegt wird. Die Protokolldateien sind hilfreich, um Probleme zu beheben.

Vorgehensweise

Fernsteuerungsprotokolldateien werden an den folgenden Positionen gespeichert.

Betriebssystem	Protokollverzeichnis
Windows 7 und 8	`%USERPROFILE%\lenovo\remoteaccess` Beispiel: `C:\Users\win_user\lenovo\remoteaccess`

Weitere Informationen zum Sammeln von Diagnosedateien und Senden der Dateien an den Lenovo-Support finden Sie unter Mit Service und Support arbeiten in der Onlinedokumentation von Lenovo XClarity Administrator.

Zugriff auf Betriebssysteme auf verwalteten Servern verwalten

Sie können den Zugriff auf Betriebssysteme auf verwalteten Servern verwalten.

Vorbereitende Schritte

Sie müssen die Berechtigungen **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** oder **lxc-hw-admin** haben, um Einheitentreiber verwalten und implementieren und Stromversorgungsaktionen auf verwalteten Servern von den Windows-Treiberaktualisierungen-Seiten durchführen zu können.

Zu dieser Aufgabe

Bevor Lenovo XClarity Administrator die BS-Einheitentreiber auf einem verwalteten System aktualisieren kann, müssen Sie Informationen für den Zugriff auf das Hostbetriebssystem bereitstellen, einschließlich BS-IP-Adresse und gespeicherter Administratoranmeldeinformationen. Weitere Informationen zur Aktualisierung von BS-Einheitentreibern finden Sie unter Windows-Einheitentreiber auf verwalteten Servern aktualisieren.

XClarity Administrator verwendet gespeicherte Anmeldeinformationen zur Authentifizierung beim Hostbetriebssystem. Weitere Informationen zum Erstellen von gespeicherten Anmeldeinformationen in XClarity Administrator finden Sie unter Gespeicherte Anmeldeinformationen verwalten.

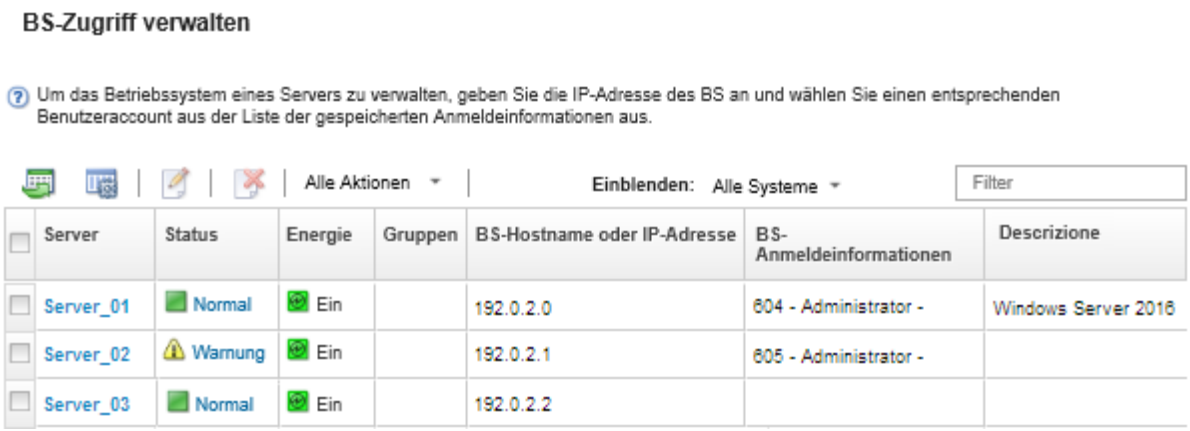
Tipp: XClarity Administrator überprüft nicht automatisch die Informationen, die Sie auf dieser Seite angeben.

Vorgehensweise

Gehen Sie wie folgt vor, um die Betriebssystemeigenschaften zu ändern.

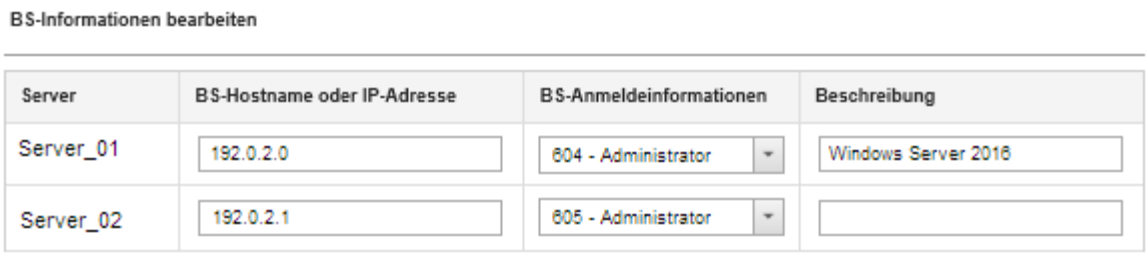
Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Zugriff verwalten**, um die Seite „BS-Zugriff verwalten“ anzuzeigen.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdown-Liste **Alle Systeme** einen Systemtyp auswählen und im Feld **Filter** Text (beispielsweise einen Systemnamen oder eine IP-Adresse) eingeben, um die angezeigten Server weiter zu filtern.



Schritt 2. Wählen Sie die zu aktualisierenden Server aus.

Schritt 3. Klicken Sie auf das Symbol **BS-Informationen bearbeiten** (), um das Dialogfeld BS-Informationen bearbeiten anzuzeigen.



Schritt 4. Geben Sie für jeden Zielserver die folgenden Informationen an:
- IP-Adresse oder Hostname des Hostbetriebssystems
- (Optional) Gespeicherte Anmeldeinformationen für den Zugriff auf das Hostbetriebssystem
- (Optional) Beschreibung des Hostbetriebssystems

Schritt 5. Klicken Sie auf **Speichern**.

Nach dieser Aufgabe

Sie können Sie die folgenden Aktionen für die Verwaltung des Betriebssystemzugriffs ausführen.

- Löschen Sie die Betriebssysteminformationen (IP-Adresse, Anmeldeinformationen und Beschreibung), indem Sie den Server auswählen und auf das Symbol **BS-Informationen entfernen** ( ) klicken.
- Testen Sie die Authentifizierung auf Windows-Servern, indem Sie auf **Bereitstellung → Windows-Treiberaktualisierungen: Übernehmen** klicken, den Zielserver auswählen und dann auf **Authentifizierung prüfen** klicken.
- Zeigen Sie Implementierungsinformationen für das Betriebssystem auf einem bestimmten Server an, indem Sie mit der Maus auf den Servernamen zeigen.

  Anmerkung: Implementierungsinformationen sind nur für Betriebssysteme verfügbar, die von der XClarity Administrator-Instanz erfolgreich implementiert wurden. Für fehlgeschlagene Implementierungen und für Implementierungen, die auf andere Weise durchgeführt wurden, z. B. von einer anderen XClarity Administrator-Instanz, sind keine Implementierungsinformationen verfügbar.

Features on Demand-Schlüssel anzeigen

Sie können eine Liste der Features on Demand-Schlüssel anzeigen, die derzeit auf den verwalteten Servern installiert sind.

Zu dieser Aufgabe

Sie können über die Lenovo XClarity Administrator-Webschnittstelle keine Features on Demand-Schlüssel erwerben, installieren oder verwalten. Weitere Informationen zur Beschaffung und Installation von Features on Demand-Schlüsseln finden Sie unter Features on Demand in der Onlinedokumentation von XClarity Administrator.

Vorgehensweise

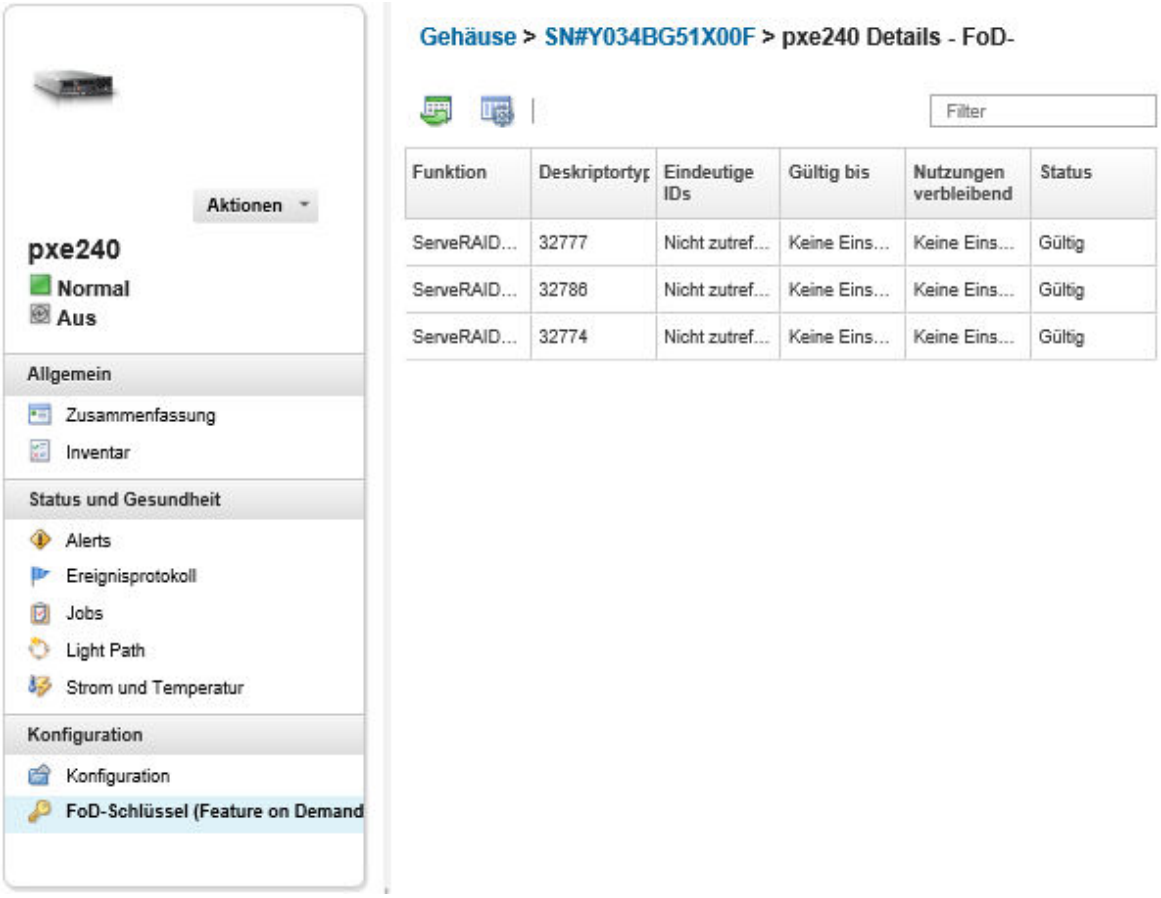
So zeigen Sie eine Liste aller FoD-Schlüssel an, die auf einem bestimmten verwalteten Server installiert sind:

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Server**. Die Seite „Server“ wird mit einer Tabellenansicht aller verwalteten Server (Rack- und Tower-Server sowie Rechenknoten) geöffnet.

Schritt 2. Klicken Sie in der Spalte **Server** auf den Servernamen. Die Statusübersichtsseite für den Server mit den Servereigenschaften und den auf dem Server installierten Komponenten wird angezeigt.

Schritt 3. Klicken Sie in der linken Navigation unter „Allgemein“ auf **Inventardetails** und erweitern Sie jeden Hardwarekomponentenabschnitt, um die eindeutige FoD-IDs für die Komponenten anzuzeigen.

Schritt 4. Klicken Sie in der linken Navigation unter „Konfiguration“ auf **Features on Demand-Schlüssel**, um Informationen zu allen auf dem Server installierten FoD-Schlüsseln anzuzeigen.



Energie und Temperatur verwalten

Sie können den Stromverbrauch und die Temperatur von Converged-, NeXtScale-, System x- und ThinkServer-Servern verwalten und überwachen und die Energieeffizienz mit Lenovo XClarity Energy Manager optimieren.

Weitere Informationen: Lenovo XClarity Energy Manager

Zu dieser Aufgabe

XClarity Administrator ist eine eigenständige Benutzerschnittstelle, mit der Sie den Stromverbrauch und die Temperatur von unterstützten Servern verwalten und überwachen können. Sie bietet unter anderem folgende Optionen:

- Überwachen des Energieverbrauchs, Einschätzen des Strombedarfs und bedarfsgerechte Energiezuweisung für die Server.
- Überwachen von Temperatur und Kühlkapazität der Server.
- Senden von Benachrichtigungen, wenn bestimmte Ereignisse auftreten oder Grenzwerte überschritten werden.
- Begrenzen des Energieverbrauchs von Einheiten mithilfe von Richtlinien.
- Optimieren der Energieeffizienz durch Überwachen der Eintrittstemperatur in Echtzeit, Ermitteln von Servern mit geringer Auslastung anhand von Out-of-Band-Daten, Messen der Leistungsbereiche für verschiedene Servermodelle und Auswerten der Verarbeitung neuer Workloads auf den Servern auf Basis der Ressourcenverfügbarkeit.

- Reduzieren des Stromverbrauchs auf ein Minimum, um die Servicezeit im Falle, dass die Notstromversorgung benötigt wird (z. B. bei einem Stromausfall im Rechenzentrum), zu verlängern.

Weitere Informationen über den Download, die Installation und die Verwendung von XClarity Administrator finden Sie unter Website zu Lenovo XClarity Energy Manager.

Einen Server ein- und ausschalten

Sie können einen Server über Lenovo XClarity Administrator ein- und ausschalten.

Vorbereitende Schritte

- Bei Red Hat® Enterprise Linux (RHEL) v7 und höher setzt ein Neustart des Betriebssystems über einen grafischen Modus den Server standardmäßig aus. Bevor Sie die Aktionen **Normal neu starten** oder **Sofort neu starten** von XClarity Administrator ausführen können, müssen Sie beim Betriebssystem manuell das Ausschalteverhalten des Netzschalters konfigurieren. Anweisungen hierzu finden Sie im Abschnitt Red Hat-Handbuch zur Datenmigration und -Verwaltung: Ändern des Verhaltens beim Drücken des Netzschalters im grafischen Zielmodus.
- Bei SUSE Linux Enterprise Server (SLES) muss zum Ausschalten des Betriebssystems in der SLES-Sitzung das Stammkennwort eingegeben werden. Bevor Sie die Aktion **Normal ausschalten** oder **Sofort ausschalten** von XClarity Administrator ausführen können, müssen Sie den Server manuell über die lokale SLES-Schnittstelle ausschalten und beim Eingeben des Kennworts die Option **Authentifizierung speichern** aktivieren. Alternativ können Sie prüfen, ob die Sicherheitsrichtlinie eine Deaktivierung der erforderlichen Authentifizierung zulässt.
- Wenn die Wake-On-LAN-Bootoption aktiviert ist, kann sie beim Ausschalten des Servers zu Konflikten mit XClarity Administrator führen. Dies gilt auch für Firmwareaktualisierungen, bei denen ein Wake-On-LAN-Client im Netzwerk „Aktivierung durch Magic Packet“-Befehle sendet.
- Mit der Stromversorgungsaktion **Zur Systemkonfiguration neu starten** erfolgt ein Neustart des Servers und das Dienstprogramm „BIOS/UEFI Startup“ wird (anstelle eines normalen Betriebssystemstarts) in einer Fernsteuerungssitzung geöffnet.
- Die Stromversorgungsaktionen **Normal ausschalten** und **Sofort ausschalten** hängen von der Konfiguration des Betriebssystems ab, das auf der Einheit installiert ist, und können nur genutzt werden, wenn sie von der Betriebssystemkonfiguration unterstützt werden.
- Sie können die Einheit mit NMI (Non-Maskable Interrupt) neu starten, indem Sie auf **Alle Aktionen → Service → NMI auslösen** klicken.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Server ein- oder auszuschalten.

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rack-Server und Rechenknoten).

Schritt 2. Wählen Sie den Server aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Stromversorgungsaktionen** und klicken Sie dann auf eine der folgenden Stromversorgungsaktionen:
- **Einschalten**: Die Einheit wird eingeschaltet.
- **Normal ausschalten**: Das Betriebssystem wird heruntergefahren und die Einheit wird ausgeschaltet.
- **Sofort ausschalten**: Die Einheit wird ausgeschaltet.
- **Normal neu starten**: Das Betriebssystem wird heruntergefahren und die Einheit wird neu gestartet.
- **Sofort neu starten**: Die Einheit wird neu gestartet.

- **Zur Systemkonfiguration neu starten**: Die Einheit wird neu gestartet und die BIOS/UEFI-Konfiguration (F1) wird aufgerufen. Dies wird für ThinkServer-fremde Server unterstützt, die ohne Einschränkung unterstützt werden.
- **Management-Controller neu starten**: Der Baseboard Management Controller (BMC) wird neu gestartet.
- **Sofort neu starten und PXE Network Boot durchführen** startet den Server sofort neu und bootet den Server im Preboot Execution Environment-(PXE-)Netzwerk. Dies wird für Lenovo Flex System-, System x- und ThinkSystem-Server unterstützt.

  Anmerkung: PXE-Boot-bezogene UEFI-Einstellungen müssen auf dem Server konfiguriert werden.

Server in einem Flex System-Gehäuse virtuell neu einsetzen

Sie können simulieren, dass ein Server in einem Flex System-Gehäuse entfernt und erneut wieder eingesetzt wurde, indem Sie den Server mit NMI (Non-Maskable Interrupt) neu starten.

Zu dieser Aufgabe

Beim virtuellen erneuten Einsetzen gehen alle bestehenden Netzwerkverbindungen zum Server verloren und der Stromversorgungsstatus des Servers ändert sich. Stellen Sie vor einem virtuellen neuen Einsetzen sicher, dass Sie alle Benutzerdaten gespeichert haben.

Achtung:

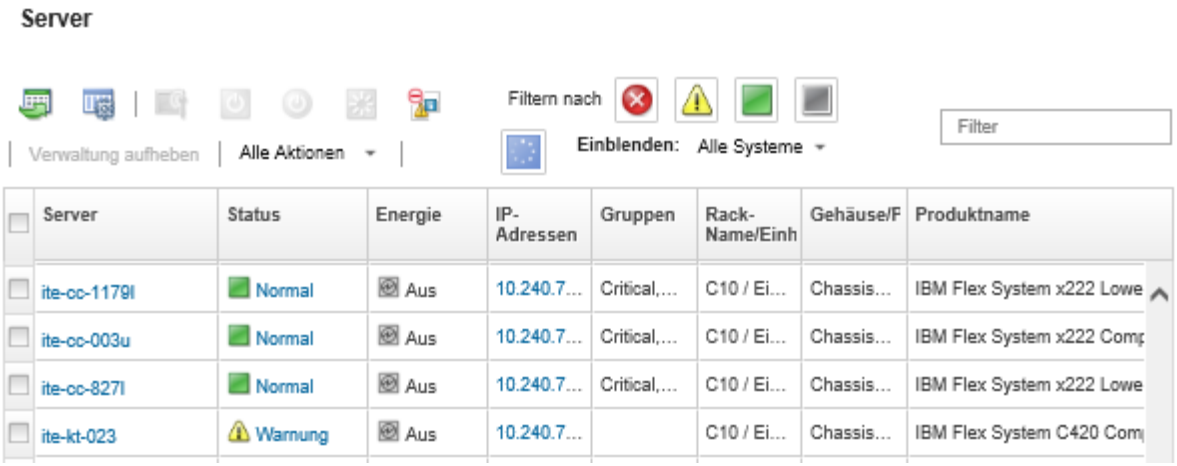
- Führen Sie ein virtuelles neues Einsetzen nur aus, wenn Sie vom Lenovo-Support dazu aufgefordert werden.
- Das virtuelle neue Einsetzen kann zu einem Datenverlust führen. Bevor Sie den Server neu einsetzen, führen Sie die erforderlichen Vorgänge zum Schutz der Benutzerdaten aus.
- Sie können einen Server auch ausschalten, anstatt ihn virtuell neu einzusetzen. Weitere Informationen zu Stromversorgungsaktionen finden Sie unter Einen Server ein- und ausschalten.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Server in einem Flex System-Gehäuse virtuell neu einzusetzen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Server**. Die Seite Server wird aufgerufen, die eine Tabellenansicht aller verwalteten Server enthält.

Sie können die Tabellenspalten sortieren, um den Server, den Sie neu einsetzen möchten, schneller zu finden. Außerdem können Sie in der Dropdown-Liste **Alle Einheiten** einen Einheitentyp auswählen und im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um die anzuzeigenden Server weiter zu filtern.



Schritt 2. Wählen Sie den Server in der Tabelle aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Service → Virtuell erneut einsetzen**.

Schritt 4. Klicken Sie auf **Virtuell erneut einsetzen**.

Management-Controller-Webschnittstelle für einen Server starten

Sie können die Management-Controller-Webschnittstelle für einen bestimmten Server über Lenovo XClarity Administrator starten.

Vorbereitende Schritte

Für den Zugriff auf ThinkSystem SR635 und SR655 Server über XClarity Administrator muss ein Benutzer die Berechtigung **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** oder **lxc-bs-admin** haben (siehe Authentifizierungsserver verwalten).

Bei Verwendung von Single Sign-On können Sie die Verwaltungsschnittstelle für einen verwalteten Server aus XClarity Administrator starten, ohne sich anmelden zu müssen. Single Sign-On wird für ThinkSystem und ThinkAgile Server (außer SR635 und SR655) unterstützt. ThinkSystem SR645 und SR665 Server erfordern die XCC-Firmwareversion 21A oder höher.

Um sich direkt mit lokalen oder externen LDAP-Benutzeraccounts beim Management-Controller anzumelden, ohne sich bei XClarity Administrator anzumelden, verwenden Sie die URL `https://{XCC_IP_adderss}/#/login`.

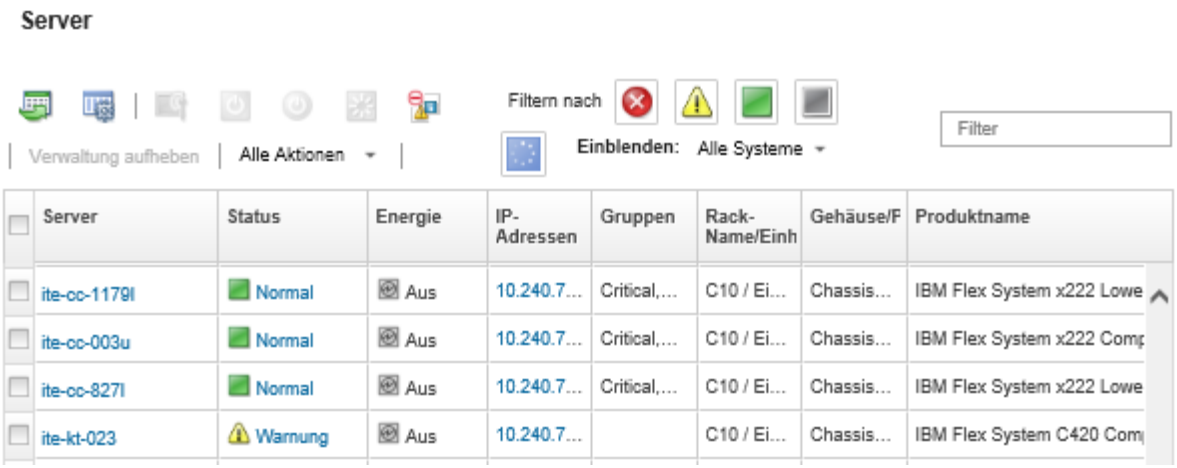
Vorgehensweise

Gehen Sie wie folgt vor, um die Management-Controller-Webschnittstelle für einen Server zu starten.

Anmerkung: Die Management-Controller-Webschnittstelle kann von Lenovo XClarity Administrator nicht über den Safari-Webbrowser gestartet werden.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Server**, um die Seite Server anzuzeigen.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Außerdem können Sie in der Dropdownliste **Alle Systeme** einen Systemtyp auswählen und im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um die anzuzeigenden Server auszuwählen.



Schritt 2. Klicken Sie in der Spalte **Server** auf die Verknüpfung zum Server. Die Statusübersichtsseite für den Server wird angezeigt.

Schritt 3. Klicken Sie auf **Alle Aktionen → Starten → Verwaltungswebschnittstelle**. Die Management-Controller-Webschnittstelle für den Server wird gestartet.

Tipp: Sie können auch in der Spalte **IP-Adressen** auf die IP-Adresse klicken, um die Management-Controller-Webschnittstelle zu starten.

Schritt 4. Melden Sie sich mit den Benutzeranmeldeinformationen von XClarity Administrator an der Management-Controller-Webschnittstelle an.

Nach dieser Aufgabe

Weitere Informationen über die Verwendung der Management-Controller-Webschnittstelle für einen Server finden Sie unter Onlinedokumentation für Integrated Management Module II und XClarity Controller-Online-Dokumentation.

Systemeigenschaften für einen Server ändern

Sie können die Systemeigenschaften für einen bestimmten Server ändern.

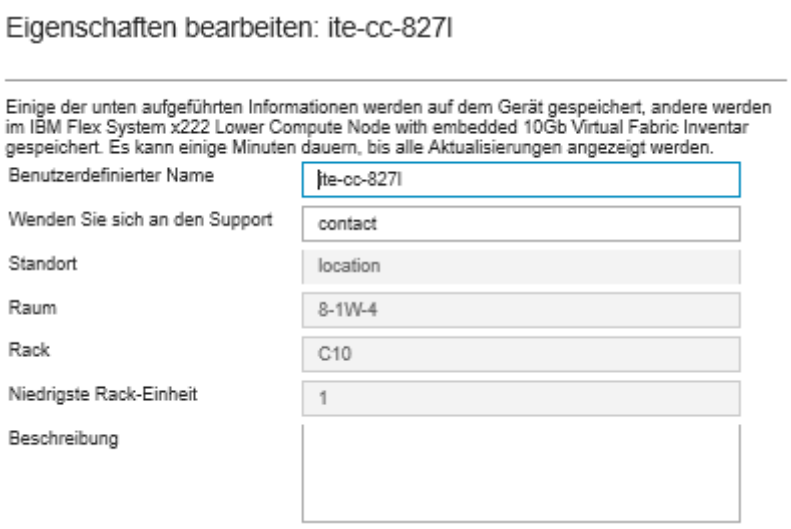
Vorgehensweise

Gehen Sie wie folgt vor, um die Systemeigenschaften zu ändern:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Hardware → Server**, um die Seite Server anzuzeigen.

Schritt 2. Wählen Sie den zu aktualisierenden Server aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**, um den Dialog Bearbeiten anzuzeigen.



Schritt 4. Ändern Sie gegebenenfalls die folgenden Daten:
- Benutzerdefinierter Name für den Server
- Wenden Sie sich an den Support
- Beschreibung

Anmerkung: Die Eigenschaften für Position, Raum, Rack und unterste Rackeinheit werden von XClarity Administrator aktualisiert, wenn Sie Einheiten in der Webschnittstelle zu einem Rack hinzufügen oder daraus entfernen (siehe Racks verwalten).

Schritt 5. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie diese Eigenschaften ändern, kann es einen Moment dauern, bis die Änderungen in der XClarity Administrator-Webschnittstelle angezeigt werden.

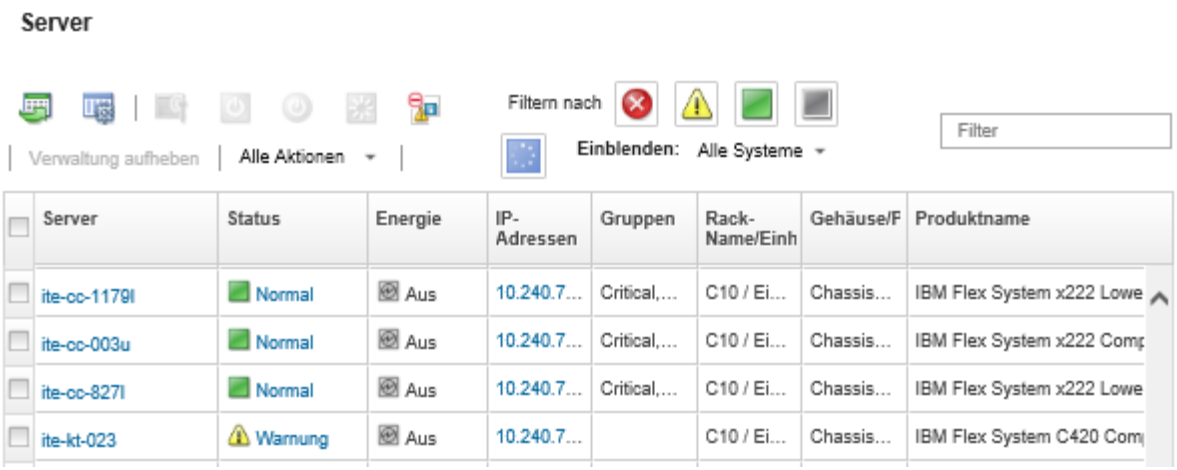
Abgelaufene oder ungültige gespeicherte Anmeldeinformationen für einen Server auflösen

Wenn gespeicherte Anmeldeinformationen auf einer Einheit ablaufen oder nicht mehr funktionsfähig sind, wird der Status für diese Einheit mit „Offline“ angezeigt.

Vorgehensweise

Zum Auflösen abgelaufener oder ungültiger gespeicherter Anmeldeinformationen für einen Server.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rack-Server und Rechenknoten).



Schritt 2. Klicken Sie auf die Spaltenüberschrift der Tabelle **Strom**, um alle Offline-Server oben in der Tabelle zu gruppieren.

Außerdem können Sie in der Dropdown-Liste „Alle Systeme“ einen Systemtyp auswählen und im Feld **Filter** Text (beispielsweise einen Systemnamen oder eine IP-Adresse) eingeben, um die angezeigten Server weiter zu filtern.

Schritt 3. Wählen Sie den Server aus, der aufgelöst werden soll.

Schritt 4. Klicken Sie auf **Alle Aktionen → Sicherheit → Gespeicherte Anmeldeinformationen bearbeiten**.

Schritt 5. Ändern Sie das Kennwort für gespeicherte Anmeldeinformationen oder wählen Sie andere gespeicherte Anmeldeinformationen aus, um diese für die verwaltete Einheit zu verwenden.

Anmerkung: Wenn Sie mehr als eine Einheit mit denselben gespeicherten Anmeldeinformationen verwaltet haben und das Kennwort für die gespeicherten Anmeldeinformationen ändern, betrifft die Änderung des Kennworts alle Einheiten, die derzeit die gespeicherten Anmeldeinformationen verwenden.

Einen ausgefallenen Server nach der Implementierung eines Servermusters wiederherstellen

Wenn ein Server ausfällt, nachdem Sie ein Servermuster implementiert haben, können Sie diesen Server wiederherstellen. Dazu heben Sie die Zuordnung des Profils zum ausgefallenen Server auf und ordnen das Profil anschließend einem Standby-Server zu.

Vorgehensweise

Gehen Sie wie folgt vor, um einen ausgefallenen Server, der die verwaltete Authentifizierung von Lenovo XClarity Administrator verwendet, wiederherzustellen.

Schritt 1. Ermitteln Sie den ausgefallenen Server.

Schritt 2. Heben Sie die Zuordnung des Serverprofils zum ausgefallenen Server auf (siehe Ein Serverprofil deaktivieren).

Achtung: Der ausgefallene Server muss ausgeschaltet sein, damit die virtuelle Adressenzuordnung *vor* der erneuten Zuordnung des Profils deaktiviert werden kann. Wenn Sie die Zuordnung des Serverprofils aufheben, wählen Sie im Dialogfenster „Serverprofilzuordnung aufheben“ die Option **Server ausschalten**, um den ausgefallenen Server auszuschalten (siehe Einen Server ein- und ausschalten).

Schritt 3. Ordnen Sie das Serverprofil einem Standby-Server zu (siehe Ein Serverprofil aktivieren).

Schritt 4. Aktivieren Sie das Profil, indem Sie entweder den Standby-Server einschalten (wenn dieser zurzeit ausgeschaltet ist) oder neu starten (wenn dieser zurzeit eingeschaltet ist) (siehe Einen Server ein- und ausschalten).

Schritt 5. Migrieren Sie die VLAN-Einstellungen der verbundenen Switches auf den Standby-Server.

Schritt 6. Stellen Sie sicher, dass der ausgefallene Server ausgeschaltet ist.

Schritt 7. Ersetzen oder reparieren Sie den ausgefallenen Server. Bei einer Serverreparatur müssen Sie sicherstellen, dass der reparierte Server auf die Standardeinstellungen zurückgesetzt wird. Gehen Sie dazu wie folgt vor:

a. Setzen Sie den BMC mithilfe der Verwaltungswebschnittstelle für den Server auf die Werkseinstellungen zurück. Weitere Informationen über die Zurücksetzung des BMC finden Sie unter ThinkSystem-, Converged-, NeXtScale-, System x M5- oder M6-Serververwaltung nach einem Verwaltungsserverausfall durch Zurücksetzen des Management-Controllers wiederherstellen.

b. Löschen Sie mithilfe der UEFI-Menüs die UEFI-Informationen (UEFI - Unified Extensible Firmware Interface) einschließlich der virtuellen Adressenzuordnung des E/A-Adapters. Weitere Informationen hierzu finden Sie in der UEFI-Dokumentation.

Booteinstellungen nach der Servermusterimplementierung wiederherstellen

Wenn ein oder mehrere Server nach der Implementierung eines neuen Servermusters auf diese Server nicht starten, ist das Problem möglicherweise, dass die Booteinstellungen mit den standardmäßigen Booteinstellungen des Servermusters überschrieben wurden. Bei Betriebssystemen, die im UEFI-Modus installiert wurden, sind im Rahmen der Wiederherstellung der Standardeinstellungen möglicherweise weitere Konfigurationsschritte erforderlich, um die Bootkonfiguration wiederherzustellen.

Vorgehensweise

Führen Sie das folgende manuelle Wiederherstellungsverfahren für jeden betroffenen Server aus, um die ursprünglichen Booteinstellungen wiederherzustellen.

- Bei Servern mit Red Hat Enterprise Linux-Installation:
  1. Stellen Sie bei einem Remote-Zugriff eine Fernsteuerungssitzung zum Server her (siehe Verwenden der Fernsteuerung zur Verwaltung von Converged-, Flex System-, NeXtScale- und System x-Servern).
  2. Starten Sie den Server neu und klicken Sie dazu auf **Extras → Start → Starten**. Wenn die UEFI-Eingangsanzeige für den Server in der Fernsteuerungssitzung angezeigt wird, drücken Sie die Taste F1, um Setup Utility anzuzeigen.
  3. Wählen Sie **Boot Manager** aus.
  4. Wählen Sie **Add Boot Option** aus.
  5. Wählen Sie **UEFI Full Path Option** aus.
  6. Wählen Sie aus der angezeigten Liste den Eintrag aus, der `SAS` enthält.
  7. Wählen Sie **EFI** aus.
  8. Wählen Sie **redhat** aus.
  9. Wählen Sie **grub.efi** aus.
  10. Aktivieren Sie das Feld **Input the Description**.
  11. Geben Sie `Red Hat Enterprise Linux` ein.
  12. Wählen Sie **Commit Changes** aus.

13. Wählen Sie `Red Hat Enterprise Linux` als erste Option in der Bootreihenfolge aus und entfernen Sie alle anderen Optionen.
14. Drücken Sie die Esc-Taste und wählen Sie **Save changes then exit this menu** aus.
15. Drücken Sie die Esc-Taste und wählen Sie **Exit the Configuration Utility and Reboot** aus. Der Rechenknoten wird neu gestartet.

- Bei Servern mit Microsoft Windows Server 2008-Installation:
  1. Schalten Sie den Server ein und drücken Sie bei Aufforderung die Taste F1, um das Setup-Programm zu öffnen.
  2. Wählen Sie **Boot Manager** aus.
  3. Wählen Sie **Boot from File** aus.
  4. Wählen Sie die Systempartition mit den GUID-Systemtabellen aus, auf der Sie Microsoft Windows Server 2008 installiert haben.
  5. Wählen Sie **EFI** aus.
  6. Wählen Sie **Microsoft** aus.
  7. Wählen Sie **Boot** aus.
  8. Wählen Sie **bootmgfw.EFI** aus.

Anmerkung: Siehe RETAIN-Tipp 5079636 für weitere Informationen.

Rack- oder Tower-Serververwaltung nach einem Verwaltungsserverausfall wiederherstellen

Wenn ein Rack- oder Tower-Server von Lenovo XClarity Administrator verwaltet wird und XClarity Administrator ausfällt, können Sie die Verwaltungsfunktionen bis zur Wiederherstellung bzw. bis zum Austausch von XClarity Administrator wiederherstellen.

Zu dieser Aufgabe

Informationen über die Wiederherstellung der Verwaltung für einen Flex System-Server finden Sie unter Verwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen.

Rack- oder Tower-Serververwaltung nach einem Verwaltungsserverausfall mit „Verwaltung erzwingen“ wiederherstellen

Sie können die Serververwaltung wiederherstellen, indem Sie den Server mit der Option „Verwaltung erzwingen“ wieder verwalten.

Vorgehensweise

Wenn die IP-Adresse von Lenovo XClarity Administrator-Austauschinstanz und ausgefallenem XClarity Administrator identisch ist, können Sie die Einheit wieder über den Account `RECOVERY_ID` und das Kennwort sowie die Option **Verwaltung erzwingen** verwalten (siehe Server verwalten).

System x- oder NeXtScale M4-Server nach fehlerhafter Verwaltungsaufhebung mit dem Management-Controller wiederherstellen

Sie können die Verwaltung eines System x- oder NeXtScale M4-Servers mit dem Baseboard Management Controller (BMC) wiederherstellen.

Vorgehensweise

Gehen Sie wie folgt vor, um die Serververwaltung eines Servers wiederherzustellen, der die verwaltete Authentifizierung von Lenovo XClarity Administrator verwendet.

Schritt 1. Melden Sie sich mit dem Benutzeraccount und dem Kennwort (beides vor der Verwaltung des Servers mit XClarity Administrator festgelegt) an der Management-Controller-Webschnittstelle an.

Schritt 2. Löschen Sie die SNMP-Trap-Einstellungen.

a. Klicken Sie auf **IMM-Verwaltung → Netzwerk**.

b. Klicken Sie auf die Registerkarte **SNMP**.

c. Klicken Sie auf die Registerkarte **Communitys**.

d. Suchen Sie nach dem vorherigen XClarity Administrator-Community-Eintrag, z. B.:
   - **LXCA-IP-Adresse:** 10.240.198.84
   - **LXCA-Host:** LXCA_maqCBlt86d
   - **Community 2:**
   - **Community-Name:** LXCA_maqCBlt86d
   - **Zugriffstyp:** Trap
   - **Empfang von Traps zur Community für bestimmte Hosts zulassen:** 10.240.198.84

e. Entfernen Sie die Werte aus den Feldern für den Community-Eintrag.

f. Klicken Sie auf **Übernehmen**.

Schritt 3. Löschen Sie die Benutzeraccounts.

a. Klicken Sie auf **IMM-Verwaltung → Benutzer**.

b. Klicken Sie auf die Registerkarte **Benutzeraccounts**.

c. Löschen Sie alle XClarity Administrator-Benutzeraccounts sowie Benutzeraccounts mit folgenden Präfixen:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Nach dieser Aufgabe

Wenn XClarity Administrator wiederhergestellt oder ausgetauscht ist, können Sie den System x- oder NeXtScale-Server wieder verwalten (siehe Server verwalten). Alle Informationen über den Server (z. B. Netzwerkeinstellungen, Serverrichtlinien und Firmwarekonformitätsrichtlinien) bleiben erhalten.

ThinkSystem-, Converged-, NeXtScale-, System x M5- oder M6-Serververwaltung nach einem Verwaltungsserverausfall durch Zurücksetzen des Management-Controllers wiederherstellen

Sie können die Verwaltung von ThinkSystem-, Converged-, NeXtScale- oder System x M5- oder M6-Servern wiederherstellen, indem Sie den Baseboard Management Controller (BMC) des Servers auf die Werkseinstellungen zurücksetzen.

Vorgehensweise

Gehen Sie wie folgt vor, um die Verwaltung eines Servers wiederherzustellen, der die verwaltete Authentifizierung von Lenovo XClarity Administrator verwendet.

Schritt 1. Wenn Encapsulation auf der Einheit aktiviert ist, stellen Sie von einem System, das zur Verwendung der IP-Adresse der ausgefallenen virtuellen XClarity Administrator-Einheit konfiguriert ist, eine Verbindung zum Ziel-Management-Controller her.

Schritt 2. Setzen Sie den Management-Controller auf die Werkseinstellungen zurück.

a. Melden Sie sich mit dem Benutzeraccount und dem Kennwort für die Wiederherstellung (vor der Verwaltung des Servers mit XClarity Administrator festgelegt) an der Management-Controller-Webschnittstelle des Servers an.

b. Klicken Sie auf die Registerkarte **IMM-Verwaltung**.

c. Klicken Sie auf **IMM auf werkseitige Voreinstellungen zurücksetzen**.

d. Klicken Sie auf **OK**, um die Zurücksetzung zu bestätigen.

Wichtig: Nachdem die BMC-Konfiguration abgeschlossen ist, wird der BMC neu gestartet. Wenn es sich um einen lokalen Server handelt, ist die TCP/IP-Verbindung unterbrochen und Sie müssen die Netzwerkschnittstelle neu konfigurieren, um wieder eine funktionsfähige Verbindung herzustellen.

Schritt 3. Melden Sie sich wieder an der Management-Controller-Webschnittstelle des Servers an.

- Der Baseboard Management Controller (BMC) ist anfänglich so konfiguriert, dass er versucht, die IP-Adresse über einen DHCP-Server abzurufen. Ist dies nicht möglich, wird die statische IPv4-Adresse `192.168.70.125` verwendet.
- Für den IMM-BMC sind anfänglich der Benutzername `USERID` und das Kennwort `PASSWORD` (mit einer Null) festgelegt. Dieser Standardbenutzeraccount hat Supervisorzugriff. Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

Schritt 4. Rekonfigurieren Sie die Netzwerkschnittstelle, um wieder eine funktionsfähige Verbindung herzustellen. Weitere Informationen finden Sie unter Onlinedokumentation für Integrated Management Module II.

Nach dieser Aufgabe

Wenn XClarity Administrator wiederhergestellt oder ausgetauscht ist, können Sie den Server wieder verwalten (siehe Server verwalten). Alle Informationen über den Server (z. B. Netzwerkeinstellungen, Serverrichtlinien und Firmwarekonformitätsrichtlinien) bleiben erhalten.

Sofern der Server mit Konfigurationsmuster konfiguriert wurde, können Sie das dem Server zugeordnete Serverprofil erst deaktivieren und dann erneut aktivieren, um die Konfiguration zu übernehmen (siehe Mit Serverprofilen arbeiten).

ThinkSystem-, Converged-, NeXtScale-, System x M5- oder M6-Serververwaltung nach einem Verwaltungsserverausfall mit dem Dienstprogramm „cimcli“ wiederherstellen

Sie können die Verwaltung von ThinkSystem-, Converged-, NeXtScale- oder System x M5- oder M6-Servern wiederherstellen, indem Sie die CIM-Abonnements mit dem Dienstprogramm `cimcli` löschen.

Vorbereitende Schritte

OpenPegasus mit dem Dienstprogramm „cimcli“ muss auf einem System installiert sein, das Netzwerkzugriff auf den Zielserver hat. Weitere Informationen über den Download, die Konfiguration und die Kompilierung von OpenPegasus finden Sie unter Website zu OpenPegasus-RPMs für Linux.

Anmerkung: In Red Hat Enterprise Linux (RHEL) Server 7 und neueren Versionen sind die Quell- und die binären RPMs von OpenPegasus bereits in der Red Hat-Distribution enthalten. Das Dienstprogramm „cimcli“ ist im Paket `top-pegasus-test.x86_64`.

Zu dieser Aufgabe

Wenn der Server wiederhergestellt ist, können Sie ihn wieder verwalten. Alle Informationen über den Server (z. B. Netzwerkeinstellungen, Serverrichtlinien und Firmwarekonformitätsrichtlinien) bleiben erhalten.

Vorgehensweise

Führen Sie die folgenden Schritte über einen Server aus, der eine verwaltete Authentifizierung von Lenovo XClarity Administrator verwendet und auf dem OpenPegasus installiert ist, um die Serververwaltung wiederherzustellen.

Schritt 1. Wenn Encapsulation auf der Einheit aktiviert ist:

a. Stellen Sie von einem System, das zur Verwendung der IP-Adresse der ausgefallenen virtuellen XClarity Administrator-Einheit konfiguriert ist, eine Verbindung zum Zielserver her.

b. Deaktivieren Sie Encapsulation, indem Sie eine SSH-Sitzung zur Einheit öffnen und folgenden Befehl ausführen:
```
encaps lite off
```

Schritt 2. Führen Sie die folgenden Befehle aus, um die CIM-Instanzen für CIM_ListenerDestinationCIMXML, CIM_Indicationfilter und CIM_IndicationSubscription zu ermitteln.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

Dabei geben <*IP_address*>, <*user_ID*> und <*password*> die IP-Adresse, die Benutzer-ID und das Kennwort für den Management-Controller an. Beispiele:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Schritt 3. Führen Sie den folgenden Befehl aus, um die CIM-Instanzen für CIM_ListenerDestinationCIMXML, CIM_Indicationfilter und CIM_IndicationSubscription nacheinander zu löschen.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

Dabei geben <*IP_address*>, <*user_ID*> und <*password*> die IP-Adresse, die Benutzer-ID und das Kennwort für den Management-Controller an und mit <*cim_instance*> werden die Informationen, die für die einzelnen CIM-Instanzen im vorigen Schritt zurückgegeben wurden, in einfachen Anführungszeichen angegeben. Beispiele:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Nach dieser Aufgabe

Wenn Lenovo XClarity Administrator wiederhergestellt oder ausgetauscht ist, können Sie den System x- oder NeXtScale-Server wieder verwalten (siehe Server verwalten). Alle Informationen über den Server (z. B. Netzwerkeinstellungen, Serverrichtlinien und Firmwarekonformitätsrichtlinien) bleiben erhalten.

ThinkServer-Serververwaltung nach einem Verwaltungsserverausfall mit der Management-Controller-Webschnittstelle wiederherstellen

Sie können die Verwaltung eines ThinkServer-Servers mit der Management-Controller-Webschnittstelle wiederherstellen.

Vorgehensweise

Führen Sie zum Wiederherstellen der Serververwaltung die folgenden Schritte aus.

Schritt 1. Melden Sie sich als Administrator wieder an der Management-Controller-Webschnittstelle des Servers an (siehe Management-Controller-Webschnittstelle für einen Server starten).

Schritt 2. Löschen Sie die von Lenovo XClarity Administrator erstellten IPMI-Accounts. Wählen Sie dazu im Hauptmenü die Option „Benutzer“ aus und entfernen Sie alle Benutzeraccounts mit dem Präfix „LXCA_“.

Alternativ können Sie den Accountbenutzernamen umbenennen und das Präfix „LXCA_“ entfernen.

Schritt 3. Löschen Sie die SNMP-Trap-Ziele. Wählen Sie dazu im Hauptmenü die Option **PEF-Verwaltung** aus, klicken Sie auf die Registerkarte **LAN-Ziel** und löschen Sie den Eintrag, der auf die IP-Adresse der XClarity Administrator-Instanz verweist.

Schritt 4. Stellen Sie sicher, dass die NTP-Einstellungen korrekt sind. Wählen Sie dazu im Hauptmenü die Option **NTP-Einstellungen** aus und konfigurieren Sie Datum und Uhrzeit manuell oder stellen Sie eine gültige NTP-Serveradresse bereit.

Verwaltung eines Rack- oder Tower-Servers aufheben

Sie können die Verwaltung eines Rack- oder Tower-Servers durch Lenovo XClarity Administrator beenden. Dieser Vorgang wird als *Aufheben der Verwaltung* bezeichnet.

Vorbereitende Schritte

Sie können XClarity Administrator so konfigurieren, dass die Verwaltung von Einheiten, die für einen bestimmten Zeitraum offline sind, automatisch aufgehoben wird. Dies ist standardmäßig deaktiviert. Um die automatische Aufhebung der Verwaltung von Offline-Einheiten zu aktivieren, klicken Sie im Menü von XClarity Administrator auf **Hardware → Neue Einheiten ermitteln und verwalten** und klicken Sie dann auf **Bearbeiten** neben **Aufheben der Verwaltung von Offline-Einheiten ist deaktiviert**. Wählen Sie anschließend **Aufheben der Verwaltung von Offline-Einheiten aktivieren** aus und legen Sie das Zeitintervall fest. Standardmäßig wird die Verwaltung von Einheiten aufgehoben, nachdem sie 24 Stunden offline waren.

Bevor Sie die Verwaltung eines Rack- oder Tower-Servers aufheben, müssen Sie sicherstellen, dass keine aktiven Jobs für den Server ausgeführt werden.

Wenn Sie das Servermuster und virtuelle Adressen vom Rack- oder Tower-Server entfernen möchten, deaktivieren Sie vor der Verwaltungsaufhebung des Servers das Serverprofil (siehe Ein Serverprofil deaktivieren).

Wenn Call-Home-Funktion in XClarity Administrator aktiviert ist, wird Call-Home-Funktion auf allen verwalteten Gehäusen und Servern deaktiviert, damit keine doppelten Problemdatensätze generiert werden. Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren - anstatt Call-Home-Funktion später auf jeder einzelnen Einheit zu aktivieren (siehe Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren in der Onlinedokumentation von XClarity Administrator).

Zu dieser Aufgabe

Bei der Verwaltungsaufhebung für einen Rack- oder Tower-Server führt Lenovo XClarity Administrator folgende Aktionen aus:

- Löscht die Konfiguration, die für die zentrale Benutzerverwaltung verwendet wird.
- Entfernt das Sicherheitszertifikat des Baseboard Management Controllers (BMC) aus dem XClarity Administrator-Truststore.
- Setzt die Firewallregeln für die Einheit auf die vor der Verwaltung der Einheit festgelegten Einstellungen, wenn Encapsulation auf der Einheit aktiviert ist.
- Entfernt die CIM-Abonnements für die XClarity Administrator-Konfiguration, sodass XClarity Administrator keine Ereignisse mehr vom Rack- oder Tower-Server erhält.
- Deaktiviert Call-Home-Funktion auf dem Rack- oder Tower-Server, sofern Call-Home-Funktion derzeit in XClarity Administrator aktiviert ist.
- Verwirft vom Rack- oder Tower-Server gesendete Ereignisse. Sie können diese Ereignisse behalten, indem Sie die Ereignisse an ein externes Repository wie syslog weiterleiten (siehe Ereignisse weiterleiten).

Wenn Sie die Verwaltung eines Rack- oder Tower-Server aufgehoben haben, behält XClarity Administrator bestimmte Informationen über den Server. Diese Informationen werden erneut angewendet, wenn Sie denselben Rack- oder Tower-Server wieder verwalten.

Wichtig: Im Fall, dass Sie die Verwaltung eines ThinkServer-Servers aufgehoben haben und diesen Server nun mit einer anderen XClarity Administrator-Instanz verwalten, sind die Serverinformationen verloren.

Tipp: Alle Demo-Einheiten, die während der Erstkonfiguration optional hinzugefügt werden, sind Knoten in einem Gehäuse. Um die Verwaltung der Demo-Einheiten aufzuheben, müssen Sie die Gehäuseverwaltung mit der Option **Aufheben der Verwaltung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aufheben.

Vorgehensweise

Gehen Sie wie folgt vor, um die Verwaltung eines Rack- oder Tower-Servers aufzuheben.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Server**, um die Seite Server anzuzeigen.

Schritt 2. Wählen Sie mindestens einen Rack- oder Tower-Server aus, für den die Verwaltung aufgehoben werden soll.

Schritt 3. Klicken Sie auf **Verwaltung aufheben**. Der Dialog „Verwaltung aufheben“ wird angezeigt.

Schritt 4. **Optional:** Wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn das Gerät nicht erreichbar ist**.

Wichtig: Wenn Sie die Verwaltung für Demo-Hardware aufheben, müssen Sie diese Option auswählen.

Schritt 5. Klicken Sie auf **Verwaltung aufheben**.Der Dialog „Verwaltung aufheben“ zeigt den Status jedes Schritts im Verwaltungsaufhebungsprozess an.

Schritt 6. Wenn der Verwaltungsaufhebungsprozess abgeschlossen ist, klicken Sie auf **OK**.

Rack- oder Tower-Server nach fehlerhafter Verwaltungsaufhebung wiederherstellen

Wenn die Verwaltung für einen Converged-, NeXtScale-, System x- oder ThinkServer-Server fehlerhaft aufgehoben wurde, muss der Server erst wiederhergestellt werden, bevor eine erneute Verwaltung möglich ist.

Rack- oder Tower-Server nach fehlerhafter Verwaltungsaufhebung mit „Verwaltung erzwingen“ wiederherstellen

Sie können die Serververwaltung wiederherstellen, indem Sie den Server mit der Option „Verwaltung erzwingen“ wieder verwalten.

Vorgehensweise

Wenn die IP-Adresse von Lenovo XClarity Administrator-Austauschinstanz und ausgefallenem XClarity Administrator identisch ist, können Sie die Einheit wieder über den Account `RECOVERY_ID` und das Kennwort sowie die Option **Verwaltung erzwingen** verwalten (siehe Server verwalten).

System x- oder NeXtScale M4-Server nach fehlerhafter Verwaltungsaufhebung mit dem Management-Controller wiederherstellen

Sie können die System x- oder NeXtScale M4-Serververwaltung mit dem Management-Controller wiederherstellen.

Vorgehensweise

Führen Sie zum Wiederherstellen der Serververwaltung die folgenden Schritte aus.

Schritt 1. Melden Sie sich mit dem Benutzeraccount und dem Kennwort (beides vor der Verwaltung des Servers mit XClarity Administrator festgelegt) an der Management-Controller-Webschnittstelle an.

Schritt 2. Löschen Sie die SNMP-Trap-Einstellungen.

a. Klicken Sie auf **IMM-Verwaltung → Netzwerk**.

b. Klicken Sie auf die Registerkarte **SNMP**.

c. Klicken Sie auf die Registerkarte **Communitys**.

d. Suchen Sie nach dem vorherigen XClarity Administrator-Community-Eintrag, z. B.:
   - **LXCA-IP-Adresse:** 10.240.198.84
   - **LXCA-Host:** LXCA_maqCBlt86d
   - **Community 2:**
   - **Community-Name:** LXCA_maqCBlt86d
   - **Zugriffstyp:** Trap
   - **Empfang von Traps zur Community für bestimmte Hosts zulassen:** 10.240.198.84

e. Entfernen Sie die Werte aus den Feldern für den Community-Eintrag.

f. Klicken Sie auf **Übernehmen**.

Schritt 3. Löschen Sie die Benutzeraccounts.

a. Klicken Sie auf **IMM-Verwaltung → Benutzer**.

b. Klicken Sie auf die Registerkarte **Benutzeraccounts**.

c. Löschen Sie alle XClarity Administrator-Benutzeraccounts sowie Benutzeraccounts mit folgenden Präfixen:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Schritt 4. Verwalten Sie den Server mit Lenovo XClarity Administrator.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.

b. Wählen Sie **Manuelle Eingabe**.

c. Klicken Sie auf **Einzelsystem**, geben Sie die IP-Adresse des zu verwaltenden Servers ein und klicken Sie auf **OK**.

d. Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung am Server an.

e. Klicken Sie auf **Verwalten**.

   Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

f. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

Sie können ThinkSystem-, Converged-, NeXtScale- oder System x M5- oder M6-Server nach einer fehlerhaften Verwaltungsaufhebung wiederherstellen, indem Sie den Management-Controller auf die Werkseinstellungen zurücksetzen.

Sie können die ThinkSystem-, Converged-, NeXtScale- oder System x M5- oder M6-Serververwaltung wiederherstellen, indem Sie den Baseboard Management Controller (BMC) des Servers auf die Werkseinstellungen zurücksetzen.

Vorgehensweise

Führen Sie zum Wiederherstellen der Serververwaltung die folgenden Schritte aus.

Schritt 1. Wenn Encapsulation auf der Einheit aktiviert ist, stellen Sie von einem System, das zur Verwendung der IP-Adresse der ausgefallenen virtuellen XClarity Administrator-Einheit konfiguriert ist, eine Verbindung zum Ziel-Management-Controller her.

Schritt 2. Setzen Sie den Management-Controller auf die Werkseinstellungen zurück.

a. Melden Sie sich mit dem Benutzeraccount und dem Kennwort für die Wiederherstellung (vor der Verwaltung des Servers mit XClarity Administrator festgelegt) an der Management-Controller-Webschnittstelle des Servers an.

b. Klicken Sie auf die Registerkarte **IMM-Verwaltung**.

c. Klicken Sie auf **IMM auf werkseitige Voreinstellungen zurücksetzen**.

d. Klicken Sie auf **OK**, um die Zurücksetzung zu bestätigen.

Wichtig: Nachdem die BMC-Konfiguration abgeschlossen ist, wird der BMC neu gestartet. Wenn es sich um einen lokalen Server handelt, ist die TCP/IP-Verbindung unterbrochen und Sie müssen die Netzwerkschnittstelle neu konfigurieren, um wieder eine funktionsfähige Verbindung herzustellen.

Schritt 3. Melden Sie sich wieder an der Management-Controller-Webschnittstelle des Servers an.

- Der Baseboard Management Controller (BMC) ist anfänglich so konfiguriert, dass er versucht, die IP-Adresse über einen DHCP-Server abzurufen. Ist dies nicht möglich, wird die statische IPv4-Adresse `192.168.70.125` verwendet.
- Für den IMM-BMC sind anfänglich der Benutzername `USERID` und das Kennwort `PASSWORD` (mit einer Null) festgelegt. Dieser Standardbenutzeraccount hat Supervisorzugriff. Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

Schritt 4. Rekonfigurieren Sie die Netzwerkschnittstelle, um wieder eine funktionsfähige Verbindung herzustellen. Weitere Informationen finden Sie unter Onlinedokumentation für Integrated Management Module II.

Schritt 5. Verwalten Sie den Server mit Lenovo XClarity Administrator.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.

b. Wählen Sie **Manuelle Eingabe**.

c. Klicken Sie auf **Einzelsystem**, geben Sie die IP-Adresse des zu verwaltenden Servers ein und klicken Sie auf **OK**.

d. Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung am Server an.

e. Klicken Sie auf **Verwalten**.

Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

f. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

Schritt 6. Sofern der Server mit Konfigurationsmuster konfiguriert wurde, deaktivieren Sie das dem Server zugeordnete Serverprofil.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Serverprofile**. Die Seite „Konfigurationsmuster: Serverprofile“ wird angezeigt.

b. Markieren Sie das Serverprofil und klicken Sie auf das Symbol **Serverprofil deaktivieren** ( ).

c. Klicken Sie auf **ITE ausschalten**, um den Server auszuschalten. Wenn der Server wieder eingeschaltet ist, werden die Zuweisungen für virtuelle Adressen auf die fest integrierten Standardwerte zurückgesetzt.

d. Klicken Sie auf **Deaktivieren**. In der Spalte „Profilstatus“ wechselt der Status des Profils zu „Inaktiv“. Hinweis: Bei einer Profildeaktivierung behalten Server ihre ID-Informationen (z. B. Hostname, IP-Adresse, virtuelle MAC-Adresse).

e. Markieren Sie das Serverprofil erneut und klicken Sie auf das Symbol **Serverprofil aktivieren** ().

f. Klicken Sie auf **Aktivieren**, um die Serverprofile auf dem Server zu aktivieren. In der Spalte „Profilstatus“ wechselt der Status des Profils zu „Aktiv“.

Schritt 7. Falls dem Server eine Konformitätsrichtlinie zugeordnet war, ordnen Sie diese erneut zu.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Übernehmen/Aktivieren**. Die Seite „Firmwareaktualisierungen: anwenden/aktivieren“ wird mit einer Liste der verwalteten Einheiten angezeigt.

b. Wählen Sie die entsprechende Richtlinie für den Server aus dem Dropdown-Menü in der Spalte **Zugeordnete Richtlinie** aus.

ThinkSystem-, Converged-, NeXtScale- oder System x M5- oder M6-Server nach fehlerhafter Verwaltungsaufhebung mit dem Dienstprogramm „cimcli“ wiederherstellen

Sie können die ThinkSystem-, Converged-, NeXtScale- oder System x-Serververwaltung wiederherstellen, indem Sie die CIM-Abonnements mit dem Dienstprogramm `cimcli` löschen.

Vorbereitende Schritte

OpenPegasus mit dem Dienstprogramm „cimcli“ muss auf einem System installiert sein, das Netzwerkzugriff auf den Zielserver hat. Weitere Informationen über den Download, die Konfiguration und die Kompilierung von OpenPegasus finden Sie unter Website zu OpenPegasus-RPMs für Linux.

Anmerkung: In Red Hat Enterprise Linux (RHEL) Server 7 und neueren Versionen sind die Quell- und die binären RPMs von OpenPegasus bereits in der Red Hat-Distribution enthalten. Das Dienstprogramm „cimcli“ ist im Paket `top-pegasus-test.x86_64`.

Zu dieser Aufgabe

Wenn der Server wiederhergestellt ist, können Sie ihn wieder verwalten. Alle Informationen über den Server (z. B. Netzwerkeinstellungen, Serverrichtlinien und Firmwarekonformitätsrichtlinien) bleiben erhalten.

Vorgehensweise

Führen Sie die folgenden Schritte über einen Server aus, der eine verwaltete Authentifizierung von Lenovo XClarity Administrator verwendet und auf dem OpenPegasus installiert ist, um die Serververwaltung wiederherzustellen.

Schritt 1. Wenn Encapsulation auf der Einheit aktiviert ist:

a. Stellen Sie von einem System, das zur Verwendung der IP-Adresse der ausgefallenen virtuellen XClarity Administrator-Einheit konfiguriert ist, eine Verbindung zum Zielserver her.

b. Deaktivieren Sie Encapsulation, indem Sie eine SSH-Sitzung zur Einheit öffnen und folgenden Befehl ausführen:

```
encaps lite off
```

Schritt 2. Führen Sie die folgenden Befehle aus, um die CIM-Instanzen für CIM_ListenerDestinationCIMXML, CIM_Indicationfilter und CIM_IndicationSubscription zu ermitteln.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

Dabei geben <*IP_address*>, <*user_ID*> und <*password*> die IP-Adresse, die Benutzer-ID und das Kennwort für den Management-Controller an. Beispiele:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Schritt 3. Führen Sie den folgenden Befehl aus, um die CIM-Instanzen für CIM_ListenerDestinationCIMXML, CIM_Indicationfilter und CIM_IndicationSubscription nacheinander zu löschen.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

Dabei geben <*IP_address*>, <*user_ID*> und <*password*> die IP-Adresse, die Benutzer-ID und das Kennwort für den Management-Controller an und mit <*cim_instance*> werden die Informationen, die für die einzelnen CIM-Instanzen im vorigen Schritt zurückgegeben wurden, in einfachen Anführungszeichen angegeben. Beispiele:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Schritt 4. Verwalten Sie den Server mit Lenovo XClarity Administrator.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.

b. Wählen Sie **Manuelle Eingabe**.

c. Klicken Sie auf **Einzelsystem**, geben Sie die IP-Adresse des zu verwaltenden Servers ein und klicken Sie auf **OK**.

d. Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung am Server an.

e. Klicken Sie auf **Verwalten**.

   Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

f. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

ThinkServer-Serververwaltung nach fehlerhafter Verwaltungsaufhebung mit der Management-Controller-Webschnittstelle wiederherstellen

Sie können die Verwaltung eines ThinkServer-Servers mit der Management-Controller-Webschnittstelle wiederherstellen.

Vorgehensweise

Führen Sie zum Wiederherstellen der Serververwaltung die folgenden Schritte aus.

Schritt 1. Melden Sie sich als Administrator wieder an der Management-Controller-Webschnittstelle des Servers an (siehe Management-Controller-Webschnittstelle für einen Server starten).

Schritt 2. Löschen Sie die von Lenovo XClarity Administrator erstellten IPMI-Accounts. Wählen Sie dazu im Hauptmenü die Option „Benutzer“ aus und entfernen Sie alle Benutzeraccounts mit dem Präfix „LXCA_“.

   Alternativ können Sie den Accountbenutzernamen umbenennen und das Präfix „LXCA_“ entfernen.

Schritt 3. Löschen Sie die SNMP-Trap-Ziele. Wählen Sie dazu im Hauptmenü die Option **PEF-Verwaltung** aus, klicken Sie auf die Registerkarte **LAN-Ziel** und löschen Sie den Eintrag, der auf die IP-Adresse der XClarity Administrator-Instanz verweist.

Schritt 4. Stellen Sie sicher, dass die NTP-Einstellungen korrekt sind. Wählen Sie dazu im Hauptmenü die Option **NTP-Einstellungen** aus und konfigurieren Sie Datum und Uhrzeit manuell oder stellen Sie eine gültige NTP-Serveradresse bereit.

Kapitel 9. Speichereinheiten verwalten

Lenovo XClarity Administrator kann zahlreiche Speichereinheiten verwalten, darunter Lenovo Storage, Flex System-Speichersysteme und Bandbibliotheken.

Weitere Informationen:  XClarity Administrator: Ermittlung

Vorbereitende Schritte

Achtung: Lesen Sie die Hinweise zur Speicherverwaltung, bevor Sie eine Speichereinheit verwalten.

Anmerkung: Flex System-Speichereinheiten werden automatisch ermittelt und verwaltet, wenn das Gehäuse, in dem sie enthalten sind, verwaltet wird. Flex System-Speichereinheiten können nicht unabhängig vom Gehäuse ermittelt und verwaltet werden.

Für die Kommunikation mit den Einheiten müssen bestimmte Ports verfügbar sein. Stellen Sie sicher, dass alle erforderlichen Ports verfügbar sind, bevor Sie versuchen, Speichereinheiten zu verwalten. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

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

Wichtig: Stellen Sie vor der Ermittlung und Verwaltung von Rack-Speichereinheiten (außer ThinkSystem DE Serie) sicher, dass die folgenden Anforderungen erfüllt sind. Weitere Informationen finden Sie unter Einheit kann nicht erkannt werden und Einheit kann nicht verwaltet werden in der Onlinedokumentation von XClarity Administrator.

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

Zu dieser Aufgabe

XClarity Administrator kann Speichereinheiten in der Umgebung automatisch ermitteln. Dabei wird nach verwaltbaren Einheiten gesucht, die im gleichen IP-Subnetz sind wie XClarity Administrator. Damit Speichereinheiten in anderen Subnetzen ermittelt werden, geben Sie eine IP-Adresse oder einen IP-Adressbereich an oder importieren Sie die Informationen aus einem Arbeitsblatt.

Nachdem die Speichereinheiten von XClarity Administrator verwaltet werden, fragt XClarity Administrator alle verwalteten Speichereinheiten regelmäßig ab, um Informationen zu sammeln, z. B. Bestand, elementare Produktdaten und Status. Sie können jede verwaltete Speichereinheit anzeigen und überwachen sowie Verwaltungsaktionen ausführen (z. B. Systemeinstellungen konfigurieren, Firmware aktualisieren, ein- und ausschalten).

Eine Einheit kann nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie es mit einem anderen XClarity Administrator verwalten möchten,

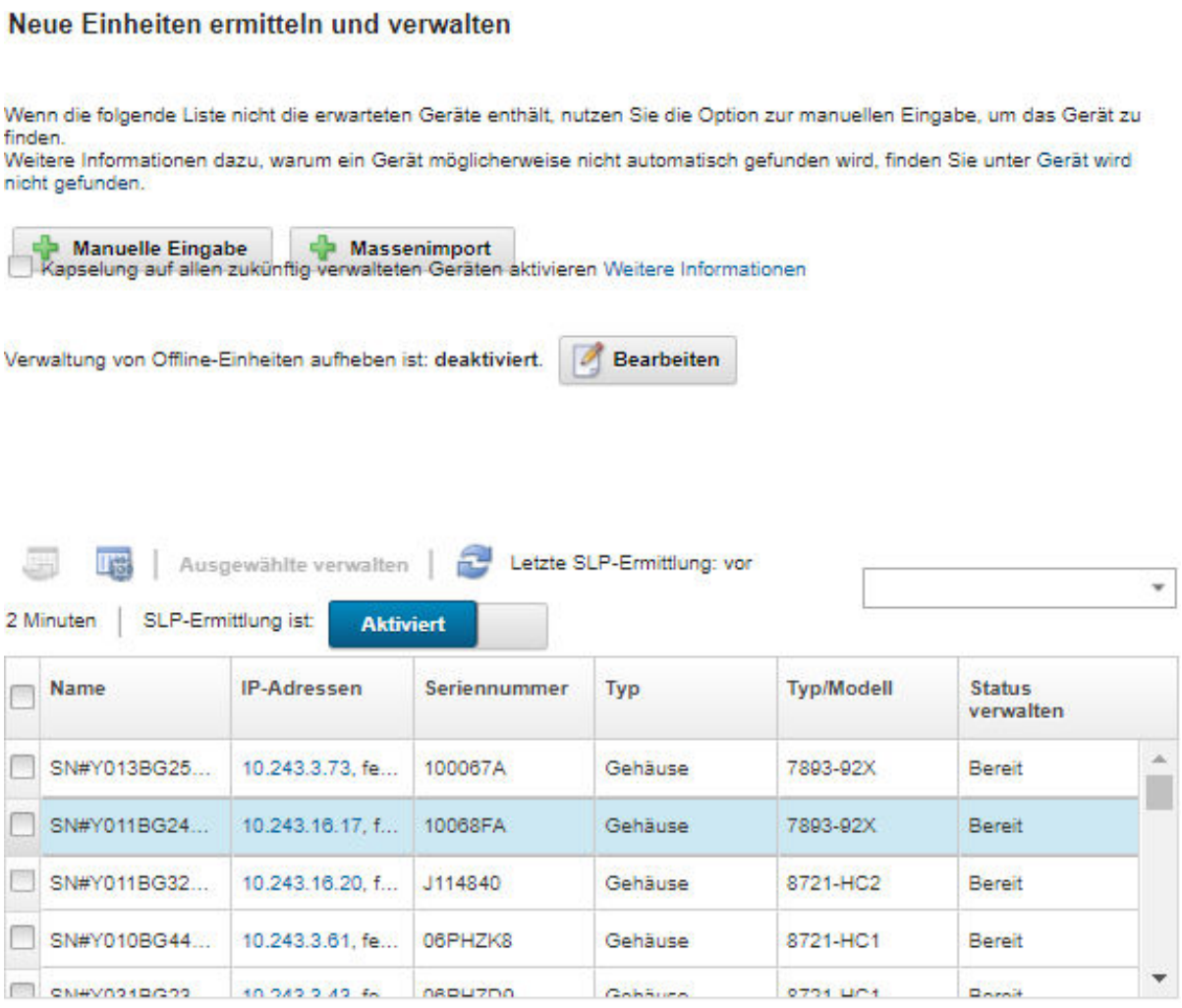
müssen Sie zuerst die erste XClarity Administrator-Verwaltung der Speichereinheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten. Falls bei der Verwaltungsaufhebung ein Fehler auftritt, können Sie bei der Verwaltung die Option **Verwaltung erzwingen** auf dem neuen XClarity Administrator auswählen.

Anmerkung: Wenn Sie das Netzwerk nach verwaltbaren Einheiten durchsuchen, weiß XClarity Administrator nicht, ob eine Einheit bereits von einem anderen Manager verwaltet wird, bis er versucht, die Einheit zu verwalten.

Vorgehensweise

Schließen Sie eine der folgenden Vorgehensweisen ab, um Speichereinheiten mit XClarity Administrator zu verwalten.

- Ermitteln und verwalten Sie eine Vielzahl von Speichereinheiten und anderen Arten von Einheiten mithilfe einer Massenimportdatei (siehe Systeme verwalten in der Onlinedokumentation von XClarity Administrator).
- Ermitteln und verwalten Sie Speichereinheiten, die im gleichen IP-Subnetz sind wie XClarity Administrator.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Neue Einheiten ermitteln und verwalten wird angezeigt.



Sie können die Tabellenspalten sortieren, um die zu verwaltenden Speichereinheiten schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse)

eingeben, um die angezeigten Speichereinheiten weiter zu filtern. Sie können die angezeigten Spalten und die Standard-Sortierreihenfolge ändern, indem Sie auf das Symbol **Spalten anpassen** () klicken.

2. Klicken Sie auf das Symbol **Aktualisieren** (), um alle verwaltbaren Einheiten in der XClarity Administrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
3. Wählen Sie eine oder mehrere zu verwaltende Speichereinheiten aus.
4. Klicken Sie auf **Ausgewählte verwalten**. Das Dialogfenster „Verwalten“ wird angezeigt.
5. Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung an der Speichereinheit an.

   Tipp: Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl, oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).
6. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

   Anmerkungen:

   – Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
   – Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.
7. Klicken Sie auf **Verwalten**.

   Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.
8. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

   Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

   – Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

     Anmerkung: Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.
   – Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
   – Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

   Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

- Ermitteln und verwalten Sie Speichereinheiten, die nicht im gleichen IP-Subnetz sind wie XClarity Administrator, indem Sie die IP-Adressen manuell angeben.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.
  2. Wählen Sie **Manuelle Eingabe**.
  3. Geben Sie die Netzwerkadressen der Speichereinheiten an, die verwaltet werden sollen:
     - Klicken Sie auf **Einzelsystem** und geben Sie einen einzelnen IP-Adress-Domänennamen oder einen vollständig qualifizierten Domänennamen (FQDN) ein.

       Anmerkung: Stellen Sie bei der Angabe eines FQDN sicher, dass ein gültiger Domänenname auf der Seite Netzwerkzugriff angegeben wird (siehe Netzwerkzugriff konfigurieren).
     - Klicken Sie auf **Mehrere Systeme** und geben Sie einen Bereich von IP-Adressen ein. Um einen weiteren Bereich hinzuzufügen, klicken Sie auf das Symbol **Hinzufügen** (). Um einen Bereich zu entfernen, klicken Sie auf das Symbol **Entfernen** ().
  4. Klicken Sie auf **OK**.
  5. Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung an der Speichereinheit an.

     Tipp: Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl, oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).
  6. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

     Anmerkungen:
     - Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
     - Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.
  7. Klicken Sie auf **Verwalten**.

     Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt, um sicherzustellen, dass der Prozess erfolgreich beendet wird.
  8. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

     Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

     Wenn die Verwaltung aufgrund einer der folgenden Fehlerbedingungen nicht erfolgreich war, wiederholen Sie dieses Verfahren mit der Option **Verwaltung erzwingen**.
     - Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

       Anmerkung: Wenn die XClarity Administrator-Austauschinstanz dieselbe IP-Adresse wie der ausgefallene XClarity Administrator verwendet, können Sie die Einheit erneut mit dem RECOVERY_ID-Account und -Kennwort (sofern zutreffend) und der Option **Verwaltung erzwingen** verwalten.
     - Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.

– Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

Nach dieser Aufgabe

- Ermitteln und verwalten Sie weitere Einheiten.
- Aktualisieren Sie die Firmware auf Einheiten, die nicht den aktuellen Richtlinien entsprechen (siehe Firmware auf verwalteten Einheiten aktualisieren).
- Fügen Sie die neuen Einheiten zum entsprechenden Rack hinzu, um die physische Umgebung widerzuspiegeln (siehe Racks verwalten).
- Überwachen Sie den Hardwarestatus und die Details (siehe Status von Speichereinheiten anzeigen).
- Überwachen Sie Ereignisse und Alerts (siehe Ereignisse handhaben und Mit Alerts arbeiten).

Hinweise zur Speicherverwaltung

Lesen Sie die folgenden wichtigen Hinweise, bevor Sie mit der Verwaltung für eine Speichereinheit beginnen.

Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von Lenovo XClarity Administrator.

Wichtig: Stellen Sie vor der Ermittlung und Verwaltung von Rack-Speichereinheiten (außer ThinkSystem DE Serie) sicher, dass die folgenden Anforderungen erfüllt sind. Weitere Informationen finden Sie unter Einheit kann nicht erkannt werden und Einheit kann nicht verwaltet werden in der Onlinedokumentation von XClarity Administrator.

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

Bei Lenovo Storage-Einheiten wird die Lufttemperatur auf Systemebene von dem Temperatursensor gemessen, der sich am dichtesten an der Systemmittelplatine befindet. Er gibt die Umgebungstemperatur des Luftstroms an, nachdem dieser die Platten passiert hat. Beachten Sie, dass die vom XClarity Administrator und die vom Management-Controller gemeldete Lufttemperatur abweichen kann, falls die Temperatur zu verschiedenen Zeitpunkten erfasst wird.

Bei Speichereinheiten der Lenovo DE Serie müssen beide Management-Controller während der ersten Verwaltung im Netzwerk erreichbar sein.

Für einige Speichereinheiten sind SNMP-Traps nur auf Englisch verfügbar.

Status von Speichereinheiten anzeigen

Sie können eine Zusammenfassung und den detaillierten Status für verwaltete Speichereinheiten über Lenovo XClarity Administrator anzeigen.

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

Zu dieser Aufgabe

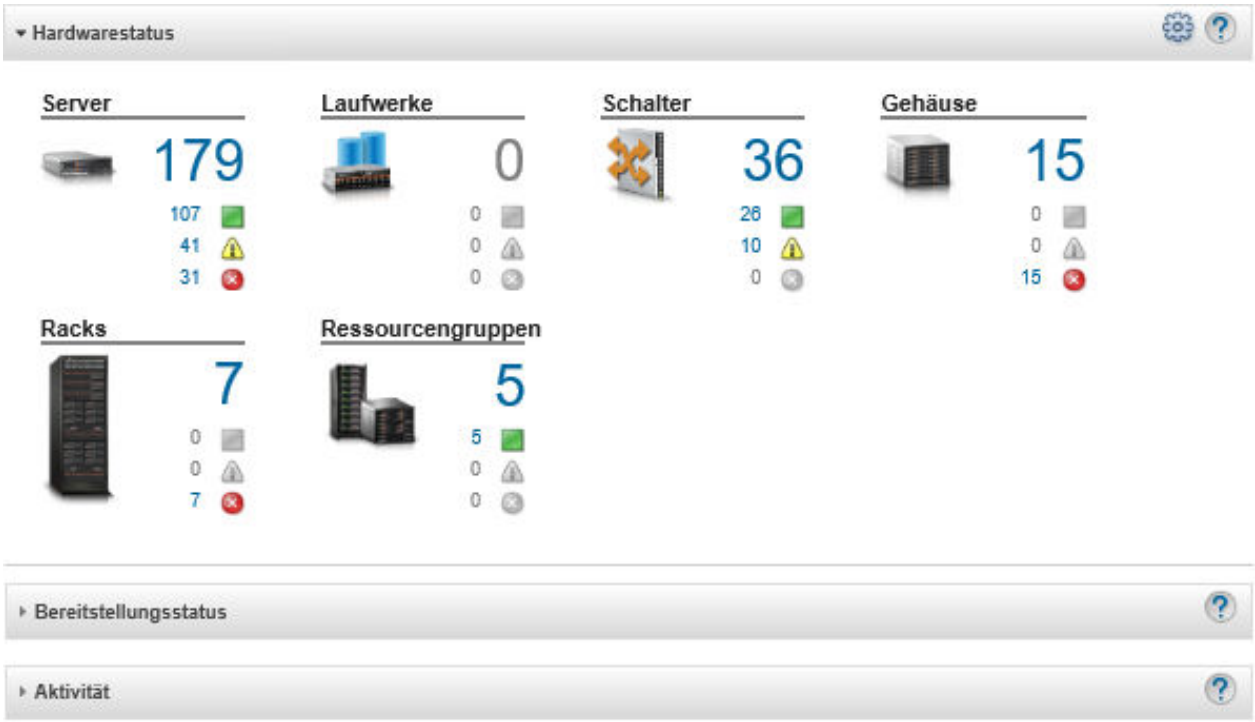
Die folgenden Statussymbole geben den allgemeinen Status der Einheit an. Wenn die Zertifikate nicht übereinstimmen, wird „(nicht vertrauenswürdig)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (nicht vertrauenswürdig)“. Wenn ein Verbindungsproblem besteht oder eine Verbindung zur Einheit nicht vertrauenswürdig ist, wird „(Verbindung)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (Verbindung)“.

- ( ) Kritisch
- ( ) Warnung
- ( ) Ausstehend
- ( ) Information
- ( ) Normal
- ( ) Offline
- ( ) Nicht bekannt

Vorgehensweise

Führen Sie eine oder mehrere der folgenden Aktionen aus, um den Status für eine verwaltete Speichereinheit anzuzeigen.

- Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Dashboard**. Die Seite „Dashboard“ wird mit einer Übersicht und dem Status aller verwalteten Speichereinheiten und anderen Ressourcen angezeigt.



- Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Hardware → Speicher**. Die Seite Storage wird mit einer Tabellenansicht aller Speichereinheiten, die im verwalteten Gehäuse installiert sind, geöffnet.

  Sie können die Tabellenspalten sortieren, um die zu verwaltenden Speichereinheiten schneller zu finden. Darüber hinaus können Sie zum weiteren Filtern der Gehäuse Text (z. B. einen Systemnamen oder eine IP-Adresse) im Feld **Filter** eingeben und auf die Statussymbole klicken, um nur die Speichereinheiten aufzulisten, die den ausgewählten Kriterien entsprechen.

  Über diese Seite können Sie die folgenden Aktionen ausführen:

  - Zeigen Sie ausführliche Informationen über die Speichereinheit und die zugehörigen Komponenten an (siehe Die Details einer Speichereinheit anzeigen).
  - Zeigen Sie eine Speichereinheit in einer grafischen Rack- oder Gehäuseansicht an. Klicken Sie dazu auf **Alle Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Alle Aktionen → Anzeigen → In der Gehäuseansicht anzeigen**.
  - Starten Sie die Management-Controller-Webschnittstelle für die Speichereinheit. Klicken Sie dazu auf die Verknüpfung **IP-Adresse** (siehe Management-Controller-Webschnittstelle für eine Speichereinheit starten).
  - Schalten Sie den Speichercontroller in der Speichereinheit ein und aus (siehe Eine Speichereinheit ein- und ausschalten).
  - Ändern Sie die Systeminformationen. Markieren Sie dazu eine Speichereinheit und klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**.
  - Aktualisieren Sie den Bestand. Markieren Sie dazu eine Speichereinheit und klicken Sie auf **Alle Aktionen → Bestand → Bestand aktualisieren**.
  - Exportieren Sie ausführliche Informationen über eine oder mehrere Speichereinheiten in eine CSV-Datei. Markieren Sie dazu die Speichereinheiten und klicken Sie auf **Alle Aktionen → Bestand → Bestand exportieren**.

    Anmerkung: Sie können Bestandsdaten für maximal 60 Einheiten gleichzeitig exportieren.

    Tipp: Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
  - Heben Sie die Verwaltung der Speichereinheit auf (siehe Verwaltung einer Speichereinheit aufheben).
  - (Nur Flex System-Speichereinheiten) Setzen Sie den Speichercontroller in der Speichereinheit virtuell neu ein (siehe Speichercontroller in Flex System-Speichereinheit virtuell neu einsetzen).
  - Schließen Sie belanglose Ereignisse auf allen Seiten aus, auf denen Ereignisse angezeigt werden. Klicken Sie dazu auf das Symbol **Ereignisse ausschließen** ( ). (siehe Ereignisse ausschließen).
  - Beheben Sie mögliche Probleme zwischen dem Sicherheitszertifikat von Lenovo XClarity Administrator und dem CMM-Sicherheitszertifikat im Gehäuse, in dem die Speichereinheit installiert ist. Markieren Sie

dazu eine Speichereinheit und klicken Sie auf **Alle Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen** (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).

– Sie können eine Speichereinheit zu einer statischen Ressourcengruppe hinzufügen oder daraus entfernen, indem Sie auf **Alle Aktionen → Gruppen → Zu Gruppe hinzufügen** oder **Alle Aktionen → Gruppen → Aus Gruppe entfernen** klicken.

Die Details einer Speichereinheit anzeigen

Sie können mit Lenovo XClarity Administrator ausführliche Informationen über verwaltete Speichereinheiten anzeigen, z. B. IP-Adresse, Produktname, Seriennummer und Einschubdetails.

Zu dieser Aufgabe

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

Bei Lenovo Storage-Einheiten wird die Lufttemperatur auf Systemebene von dem Temperatursensor gemessen, der sich am dichtesten an der Systemmittelplatine befindet. Er gibt die Umgebungstemperatur des Luftstroms an, nachdem dieser die Platten passiert hat. Beachten Sie, dass die vom XClarity Administrator und die vom Management-Controller gemeldete Lufttemperatur abweichen kann, falls die Temperatur zu verschiedenen Zeitpunkten erfasst wird.

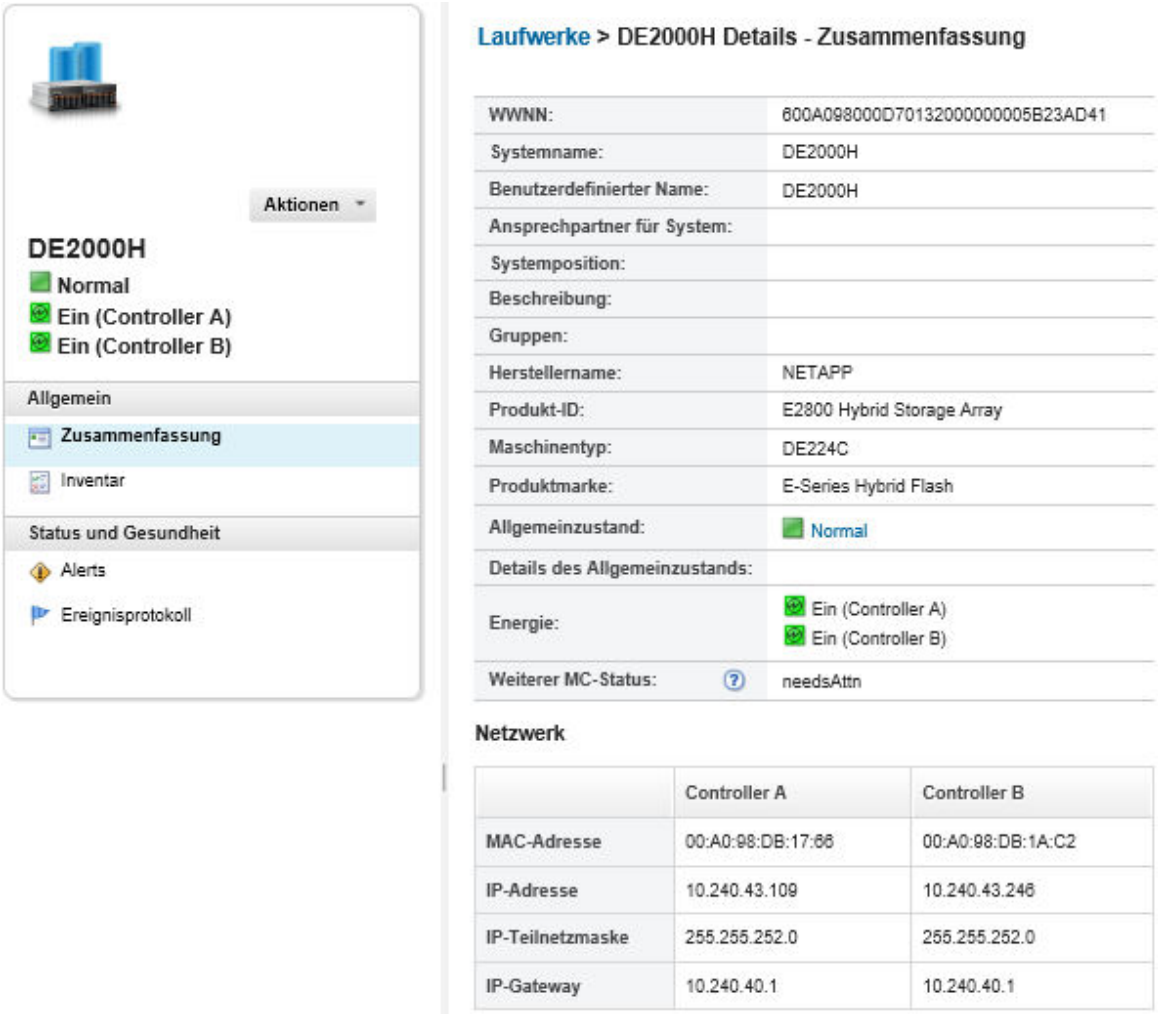
Vorgehensweise

Gehen Sie wie folgt vor, um die Details für eine bestimmte verwaltete Speichereinheit anzuzeigen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Speicher**. Die Seite Storage wird mit einer Tabellenansicht aller Speichereinheiten, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Speichereinheiten zu erleichtern. Darüber hinaus können Sie Text (z. B. einen Systemnamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Speichereinheiten weiter zu filtern.

Schritt 2. Klicken Sie in der Spalte **Storage** auf den Namen der Speichereinheit. Die Seite „Zusammenfassung“ wird mit den Eigenschaften und einer Liste der für die Speichereinheit installierten Komponenten angezeigt.



Schritt 3. Führen Sie eine oder mehrere der folgenden Aktionen aus, um die Speicherdetails anzuzeigen. Die angezeigten Daten können je nach Art der Speichereinheit unterschiedlich sein.

- Klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung für den Server und die installierten Komponenten einschließlich der Systeminformationen und der installierten Einheiten anzuzeigen (siehe Status von Speichereinheiten anzeigen).
- Klicken Sie auf **Inventardetails**, um Details zu den Komponenten der Speichereinheit anzuzeigen. Dazu gehören:
  - Firmwareversionen für die Speichereinheit
  - Details des Management-Controller-Netzwerks, z. B. Hostname, IPv4-Adresse, IPv6-Adresse und MAC-Adressen
  - Anlagendetails der Speichereinheit
  - Details zu jedem Einschub in der Speichereinheit

  Tipp: Wenn ein Erweiterungsknoten (wie z. B. ein Flex System Storage Expansion Node oder ein Flex System PCIe Expansion Node) im Gehäuse installiert und mit einer Speichereinheit verbunden ist, werden auch die Bestandsdetails für den Erweiterungsknoten angezeigt.
- Klicken Sie auf **Alerts**, um Alerts für die Speichereinheit in der Alert-Liste anzuzeigen (siehe Mit Alerts arbeiten).
- Klicken Sie auf **Ereignisprotokoll**, um die der Speichereinheit zugeordneten Ereignisse im Ereignisprotokoll anzuzeigenSpeichereinheit (siehe Ereignisse handhaben).

- Klicken Sie auf **Jobs**, um eine Liste der dieser Speichereinheit zugeordneten Jobs anzuzeigen (siehe Jobs überwachen).
- Klicken Sie auf **Light Path**, um den derzeitigen Status aller Anzeigen der Speichereinheit anzuzeigen.
- Klicken Sie auf **Strom und Temperatur**, um die Energie- und Temperatureigenschaften für die Speichereinheit anzuzeigen.

  Tipp: Verwenden Sie die Aktualisierungsschaltfläche des Webbrowsers, um die neuesten Strom- und Temperaturdaten zu erfassen. Die Datenerfassung kann mehrere Minuten in Anspruch nehmen.

Nach dieser Aufgabe

Außer der Anzeige von Übersichts- und Detailinformationen zu einer Speichereinheit können Sie die folgenden Aktionen durchführen:

- Zeigen Sie eine Speichereinheit in einer grafischen Rack- oder Gehäuseansicht an. Klicken Sie dazu auf **Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Aktionen → Anzeigen → In der Gehäuseansicht anzeigen**.
- Exportieren Sie ausführliche Informationen über die Speichereinheit in eine CSV-Datei. Klicken Sie dazu auf **Aktionen → Bestand → Bestand exportieren**.

  Anmerkungen:

  – Weitere Informationen zu Bestandsdaten in der CSV-Datei finden Sie unter GET /storage/<*UUID_list*> REST API in der Onlinedokumentation zu Lenovo XClarity Administrator.

  – Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Starten Sie die Management-Controller-Webschnittstelle für die Speichereinheit. Klicken Sie dazu auf die Verknüpfung **IP-Adresse** (siehe Management-Controller-Webschnittstelle für eine Speichereinheit starten).
- Schalten Sie den Speichercontroller in der Speichereinheit ein und aus (siehe Eine Speichereinheit ein- und ausschalten).
- Setzen Sie den Speichercontroller für die Speichereinheit virtuell neu ein (siehe Server in einem Flex System-Gehäuse virtuell neu einsetzen).
- Ändern Sie die Systeminformationen. Markieren Sie dazu eine Speichereinheit und klicken Sie auf **Eigenschaften bearbeiten**.
- Aktualisieren Sie den Bestand. Markieren Sie dazu eine Speichereinheit und klicken Sie auf **Aktionen → Bestand → Bestand aktualisieren**.
- Schließen Sie belanglose Ereignisse auf allen Seiten aus, auf denen Ereignisse angezeigt werden. Klicken Sie dazu auf **Aktionen → Servicerücksetzung → Ereignisse ausschließen** (siehe Ereignisse ausschließen).
- Beheben Sie mögliche Probleme zwischen dem Sicherheitszertifikat von XClarity Administrator und dem CMM-Sicherheitszertifikat im Gehäuse, in dem die Speichereinheit installiert ist. Markieren Sie dazu eine Speichereinheit und klicken Sie auf **Aktionen → Service → Nicht vertrauenswürdige Zertifikate auflösen** (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).

Speicherkonfigurationsdaten sichern und wiederherstellen

Lenovo XClarity Administrator enthält keine integrierten Sicherungsfunktionen für Speicherkonfigurationsdaten. Verwenden Sie stattdessen die Sicherungsfunktionen, die für Ihre verwaltete Speichereinheit verfügbar sind.

Informationen zur Wiederherstellung der Einheit finden Sie in der Produktdokumentation, die mit Ihrer Speichereinheit geliefert wird.

- Informationen zu Lenovo Storage-Einheiten finden Sie in der Produktdokumentation für Lenovo Storage S2200/S3200.
- Informationen zu Lenovo ThinkSystem-Speichereinheit finden Sie unter ThinkSystem Storage-Produktdokumentation.

Eine Speichereinheit ein- und ausschalten

Sie können eine Speichereinheit über Lenovo XClarity Administrator ein- und ausschalten.

Zu dieser Aufgabe

Wenn ein Speichercontroller einer Flex System-Speichereinheit ausgeschaltet wird, werden die Daten zunächst auf dem internen Laufwerk gespeichert und die Speichereinheit geht in einen Standby-Modus. Im Standby-Modus kann auf die von der Speichereinheit bereitgestellten Volumes nicht mehr zugegriffen werden.

Um eine Speichereinheit der ThinkSystem DM Serie einzuschalten, stellen Sie sicher, dass der für die Verwaltung verwendete Speichercontroller online ist und dass dessen IP-Adresse direkt mit dem Serviceprozessor des ausgeschalteten Speichercontrollers über das externe Netzwerk kommunizieren kann.

Vorgehensweise

Gehen Sie wie folgt vor, um eine verwaltete Speichereinheit ein- und auszuschalten.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Speicher**. Die Seite Storage wird mit einer Tabellenansicht aller Speichereinheiten, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Suche nach einer bestimmten Speichereinheit zu erleichtern. Darüber hinaus können Sie Text (z. B. einen Systemnamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Speichereinheiten weiter zu filtern.

Schritt 2. Wählen Sie die ein- oder auszuschaltende Speichereinheit aus.

Schritt 3. Klicken Sie auf **Alle Aktionen** und dann auf eine der folgenden Stromversorgungsaktionen:

- **Controller A einschalten**
- **Controller B einschalten**
- **Controller A ausschalten**

- **Controller B ausschalten**
- **Controller A neu starten**
- **Controller B neu starten**

Speichercontroller in Flex System-Speichereinheit virtuell neu einsetzen

Sie können einen Speichercontroller (Einschub) virtuell neu einsetzen und somit simulieren, dass der Speichercontroller aus der Position entfernt und erneut wieder eingesetzt wurde.

Zu dieser Aufgabe

Beim diesem virtuellen neuen Einsetzen gehen alle bestehenden Netzwerkverbindungen zur Speichereinheit verloren und der Stromversorgungsstatus der Speichereinheit ändert sich. Stellen Sie vor einem virtuellen neuen Einsetzen sicher, dass Sie alle Benutzerdaten gespeichert haben.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Speichercontroller virtuell neu einzusetzen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Hardware → Speicher**. Die Seite Storage wird mit einer Tabellenansicht aller Speichereinheiten geöffnet.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Speichereinheiten zu erleichtern. Darüber hinaus können Sie Text (z. B. einen Systemnamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Speichereinheiten weiter zu filtern.

Schritt 2. Wählen Sie die Flex System-Speichereinheit aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Service** und dann auf **Controller A virtuell neu einsetzen** oder **Controller B virtuell neu einsetzen**.

Schritt 4. Klicken Sie auf **Virtuell erneut einsetzen**.

Management-Controller-Webschnittstelle für eine Speichereinheit starten

Sie können die Management-Controller-Webschnittstelle für das Gehäuse, in dem die Speichereinheit installiert ist, über Lenovo XClarity Administrator starten.

Vorgehensweise

Gehen Sie wie folgt vor, um die Management-Controller-Webschnittstelle zu starten.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Speicher**. Die Seite Storage wird mit einer Tabellenansicht aller verwalteten Speichereinheiten geöffnet.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Speichereinheiten zu erleichtern. Darüber hinaus können Sie Text (z. B. einen Einheitennamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Speichereinheiten weiter zu filtern.

Schritt 2. Wählen Sie die Speichereinheit aus.

Schritt 3. Klicken Sie auf **Aktionen → Starten → Verwaltungswebschnittstelle**. Die Management-Controller-Webschnittstelle wird gestartet.

Schritt 4. Melden Sie sich an der Management-Controller-Webschnittstelle an.

Anmerkung: Bei Flex System-Speichereinheiten verwenden Sie die Benutzeranmeldeinformationen von XClarity Administrator.

Die Systemeigenschaften für eine Speichereinheit ändern

Sie können die Systemeigenschaften für eine bestimmte Speichereinheit ändern.

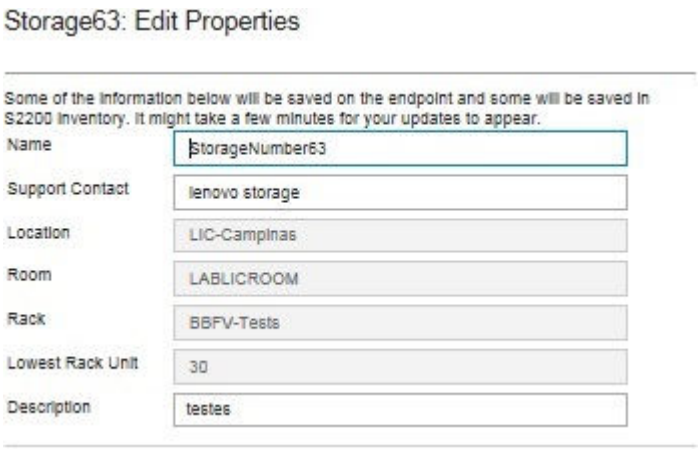
Vorgehensweise

Gehen Sie wie folgt vor, um die Systemeigenschaften zu ändern.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Hardware → Storage**, um die Seite Storage anzuzeigen.

Schritt 2. Wählen Sie die zu aktualisierende Speichereinheit aus.

Schritt 3. Klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**, um den Dialog Bearbeiten anzuzeigen.



Schritt 4. Ändern Sie gegebenenfalls die folgenden Daten:
- Name
- Wenden Sie sich an den Support
- Beschreibung

Anmerkung: Die Eigenschaften für Position, Raum, Rack und unterstes Rack werden von XClarity Administrator aktualisiert, wenn Sie Einheiten über die Webschnittstelle zu einem Rack hinzufügen oder daraus entfernen (siehe Racks verwalten).

Schritt 5. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie diese Eigenschaften ändern, kann es einen Moment dauern, bis die Änderungen in der XClarity Administrator-Webschnittstelle angezeigt werden.

Verwaltung einer Rack-Speichereinheit nach einem Verwaltungsserverausfall wiederherstellen

Wenn die Verwaltung für eine Rack-Speichereinheit fehlerhaft aufgehoben wurde, muss die Speichereinheit erst wiederhergestellt werden, bevor eine erneute Verwaltung möglich ist. Sie können die Verwaltung wiederherstellen, indem Sie für die Speichereinheit bestimmte Konfigurationsbereiche löschen, die zuvor von Lenovo XClarity Administrator definiert wurden.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um eine Rack-Speichereinheit wiederherzustellen.

- Wenn die IP-Adresse von XClarity Administrator-Austauschinstanz und ausgefallenem XClarity Administrator identisch ist, können Sie die Einheit über die Option **Verwaltung erzwingen** wieder verwalten (siehe Speichereinheiten verwalten).
- Entfernen Sie alle Benutzeraccounts mit dem Präfix „LXCA_“ und optional auch Benutzeraccounts mit dem Präfix „SYSMGR_“ und geben Sie dann über die Speichereinheit „SNMPv3“ ein.

Nach dieser Aufgabe

Nachdem XClarity Administrator wiederhergestellt oder ausgetauscht wurde, können Sie die Speichereinheit wieder verwalten (siehe Speichereinheiten verwalten). Alle Informationen über die Speichereinheit (z. B. die Systemeigenschaften) bleiben erhalten.

Verwaltung einer Speichereinheit der Lenovo ThinkSystem DE Serie nach einem Verwaltungsserverausfall wiederherstellen

Wenn die Verwaltung für eine Speichereinheit der Lenovo ThinkSystem DE Serie fehlerhaft aufgehoben wurde, muss die Speichereinheit erst wiederhergestellt werden, bevor eine erneute Verwaltung möglich ist. Sie können die Verwaltung wiederherstellen, indem Sie für die Speichereinheit bestimmte Konfigurationsbereiche löschen, die zuvor von Lenovo XClarity Administrator definiert wurden.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um eine Speichereinheit der Lenovo ThinkSystem DE Serie wiederherzustellen.

- Wenn die IP-Adresse von XClarity Administrator-Austauschinstanz und ausgefallenem XClarity Administrator identisch ist, können Sie die Einheit über die Option **Verwaltung erzwingen** wieder verwalten (siehe Speichereinheiten verwalten).
- Entfernen Sie den Schlüsselpaareintrag „LXCA_REMOTE_MANAGMENT_VERIFICATION“ aus der Schlüsselpaar-API der Speichereinheit.

Nach dieser Aufgabe

Nachdem XClarity Administrator wiederhergestellt oder ausgetauscht wurde, können Sie die Speichereinheit wieder verwalten (siehe Speichereinheiten verwalten). Alle Informationen über die Speichereinheit (z. B. die Systemeigenschaften) bleiben erhalten.

Verwaltung einer Speichereinheit aufheben

Sie können die Verwaltung einer Speichereinheit durch Lenovo XClarity Administrator aufheben. Dieser Vorgang wird als *Aufheben der Verwaltung* bezeichnet.

Vorbereitende Schritte

Bevor Sie die Verwaltung einer Speichereinheit aufheben, müssen Sie sicherstellen, dass für den Switch keine aktiven Jobs ausgeführt werden.

Zu dieser Aufgabe

Wenn Sie die Verwaltung einer Speichereinheit aufgehoben haben, behält XClarity Administrator bestimmte Informationen über die Speichereinheit. Diese Informationen werden erneut angewendet, wenn Sie dieselbe Speichereinheit wieder verwalten.

Tipp: Alle Demo-Einheiten, die während der Erstkonfiguration optional hinzugefügt werden, sind Knoten in einem Gehäuse. Um die Verwaltung der Demo-Einheiten aufzuheben, müssen Sie die Gehäuseverwaltung mit der Option **Aufheben der Verwaltung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aufheben.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verwaltung einer Speichereinheit aufzuheben.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Storage**, um die Seite Storage anzuzeigen.

Schritt 2. Wählen Sie eine oder mehrere Speichereinheiten aus der Liste der verwalteten Switches aus.

Schritt 3. Klicken Sie auf **Verwaltung aufheben**. Der Dialog „Verwaltung aufheben“ wird angezeigt.

Schritt 4. **Optional:** Wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn das Gerät nicht erreichbar ist**.

Wichtig: Wenn Sie die Verwaltung für Demo-Hardware aufheben, müssen Sie diese Option auswählen.

Schritt 5. Klicken Sie auf **Verwaltung aufheben**.Der Dialog „Verwaltung aufheben“ zeigt den Status jedes Schritts im Verwaltungsaufhebungsprozess an.

Schritt 6. Wenn der Verwaltungsaufhebungsprozess abgeschlossen ist, klicken Sie auf **OK**.

Rack-Speichereinheit nach fehlerhafter Verwaltungsaufhebung wiederherstellen

Wenn Lenovo XClarity Administrator eine Rack-Speichereinheit verwaltet und XClarity Administrator ausfällt, können Sie die Verwaltungsfunktionen bis zur Wiederherstellung bzw. bis zum Austausch des Verwaltungsservers wiederherstellen. Sie können die Systemverwaltung wiederherstellen, indem Sie für die Speichereinheit bestimmte Konfigurationsbereiche löschen, die zuvor von XClarity Administrator definiert wurden.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um eine Rack-Speichereinheit wiederherzustellen.

- Wenn die IP-Adresse von XClarity Administrator-Austauschinstanz und ausgefallenem XClarity Administrator identisch ist, können Sie die Einheit über die Option **Verwaltung erzwingen** wieder verwalten (siehe Speichereinheiten verwalten).
- Entfernen Sie alle Benutzeraccounts mit dem Präfix „LXCA_“ und optional auch Benutzeraccounts mit dem Präfix „SYSMGR_“ und geben Sie dann über die Speichereinheit „SNMPv3“ ein.

Nach dieser Aufgabe

Nachdem XClarity Administrator wiederhergestellt oder ausgetauscht wurde, können Sie die Speichereinheit wieder verwalten (siehe Speichereinheiten verwalten). Alle Informationen über die Speichereinheit (z. B. die Systemeigenschaften) bleiben erhalten.

Kapitel 10. Switches verwalten

Lenovo XClarity Administrator kann Netzwerkswitches verwalten.

Weitere Informationen:

- XClarity Administrator: Ermittlung
- XClarity Administrator: Switches verwalten

Vorbereitende Schritte

Achtung: Lesen Sie die Hinweise zum Verwalten von Switches, bevor Sie damit für einen Switch beginnen. Informationen hierzu finden Sie unter Hinweise zur Verwaltung von Switches.

Anmerkung: Flex-Switches werden automatisch ermittelt und verwaltet, wenn das Gehäuse, in dem sie enthalten sind, verwaltet wird. Sie können Flex-Switches nicht unabhängig vom Gehäuse ermitteln und verwalten.

Für die Kommunikation mit den Switches müssen bestimmte Ports verfügbar sein. Stellen Sie sicher, dass alle erforderlichen Ports zur Verfügung stehen, bevor Sie die Verwaltung eines Switches in Angriff nehmen. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

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

Stellen Sie sicher, dass Sie vor der Verwaltung von Rack-Switches gespeicherte Anmeldeinformationen in XClarity Administrator erstellen. XClarity Administrator verwendet nur gespeicherte Anmeldeinformationen für die Authentifizierung der Rack-Switches. Die gespeicherte Anmeldeinformationen müssen mit einem aktiven Benutzeraccount auf der Einheit übereinstimmen. Sie können gespeicherte Anmeldeinformationen über die Dialogfelder zur Verwaltung oder auf der Seite „Gespeicherte Anmeldeinformationen“ erstellen. Siehe Gespeicherte Anmeldeinformationen verwalten für weitere Informationen.

Die Verwaltung mit Loopback-Schnittstellen wird für alle RackSwitch-Einheiten unterstützt. Stellen Sie sicher, dass XClarity Administrator eine Verbindung zur Loopback-Schnittstelle herstellen kann, entweder durch Hinzufügen einer statischen Route oder durch Übermittlung der Adresse über ein Routing-Protokoll. Beachten Sie, dass kein Routing zwischen dem Verwaltungsport und *beliebigen* Datenports (einschließlich Loopback) möglich ist.

Für Switches der Lenovo ThinkSystem DB Serie:

- FOS 8.2.3 oder höher ist erforderlich
- Stellen Sie sicher, dass Sie den SNMPv3-Benutzer bei Index 1 auf dem Switch konfigurieren, *bevor* Sie den Switch verwalten, indem Sie den folgenden Befehl auf dem Switch ausführen: `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw`
- Vergewissern Sie sich, dass REST auf dem Switch aktiviert ist. Führen Sie den folgenden Befehl aus, um REST zu aktivieren: `mgmtapp --enable rest`
- Stellen Sie sicher, dass die Anzahl der zulässigen REST-Sitzungen 10 ist. Führen Sie den folgenden Befehl aus, um die Anzahl der REST-Sitzungen festzulegen: `mgmtapp --config -maxrestsession 10`

- Switches der Lenovo ThinkSystem DB Serie können nicht mithilfe von Service-Ermittlungsprotokollen ermittelt werden. Um diese Switches zu verwalten, verwenden Sie die Option **Manuelle Eingabe**, deaktivieren Sie **Benutzerservice-Ermittlungsprotokolle zur Identifizierung des Einheitentyps** und wählen Sie anschließend „Switch der Lenovo ThinkSystem DB Serie“ aus der Liste **Einheitentyp** aus. Weitere Details finden Sie in der folgenden Vorgehensweise zum Ermitteln und Verwalten von Switches, die sich nicht im selben IP-Subnetz wie XClarity Administrator befinden.

Für NVIDIA-Switches:

- Cumulus 4.3 oder höher ist erforderlich
- NVIDIA-Switches können nicht mithilfe von Service-Ermittlungsprotokollen ermittelt werden. Um diese Switches zu verwalten, verwenden Sie die Option **Manuelle Eingabe**, deaktivieren Sie Benutzerservice-Ermittlungsprotokolle zur Identifizierung des Einheitentyps und wählen Sie anschließend „NVIDIA-Switch“ aus der Liste **Einheitentyp** aus. Weitere Details finden Sie in der folgenden Vorgehensweise zum Ermitteln und Verwalten von Switches, die sich nicht im selben IP-Subnetz wie XClarity Administrator befinden.

Zu dieser Aufgabe

XClarity Administrator kann RackSwitch-Switches in der Umgebung automatisch ermitteln. Dabei wird nach verwaltbaren Einheiten gesucht, die im gleichen IP-Subnetz wie XClarity Administrator sind. Um Switches zu ermitteln, die sich in anderen Subnetzen befinden, geben Sie eine IP-Adresse bzw. einen IP-Adressbereich an oder importieren Sie Informationen von einem Arbeitsblatt.

Anmerkung: Manuelle Anmeldeinformationen werden für Rack-Switches in XClarity Administrator nicht unterstützt.

Nachdem die Switches von XClarity Administrator verwaltet werden, fragt XClarity Administrator alle verwalteten Switches regelmäßig ab, um Informationen zu sammeln, z. B. Bestandsdaten, elementare Produktdaten und Status. Sie können alle verwalteten Switches anzeigen und überwachen sowie Verwaltungstasks ausführen, beispielsweise einen Start der Verwaltungskonsole und Ein- oder Ausschalten.

Falls XClarity Administrator beim Erfassen von Bestandsdaten während des Verwaltungsprozesses die Kommunikation mit dem Switch verliert (z. B. wegen eines Stromausfalls oder Netzwerkfehlers oder wenn der Switch offline ist), wird die Verwaltung erfolgreich abgeschlossen, allerdings sind einige Bestandsinformationen möglicherweise unvollständig. Warten Sie, bis der Switch wieder online ist und XClarity Administrator den Bestand vom Switch abfragt oder erfassen Sie den Bestand vom Switch manuell. Rufen Sie dazu die Seite „Switches“ auf, wählen den Switch auf und klicken auf **Alle Aktionen → Bestand → Bestand aktualisieren**.

Anmerkung: Switches können gestapelt werden. Ein *Stacking-Switch* ist eine Gruppe von Switches, die als einzelner Netzwerkswitch betrieben werden. Der Stack enthält einen *Master-Switch* und einen oder mehrere *Member-Switches*. Bei Flex-Switches können Sie alle Switches im Stack anzeigen und überwachen sowie Diagnosedaten sammeln. Allerdings gilt für alle Stacking-Switches, dass keine Verwaltungstasks wie z. B. Firmwareaktualisierungen und Serverkonfigurationen ausgeführt werden können. Diese XClarity Administrator-Verwaltungstasks sind für sämtliche Stacking-Switches einschließlich des Master-Switches deaktiviert. Firmwareaktualisierungen auf dem Stacking-Switch sind direkt über die Befehlszeilenschnittstelle des Master-Switches ausführbar. Bei RackSwitch-Switches können Sie nur die Informationen über den Master-Switch anzeigen und überwachen. Die Member-Switches werden von XClarity Administrator nicht ermittelt.

Die Verwaltungstasks sind auch für Flex-Switches im Schutzmodus deaktiviert.

Eine Einheit kann nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie es mit einem anderen XClarity Administrator verwalten möchten,

müssen Sie zuerst die erste XClarity Administrator-Verwaltung der Speichereinheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten. Falls bei der Verwaltungsaufhebung ein Fehler auftritt, können Sie bei der Verwaltung die Option **Verwaltung erzwingen** auf dem neuen XClarity Administrator auswählen.

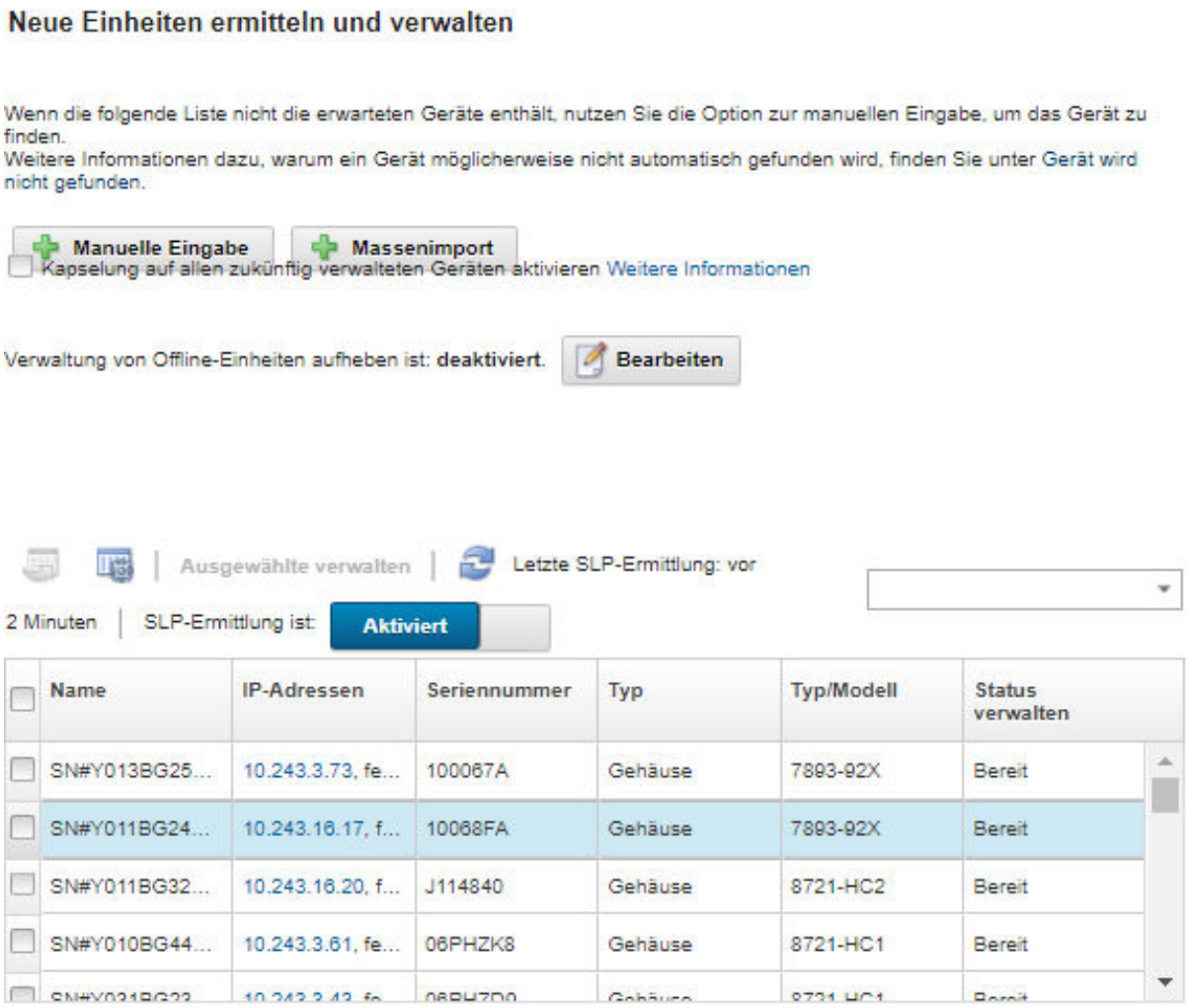
Anmerkung: Wenn Sie das Netzwerk nach verwaltbaren Einheiten durchsuchen, weiß XClarity Administrator nicht, ob eine Einheit bereits von einem anderen Manager verwaltet wird, bis er versucht, die Einheit zu verwalten.

Wenn ein Switch entweder direkt über SSH oder indirekt über ein CMM verwaltet wird, erkennt XClarity Administrator ihn als verwalteten Switch. Die notwendige Konfiguration für Interaktionen erfolgt und der Bestand wird erfasst.

Vorgehensweise

Verwenden Sie eine der folgenden Vorgehensweisen, um die RackSwitch-Switches mit XClarity Administrator zu ermitteln und zu verwalten.

- Ermitteln und verwalten Sie eine Vielzahl von Switches und anderen Einheiten mithilfe einer Massenimportdatei (siehe Systeme verwalten in der Onlinedokumentation von Lenovo XClarity Administrator).
- Ermitteln und verwalten Sie RackSwitch-Switches, die sich im gleichen IP-Subnetz wie XClarity Administrator befinden.
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite „Neue Einheiten ermitteln und verwalten“ wird angezeigt.



Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text eingeben (z. B. einen Namen oder eine IP-Adresse), um die angezeigten Switches weiter zu filtern. Sie können die angezeigten Spalten und die Standard-Sortierreihenfolge ändern, indem Sie auf das Symbol **Spalten anpassen** ( ) klicken.

2. Klicken Sie auf das Symbol **Aktualisieren** ( ), um alle verwaltbaren Einheiten in der XClarity Administrator-Domäne zu ermitteln. Die Ermittlung kann mehrere Minuten dauern.
3. Wählen Sie einen oder mehrere Switches aus, die Sie verwalten möchten.
4. Klicken Sie auf **Ausgewählte verwalten**.
5. Geben Sie die gespeicherten Anmeldeinformationen für die Authentifizierung an den Switches an.

   Tipp:

   – Klicken Sie auf **Gespeicherte Anmeldeinformationen verwalten**, um gespeicherte Anmeldeinformationen in XClarity Administrator zu erstellen und zu verwalten (siehe Gespeicherte Anmeldeinformationen verwalten).

   – Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl. Oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).

6. (Nur Switches, auf denen ENOS ausgeführt wird) Falls festgelegt, geben Sie das „enable“-Kennwort an, um den Privileged Exec-Modus auf dem Switch zu aktivieren.

   Bei der Verwaltung von einem RackSwitch-Switch, auf dem ENOS ausgeführt wird, ist der Zugriff auf den Privileged Exec-Modus erforderlich. Er wird von XClarity Administrator bei der Ausgabe des „enable“-Befehls an den Switch verwendet. Standardmäßig ist kein Kennwort für diesen Befehl auf dem Switch eingerichtet. Wenn der Switchadministrator allerdings zur Erhöhung der Sicherheit ein Kennwort für diesen Befehl festgelegt hat, muss es angegeben werden, damit XClarity Administrator den Switch erfolgreich verwalten kann.

7. Optional: (nur Switches mit ENOS) Wählen Sie, ob HTTPS auf dem Switch aktiviert wird, indem Sie auf **Erweitert** klicken und anschließend **HTTPS aktivieren** auswählen. Dies ist standardmäßig aktiviert.

   Anmerkungen:

   – Bei Switches mit CNOS muss HTTPS vor der Verwaltung auf dem Switch aktiviert werden (siehe Hinweise zur Verwaltung von Switches).
   – Wenn Sie HTTPS nicht aktivieren, wird die aktuelle Einstellung auf dem Switch verwendet.
   – Wenn die Verwaltung des Switches aufgehoben wird, setzt XClarity Administrator HTTPS auf die ursprüngliche Einstellung zurück.

8. Optional: Wählen Sie, ob Sie die NTP-Konfiguration auf dem Switch mit den NTP-Einstellungen für Konfiguration und Zeitzone ersetzen, die für Lenovo XClarity Administrator die definiert sind. Klicken Sie dazu auf **Erweitert** und wählen Sie anschließend **NTP-Clients für die Verwendung der NTP-Einstellungen vom Verwaltungsserver konfigurieren**. Dies ist standardmäßig aktiviert.

   Anmerkungen:

   – Wenn Sie die NTP-Konfiguration und Zeitzone *nicht* ersetzen, sind die Zeitstempel für Protokolleinträge und Ereignisse beim verwalteten Switch und Verwaltungsserver möglicherweise nicht mehr synchron.
   – Wenn die Verwaltung des Switches aufgehoben wird, setzt XClarity Administrator die NTP-Konfiguration und Zeitzone auf die ursprünglichen Einstellungen zurück.

9. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

   Anmerkungen:

   – Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
   – Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.

10. Klicken Sie auf **Verwalten**.

    Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt des Jobs, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

11. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

    Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

    – Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

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

- Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

- Ermitteln und verwalten Sie RackSwitch-Switches, die sich in einem anderen IP-Subnetz als XClarity Administrator befinden, durch manuelles Eingeben von IP-Adressen.
  1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Hardware → Neue Einheiten ermitteln und verwalten**. Die Seite Ermitteln und verwalten wird angezeigt.
  2. Wählen Sie **Manuelle Eingabe**.
  3. Geben Sie die Netzwerkadressen der Switches an, die Sie verwalten möchten:
     - Klicken Sie auf **Einzelsystem** und geben Sie einen einzelnen IP-Adress-Domänennamen oder einen vollständig qualifizierten Domänennamen (FQDN) ein.

       Anmerkung: Stellen Sie bei der Angabe eines FQDN sicher, dass ein gültiger Domänenname auf der Seite Netzwerkzugriff angegeben wird (siehe Netzwerkzugriff konfigurieren).
     - Klicken Sie auf **Mehrere Systeme** und geben Sie einen Bereich von IP-Adressen ein. Um einen weiteren Bereich hinzuzufügen, klicken Sie auf das Symbol **Hinzufügen** (). Um einen Bereich zu entfernen, klicken Sie auf das Symbol **Entfernen** ().
  4. Wenn der Einheitentyp nicht mithilfe der Service-Ermittlungsprotokolle erkannt werden kann, deaktivieren Sie „Benutzerservice-Ermittlungsprotokolle zur Identifizierung des Einheitentyps“ und wählen Sie dann den zu verwaltenden Einheitentyp in der Dropdown-Liste aus.

     Mithilfe von Netzwerkprotokollen wie SLP und SSDP kann XClarity Administrator automatisch den Typ der Einheit ermitteln, die verwaltet werden soll, und dann den entsprechenden Mechanismus zur Verwaltung der Einheit verwenden. Einige Einheitentypen unterstützen keine Netzwerkprotokolle und in einigen Umgebungen werden Netzwerkprotokolle gezielt ausgeschaltet. In beiden Fällen müssen Sie den entsprechenden Einheitentyp auswählen, um den Verwaltungsprozess abzuschließen. Die folgenden Einheitentypen müssen explizit identifiziert werden.
     - Switch der Lenovo ThinkSystem DB Serie
     - NVIDIA Mellanox Switch
  5. Klicken Sie auf **OK**.
  6. Geben Sie die gespeicherten Anmeldeinformationen für die Authentifizierung an den Switches an.

     Tipp:

     - Klicken Sie auf **Gespeicherte Anmeldeinformationen verwalten**, um gespeicherte Anmeldeinformationen in XClarity Administrator zu erstellen und zu verwalten (siehe Gespeicherte Anmeldeinformationen verwalten).
     - Es wird empfohlen, zur Verwaltung der Einheit einen Supervisor- oder Administratoraccount zu verwenden. Wenn ein Account mit einer niedrigeren Berechtigungsstufe verwendet wird, schlägt die Verwaltung möglicherweise fehl. Oder sie funktioniert zwar, aber andere XClarity Administrator-Vorgänge auf der Einheit schlagen fehl (insbesondere wenn die Einheit ohne verwaltete Authentifizierung verwendet wird).

7. (Nur Switches, auf denen ENOS ausgeführt wird) Falls festgelegt, geben Sie das „enable“-Kennwort an, um den Privileged Exec-Modus auf dem Switch zu aktivieren.

   Bei der Verwaltung von einem RackSwitch-Switch, auf dem ENOS ausgeführt wird, ist der Zugriff auf den Privileged Exec-Modus erforderlich. Er wird von XClarity Administrator bei der Ausgabe des „enable“-Befehls an den Switch verwendet. Standardmäßig ist kein Kennwort für diesen Befehl auf dem Switch eingerichtet. Wenn der Switchadministrator allerdings zur Erhöhung der Sicherheit ein Kennwort für diesen Befehl festgelegt hat, muss es angegeben werden, damit XClarity Administrator den Switch erfolgreich verwalten kann.

8. Optional: (nur Switches mit ENOS) Wählen Sie, ob HTTPS auf dem Switch aktiviert wird, indem Sie auf **Erweitert** klicken und anschließend **HTTPS aktivieren** auswählen. Dies ist standardmäßig aktiviert.

   Anmerkungen:

   – Bei Switches mit CNOS muss HTTPS vor der Verwaltung auf dem Switch aktiviert werden (siehe Hinweise zur Verwaltung von Switches).
   – Wenn Sie HTTPS nicht aktivieren, wird die aktuelle Einstellung auf dem Switch verwendet.
   – Wenn die Verwaltung des Switches aufgehoben wird, setzt XClarity Administrator HTTPS auf die ursprüngliche Einstellung zurück.

9. Optional: Wählen Sie, ob Sie die NTP-Konfiguration auf dem Switch mit den NTP-Einstellungen für Konfiguration und Zeitzone ersetzen, die für Lenovo XClarity Administrator die definiert sind. Klicken Sie dazu auf **Erweitert** und wählen Sie anschließend **NTP-Clients für die Verwendung der NTP-Einstellungen vom Verwaltungsserver konfigurieren**. Dies ist standardmäßig aktiviert.

   Anmerkungen:

   – Wenn Sie die NTP-Konfiguration und Zeitzone *nicht* ersetzen, sind die Zeitstempel für Protokolleinträge und Ereignisse beim verwalteten Switch und Verwaltungsserver möglicherweise nicht mehr synchron.
   – Wenn die Verwaltung des Switches aufgehoben wird, setzt XClarity Administrator die NTP-Konfiguration und Zeitzone auf die ursprünglichen Einstellungen zurück.

10. Klicken Sie auf **Ändern**, um die Rollengruppen zu ändern, die den Einheiten zugeordnet werden sollen.

    Anmerkungen:

    – Sie können aus einer Liste der Rollengruppen auswählen, die dem aktuellen Benutzer zugeordnet sind.
    – Wenn Sie die Rollengruppen nicht ändern, werden die Standardrollengruppen verwendet. Weitere Informationen zu den Standardrollengruppen finden Sie unter Standardberechtigungen ändern.

11. Klicken Sie auf **Verwalten**.

    Ein Dialog wird angezeigt, der den Fortschritt dieses Verwaltungsprozesses anzeigt. Überwachen Sie den Fortschritt des Jobs, um sicherzustellen, dass der Prozess erfolgreich beendet wird.

12. Wenn der Prozess abgeschlossen ist, klicken Sie auf **OK**.

    Die Einheit wird jetzt von XClarity Administrator verwaltet und die verwaltete Einheit wird in regelmäßigen Abständen automatisch abgefragt, um aktualisierte Informationen zu erfassen, z. B. den Bestand.

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

    – Wenn die Verwaltung von XClarity Administrator fehlgeschlagen ist und nicht wiederhergestellt werden kann.

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

- Wenn der verwaltende XClarity Administrator heruntergefahren wurde, bevor die Verwaltung der Einheiten aufgehoben wurde.
- Wenn die Verwaltung der Einheiten nicht erfolgreich aufgehoben werden konnte.

Achtung: Einheiten können nur von jeweils einer XClarity Administrator-Instanz verwaltet werden. Die Verwaltung durch mehrere XClarity Administrator-Instanzen wird nicht unterstützt. Wenn eine Einheit von einem XClarity Administrator verwaltet wird und Sie diese mit einem anderen XClarity Administrator verwalten möchten, müssen Sie zuerst die ursprüngliche XClarity Administrator-Verwaltung der Einheit aufheben und diese dann mit dem neuen XClarity Administrator verwalten.

Nach dieser Aufgabe

- Ermitteln und verwalten Sie weitere Einheiten.
- Fügen Sie die neu verwalteten Einheiten zum entsprechenden Rack hinzu, um die physische Umgebung widerzuspiegeln (siehe Racks verwalten).
- Überwachen Sie den Hardwarestatus und die Details (siehe Status von Switches anzeigen).
- Überwachen Sie Ereignisse (siehe Ereignisse handhaben).

Hinweise zur Verwaltung von Switches

Lesen Sie die folgenden wichtigen Hinweise, bevor Sie mit der Verwaltung für einen Switch beginnen.

Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von Lenovo XClarity Administrator.

RackSwitch-Einheiten können über einen Verwaltungsport oder einen der Datenports verwaltet werden. RackSwitch-Einheiten mit CNOS können nur über Schnittstellen verwaltet werden, die entweder der VRF „Verwaltung“ oder „Standard“ angehören.

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

XClarity-Ereignisse und SNMP-Trap-Konfiguration

Bei Verwaltung einer RackSwitch-Einheit, auf der ENOS (jede Version) ausgeführt wird, wird die SNMP-Trap-Quelle auf die Schnittstelle mit der IP-Adresse festgelegt, die für die Verwaltung verwendet wird.

Bei Verwaltung einer RackSwitch-Einheit mit CNOS v10.8.1 oder höher wird die SNMP-Trap-Quellen-VRF überprüft und so geändert, dass sie mit dem Port übereinstimmt, der für die Verwaltung verwendet wird.

Bei RackSwitch-Einheiten mit CNOS bis v10.8.1 muss die SNMP-Trap-Quelle für XClarity Administrator die VRF sein, die mit dem Port verbunden ist, der für die Verwaltung verwendet wird. Der Standardwert „alle“ ermöglicht, dass entweder Verwaltungs- oder Datenports verwendet werden können. Wenn die Switch-Konfiguration nicht den Standardwert verwendet, muss sie entsprechend geändert werden, damit sie mit dem Port übereinstimmt, der für die Verwaltung verwendet wird.

- Wenn der Verwaltungsport für die Verwaltung verwendet wird, müssen Sie die SNMP-Trap-Quellen-VRF auf „alle“ oder „Verwaltung“ festlegen.
- Wenn einer der Datenports für die Verwaltung verwendet wird, müssen Sie die SNMP-Trap-Quellen-VRF auf „alle“ oder „Standard“ festlegen.

RackSwitch-Switches, auf denen CNOS ausgeführt wird

HTTPS muss für die Verwaltung aktiviert sein, und SLP muss für die Ermittlung aktiviert sein.

Anmerkung: Auf CNOS ist HTTPS standardmäßig aktiviert. Wenn Sie die Standardkonfiguration von restApi geändert haben (mithilfe des Befehls `feature restApi http`), können Sie sie mithilfe des Befehls `feature restApi` wieder in HTTPS ändern. Verwenden Sie den Befehl `display restApi server`, um den aktuellen Status zu überprüfen. Die Ausgabe zeigt den aktuellen Status an. Wenn auf die Portnummer „(HTTP)“ folgt, bedeutet dies, dass HTTPS *deaktiviert* ist. Andernfalls muss der Port 443 sein.

Wenn die Verwaltung einer RackSwitch-Einheit aufgehoben wird, stellt XClarity Administrator die Option „Bevorzugen“ möglicherweise nicht auf den Wert wieder her, der vor der Verwaltung der Einheit definiert war (je nach CNOS-Firmwareversion).

RackSwitch-Switches, auf denen ENOS ausgeführt wird

- Wenn sich RackSwitch-Switches in einem anderen Netzwerk befinden als XClarity Administrator, muss dieses Netzwerk so konfiguriert sein, dass eingehender UDP-Datenverkehr über die Ports 161 und 162 zulässig ist, damit XClarity Administrator Ereignisse empfangen und diese Einheiten verwalten kann.
- SSH muss für die Verwaltung aktiviert sein, und SLP muss für die Ermittlung aktiviert sein. HTTPS ist optional; muss jedoch aktiviert sein, um die Switch-Webschnittstelle zu starten.
- Abhängig von der Firmwareversion des RackSwitch-Switches müssen Sie möglicherweise die Multicast-SLP-Weiterleitung und SSH auf allen entsprechenden Switches manuell mithilfe der unten stehenden Befehle aktivieren, bevor die Switches von XClarity Administrator erkannt und verwaltet werden. Weitere Informationen finden Sie unter Online-Dokumentation zu Rack-Switches im System x.
  - `ip slp enable`
  - `ssh enable`
- Bei der Verwaltung eines RackSwitch-Switches ändert XClarity Administrator die folgenden Konfigurationseinstellungen. Die Modifizierung dieser Einstellungen auf einem verwalteten Switch kann zu Verbindungsunterbrechungen führen und verhindern, dass Verwaltungsaktionen ordnungsgemäß durchgeführt werden. Wenn die Verwaltung eines RackSwitch-Switches aufgehoben wird, werden die Konfigurationseinstellungen auf ihre ursprünglichen Werte (vor der Verwaltung) wiederhergestellt.
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - snmp-server version <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

  Sie können die folgenden Konfigurationseinstellungen mit XClarity Administrator ändern, indem Sie die Support-Kontaktinformationen, den Namen oder die Standorteigenschaften für den Switch bearbeiten. Der Standort wird geändert, wenn Sie den Switch zu einem Rack hinzufügen.
  - hostname "<*device_name*>"
  - snmp-server location "Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>"
  - snmp-server contact "<*contact_name*>"

Status von Switches anzeigen

Sie können den Status aller Switches anzeigen, die von Lenovo XClarity Administrator verwaltet werden.

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

Zu dieser Aufgabe

Die folgenden Statussymbole geben den allgemeinen Status der Einheit an. Wenn die Zertifikate nicht übereinstimmen, wird „(nicht vertrauenswürdig)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (nicht vertrauenswürdig)“. Wenn ein Verbindungsproblem besteht oder eine Verbindung zur Einheit nicht vertrauenswürdig ist, wird „(Verbindung)“ an den Status jeder entsprechenden Einheit angehängt, z. B. „Warnung (Verbindung)“.

- ( ) Kritisch
  - Mindestens ein Temperatursensor misst Werte im Ausfallbereich.
  - Lüftermodule oder Lüfter funktionieren nicht ordnungsgemäß, wie im Folgenden beschrieben:
    - RackSwitch G8124-E: Mindestens ein Lüfter läuft mit 100 Umdrehungen oder weniger pro Minute (U/min).
    - RackSwitch G8052: Weniger als drei Lüftermodule sind in gutem Zustand. Der Zustand des Lüftermoduls ist gut, wenn die darin enthaltenen Lüfter mit mehr als 500 Umdrehungen pro Minute (U/min) laufen.
    - RackSwitch G8264, G8264CS, G8332, G8272: Weniger als vier Lüftermodule sind in gutem Zustand. Der Zustand des Lüftermoduls ist gut, wenn die darin enthaltenen Lüfter mit mehr als 500 Umdrehungen pro Minute (U/min) laufen.
    - RackSwitch G8296: Weniger als drei Lüfter befinden sich in gutem Zustand. Der Zustand des Lüftermoduls ist gut, wenn die Lüfter in diesem Modul mit mehr als 480 Umdrehungen pro Minute (U/min) laufen.
    - RackSwitch G7028, G7052: Weniger als drei Lüftermodule sind in gutem Zustand. Der Zustand des Lüftermoduls ist gut, wenn die darin enthaltenen Lüfter mit mehr als 500 Umdrehungen pro Minute (U/min) laufen.
  - Ein Netzteil ist ausgeschaltet.
- ( ) Warnung
  - Mindestens ein Temperatursensor misst Werte im Warnbereich.
  - Im Flash-Speicher ist eine Paniksicherung vorhanden.
- ( ) Ausstehend
- ( ) Information
- ( ) Normal
  - Alle Temperatursensoren messen Werte im normalen Bereich.
  - Alle Lüftermodule oder Lüfter funktionieren ordnungsgemäß.
  - Beide Netzteile sind eingeschaltet.
  - Im Flash-Speicher ist keine Paniksicherung gespeichert.
- ( ) Offline
- ( ) Nicht bekannt

Eine Einheit kann einen der folgenden Stromversorgungsstatus aufweisen:

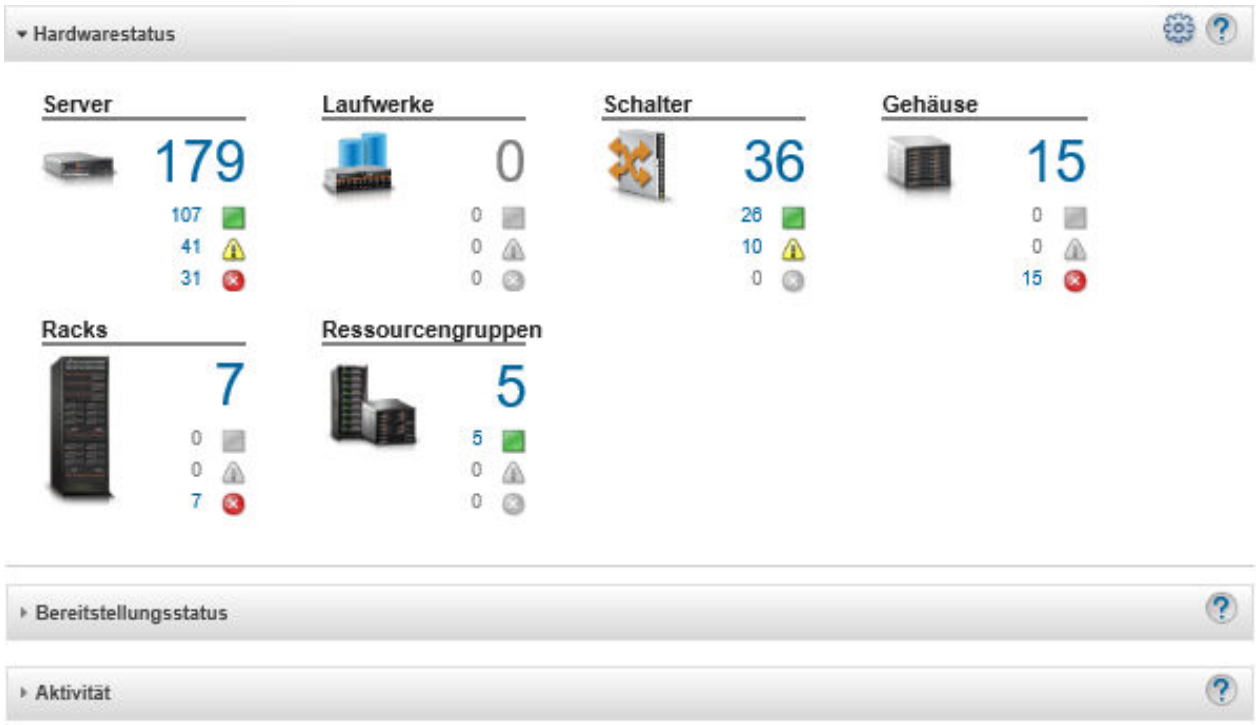
- Ein
- Aus
- Wird heruntergefahren

- Standby
- Hibernation
- Unbekannt

Vorgehensweise

Führen Sie eine oder mehrere der folgenden Aktionen aus, um den Status für einen verwalteten Switch anzuzeigen.

- Klicken Sie in der Menüleiste von XClarity Administrator auf **Dashboard**. Die Dashboard-Seite mit einer Übersicht und dem Status von allen verwalteten Switches und anderen Ressourcen wird angezeigt.



- Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird aufgerufen, die eine Tabellenansicht aller verwalteten Switches enthält.

  Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie zum weiteren Filtern der Gehäuse Text (z. B. einen Gehäusenamen oder eine IP-Adresse) im Feld **Filter** eingeben und auf die Statussymbole klicken, um nur die Switches aufzulisten, die den ausgewählten Kriterien entsprechen.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Zeigen Sie Detailinformationen zu dem Switch an (siehe Details eines Switches anzeigen).
- Zeigen Sie einen Flex-Switch in einer grafischen Rack- oder Gehäuseansicht an, indem Sie auf **Alle Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Alle Aktionen → Anzeigen → In der Gehäuseansicht anzeigen** klicken.
- Zeigen Sie einen RackSwitch-Switch in einer grafischen Rack-Ansicht an, indem Sie **Alle Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** auswählen.
- Starten Sie die Management-Controller-Webschnittstelle für den Switch. Klicken Sie dazu auf den Link **IP-Adresse** (siehe Management-Controller-Webschnittstelle für einen Switch starten).
- Starten Sie die SSH-Konsole für den Switch (siehe Remote-SSH-Sitzung für einen Switch starten).
- Schalten Sie den Switch ein und aus (siehe Switch ein- und ausschalten).
- (Nur RackSwitch-Switches) Ändern Sie die Systeminformationen. Markieren Sie dazu einen Switch und klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**.
- Aktualisieren Sie den Bestand. Markieren Sie dazu einen Server und klicken Sie auf **Alle Aktionen → Bestand → Bestand aktualisieren**.
- Exportieren Sie ausführliche Informationen über einen oder mehrere Switches in eine CSV-Datei. Markieren Sie dazu die Switches und klicken Sie auf **Alle Aktionen → Bestand → Bestand exportieren** (siehe Ereignisse ausschließen).

  Anmerkung: Sie können Bestandsdaten für maximal 60 Einheiten gleichzeitig exportieren.

  Tipp: Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Schließen Sie belanglose Ereignisse auf allen Seiten aus, auf denen Ereignisse angezeigt werden. Klicken Sie dazu auf das Symbol **Ereignisse ausschließen** ( ) (siehe Ereignisse ausschließen).
- (Nur Flex-Switches) Möglicherweise treten Probleme zwischen dem Sicherheitszertifikat von XClarity Administrator und dem Sicherheitszertifikat des CMMs in dem Gehäuse auf, in dem der Switch eingebaut wurde. Sie können die Probleme beheben, indem Sie den Switch auswählen und auf **Alle Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen** klicken (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben).
- Sie können einen Switch zu einer statischen Ressourcengruppe hinzufügen oder daraus entfernen, indem Sie auf **Alle Aktionen → Gruppen → Zu Gruppe hinzufügen** oder **Alle Aktionen → Gruppen → Aus Gruppe entfernen** klicken.

Details eines Switches anzeigen

Sie können in Lenovo XClarity Administrator ausführliche Informationen über einen verwalteten Switch anzeigen. Dazu gehören die Firmwareversionen und IP-Adressen.

Weitere Informationen:

- XClarity Administrator: Bestand
- XClarity Administrator: Überwachung

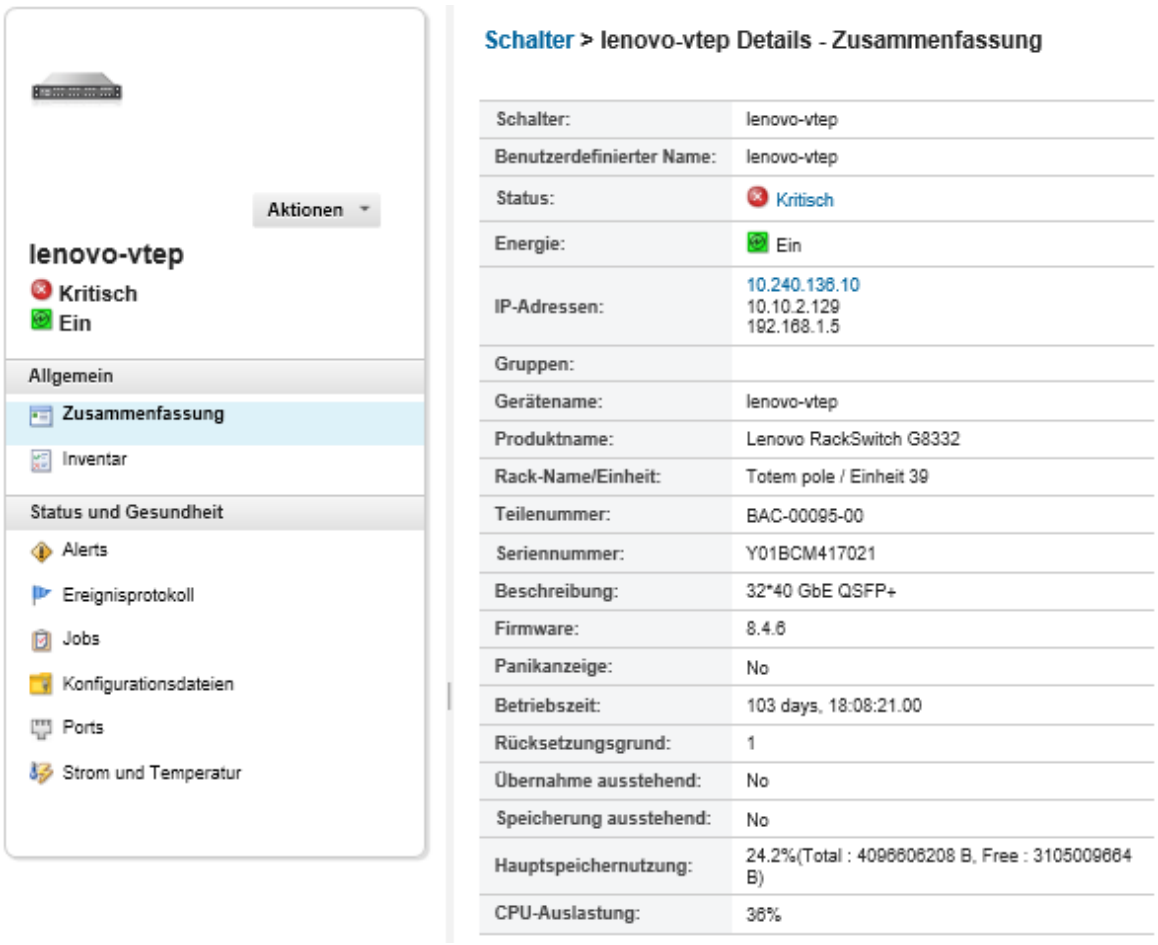
Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Details für einen bestimmten Switch anzuzeigen, der mit XClarity Administrator verwaltet wird.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 2. Klicken Sie in der Spalte **Switches** auf den Switch. Die Seite „Zusammenfassung“ mit den Eigenschaften und einer Liste der auf dem Switch installierten Komponenten wird angezeigt.



Schritt 3. Gehen Sie wie folgt vor, um detaillierte Bestandsinformationen aufzurufen:

Anmerkung: Einige Details sind möglicherweise nicht für alle Switches verfügbar.

- Klicken Sie auf **Zusammenfassung**, um eine Zusammenfassung für den Switch anzuzeigen, einschließlich Systeminformationen und Firmware (siehe Status von Speichereinheiten anzeigen).
- Klicken Sie auf **Inventardetails**, um Details zu den Switchkomponenten anzuzeigen. Dazu zählen:
  - Firmwareversionen für den Switch
  - Details des Management-Controller-Netzwerks, z. B. Hostname, IPv4-Adresse, IPv6-Adresse und MAC-Adressen
  - Asset-Details für den Switch
- Klicken Sie auf **E/A-Verbindung**, um die Verbindungsdetails für den ausgewählten Switch und die zugeordneten Netzwerkadapter, die auf dem Switch installiert sind, anzuzeigen.
- Wählen Sie **Alerts** aus, um die Alerts in der Alert-Liste zu sehen, die sich auf diesen Switch beziehen (siehe Mit Alerts arbeiten).
- Klicken Sie auf **Ereignisprotokoll**, um darin die Ereignisse anzuzeigen, die zu dem Switch gehören (siehe Ereignisse handhaben).
- Klicken Sie auf **Konfigurationsdateien**, um die Switch-Konfiguration zu sichern und wiederherzustellen (siehe Switch-Konfigurationsdaten sichern und wiederherstellen).

- Klicken Sie auf **Implementierungsverlauf**, um Informationen zu Switch-Konfigurationsvorlagen anzuzeigen, die für den Switch implementiert wurden (siehe Verlauf der Switch-Konfigurationsimplementierung anzeigen).
- Klicken Sie auf **Jobs**, um die Konfigurationsdatendateien für den Switch anzuzeigen (siehe Jobs überwachen).
- Klicken Sie auf **Ports**, um den Status und die Konfiguration aller Ports in einem verwalteten Switch anzuzeigen und die Switch-Ports zu aktivieren oder zu deaktivieren.

  Anmerkung: Klicken Sie bei Flex-Switches auf das Symbol **Aktualisieren** (), um die aktuellen Portdaten zu erfassen. Die Datenerfassung kann mehrere Minuten in Anspruch nehmen.
- Klicken Sie auf **Light Path**, um den derzeitigen Status aller Anzeigen auf dem Switch zu sehen.
- Wählen Sie **Strom und Temperatur** aus, um Informationen zur Temperatur, zu Netzteilen und Lüftern anzuzeigen.

  Tipp: Verwenden Sie die Aktualisierungsschaltfläche des Webbrowsers, um die neuesten Strom- und Temperaturdaten zu erfassen. Die Datenerfassung kann mehrere Minuten in Anspruch nehmen.

Nach dieser Aufgabe

Außer der Anzeige von Übersichts- und Detailinformationen zu einem Switch können Sie die folgenden Aktionen durchführen:

- Zeigen Sie einen Flex-Switch in einer grafischen Rack- oder Gehäuseansicht an, indem Sie auf **Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** oder **Aktionen → Anzeigen → In der Gehäuseansicht anzeigen** klicken.
- Zeigen Sie einen RackSwitch-Switch in einer grafischen Rack-Ansicht an, indem Sie **Aktionen → Anzeigen → In der Rack-Ansicht anzeigen** auswählen.
- Starten Sie die Management-Controller-Webschnittstelle für den Switch. Klicken Sie dazu auf den Link **IP-Adresse** (siehe Management-Controller-Webschnittstelle für einen Switch starten).
- Starten Sie die SSH-Konsole für den Switch (siehe Remote-SSH-Sitzung für einen Switch starten).
- Schalten Sie den Switch ein und aus (siehe Switch ein- und ausschalten).
- (Nur RackSwitches) Ändern Sie die Systeminformationen. Markieren Sie dazu einen Switch und klicken Sie auf **Eigenschaften bearbeiten**.
- Exportieren Sie ausführliche Informationen über den Switch in eine CSV-Datei, indem Sie auf **Aktionen → Bestand → Bestand exportieren** klicken.

  Anmerkungen:

  – Weitere Informationen zu Bestandsdaten in der CSV-Datei finden Sie unter GET /switches/<*UUID_list*> REST API in der Onlinedokumentation zu XClarity Administrator.

  – Beim Importieren einer CSV-Datei in Microsoft Excel behandelt Excel Textwerte, die nur Zahlen enthalten, als numerische Werte (zum Beispiel für UUIDs). Formatieren Sie jede Zelle als Text, um diesen Fehler zu beheben.
- Schließen Sie belanglose Ereignisse auf allen Seiten aus, auf denen Ereignisse angezeigt werden. Klicken Sie dazu auf **Aktionen → Servicerücksetzung → Ereignisse ausschließen** (siehe Ereignisse ausschließen).
- Möglicherweise treten Probleme zwischen dem Sicherheitszertifikat von XClarity Administrator und dem Sicherheitszertifikat des Rack-Switches oder CMM in dem Gehäuse auf, in dem der Flex System-Switch eingebaut wurde. Sie können die Probleme beheben, indem Sie einen Switch auswählen und auf

Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen (siehe Ein nicht vertrauenswürdiges Serverzertifikat beheben) klicken.

Switch ein- und ausschalten

Sie können einen Flex System- oder RackSwitch-Switch über Lenovo XClarity Administrator ein- und ausschalten sowie neu starten.

Vorgehensweise

Gehen Sie wie folgt vor, um einen verwalteten Switch ein- oder auszuschalten.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 2. Wählen Sie den Switch aus, den Sie ein- bzw. ausschalten oder neu starten möchten.

Schritt 3. Klicken Sie auf **Alle Aktionen** und dann auf eine der folgenden Stromversorgungsaktionen:
- **Einschalten** (nur Flex System-Switches)
- **Ausschalten** (nur Flex System-Switches)
- **Neu starten**. Der Switch wird neu gestartet, nachdem alle aktuell laufenden Vorgänge beendet sind. Während des Switch-Neustarts gestartete Vorgänge werden abgelehnt.

Switch-Ports aktivieren und deaktivieren

Sie können bestimmte Ports auf einem RackSwitch- oder Flex System-Switch aktivieren oder deaktivieren.

Vorgehensweise

So aktivieren oder deaktivieren Sie Switch-Ports.

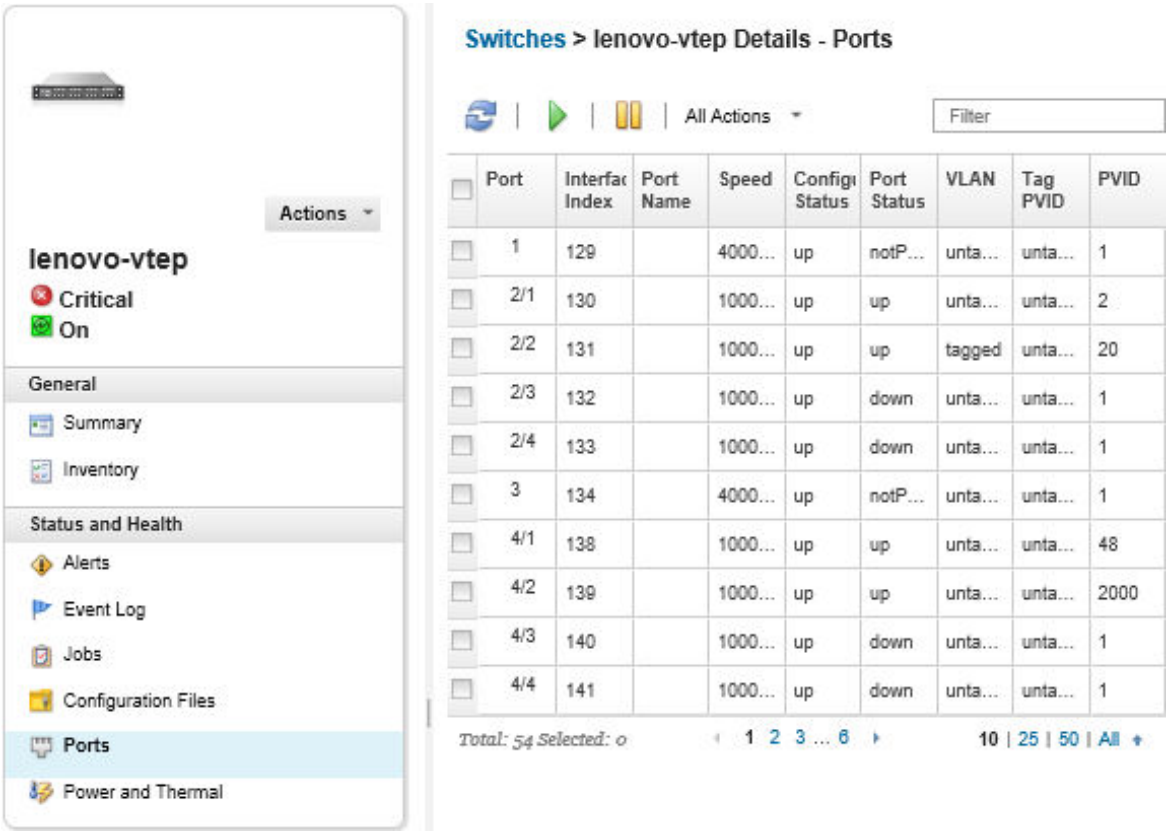
Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 2. Klicken Sie in der Spalte **Switches** auf den Switch. Die Seite „Zusammenfassung“ mit den Eigenschaften und einer Liste der auf dem Switch installierten Komponenten wird angezeigt.

Schritt 3. Klicken Sie in der linken Navigation auf **Ports**, um den Status und die Konfiguration sämtlicher Ports im Switch anzuzeigen:

Anmerkung: Klicken Sie bei Flex-Switches auf das Symbol **Aktualisieren** (), um die aktuellen Portdaten zu erfassen. Die Datenerfassung kann mehrere Minuten in Anspruch nehmen.



Schritt 4. Wählen Sie den Port aus und klicken Sie auf das Symbol **Aktivieren** () oder auf das Symbol **Deaktivieren** ().

Switch-Konfigurationsdaten sichern und wiederherstellen

Sie können Lenovo XClarity Administrator verwenden, um RackSwitch- und Flex System-Switches zu sichern und wiederherzustellen. Sie können Switch-Konfigurationsdateien auch in Ihr lokales System exportieren und Switch-Konfigurationsdateien in XClarity Administrator importieren.

Switch-Konfigurationsdaten sichern

Sie können Konfigurationsdaten für Flex System- oder RackSwitch-Switches sichern. Bei der Sicherung eines Switches werden die Konfigurationsdaten inLenovo XClarity Administrator aus dem Ziel-Switch als Switch-Konfigurationsdatei importiert.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Konfigurationsdaten für einen verwalteten Switch zu sichern.

- Für einen einzelnen Switch:
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

     Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

  2. Klicken Sie in der Spalte **Switches** auf den Switch. Die Seite „Zusammenfassung“ mit den Eigenschaften und einer Liste der auf dem Switch installierten Komponenten wird angezeigt.
  3. Klicken Sie auf **Konfiguration**, um die Konfigurationsdateien für den Switch anzuzeigen.
  4. Klicken Sie auf das Symbol **Konfigurationsdaten sichern** (), um die Switch-Konfiguration zu sichern.
  5. (Optional) Geben Sie einen Namen für die Switch-Konfigurationsdatei an.

     Für CNOS-Einheiten kann der Dateiname alphanumerische Zeichen und die folgenden Sonderzeichen enthalten: Unterstrich (_), Bindestrich (-) und Punkt (.). Bei ENOS-Switches kann der Dateiname alphanumerischen Zeichen und Sonderzeichen enthalten.

     Ist ein Dateiname nicht angegeben, wird der folgende Standardname verwendet: „*<Switch_Name>_<IP_Adresse>_<Zeitstempel>*.cfg.“
  6. (Optional) Fügen Sie einen Kommentar hinzu, der die Sicherung beschreibt.

7. Klicken Sie auf **Sichern**, um Switch-Konfigurationsdaten sofort zu sichern, oder klicken Sie auf **Zeitplan**, um diese Sicherung geplant zu einem späteren Zeitpunkt auszuführen.

   Wenn Sie eine Sicherung einplanen möchten, können Sie **Überschreiben** auswählen, um die Switch-Konfigurationsdaten bei jeder Ausführung des Jobs in die gleiche Datei zu schreiben, sodass deren Inhalt überschrieben wird. Wenn Sie angeben, dass die Datei nicht überschrieben werden soll, wird an die Dateinamen nachfolgender Backups eine eindeutige Nummer angehängt (z. B. MyBackup_33.cfg).

   Anmerkung: Bei der Planung einer Sicherung können Sie keine dynamischen Dateinamen oder Kommentare für jeden geplanten Job auswählen.

- Für mehrere Switches:
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.
  2. Wählen Sie einen oder mehrere Switches aus.
  3. Klicken Sie auf **Alle Aktionen → Konfiguration → Konfigurationsdatei sichern**.
  4. (Optional) Geben Sie einen Namen für die Switch-Konfigurationsdatei an.

     Für CNOS-Einheiten kann der Dateiname alphanumerische Zeichen und die folgenden Sonderzeichen enthalten: Unterstrich (_), Bindestrich (-) und Punkt (.). Bei ENOS-Switches kann der Dateiname alphanumerischen Zeichen und Sonderzeichen enthalten.

     Ist ein Dateiname nicht angegeben, wird der folgende Standardname verwendet: „<*Switch_Name*>_<*IP_Adresse*>_<*Zeitstempel*>.cfg.“
  5. (Optional) Fügen Sie einen Kommentar hinzu, der die Sicherung beschreibt.
  6. Klicken Sie auf **Sichern**, um Switch-Konfigurationsdaten sofort zu sichern, oder klicken Sie auf **Zeitplan**, um diese Sicherung geplant zu einem späteren Zeitpunkt auszuführen.

     Wenn Sie eine Sicherung einplanen möchten, können Sie **Überschreiben** auswählen, um die Switch-Konfigurationsdaten bei jeder Ausführung des Jobs in die gleiche Datei zu schreiben, sodass deren Inhalt überschrieben wird. Wenn Sie angeben, dass die Datei nicht überschrieben werden soll, wird an die Dateinamen nachfolgender Backups eine eindeutige Nummer angehängt (z. B. MyBackup_33.cfg).

     Anmerkung: Bei der Planung einer Sicherung können Sie keine dynamischen Dateinamen oder Kommentare für jeden geplanten Job auswählen.

Nach dieser Aufgabe

Nach Abschluss des Sicherungsprozesses wird die Switch-Konfigurationsdatei der Registerkarte **Konfigurationsdateien** auf der Seite „Switch-Details“ hinzugefügt.

Auf dieser Seite können Sie die folgenden Aktionen für eine ausgewählte Switch-Konfigurationsdatei ausführen:

- Stellen Sie die Switch-Konfiguration wieder her, indem Sie die Switch-Konfigurationsdatei auswählen und auf das Symbol **Konfigurationsdaten wiederherstellen** klicken ().
- Löschen Sie die Switch-Konfigurationsdateien ausXClarity Administrator, indem Sie auf das Symbol **Löschen** klicken ().
- Exportieren Sie die Switch-Konfigurationsdateien auf Ihr lokales System, indem Sie die Dateien auswählen und auf das Symbol **Konfigurationsdatei exportieren** klicken ().

- Importieren Sie die Switch-Konfigurationsdateien in XClarity Administrator, indem Sie auf das Symbol **Konfigurationsdatei importieren** klicken ( ).

Switch-Konfigurationsdaten wiederherstellen

Sie können die Konfigurationsdaten, die in Lenovo XClarity Administrator für einen Flex System- oder RackSwitch-Switch gesichert oder importiert wurden, wiederherstellen. Die Switch-Konfigurationsdatei wird aus XClarity Administrator auf den Ziel-Switch heruntergeladen. Die Konfiguration wird automatisch ausgeführt.

Die Konfigurationsdateien werden einem bestimmten Switch zugeordnet. Sie können eine Konfigurationsdatei nur auf dem Switch wiederherstellen, der ihr zugeordnet ist. Sie können keine Konfigurationsdatei verwenden, die für einen Switch zur Wiederherstellung der Konfiguration auf einem anderen Switch gesichert wurde.

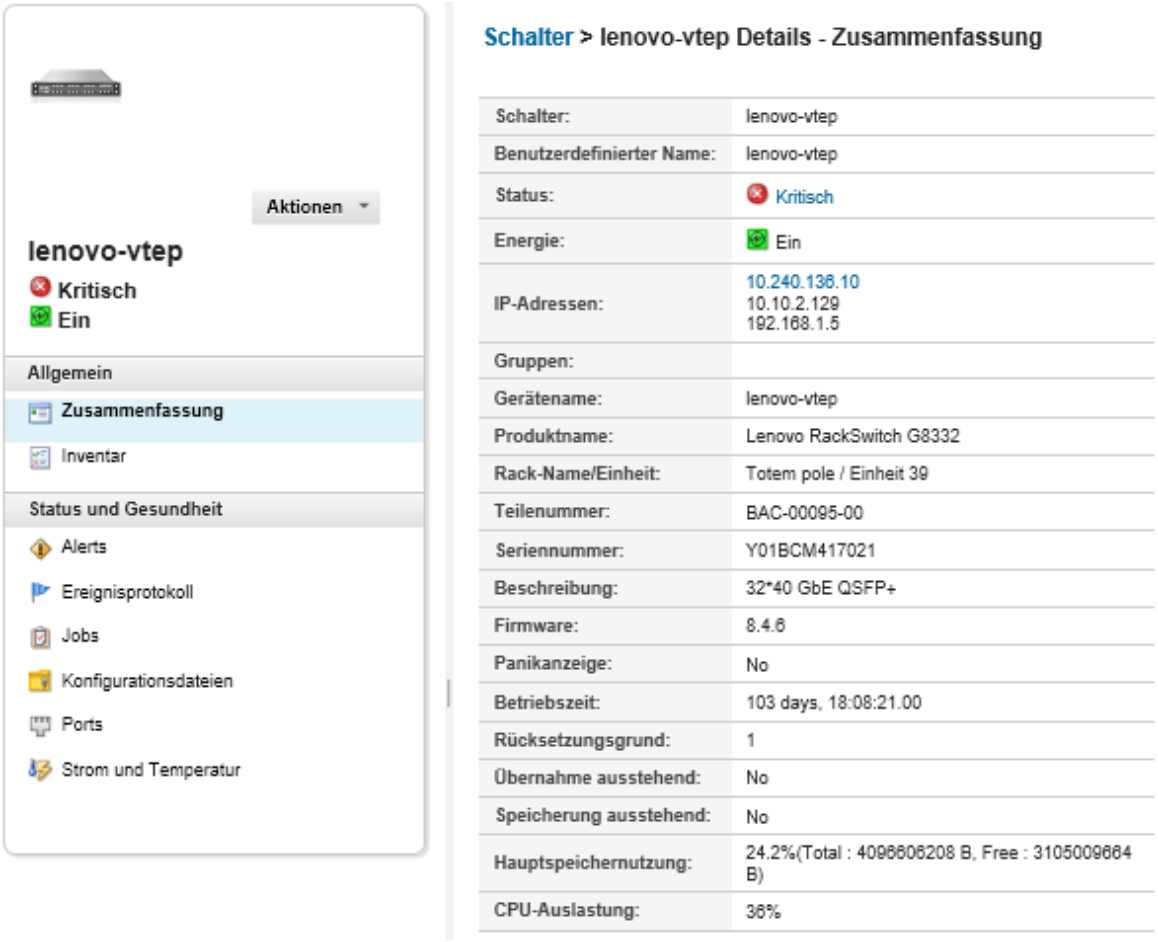
Vorgehensweise

Führen Sie die folgenden Schritte aus, um Konfigurationsdaten auf einem verwalteten Switch wiederherzustellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 2. Klicken Sie in der Spalte **Switches** auf den Switch. Die Seite „Zusammenfassung“ mit den Eigenschaften und einer Liste der auf dem Switch installierten Komponenten wird angezeigt.



Schritt 3. Klicken Sie auf **Konfigurationsdateien**, um die Konfigurationsdateien für den Switch anzuzeigen.

Schritt 4. Wählen Sie die Konfigurationsdatei aus, die auf dem Switch wiederhergestellt werden soll, und klicken Sie auf das Symbol **Konfigurationsdaten wiederherstellen** ( ). Das Dialogfenster zum Wiederherstellen wird angezeigt.

Schritt 5. (Nur Switches mit CNOS) Geben Sie an, ob der Switch neu gestartet werden soll, wenn die Wiederherstellung abgeschlossen ist.

Wenn der Switch nicht automatisch neu gestartet werden soll, müssen Sie den CNOS-Switch manuell wiederherstellen, um die wiederhergestellten Konfigurationsdaten zu aktivieren. Wenn Sie zu lange warten und ein Speichervorgang auftritt (zum Beispiel, wenn ein Port aktiviert oder deaktiviert wird), wird die Wiederherstellung abgebrochen und die laufenden Konfigurationsdaten werden verwendet.

Schritt 6. Klicken Sie auf **Wiederherstellen**, um die Switch-Konfigurationsdaten sofort wiederherzustellen, oder klicken Sie auf **Zeitplan**, um diese Wiederherstellung geplant zu einem späteren Zeitpunkt auszuführen.

Anmerkung: Seien Sie bei der Planung wiederkehrender Wiederherstellungsjobs vorsichtig. Wenn Ihr Switch auf eine frühere Konfiguration zurückgesetzt wird, überprüfen Sie die Seite Geplante Jobs auf geplante Wiederherstellungsjobs.

Switch-Konfigurationsdateien exportieren und importieren

Sie können Switch-Konfigurationsdateien in Ihr lokales System exportieren und Switch-Konfigurationsdateien in Lenovo XClarity Administrator importieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Konfigurationsdaten für einen verwalteten Switch zu sichern.

- Switch-Konfigurationsdateien exportieren
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

     Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

  2. Klicken Sie in der Spalte **Switches** auf den Switch. Die Seite „Zusammenfassung“ mit den Eigenschaften und einer Liste der auf dem Switch installierten Komponenten wird angezeigt.
  3. Klicken Sie auf **Konfiguration**, um die Konfigurationsdateien für den Switch anzuzeigen.
  4. Wählen Sie die zu exportierenden Switch-Konfigurationsdateien aus.
  5. Klicken Sie auf das Symbol **Konfigurationsdatei exportieren** ( ), um die Switch-Konfiguration zu sichern.
- Switch-Konfigurationsdateien importieren
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

     Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

2. Klicken Sie in der Spalte **Switches** auf den Switch. Die Seite „Zusammenfassung“ mit den Eigenschaften und einer Liste der auf dem Switch installierten Komponenten wird angezeigt.
3. Klicken Sie auf **Konfiguration**, um die Konfigurationsdateien für den Switch anzuzeigen.
4. Klicken Sie auf das Symbol **Konfigurationsdatei importieren** ( ), um die Switch-Konfiguration zu sichern.
5. Geben Sie den Dateinamen für die Switch-Konfiguration ein oder klicken Sie auf **Durchsuchen**, um nach der Boot-Datei zu suchen, die Sie importieren möchten.
6. **Optional:** Geben Sie eine Beschreibung für die Switch-Konfigurationsdatei ein.
7. Klicken Sie auf **Importieren**.

   Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des Hochladevorgangs schließen, schlägt der Import fehl.

Management-Controller-Webschnittstelle für einen Switch starten

Sie können in Lenovo XClarity Administrator die Management-Controller-Webschnittstelle für einen RackSwitch- oder Flex System-Switch starten, auf dem ENOS ausgeführt wird.

Vorgehensweise

Gehen Sie wie folgt vor, um die Management-Controller-Webschnittstelle für einen Switch zu starten.

Anmerkung: Die Management-Controller-Webschnittstelle kann von XClarity Administrator nicht über den Safari-Webbrowser gestartet werden.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 2. Wählen Sie den Switch aus und klicken Sie auf **Alle Aktionen → Starten → Verwaltungswebschnittstelle**. Die Management-Controller-Webschnittstelle für den Switch wird gestartet.

Tipp: Alternativ können Sie die Management-Controller-Schnittstelle starten, indem Sie auf den Link in der Spalte **IP-Adresse** klicken, oder über die Übersichts- und Detailseiten zu den Switches.

Schritt 3. Melden Sie sich an der Management-Controller-Webschnittstelle an.

Tipp: Verwenden Sie für Flex-Switches die XClarity Administrator-Anmeldeinformationen. Für XClarity Administrator-Switches benötigen Sie die Anmeldeinformationen für den Switch.

Remote-SSH-Sitzung für einen Switch starten

Sie können in Lenovo XClarity Administrator eine Remote-SSH-Sitzung für einen verwalteten RackSwitch- oder Flex-Switch starten. Innerhalb dieser Sitzung können Sie über die Befehlszeilenschnittstelle Verwaltungstasks ausführen, die nicht über XClarity Administrator verfügbar sind.

Vorbereitende Schritte

Stellen Sie sicher, dass SSH in der Switchkonfiguration aktiviert ist. Auf RackSwitch-Switches wird SSH aktiviert, wenn der Switch mit XClarity Administrator verwaltet wird. Auf Flex-Switches ist SSH in der Regel standardmäßig aktiviert. Ist dies nicht der Fall, muss SSH aktiviert werden, bevor der Switch mit XClarity Administrator verwaltet wird.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Remote-SSH-Sitzung für einen verwalteten Switch zu starten.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird mit einer Tabellenansicht aller Switches, die im verwalteten Gehäuse installiert sind, geöffnet.

Sie können die Tabellenspalten sortieren, um die Switches, die Sie verwalten möchten, schneller zu finden. Darüber hinaus können Sie im Feld **Filter** Text (z. B. einen Namen oder eine IP-Adresse) eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 2. Wählen Sie den Switch aus, für den Sie eine SSH-Sitzung starten möchten.

Schritt 3. Klicken Sie auf **Alle Aktionen → starten → SSH-Konsole**.

Schritt 4. Falls erforderlich, melden Sie sich bei dem Switch mit Ihrer Benutzer-ID und dem Kennwort an.

Systemeigenschaften für einen Switch ändern

Sie können die Systemeigenschaften für einen bestimmten Flex System- oder RackSwitch-Switch ändern.

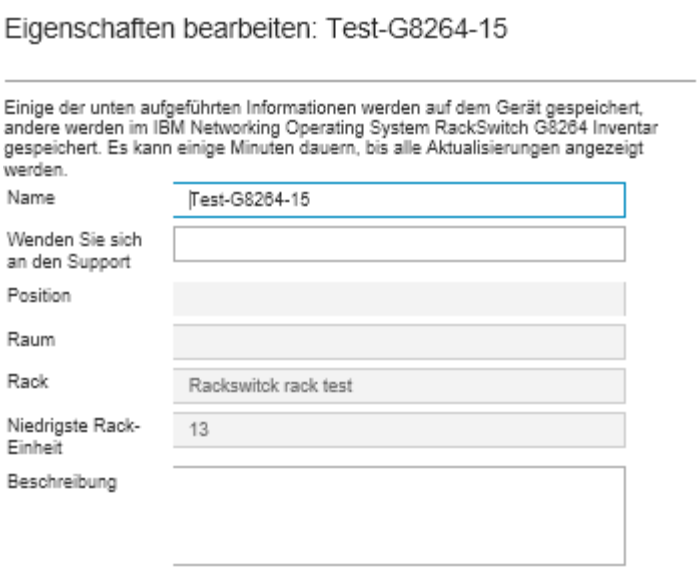
Vorgehensweise

Gehen Sie wie folgt vor, um die Systemeigenschaften zu ändern:

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Switches**, um die Seite Switches anzuzeigen.

Schritt 2. Wählen Sie den Switch aus, den Sie aktualisieren möchten.

Schritt 3. Klicken Sie auf **Alle Aktionen → Bestand → Eigenschaften bearbeiten**, um den Dialog Bearbeiten anzuzeigen.



Schritt 4. Ändern Sie gegebenenfalls die folgenden Daten:
- Switchname
- Wenden Sie sich an den Support
- Beschreibung

Anmerkung: Die Eigenschaften für Position, Raum, Rack und unterste Rackeinheit werden von XClarity Administrator aktualisiert, wenn Sie Einheiten in der Webschnittstelle zu einem Rack hinzufügen oder daraus entfernen (siehe Racks verwalten).

Schritt 5. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie diese Eigenschaften ändern, kann es einen Moment dauern, bis die Änderungen in der XClarity Administrator-Webschnittstelle angezeigt werden.

Abgelaufene oder ungültige gespeicherte Anmeldeinformationen für einen Schalter auflösen

Wenn gespeicherte Anmeldeinformationen auf einer Einheit ablaufen oder nicht mehr funktionsfähig sind, wird der Status für diese Einheit mit „Offline“ angezeigt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um abgelaufene oder ungültige gespeicherte Anmeldeinformationen für einen Schalter aufzulösen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Switches**. Die Seite Switches wird aufgerufen, die eine Tabellenansicht aller verwalteten Switches enthält.

Schritt 2. Klicken Sie auf die Spaltenüberschrift der Tabelle **Power**, um alle Offline-Switches oben in der Tabelle zu gruppieren.

Sie können die Tabellenspalten sortieren, um den zu verwaltenden Schalter schneller zu finden. Darüber hinaus können Sie Text (z. B. einen Systemnamen oder eine IP-Adresse) im Feld **Filter** eingeben, um die angezeigten Switches weiter zu filtern.

Schritt 3. Wählen Sie den aufzulösenden Schalter aus.

Schritt 4. Klicken Sie auf **Alle Aktionen → Sicherheit → Gespeicherte Anmeldeinformationen bearbeiten**.

Schritt 5. Ändern Sie das Kennwort für gespeicherte Anmeldeinformationen oder wählen Sie andere gespeicherte Anmeldeinformationen aus, um diese für die verwaltete Einheit zu verwenden.

Anmerkung: Wenn Sie mehr als eine Einheit mit denselben gespeicherten Anmeldeinformationen verwaltet haben und das Kennwort für die gespeicherten Anmeldeinformationen ändern, betrifft die Änderung des Kennworts alle Einheiten, die derzeit die gespeicherten Anmeldeinformationen verwenden.

Verwaltung eines Switches nach einem Verwaltungsserverausfall wiederherstellen

Sie können die Verwaltung eines Switches wiederherstellen, wenn diese nicht ordnungsgemäß aufgehoben wurde, z. B. aufgrund von Verbindungsproblemen während der Aufhebung oder bei einem Ausfall des für die Verwaltung verwendeten Lenovo XClarity Administrator.

Vorgehensweise

- Nutzen Sie die Option **Verwaltung erzwingen** (siehe Switches verwalten), um den Switch erneut zu verwalten.
- Gehen Sie wie folgt vor, um die XClarity Administrator-spezifische Konfiguration auf einem Switch zu entfernen, dessen Verwaltung nicht ordnungsgemäß aufgehoben wurde und der nicht erneut verwaltet werden soll.
  - Verwenden Sie die Option **Verwaltung erzwingen** (siehe Switches verwalten), um den Switch wieder zu verwalten. Heben Sie anschließend die Verwaltung für den Switch auf, um die Konfiguration zu bereinigen (siehe Verwaltung eines Switch aufheben).
  - (ENOS) Melden Sie sich über den Konsolenport des Switches oder eine SSH- bzw. Telnet-Sitzung bei dem Switch an. Führen Sie die Konfigurationsbefehle in der angegebenen Reihenfolge aus, um die Switchkonfiguration zu löschen.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Verwaltung eines Switch aufheben

Sie können die Verwaltung eines Switches durch Lenovo XClarity Administrator aufheben. Dieser Vorgang wird als *Aufheben der Verwaltung* bezeichnet.

Vorbereitende Schritte

Sie können XClarity Administrator so konfigurieren, dass die Verwaltung von Einheiten, die für einen bestimmten Zeitraum offline sind, automatisch aufgehoben wird. Dies ist standardmäßig deaktiviert. Um die automatische Aufhebung der Verwaltung von Offline-Einheiten zu aktivieren, klicken Sie im Menü von XClarity Administrator auf **Hardware → Neue Einheiten ermitteln und verwalten** und klicken Sie dann auf **Bearbeiten** neben **Aufheben der Verwaltung von Offline-Einheiten ist deaktiviert**. Wählen Sie anschließend **Aufheben der Verwaltung von Offline-Einheiten aktivieren** aus und legen Sie das Zeitintervall fest. Standardmäßig wird die Verwaltung von Einheiten aufgehoben, nachdem sie 24 Stunden offline waren.

Bevor Sie die Verwaltung eines Switches aufheben, müssen Sie sicherstellen, dass für den Switch keine aktiven Jobs ausgeführt werden.

Zu dieser Aufgabe

Wenn Sie die Verwaltung für einen Switch aufgehoben haben, speichert XClarity Administrator bestimmte Informationen über den Switch. Diese Informationen werden erneut angewendet, wenn Sie denselben Switch wieder verwalten.

Tipp: Alle Demo-Einheiten, die während der Erstkonfiguration optional hinzugefügt werden, sind Knoten in einem Gehäuse. Um die Verwaltung der Demo-Einheiten aufzuheben, müssen Sie die Gehäuseverwaltung mit der Option **Aufheben der Verwaltung erzwingen, selbst wenn die Einheit nicht erreichbar ist** aufheben.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verwaltung eines Switches aufzuheben.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Switches**, um die Seite Switches anzuzeigen.

Schritt 2. Wählen Sie einen oder mehrere Switches aus der Liste der verwalteten Switches aus.

Schritt 3. Klicken Sie auf **Verwaltung des Switches aufheben**. Der Dialog „Verwaltung aufheben“ wird angezeigt.

Schritt 4. **Optional:** Wählen Sie **Verwaltungsaufhebung erzwingen, selbst wenn das Gerät nicht erreichbar ist**.

Wichtig: Wenn Sie die Verwaltung für Demo-Hardware aufheben, müssen Sie diese Option auswählen.

Schritt 5. Klicken Sie auf **Verwaltung aufheben**.Der Dialog „Verwaltung aufheben“ zeigt den Status jedes Schritts im Verwaltungsaufhebungsprozess an.

Schritt 6. Wenn der Verwaltungsaufhebungsprozess abgeschlossen ist, klicken Sie auf **OK**.

Einen Switch wiederherstellen, für den die Verwaltung nicht ordnungsgemäß aufgehoben wurde

Wenn ein Switch von Lenovo XClarity Administrator verwaltet wird und XClarity Administrator ausfällt, können Sie die Verwaltungsfunktionen wiederherstellen, bis der Verwaltungsserver wiederherstellt oder ausgetauscht wird.

Vorgehensweise

- Nutzen Sie die Option **Verwaltung erzwingen** (siehe Switches verwalten), um den Switch erneut zu verwalten.
- Gehen Sie wie folgt vor, um die XClarity Administrator-spezifische Konfiguration auf einem Switch zu entfernen, dessen Verwaltung nicht ordnungsgemäß aufgehoben wurde und der nicht erneut verwaltet werden soll.
  - Verwenden Sie die Option **Verwaltung erzwingen** (siehe Switches verwalten), um den Switch wieder zu verwalten. Heben Sie anschließend die Verwaltung für den Switch auf, um die Konfiguration zu bereinigen (siehe Verwaltung eines Switch aufheben).
  - (ENOS) Melden Sie sich über den Konsolenport des Switches oder eine SSH- bzw. Telnet-Sitzung bei dem Switch an. Führen Sie die Konfigurationsbefehle in der angegebenen Reihenfolge aus, um die Switchkonfiguration zu löschen.

    ```
    no snmp-server access 32
    no snmp-server group 16
    no snmp-server notify 16
    no snmp-server target-parameters 16
    no snmp-server target-address 16
    no snmp-server user 16
    ```

Kapitel 11. Server mithilfe von Konfigurationsmustern konfigurieren

Servermuster werden verwendet, um mehrere Server (Rack- und Tower-Server sowie Rechenknoten) schnell über einen einzelnen Satz definierter Konfigurationseinstellungen bereitzustellen.

Weitere Informationen:

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

Vorbereitende Schritte

Sie können XClarity Administrator nach Ablauf der 90 Tage weiterhin kostenlos verwenden, um Hardware zu verwalten und zu überwachen. Sie müssen jedoch Lizenzen für den vollständigen Funktionsumfang für jeden verwalteten Server erwerben, der erweiterte Lenovo XClarity Administrator-Funktionen unterstützt, um die Funktion „Serverkonfiguration“ verwenden zu können. Lenovo XClarity Pro umfasst die Berechtigung für Service und Support sowie die Lizenz für den vollständigen Funktionsumfang. Weitere Informationen zum Kauf von Lenovo XClarity Pro erhalten Sie von Ihrem Lenovo-Ansprechpartner oder autorisierten Business Partner. Weitere Informationen finden Sie unter Lizenz für den vollständigen Funktionsumfang installieren in der Onlinedokumentation zu XClarity Administrator.

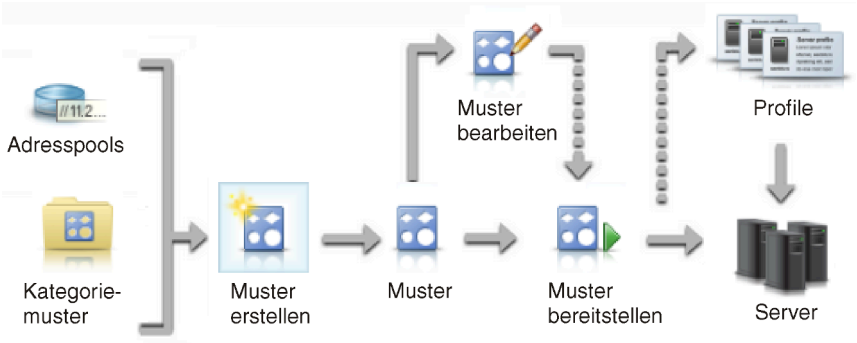
Lesen Sie Konfigurationshinweise, um wichtige Informationen zur Konfigurationsunterstützung für bestimmte Server und Einheiten zu erhalten.

Zu dieser Aufgabe

In XClarity Administrator können Sie Servermuster verwenden, um den lokalen Speicher, E/A-Adapter, die Bootreihenfolge und andere Baseboard Management Controller- und UEFI- Einstellungen (Unified Extensible Firmware Interface) auf verwalteten Servern zu konfigurieren. Servermuster integrieren außerdem 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. Mit virtualisierten (vorkonfigurierten) Fibre Channel-Adressen können Sie außerdem vor dem Zugang neuer Hardware SAN-Zoning-Änderungsanforderungen erstellen.

Vorgehensweise

In der folgenden Abbildung wird der Ablauf der Konfiguration von verwalteten Servern dargestellt. Die durchgezogenen Pfeile stellen Ihre Aktionen dar. Die gestrichelten Pfeile sind die Aktionen, die automatisch durch XClarity Administrator ausgeführt werden.



Schritt 1. **Adresspools erstellen.**Ein *Adresspool* ist ein definierter Satz von Adressbereichen. Lenovo XClarity Administrator verwendet Adresspools, um bei der Bereitstellung von Servermustern auf Servern IP- und E/A-Adressen zu den jeweiligen Servern zuzuweisen.

Weitere Informationen zum Erstellen von Adressenpools finden Sie unter Adresspools definieren.

Schritt 2. **Kategoriemuster erstellen.**

Ein *Kategoriemuster* fasst bestimmte Firmwareeinstellungen zusammen und kann in mehreren Servermustern wiederverwendet werden. Sie können Muster für die folgenden Firmwarekategorien erstellen:

- Systeminformationen
- Verwaltungsschnittstellen
- Einheiten und Ein-/Ausgangsanschlüsse
- FC-Bootziele
- E/A-Adapteranschlüsse

Weitere Informationen zu Kategoriemustern finden Sie unter Mit Servermustern arbeiten.

Schritt 3. **Erstellen Sie ein Servermuster.**

Ein *Servermuster* ist eine Serverkonfiguration vor der Betriebssysteminstallation (einschließlich Konfiguration des lokalen Speichers, E/A-Adapterkonfiguration, Booteinstellungen und anderen Baseboard Management Controller- und UEFI-Firmware Einstellungen). Ein Servermuster ist ein Gesamtmuster für die schnelle Konfiguration mehrerer Server.

Sie können mehrere Servermuster definieren, um so die verschiedenen, in Ihrem Rechenzentrum verwendeten Konfigurationen abzubilden.

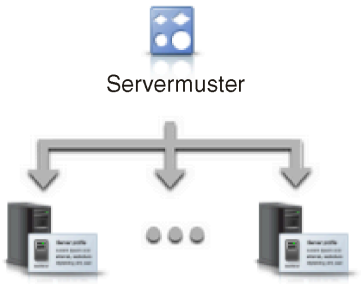
Wenn Sie ein Servermuster definieren, wählen Sie zum Erstellen der Konfiguration für eine bestimmte Servergruppe die jeweils zutreffenden Kategoriemuster und Adresspools aus. Ein Kategoriemuster fasst bestimmte Konfigurationseinstellungen zusammen und kann in mehreren Servermustern wiederverwendet werden.

Sie können ein Servermuster für Converged-, Flex System-, NeXtScale- und System x-Server von Grund auf erstellen und so eine gewünschte Konfiguration vor dem Eintreffen der Hardware definieren. Oder Sie können ein Servermuster über einen vorhandenen verwalteten Server erstellen. Wenn Sie ein Servermuster über einen vorhandenen Server erstellen, erstellt XClarity Administrator die Kategoriemuster auf Basis des ausgewählten Servers.

Weitere Informationen zum Erstellen von Servermustern finden Sie unter Ein Servermuster erstellen.

Schritt 4. **Stellen Sie das Servermuster bereit.**

Sie können ein Servermuster für einen oder mehrere einzelne Server oder Servergruppen implementieren. Sie können beispielsweise ein Servermuster für ein Gehäuse bereitstellen. So werden alle Rechenknoten in diesem Gehäuse identisch konfiguriert. Während der Bereitstellung erstellt XClarity Administrator ein Serverprofil für jeden Server, auf dem das Servermuster bereitgestellt wurde. Die *Serverprofile* stellen jeweils eine bestimmte Konfiguration für einen einzelnen Server dar. Es erbt Einstellungen des Servermusters und enthält außerdem serverspezifische Informationen (z. B. zugewiesene IP-Adressen und MAC-Adressen). Da das Serverprofil die Einstellungen des Servermusters erbt, ändert sich bei einer Veränderung am Servermuster auch automatisch das Serverprofil. Auf diese Weise können Sie gemeinsame Konfigurationen über einen einzigen Bereich verwalten.



Anmerkung: Die Einstellungen auf einem Server können nicht mehr konform mit dem jeweiligen Serverprofil sein, wenn Einstellungen ohne den Einsatz von Konfigurationsmustern geändert werden oder während der Implementierung ein Fehler aufgetreten ist, beispielsweise ein Fehler bei der Firmware oder eine ungültige Einstellung. Sie können den Konformitätsstatus jedes Servers über die Seite „Konfigurationsmuster: Serverprofile“ ermitteln.

Auf den folgenden Komponenten können Sie ein Servermuster bereitstellen:

- **Vorhandene Server**. Für jeden einzelnen Server wird ein Serverprofil erstellt. Das Serverprofil wird aktiviert, nachdem der zugeordnete Server neu gestartet wurde.
- **Leere Positionen in einem vorhandenen Gehäuse**. Für jede einzelne Position wird ein Serverprofil erstellt. Das Serverprofil, das der leeren Position zugeordnet ist, kann nach der physischen Installation des Rechenknotens aktiviert werden.
- **Platzhalter für ein noch nicht vorhandenes Gehäuse**. Über die Definition eines *Platzhaltergehäuses* als Ziel für die Servermuster können Sie noch nicht vorhandene Rechenknoten vor deren Eintreffen bereitstellen. Das Platzhaltergehäuse fasst alle Serverprofile zusammen, die für die jeweilige leere Rechenknotenpositionen erstellt werden. Wenn die Hardware eintrifft, können Sie die Serverprofile für alle Rechenknoten im neuen Gehäuse zuweisen, indem Sie das Platzhaltergehäuse für das neue Gehäuse bereitstellen. Die Serverprofile werden nach der Zuordnung zum Rechenknoten beim nächsten Neustart aktiviert.

Anmerkung: Sie können ein Servermuster für mehrere Server implementieren, mehrere Muster können jedoch nicht für einen einzelnen Server implementiert werden.

Weitere Informationen zum Bereitstellen eines Servermusters finden Sie unter Servermuster für einen Server bereitstellen und Ein Platzhaltergehäuse implementieren.

Schritt 5. **Das Servermuster bearbeiten.**

Mit Servermustern sorgen Sie über einen einzigen Verwaltungspunkt für eine einheitliche Konfiguration. Sie müssen die Einstellungen nicht mehr direkt auf den Servern konfigurieren. Stattdessen aktualisieren Sie die Kategoriemuster und Servermuster und die Änderungen werden automatisch für alle zugeordneten Profile und deren Server bereitgestellt.

Weitere Informationen zum Bearbeiten eines Servermusters finden Sie unter Ein Servermuster ändern.

Konfigurationshinweise

Bevor Sie mit der Konfiguration von Servern über Lenovo XClarity Administrator beginnen, sollten Sie die folgenden Aspekte berücksichtigen.

- Wenn ein Serverprofil frühere Firmwareversionen enthält und Sie die Firmware auf spätere Versionen aktualisieren, vergleicht XClarity Administrator die gespeicherten Profileinstellungen mit den Servereinstellungen und meldet „Nicht konform“. Bewegen Sie den Cursor über den Status „Nicht konform“, um den Grund für die mangelnde Konformität anzuzeigen.

Sie können den Status von Einheiten mit dem Status „Nicht konform“ manuell zu „Konform“ ändern, ohne das Profil erneut zu implementieren. Wählen Sie dazu die Einheiten aus und klicken Sie auf **Alle Aktionen → Konform machen**.

- Nach dem Aktualisieren der Firmware (z. B. UEFI, BMC oder E/A-Controller) auf einem Server ändern sich einige Konfigurationen möglicherweise (z. B. beim Hinzufügen neuer Elemente, Löschen vorhandener Elemente oder Ändern des Verhaltens oder des Wertebereichs eines Elements). Daher ist das Serverprofil ggf. nicht mehr konform oder das Anwenden des Servermusters schlägt fehl, wenn es mit einer vorherigen Firmwareversion erstellt wird. In diesem Fall wird empfohlen, ein neues Muster basierend auf der aktualisierten Firmware zu übernehmen oder das fehlerhafte Muster zu bearbeiten, um die Konfiguration bestimmter Elemente auszuschließen, und dieses Muster dann auf den Server anzuwenden.
- Der QLogic 8200 10 GbE SFP+ VFA-Adapter mit 2 Anschlüssen hat ungültige Werte für diese Einstellungen: iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName und IPv6LinkLocalAddress. Sie müssen diese Werte manuell in der Systemkonfiguration korrigieren, bevor Sie das Konfigurationsmuster vom Server übernehmen, oder die Werte im übernommenen Konfigurationsmuster korrigieren.
- Bei Flex System x240 und x440 Rechenknoten mit integrierten RAID-Adaptern, können Servermuster, die RAID-Konfigurationsdefinitionen definieren, nur auf Servern bereitgestellt werden, die über keine vorhandenen RAID-Konfigurationen verfügen. Wenn ein Servermuster auf einem Server mit vorhandener RAID-Konfiguration bereitgestellt wird, werden die vorhandenen Arrays und Volumen nicht überschrieben. Um die im Servermuster definierte RAID-Konfiguration zu übernehmen, müssen Sie zuerst die vorhandene RAID-Konfiguration des Servers löschen (siehe Speicheradapter auf Standardwerte zurücksetzen) und dann das Serverprofil über die Auswahl des Servers und einen Klick auf **Mehr → Serverprofil implementieren** bereitstellen.
- Die integrierten Speichercontroller in Flex System x220, Flex System x222 und ThinkSystem-Servern unterstützen softwarebasierte RAID. Die Konfiguration von Software-RAID mit Konfigurationsmustern wird jedoch nicht unterstützt.
- Wenn RAID mit Konfigurationsmuster konfiguriert wird und der Server ausgeschaltet ist, bootet der Server automatisch zur BIOS-/UEFI-Konfiguration, bevor das Serverprofil aktiviert wird.
- Konfigurationsmuster werden für ThinkServer-Server nicht unterstützt.
- Bestimmte E/A-Einheiten können nicht mithilfe von Servermustern konfiguriert werden. Siehe Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator für weitere Informationen.
- Wenn erweiterte Funktionen (z. B. SPAR, Easy Connect und Stack) auf den Flex-Switches EN4093R, CN4093, SI4093 oder SI4091 aktiviert sind, werden Netzwerkkonfigurationen möglicherweise nicht ordnungsgemäß auf die internen Ports angewendet.
- Flex-Switch SI4093 wird standardmäßig mit aktivierter SPAR ausgeliefert. Wenn Sie Netzwerkeinstellungen über Anschlussmuster für interne Ports auf diesen Switches bereitstellen müssen, müssen Sie die internen Ports des Switches manuell aus SPAR entfernen oder die SPAR-Konfigurationen vom Switch entfernen.
- Es wird empfohlen, Converged- und ThinkAgile-EinheitenXClarity Administrator *nicht* über Konfigurationsmuster zu konfigurieren.
- Stellen Sie sicher, dass alle verfügbaren Anschlüsse auf den installierten Adaptern aktiviert sind, bevor Sie die Konfigurationsmuster von einem vorhandenen Server erstellen, damit alle verfügbaren Anschlüsse und Einstellungen im Muster enthalten sind. Anschließend können Sie bei Bedarf alle Anschlüsse über die entsprechenden Einstellungen deaktivieren, die im Servermuster definiert sind. Wenn beim Erstellen des Musters Anschlüsse deaktiviert sind, wird das Muster möglicherweise nicht ordnungsgemäß erstellt und bereitgestellt.

Adresspools definieren

Ein *Adresspool* ist ein definierter Satz von Adressbereichen. Lenovo XClarity Administrator verwendet Adresspools, um bei der Bereitstellung von Servermustern auf Servern IP- und E/A-Adressen zu den jeweiligen Servern zuzuweisen.

Zu dieser Aufgabe

XClarity Administrator unterstützt IP- und E/A-Adresspools.

IP-Adresspools

IP-Adresspools definiert IP-Adressbereiche, die zum Konfigurieren der Netzwerkschnittstelle des Baseboard Management Controllers Ihrer Server verwendet werden. Sie können je nach Bedarf vordefinierte Adresspools anpassen oder neue Pools erstellen. Wenn Sie Servermuster erstellen, können Sie den während der Bereitstellung verwendeten IP-Adresspool auswählen. Wenn das Servermuster bereitgestellt wird, werden IP-Adressen aus dem gewählten Pool abgerufen und den einzelnen Management-Controllern zugewiesen.

Anmerkung: Verwenden Sie diese Option nicht, wenn Sie mit der Management-Controller-Netzwerkkonfiguration zufrieden sind.

Achtung:

- Stellen Sie sicher, dass Sie einen IP-Adressunterbereich auswählen, der nicht mit vorhandenen E/A-Adressen in Ihrem Rechenzentrum im Konflikt steht.
- Stellen Sie sicher, dass die IP-Adressen in den angegebenen Bereichen Teil desselben Subnetzes und von XClarity Administrator erreichbar sind.
- Stellen Sie sicher, dass die IP-Adressen in den angegebenen Bereichen für jede XClarity Administrator-Domäne und die vorhandenen IP-Verwaltungstools eindeutig sind, um Adresskonflikte zu verhindern.

Der Gesamtadresspoolbereich wird von über die angegebene Routingpräfix-Länge und das Gateway oder den anfänglichen Bereich festgelegt. Sie können je nach Routing-Präfixlänge Pools mit verschiedenen Größen erstellen. Gesamtpoolbereiche müssen jedoch in der XClarity Administrator-Domäne eindeutig sein. Die Bereiche werden dann aus dem gesamten Poolbereich erstellt.

Adressbereiche können verwendet werden, um Hosts zu trennen (z. b. nach Betriebssystemtyp, Workload-Typ und geschäftlicher Funktion). Adressbereiche können außerdem an organisatorische Netzwerkregeln gebunden werden.

Ethernet-Adresspools

Ethernet-Adresspools sind Zusammenstellungen mit eindeutigen MAC-Adressen, die bei der Konfiguration von Servern zu Netzwerkadaptern zugewiesen werden können. Sie können je nach Bedarf vordefinierte Adresspools anpassen oder neue Pools erstellen. Wenn Sie Servermuster erstellen, können Sie den während der Bereitstellung verwendeten Ethernet-Adresspool auswählen. Wenn das Servermuster bereitgestellt wird, werden IP-Adressen aus dem gewählten Pool abgerufen und den einzelnen Adapterports zugewiesen.

Der folgende vordefinierte MAC-Adresspool ist verfügbar:

- Lenovo MAC-Adresspool

Eine Liste mit den MAC-Adressbereichen in diesem Pool finden Sie unter Ethernet-Adresspool (MAC).

Fibre Channel-Adresspools

Fibre Channel-Adresspools sind Zusammenstellungen mit eindeutigen WWNN- und WWPN-Adressen, die bei der Konfiguration von Servern zu Fibre Channel-Adaptern zugewiesen werden können. Sie können je nach Bedarf vordefinierte Adresspools anpassen oder neue Pools erstellen. Wenn Sie Servermuster erstellen, können Sie den während der Bereitstellung verwendeten Fibre Channel-Adresspool auswählen. Wenn das Servermuster bereitgestellt wird, werden IP-Adressen aus dem gewählten Pool abgerufen und den einzelnen Adapterports zugewiesen.

Die folgenden vordefinierten Fibre Channel-Adresspools sind verfügbar:
- Lenovo WWN-Adressen
- Brocade WWN-Adressen
- Emulex WWN-Adressen
- QLogic WWN-Adressen

Eine Liste mit den WWN-Adressbereichen in diesem Pool finden Sie unter Fibre Channel-Adresspools (WWN).

Der Adressbereich in den Adresspools muss innerhalb der XClarity Administrator-Domäne eindeutig sein. XClarity Administrator stellt sicher, dass die definierten Bereiche und die zugewiesenen Adressen in der Verwaltungsdomäne eindeutig sind.

Wichtig: Stellen Sie in großen Umgebungen mit mehreren XClarity Administrator-Instanzen sicher, dass von jedem XClarity Administrator eindeutige Adressbereiche verwendet werden, um doppelte Adressen zu verhindern.

Ethernet- und Fibre Channel-Adresspools werden mit einer virtuellen E/A-Adapteradressierung verwendet, um organisatorisch eindeutige E/A-Adressen zuzuweisen. Wenn Sie ein Servermuster für einen Rechenknoten erstellen, können Sie die virtuelle Adressierung im Rahmen der Konfiguration der Einheiten und E/A-Adapter aktivieren. Wenn die virtuelle Adressierung aktiviert ist, werden Adressen aus den Ethernet- und den Fibre Channel-Adresspools zugewiesen. So werden Adresskonflikten verhindert.

Einschränkung: Die virtuelle Adressierung wird nur für Flex System-Rechenknoten unterstützt. Eigenständige Rack- und Tower-Server werden nicht unterstützt.

Informationen zum Erstellen von Servermustern finden Sie unter Ein Servermuster erstellen.

Einen IP-Adresspool erstellen

Ein *IP-Adresspool* definiert einen IP-Adressbereich, der zum Konfigurieren der Netzwerkschnittstelle des Baseboard Management Controllers Ihrer Server verwendet wird. Wenn das zugeordnete Servermuster bereitgestellt wird, werden IP-Adressen aus dem angegebenen Pool abgerufen und den einzelnen Servern zugewiesen.

Zu dieser Aufgabe

Die Daten in der Tabelle „Gesamte Netzwerkinformationen“ im Dialog Neuer IP-Adresspool werden aus der angegebenen Subnetzmaske und dem Gateway oder den anfänglichen Bereich abgeleitet. Je nach Subnetzmaske können Sie unterschiedlich große Pools erstellen, wobei der gesamte Poolbereich innerhalb der Verwaltungsdomäne eindeutig sein muss. Die Bereiche werden dann aus dem gesamten Poolbereich erstellt. Alle Bereiche müssen Teil desselben Subnetzes sein und werden durch die Grenzen in der Tabelle „Gesamte Netzwerkinformationen“ beschränkt.

Der Pool und die Bereiche einen Lenovo XClarity Administrator-Bereich. Erstellen Sie in großen Umgebungen mit mehreren XClarity Administrator-Instanzen eigene Pools und Bereiche für jeden XClarity Administrator, um Adresskonflikte zwischen den Instanzen mit vorhandenen IP-Verwaltungstools zu vermeiden. Bereiche

können außerdem zum Trennen von Hosts (z. B. nach Betriebssystemtyp, Workload-Typ und geschäftlicher Funktion) und zum Umsetzen von organisatorischen Netzwerkregeln genutzt werden.

Vorgehensweise

Gehen Sie wie folgt vor, um einen IP-Adresspool zu erstellen:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Adresspools**. Die Seite Konfigurationsmuster: Adresspools wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **IP-Adresspools**.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ). Der Dialog Assistent für neuen IP-Adresspool wird angezeigt.

Schritt 4. Tragen Sie die folgenden Informationen ein.

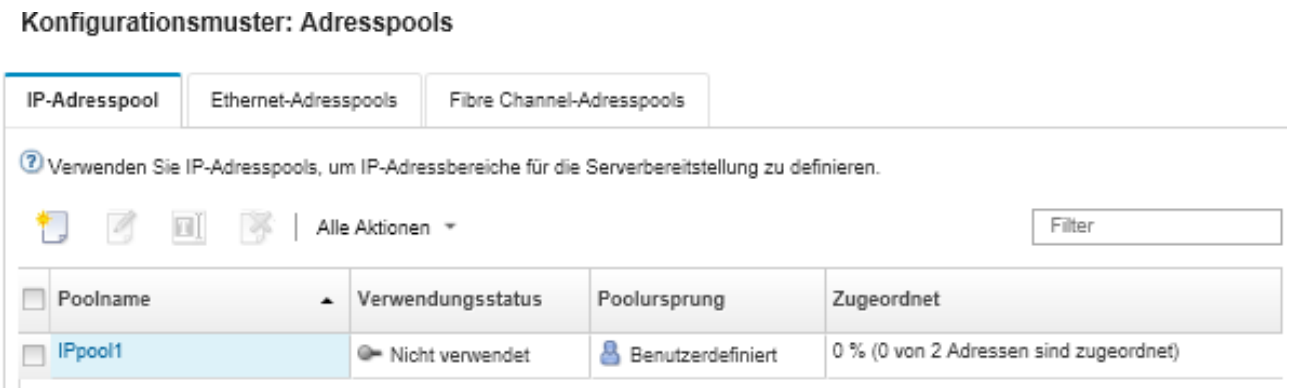
- Name und Beschreibung des Adresspools.
- Wählen Sie aus, ob IPv4- oder IPv6-Adressen verwendet werden sollen.
- Wählen Sie eine Subnetzmaske (für IPv4) oder eine Routingpräfix-Länge (für IPv6) aus.
- Geben Sie die Gateway-Adresse an.Die Werte für die Netzwerkinformationen werden über die angegebene Subnetzmaske und das Gateway oder den anfänglichen Bereich abgeleitet und in die Tabelle eingetragen.
- Fügen Sie einen oder mehrere Adressbereiche hinzu:
  1. Klicken Sie auf **Bereich hinzufügen**, um einen Adressbereich hinzuzufügen. Der Dialog Neuer IP-Adressbereich hinzufügen wird angezeigt.
  2. Geben Sie einen Bereichsnamen, die erste Adresse und die Größe des Bereichs ein.Die letzte Adresse wird automatisch berechnet.
  3. Klicken Sie auf **OK**.Der Bereich wird zur Tabelle **IP-Adressenpoolbereich definieren** hinzugefügt. Die Felder im Zusammenfassungsabschnitt werden automatisch aktualisiert.

  Mit dem Symbol **Bearbeiten** ( ) können Sie den Bereich bearbeiten. Über das Symbol **Entfernen** ( ) können Sie den Bereich löschen.

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

Nach dieser Aufgabe

Der neue IP-Adresspool wird in der Tabelle auf der Seite „IP-Adresspools“ aufgeführt:



Auf dieser Seite können Sie die folgenden Aktionen für einen ausgewählten Adresspool ausführen:

- Ändern des Adresspools über das Symbol **Bearbeiten** ( ).
- Umbenennen des Adresspools über das Symbol **Umbenennen**.

- Löschen des Adresspools über das Symbol **Löschen** ().
- Zeigen Sie Details zum Adressenpool an, einschließlich einer Zuordnung zwischen den virtuellen Adressen und den Ports der installierten Adapter und den reservierten Adressen, indem Sie auf den Poolnamen in der Spalte **Poolname** klicken.

Einen Ethernet-Adresspool erstellen

Ethernet-Adresspools sind Sammlungen mit eindeutigen MAC-Adressen (Media Access Control), die Netzwerkadaptern zugewiesen werden können. Sie können je nach Bedarf vordefinierte Adresspools anpassen oder neue Adresspools erstellen. Wenn Sie ein Servermuster erstellen und die virtuelle Adressierung für Ethernet-Adapter aktivieren, können Sie den zur Bereitstellung des Musters verwendeten Ethernet-Adresspool auswählen. Wenn das zugeordnete Servermuster bereitgestellt ist, werden MAC-Adressen aus dem angegebenen Pool abgerufen und den einzelnen Netzwerkadaptern der Server zugewiesen.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Ethernet-Adresspool zu erstellen:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Adresspools**. Die Seite Konfigurationsmuster: Adresspools wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ethernet-Adresspools**.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** (). Der Dialog Neue Ethernet-Adresspools (MAC) wird angezeigt.

Schritt 4. Geben Sie Name und Beschreibung des Adresspools ein.

Schritt 5. Fügen Sie einen oder mehrere Adressbereiche hinzu:

a. Klicken Sie auf **Bereich hinzufügen**, um einen Adressbereich hinzuzufügen. Der Dialog „Ethernet-Adresspool (MAC)“ wird angezeigt.

b. Geben Sie einen Bereichsnamen, die erste MAC-Adresse und die Größe des Bereichs ein.

   Die letzte MAC-Adresse wird automatisch berechnet.

c. Klicken Sie auf **Hinzufügen**.

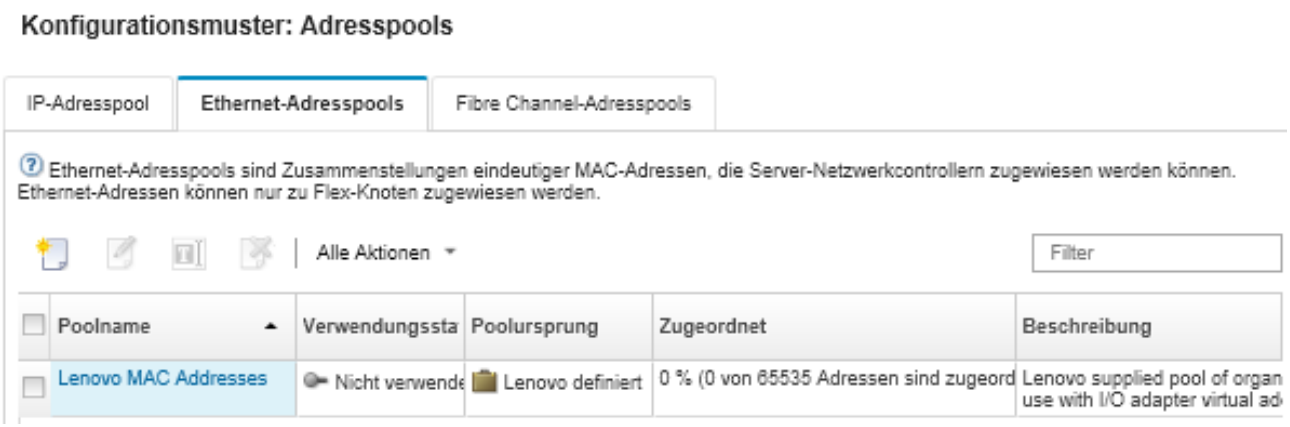
   Der Bereich wird zur Tabelle **Ethernet (MAC)-Pool – Adressbereiche definieren** hinzugefügt. Die Felder im Zusammenfassungsabschnitt werden automatisch aktualisiert.

   Mit dem Symbol **Bearbeiten** () können Sie den Bereich bearbeiten. Über das Symbol **Entfernen** () können Sie den Bereich löschen.

Schritt 6. Klicken Sie auf **Speichern**.

Nach dieser Aufgabe

Der neue Ethernet-Adressenpool wird auf der Seite „Ethernet-Adressenpools“ aufgeführt.



Auf dieser Seite können Sie die folgenden Aktionen für einen ausgewählten Adresspool ausführen:

- Ändern des Adresspools über das Symbol **Bearbeiten** ( ).
- Umbenennen des Adresspools über das Symbol **Umbenennen**.
- Löschen des Adresspools über das Symbol **Löschen** ( ).
- Zeigen Sie Details zum Adressenpool an, einschließlich einer Zuordnung zwischen den virtuellen Adressen und den Ports der installierten Adapter und den reservierten Adressen, indem Sie auf den Poolnamen in der Spalte **Poolname** klicken.

Ethernet-Adresspool (MAC)

Ethernet-Adresspools sind Sammlungen mit eindeutigen MAC-Adressen (Media Access Control), die Netzwerkadaptern zugewiesen werden können. Sie können die folgenden vordefinierten Adresspools in den Servermustern verwenden.

Tabelle 3. Lenovo MAC-Adresspool

Vordefinierter Bereich	Startadresse	Endadresse
Bereich 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Bereich 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Bereich 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Bereich 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Bereich 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
Bereich 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Bereich 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Bereich 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Bereich 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Einen Fibre Channel-Adresspool erstellen

Fibre Channel-Adresspools sind Sammlungen mit eindeutigen WWNN-Adressen (World Wide Node Name) und WWPN-Adressen (World Wide Port Name), die den Fibre Channel-Adaptern zugeordnet werden können. Sie können je nach Bedarf vordefinierte Adresspools anpassen oder neue Pools erstellen. Wenn Sie Servermuster erstellen und die virtuelle Adressierung für Ethernet-Adapter aktivieren, können Sie den zur Bereitstellung des Musters verwendeten Fibre Channel-Adresspool auswählen. Wenn das zugeordnete Servermuster bereitgestellt wird, werden WWNN- und WWPN-Adressen aus dem angegebenen Pool abgerufen und den einzelnen Servern zugewiesen.

Vorgehensweise

So erstellen Sie einen Fibre Channel-Adresspool:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Adresspools**. Die Seite Konfigurationsmuster: Adresspools wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Fibre Channel-Adresspools**.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ). Der Dialog Fibre Channel-Adressenpools wird angezeigt.

Schritt 4. Geben Sie Name und Beschreibung des Adresspools ein.

Schritt 5. Fügen Sie einen oder mehrere Adressbereiche hinzu:

a. Klicken Sie auf **Bereich hinzufügen**, um einen Adressbereich hinzuzufügen. Der Dialog „Fibre Channel-Adressbereich (WWN)“ wird angezeigt.

b. Geben Sie einen Bereichsnamen, die Bereichsgröße und die erste Adresse für jede Fabric ein.

Die letzten Adressen werden automatisch berechnet.

c. Klicken Sie auf **Hinzufügen**.

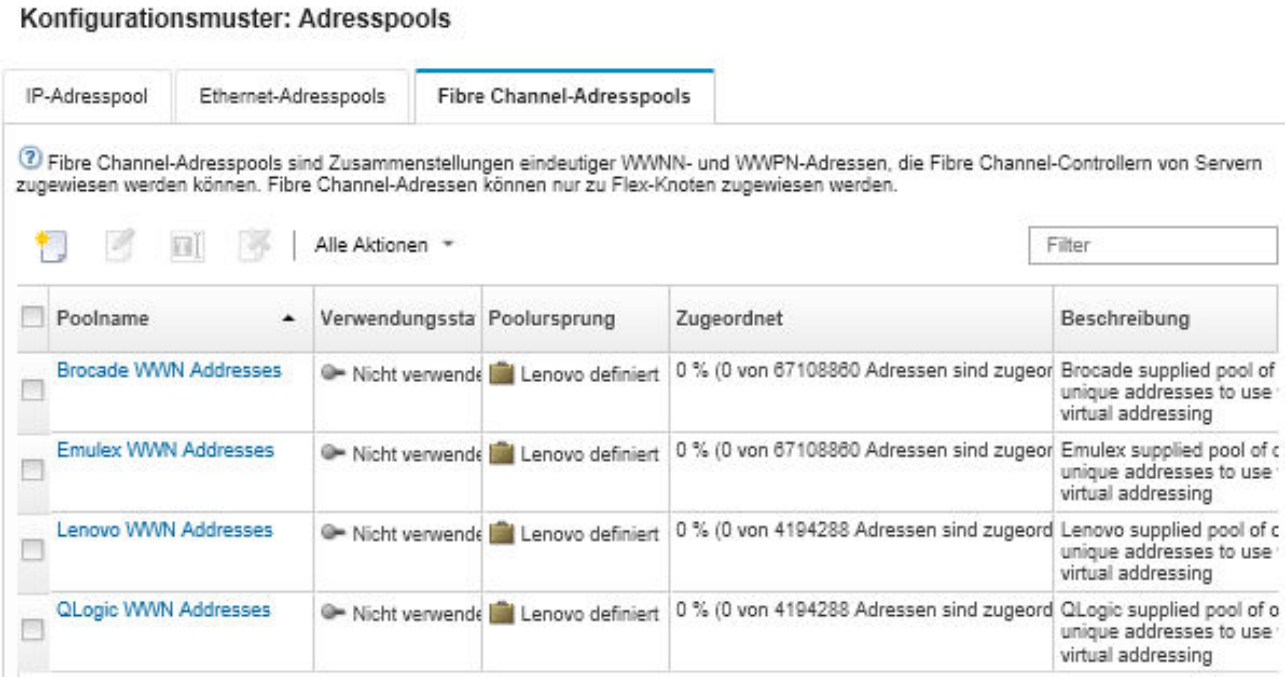
Der Bereich wird zur Tabelle **Fibre Channel-Pool-Adressbereiche definieren** hinzugefügt. Die Felder im Zusammenfassungsabschnitt werden automatisch aktualisiert.

Mit dem Symbol **Bearbeiten** ( ) können Sie den Bereich bearbeiten. Über das Symbol **Entfernen** ( ) können Sie den Bereich löschen.

Schritt 6. Klicken Sie auf **Speichern**.

Nach dieser Aufgabe

Der neue Fibre Channel-Adresspool wird in der Tabelle „Fibre Channel-Adresspools“ aufgeführt.



Auf dieser Seite können Sie die folgenden Aktionen für einen ausgewählten Adresspool ausführen:

- Ändern des Adresspools über das Symbol **Bearbeiten** ( ).

- Löschen des Adresspools über das Symbol **Löschen** ( ).
- Zeigen Sie Details zum Adressenpool an, einschließlich einer Zuordnung zwischen den virtuellen Adressen und den Ports der installierten Adapter und den reservierten Adressen, indem Sie auf den Poolnamen in der Spalte **Poolname** klicken.

Fibre Channel-Adresspools (WWN)

Fibre Channel-Adresspools sind Sammlungen mit eindeutigen WWNN-Adressen (World Wide Node Name) und WWPN-Adressen (World Wide Port Name), die den Fibre Channel-Adaptern zugeordnet werden können. Sie können die folgenden vordefinierten Adresspools in den Servermustern verwenden.

Tabelle 4 „Brocade WWN-Adresspool“ auf Seite 355 führt die Brocade WWN-Adresspools auf. Jeder Brocade-Bereich enthält 1.864.135 Adressen.

Tabelle 5 „Emulex WWN-Adresspool“ auf Seite 356 führt die Emulex WWN-Adresspools auf. Jeder Emulex-Bereich enthält 1.864.135 Adressen.

Tabelle 6 „Lenovo WWN-Adresspool“ auf Seite 357 führt die Lenovo WWN-Adresspools auf. Jeder Lenovo WWN-Bereich enthält 116.508 Adressen.

Tabelle 7 „QLogic WWN-Adresspool“ auf Seite 358 führt die QLogic WWN-Adresspools auf. Jeder QLogic WWN-Bereich enthält 116.508 Adressen.

Tabelle 4. Brocade WWN-Adresspool

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Anfangsadresse	Weltweiter Portname (WWPN) Endadresse
Struktur A				
Bereich 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Bereich 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
Bereich 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Bereich 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Bereich 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Bereich 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Bereich 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Bereich 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Bereich 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Struktur B				
Bereich 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Bereich 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D

Tabelle 4. Brocade WWN-Adresspool (Forts.)

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Anfangsadresse	Weltweiter Portname (WWPN) Endadresse
Bereich 3	2B:FB:00:05:1E:38: E3:8E	2B: FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38: E3:8E	2B: FD:00:05:1E:55:55:54
Bereich 4	2B: FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71: C7:1B	2B: FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71: C7:1B
Bereich 5	2B:FB:00:05:1E:71: C7:1C	2B:FB:00:05:1E:8E:38: E2	2B:FD:00:05:1E:71: C7:1C	2B:FD:00:05:1E:8E:38: E2
Bereich 6	2B:FB:00:05:1E:8E:38: E3	2B:FB:00:05:1E:AA:AA: A9	2B:FD:00:05:1E:8E:38: E3	2B:FD:00:05:1E:AA:AA: A9
Bereich 7	2B:FB:00:05:1E:AA:AA: AA	2B:FB:00:05:1E: C7:1C:70	2B:FD:00:05:1E:AA:AA: AA	2B:FD:00:05:1E: C7:1C:70
Bereich 8	2B:FB:00:05:1E: C7:1C:71	2B:FB:00:05:1E: E3:8E:37	2B:FD:00:05:1E: C7:1C:71	2B:FD:00:05:1E: E3:8E:37
Bereich 9	2B:FB:00:05:1E: E3:8E:38	2B:FB:00:05:1E:FF:FF: FE	2B:FD:00:05:1E: E3:8E:38	2B:FD:00:05:1E:FF:FF: FE

Tabelle 5. Emulex WWN-Adresspool

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Anfangsadresse	Weltweiter Portname (WWPN) Endadresse
Struktur A				
Bereich 1	2F:FE:00:00: C9:00:00:00	2F:FE:00:00:C9:1C:71: C6	2F:FC:00:00: C9:00:00:00	2F:FC:00:00:C9:1C:71: C6
Bereich 2	2F:FE:00:00:C9:1C:71: C7	2F:FE:00:00:C9:38: E3:8D	2F:FC:00:00:C9:1C:71: C7	2F:FC:00:00:C9:38: E3:8D
Bereich 3	2F:FE:00:00:C9:38: E3:8E	2F:FE:00:00: C9:55:55:54	2F:FC:00:00:C9:38: E3:8E	2F:FC:00:00: C9:55:55:54
Bereich 4	2F:FE:00:00: C9:55:55:55	2F:FE:00:00:C9:71: C7:1B	2F:FC:00:00: C9:55:55:55	2F:FC:00:00:C9:71: C7:1B
Bereich 5	2F:FE:00:00:C9:71: C7:1C	2F:FE:00:00:C9:8E:38: E2	2F:FC:00:00:C9:71: C7:1C	2F:FC:00:00:C9:8E:38: E2
Bereich 6	2F:FE:00:00:C9:8E:38: E3	2F:FE:00:00:C9:AA:AA: A9	2F:FC:00:00:C9:8E:38: E3	2F:FC:00:00:C9:AA:AA: A9
Bereich 7	2F:FE:00:00:C9:AA:AA: AA	2F:FE:00:00:C9: C7:1C:70	2F:FC:00:00:C9:AA:AA: AA	2F:FC:00:00:C9: C7:1C:70
Bereich 8	2F:FE:00:00:C9: C7:1C:71	2F:FE:00:00:C9: E3:8E:37	2F:FC:00:00:C9: C7:1C:71	2F:FC:00:00:C9: E3:8E:37
Bereich 9	2F:FE:00:00:C9: E3:8E:38	2F:FE:00:00:C9:FF:FF: FE	2F:FC:00:00:C9: E3:8E:38	2F:FC:00:00:C9:FF:FF: FE
Struktur B				
Bereich 1	2F:FF:00:00: C9:00:00:00	2F:FF:00:00:C9:1C:71: C6	2F:FD:00:00: C9:00:00:00	2F:FD:00:00:C9:1C:71: C6
Bereich 2	2F:FF:00:00:C9:1C:71: C7	2F:FF:00:00:C9:38: E3:8D	2F:FD:00:00:C9:1C:71: C7	2F:FD:00:00:C9:38: E3:8D

Tabelle 5. Emulex WWN-Adresspool (Forts.)

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Anfangsadresse	Weltweiter Portname (WWPN) Endadresse
Bereich 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
Bereich 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
Bereich 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Bereich 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Bereich 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Bereich 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Bereich 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Tabelle 6. Lenovo WWN-Adresspool

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Anfangsadresse	Weltweiter Portname (WWPN) Endadresse
Struktur A				
Bereich 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Bereich 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
Bereich 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Bereich 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Bereich 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Bereich 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Bereich 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Bereich 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Bereich 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Struktur B				
Bereich 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Bereich 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37

Tabelle 6. Lenovo WWN-Adresspool (Forts.)

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Anfangsadresse	Weltweiter Portname (WWPN) Endadresse
Bereich 3	20:81:00:50:76:23:8E:3-8	20:81:00:50:76:25:55:5-3	21:81:00:50:76:23:8E:3-8	21:81:00:50:76:25:55:5-3
Bereich 4	20:81:00:50:76:25:55:5-4	20:81:00:50:76:27:1C:-6F	21:81:00:50:76:25:55:5-4	21:81:00:50:76:27:1C:-6F
Bereich 5	20:81:00:50:76:27:1C:-70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:-70	21:81:00:50:76:28:E3:8B
Bereich 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Bereich 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Bereich 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Bereich 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Tabelle 7. QLogic WWN-Adresspool

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Endadresse	Weltweiter Portname (WWPN) Endadresse
Struktur A				
Bereich 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
Bereich 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
Bereich 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
Bereich 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
Bereich 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
Bereich 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
Bereich 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
Bereich 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
Bereich 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
Struktur B				
Bereich 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
Bereich 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37

Tabelle 7. QLogic WWN-Adresspool (Forts.)

Vordefinierter Bereich	Weltweiter Knotenname (WWNN) Anfangsadresse	Weltweiter Knotenname (WWNN) Endadresse	Weltweiter Portname (WWPN) Endadresse	Weltweiter Portname (WWPN) Endadresse
Bereich 3	20:81:00: E0:8B:23:8E:38	20:81:00: E0:8B:25:55:53	21:81:00: E0:8B:23:8E:38	21:81:00: E0:8B:25:55:53
Bereich 4	20:81:00: E0:8B:25:55:54	20:81:00: E0:8B:27:1C:6F	21:81:00: E0:8B:25:55:54	21:81:00: E0:8B:27:1C:6F
Bereich 5	20:81:00: E0:8B:27:1C:70	20:81:00:E0:8B:28: E3:8B	21:81:00: E0:8B:27:1C:70	21:81:00:E0:8B:28: E3:8B
Bereich 6	20:81:00:E0:8B:28: E3:8C	20:81:00:E0:8B:2A:AA: A7	21:81:00:E0:8B:28: E3:8C	21:81:00:E0:8B:2A:AA: A7
Bereich 7	20:81:00:E0:8B:2A:AA: A8	20:81:00:E0:8B:2C:71: C3	21:81:00:E0:8B:2A:AA: A8	21:81:00:E0:8B:2C:71: C3
Bereich 8	20:81:00:E0:8B:2C:71: C4	20:81:00:E0:8B:2E:38: DF	21:81:00:E0:8B:2C:71: C4	21:81:00:E0:8B:2E:38: DF
Bereich 9	20:81:00:E0:8B:2E:38: E0	20:81:00:E0:8B:2F:FF: FB	21:81:00:E0:8B:2E:38: E0	21:81:00:E0:8B:2F:FF: FB

Mit Servermustern arbeiten

Ein *Servermuster* ist eine vor der Betriebssysteminstallation vorgenommene Serverkonfiguration mit Einstellungen für den lokalen Speicher, E/A-Adapter, SAN-Boot und weitere Baseboard Management Controller- und UEFI-Firmwareeinstellungen. Servermuster bieten außerdem integrierte Unterstützung für die Virtualisierung von E/A-Adressen, sodass Sie Server-Fabric-Verbindungen virtualisieren oder Server unterbrechungsfrei einem anderen Zweck zuführen können. Ein Servermuster ist ein Gesamtmuster für die schnelle Konfiguration mehrerer Server.

Zu dieser Aufgabe

Sie können mehrere Servermuster definieren, um so die verschiedenen, in Ihrem Rechenzentrum verwendeten Konfigurationen abzubilden.

Wenn Sie ein Servermuster definieren, können Sie die benötigten Kategoriemuster und Adresspools für die gewünschte Konfiguration einer bestimmten Servergruppe auswählen oder ggf. erstellen. Ein *Kategoriemuster* definiert bestimmte Firmwareeinstellungen, die in mehreren Servermustern wiederverwendet werden können. Sie können Adresspools für die Definition von Adressbereichen verwenden und damit den einzelnen Servern bei der Musterimplementierung Adressen zuordnen. Es gibt IP-Adresspools, Ethernet-Adresspools (MAC) und Fibre Channel-Adresspools (WWN).

Wird ein Servermuster für mehrere Server implementiert, werden automatisch mehrere Serverprofile generiert (ein Profil für jeden Server). Jedes Profil übernimmt die Einstellungen vom jeweils übergeordneten Servermuster, sodass Sie eine einheitliche Konfiguration von einem zentralen Ort aus steuern können.

Sie können auch ein völlig neues Servermuster erstellen und die gewünschte Konfiguration vor Eintreffen Ihrer Hardware definieren. Alternativ können Sie ein Servermuster von einem vorhandenen Server übernehmen und dieses für die verbleibenden Server bereitstellen. Bei der Übernahme eines Servermusters von einem vorhandenen Server werden erweiterte Kategoriemuster aus den derzeitigen Servereinstellungen übernommen und dynamisch erstellt. Wenn Sie die Kategorieeinstellungen ändern möchten, können Sie diese direkt in den Servermustern bearbeiten.

Achtung: Wenn Sie ein völlig neues Servermuster erstellen, müssen Sie die Booteinstellungen für die Server definieren. Im Rahmen der Musterimplementierung wird die vorhandene Bootreihenfolge auf den Servern mit den Standardeinstellungen der Bootreihenfolge im Servermuster überschrieben. Falls die Server nach einer Musterimplementierung nicht starten, kann das daran liegen, dass die ursprünglichen Booteinstellungen mit den Standardeinstellungen der Bootreihenfolge des neuen Servermusters überschrieben wurden. Informationen über die Wiederherstellung der ursprünglichen Booteinstellungen auf den Servern finden Sie unter Booteinstellungen nach der Servermusterimplementierung wiederherstellen.

Wichtig: Beim Erstellen von Servermustern müssen Sie sicherstellen, dass die Erstellung für die verschiedenen Servertypen erfolgt. Beispielsweise können Sie ein Servermuster für alle Flex System x240 Rechenknoten und ein weiteres Servermuster für alle Flex System x440 Rechenknoten erstellen. Implementieren Sie kein Servermuster, das für einen bestimmten Servertyp erstellt wurde, für einen anderen Servertyp.

Wichtig: Wenn der Verwaltungsknoten ausfällt, verlieren Sie unter Umständen Ihre Servermuster. Speichern Sie stets die Verwaltungssoftware nach jeder Erstellung oder Bearbeitung von Servermustern (siehe Lenovo XClarity Administrator sichern).

Einstellungen für Netzwerkeinheiten

Einige Flex System-Netzwerkeinheiten bieten mehr Konfigurationsoptionen für Servermuster als andere Einheiten.

Obwohl Servermuster für alle Netzwerkeinheiten verwendet werden können, sind einige Servermusterfunktionen auf bestimmte Netzwerkadapter beschränkt. Zudem werden einige erweiterte Einstellungen für Ethernet-Netzwerkadapter (z. B. Kompatibilitätseinstellungen für Adapter und Ports) derzeit nicht unterstützt.

Servermuster können vorhandene Konfigurationsdaten und -einstellungen für unterstützte Netzwerkadapter übernehmen und Konfigurationseinstellungen durch die Musterimplementierung ändern.

Kategoriemuster

Die Firmwareeinstellungen sind in Kategorien mit ähnlichen Einstellungen zusammengefasst. Sie können für jede Kategorie ein *Kategoriemuster* mit einheitlichen Firmwareeinstellungen erstellen, die in mehreren Servermustern wiederverwendet werden können. Die meisten Firmwareeinstellungen lassen sich sowohl direkt per Baseboard Management Controller und UEFI als auch mithilfe von Kategoriemustern konfigurieren. Welche Firmwareeinstellungen verfügbar sind, hängt vom Servertyp, der Flex System-Umgebung und dem Funktionsumfang des Servermusters ab.

Sie können Kategoriemuster unabhängig von Servermustern erstellen.

Kategoriemuster können vordefiniert, benutzerdefiniert oder von vorhandenen Servern übernommen werden.

- **Erweiterte Kategoriemuster**

  Erweiterte Kategoriemuster werden für einige E/A-Adapterports, erweiterte UEFI- und Baseboard Management-Controller(BMC)-Einstellungen verwendet, die vom angegebenen verwalteten Server übernommen und dynamisch erstellt werden. Wenn Sie ein Servermuster von einem vorhandenen Server erstellen, generiert Lenovo XClarity Administrator diese Muster. Erweiterte Kategoriemuster können nicht manuell erstellt werden, aber Sie können die Muster nach der Erstellung bearbeiten.

  Die folgenden erweiterten UEFI-Muster werden von XClarity Administrator vordefiniert, um Ihre Server für spezielle Umgebungen zu optimieren.
  - **ESXi-Installationsoptionen**
  - **Effizienz – Schwerpunkt Leistung**
  - **Effizienz – Schwerpunkt Stromersparnis**

  - **Maximale Leistung**
  - **Minimaler Stromverbrauch**
- **Benutzerdefinierte Kategoriemuster**

  Benutzerdefinierte Kategoriemuster werden von Ihnen erstellt und umfassen Systeminformationen, Verwaltungsschnittstellen, Einheiten und E/A-Ports, Fibre Channel-Bootziele und E/A-Adapterports. Sie können die folgenden Kategoriemuster erstellen:

  - **Systeminformationen**. Zu den Einstellungen gehören die automatische Systemnamengenerierung sowie Kontaktnamen und Standorte.
  - **Verwaltungsschnittstelle**. Zu den Einstellungen gehören die automatische Hostnamengenerierung, IP-Adresse, DNS (Domain Name System), Internetverbindungsgeschwindigkeit und Portzuordnungen für die Verwaltungsschnittstelle.Duplexeinstellungen werden von Servermustern nicht unterstützt.
  - **Einheiten und E/A-Ports**. Zu den Einstellungen gehören Konsolenumleitungen und COM-Ports. Mit Servermustern können Sie Serial over LAN im Bereich „Konsolenumleitung“ aktivieren. Bei Aktivierung von Serial over LAN unterstützen die Servermuster jedoch nur die Einstellung **Dediziert** als Zugriffsmodus für serielle Ports; die IPMI-Einstellungen **Shared** und **Pre-Boot** stehen als Zugriffsmodi für serielle Ports in Servermustern nicht zur Verfügung.

    Wichtig: Wenn Sie ein Servermuster von einem vorhandenen Server erstellen und für diesen Server **Shared** oder **Pre-Boot** als Zugriffsmodus für serielle Ports eingestellt ist, weist das vom Server übernommene Muster für Einheiten und E/A-Ports die Einstellung **Dediziert** auf.
  - **Fibre Channel-Bootziele**. Zu den Einstellungen gehören primäre und sekundäre Fibre Channel-Bootziele (WWN).
  - **Ports**. Zu den Einstellungen gehören E/A-Adapter und Ports für die Fabric-Verbindungskonfiguration.

Ein Servermuster erstellen

Wenn Sie ein Servermuster erstellen, definieren Sie die Konfigurationseigenschaften für einen bestimmten Servertyp. Sie können ein Servermuster mit den Standardeinstellungen von Grund auf neu erstellen oder Einstellungen eines vorhandenen Servers nutzen.

Zu dieser Aufgabe

Berücksichtigen Sie vor der Erstellung eines Servermusters die folgenden Aspekte.

- Verwenden Sie einen vorhandenen Server zum ersten Erstellen eines Servermusters. Wenn Sie ein Servermuster von einem vorhandenen Server erstellen, übernimmt und erstellt Lenovo XClarity Administrator erweiterte Kategoriemuster für einige E/A-Adapteranschlüssel, UEFI und Baseboard Management Controller-Einstellungen. Anschließend können diese Kategoriemuster für jedes nachfolgend erstellte Servermuster genutzt werden. Weitere Informationen zu Kategoriemustern finden Sie unter Firmwareeinstellungen definieren.
- Ermitteln Sie Servergruppen mit den gleichen Hardwareoptionen, die identisch konfiguriert werden sollen. Sie können ein Servermuster verwenden, um dieselben Konfigurationseinstellungen auf mehrere Server anzuwenden und so über einen zentralen Ort eine gemeinsame Konfiguration umsetzen.
- Die Aspekte der Konfiguration angeben, die für das Servermuster angepasst werden sollen (z. B. Einstellungen zum lokalen Speicher, zu den Netzwerkadaptern, Booteinstellungen, Management Controller-Einstellungen und UEFI-Einstellungen).
- Sie können mithilfe von Konfigurationsmustern weder lokale Benutzeraccounts verwalten noch den LDAP-Server konfigurieren.

Wichtig: Wenn der Verwaltungsknoten ausfällt, verlieren Sie unter Umständen Ihre Servermuster. Sichern Sie die Verwaltungssoftware nach jeder Erstellung oder Bearbeitung von Servermustern (siehe Lenovo XClarity Administrator sichern).

Vorgehensweise

So erstellen Sie ein Servermuster.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Servermuster**.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ). Der Neue Assistent für Servermuster wird angezeigt.

Schritt 4. So erstellen Sie das Servermuster:

- Klicken Sie auf **Neues Muster auf Basis eines vorhandenen Servers erstellen**, um Einstellungen von einem vorhandenen Server zu verwenden. Wählen Sie anschließend in der angezeigten Liste den verwalteten Server aus, auf dem das neue Muster basieren soll.

  Wenn Sie ein Servermuster von einem vorhandenen Server erstellen, übernimmt XClarity Administrator die Einstellungen von dem angegebenen verwalteten Server (einschließlich der Einstellungen für den erweiterten Anschluss, UEFI und Baseboard Management Controller) und erstellt dynamisch Kategoriemuster für diese Einstellungen. Bei einem völlig neuen Server übernimmt Lenovo XClarity Administrator die werkseitigen Voreinstellungen. Wenn der Server von XClarity Administrator verwaltet wird, verwendet XClarity Administrator die angepassten Einstellungen. Sie können die Einstellungen anschließend für die Server anpassen, auf denen das Muster bereitgestellt wird.
- Klicken Sie auf **Völlig neues Muster erstellen**, um Standardeinstellungen zu verwenden. Wählen Sie anschließend im Feld **Abmessungen** den Servertyp aus.

Anmerkung: Die Optionen auf den verbleibenden Registerkarten können sich, je nach dem Typ des Servers, für den Sie ein Muster erstellen, unterscheiden.

Schritt 5. Geben Sie den Namen des Musters und eine Beschreibung ein.

Schritt 6. Passen Sie den Serverprofilnamen an, indem Sie die Option **Anpassen** auswählen und dann ein oder mehrere Elemente auswählen, die in das Benennungsschema aufgenommen werden sollen (z. B. angepasster Text, Servername und fortlaufende Nummer) und die Reihenfolge.

Schritt 7. Klicken Sie auf **Weiter**.

Schritt 8. Wählen Sie die lokale Speicherkonfiguration aus, die bei der Bereitstellung dieses Musters auf einem Server angewendet wird. Klicken Sie auf **Weiter**.

Informationen zu den lokalen Speichereinstellungen finden Sie unter Lokalen Speicher definieren.

Schritt 9. **Optional:** Ändern Sie die E/A-Adapteradressierung und definieren Sie zusätzliche E/A-Adapter zur Anpassung an die Hardware, die Sie vermutlich mit diesem Muster konfigurieren werden. Klicken Sie auf **Weiter**.

Informationen zu den E/A-Adaptereinstellungen finden Sie unter E/A-Adapter definieren.

Schritt 10. Definieren Sie die Bootreihenfolge, die bei der Bereitstellung dieses Musters auf einem Server angewendet wird. Klicken Sie auf **Weiter**.

Informationen zu Einstellungen für SAN-Bootziele finden Sie unter Bootoptionen definieren.

Schritt 11. Ausgewählte Firmwareeinstellungen aus der Liste vorhandener Kategoriemuster.

Sie können neue Kategoriemuster erstellen. Klicken Sie dazu auf das Symbol **Erstellen** ( ).

Weitere Informationen zu Firmwareeinstellungen finden Sie unter Firmwareeinstellungen definieren.

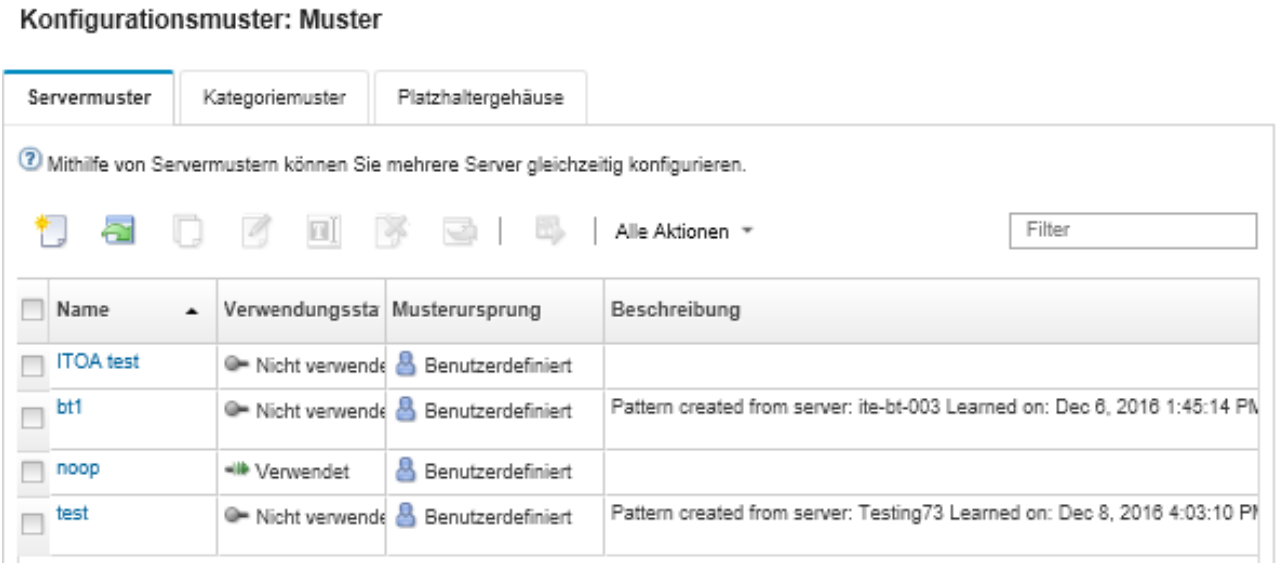
Schritt 12. Klicken Sie auf **Speichern**, um das Muster zu speichern, oder klicken Sie auf **Speichern und Bereitstellen**, um das Muster zu speichern und sofort auf einem oder mehreren Servern bereitzustellen.

Informationen zum Implementieren von Servermustern finden Sie unter Servermuster für einen Server bereitstellen.

Nach dieser Aufgabe

Wenn Sie auf **Speichern und Bereitstellen** klicken, wird die Seite Servermuster bereitstellen angezeigt. Auf dieser Seite können Sie das Servermuster auf bestimmten Servern bereitstellen.

Wenn Sie auf **Speichern** klicken, werden die Servermuster und alle Kategoriemuster auf der Seite Servermuster gespeichert.



Auf dieser Seite können Sie die folgenden Aktionen für ausgewählte Servermuster ausführen:

- Klicken Sie auf den Musternamen in der Spalte **Name** zum Anzeigen von Informationen zum ausgewählten Muster.
- Bereitstellen des Musters (siehe Servermuster für einen Server bereitstellen).
- Kopieren des Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Bearbeiten des Musters (siehe Ein Servermuster ändern).
- Umbenennen des Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Löschen des Musters über einen Klick auf das Symbol **Löschen** ( ).
- Export und Import von Servermustern (siehe Server- und Kategoriemuster exportieren und importieren).

Lokalen Speicher definieren

Sie können die Konfiguration des lokalen Speichers definieren, die bei der Implementierung dieses Musters auf die Zielserver angewendet wird.

Zu dieser Aufgabe

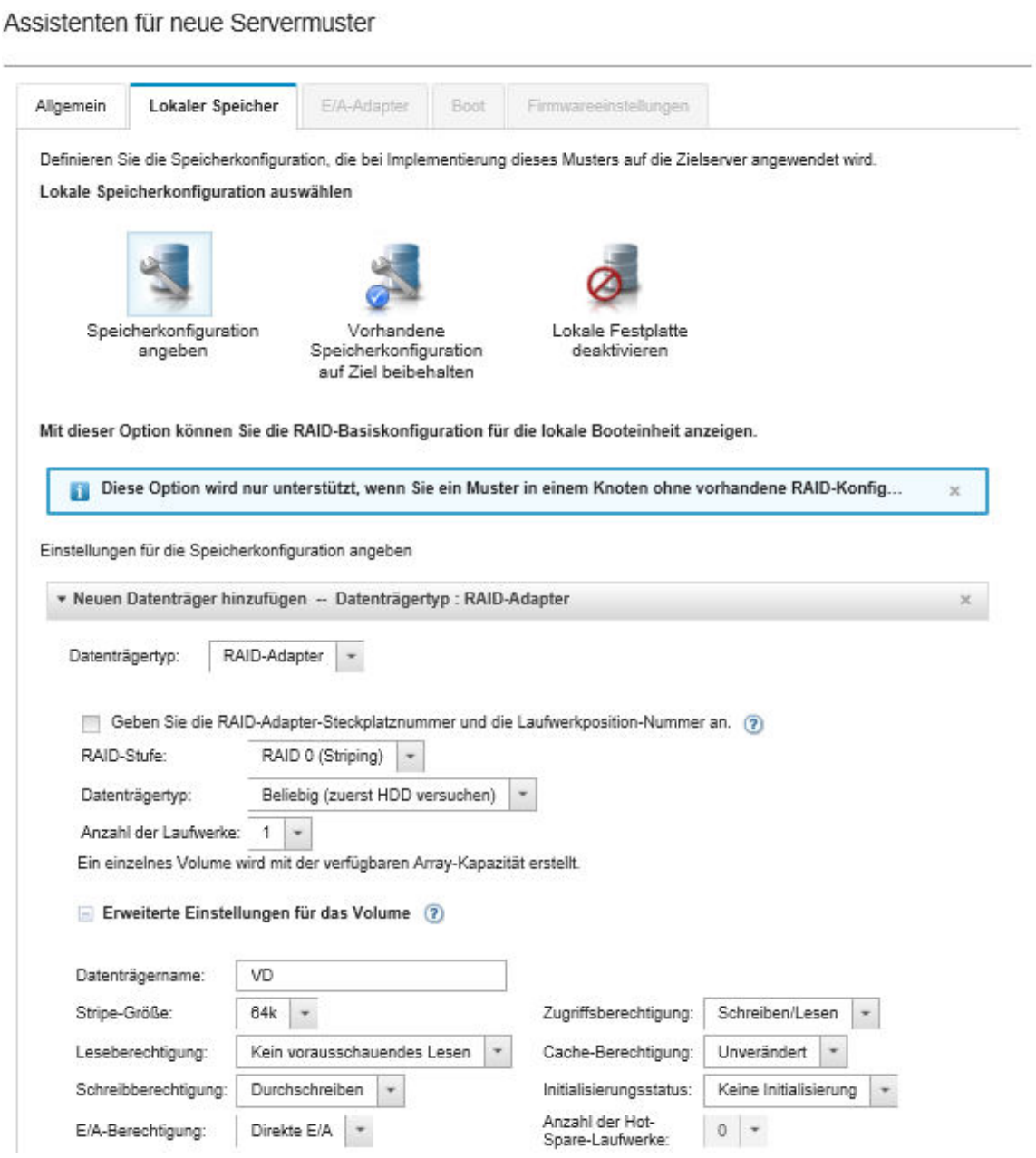
Anmerkungen:

- Die integrierten Speichercontroller in Flex System x220, Flex System x222 und ThinkSystem-Servern unterstützen softwarebasierte RAID. Die Konfiguration von Software-RAID mit Konfigurationsmustern wird jedoch nicht unterstützt.
- Wenn RAID mit Konfigurationsmuster konfiguriert wird und der Server ausgeschaltet ist, bootet der Server automatisch zur BIOS-/UEFI-Konfiguration, bevor das Serverprofil aktiviert wird.

Vorgehensweise

Gehen Sie wie folgt vor, um die Konfiguration des lokalen Speichers zu definieren.

Schritt 1. Klicken Sie im Assistenten für neue Servermuster auf die Registerkarte **Lokaler Speicher**.



Schritt 2. Wählen Sie eine der folgenden Optionen aus, um die Einstellungen für den lokalen Speicher zu definieren.

- **Speicherkonfiguration angeben**. (Nur Einheiten ohne vorhandene RAID-Konfigurationen) Die RAID-Grundeinstellungen werden auf der lokalen Booteinheit während der Implementierung konfiguriert.

  Geben Sie die Speicherkonfiguration basierend auf der Speicheroption an. Sie können weitere Speicheroptionen hinzufügen, indem Sie auf das Symbol **Hinzufügen** () klicken.

  - **RAID-Adapter**. Wählen Sie die RAID-Stufe, Eigenschaften und die Anzahl der auf dem Server installierten Laufwerke aus. Es werden RAID 0, 1 und 5 unterstützt. Darüber hinaus können Sie erweiterte Datenträgereinstellungen auswählen, z. B. Stripe-Größe, Richtlinien und Anzahl der Hot-Spare-Laufwerke.

    ThinkSystem Server mit XCC-Version 2.1 und höher (ThinkSystem SR950 erfordert XCC-Version 1.4 oder höher): Sie können auch die RAID-Adapter-Steckplatznummer und die Nummern der Laufwerkpositionen angeben, um einen einzelnen Datenträger mit der verfügbaren Arraykapazität zu erstellen. In diesem Fall werden die RAID-Stufen 0, 1, 5, 6, 10, 50, 60 und 00 unterstützt. Darüber hinaus können Sie erweiterte Datenträgereinstellungen auswählen, z. B. Stripe-Größe, Richtlinien und Hot-Spare-Laufwerke.

    Anmerkung: Stellen Sie auf dem Zielserver sicher, dass genügend Laufwerke des entsprechenden Typs vorhanden sind. Achten Sie zudem darauf, dass der RAID-Status der Laufwerke „Unconfigured Good“ lautet, wie im Abschnitt **Laufwerke** auf der Seite „Inventardetails“ des Servers angegeben (siehe Die Details eines verwalteten Servers anzeigen
  - **Lenovo SD-Medienadapter**. Legen Sie fest, wo der Datenträger und die Datenträgergröße erstellt werden sollen. Sie können auch erweiterte Datenträgereinstellungen auswählen, z. B Medientyp und Zugriffsrichtlinie.
  - **ThinkSystem M.2 mit Spiegelung**. Wählen Sie den PCI-Steckplatz, die RAID-Stufe, den Datenträgernamen und die Stripe-Größe aus, um einen einzelnen Datenträger mit der verfügbaren Arraykapazität zu erstellen.

    - Sie können mehrere ThinkSystem M.2 mit Speicheradaptern für die Spiegelung definieren, die sich jeweils in einem anderen PCI-Steckplatz befinden.
    - Für ThinkSystem Edge Server müssen Sie eine bestimmte PCI-Steckplatznummer angeben. Für andere ThinkSystem Server, auf denen nur ein M.2-RAID-Adapter installiert ist, können Sie „Erste Übereinstimmung“ (der Standardwert) oder eine bestimmte PCI-Steckplatznummer angeben.
  - **Nichtflüchtiger Intel Optane DC Speicher**. Wählen Sie den Typ des nichtflüchtigen Speichers, den Warnungsschwellenwert für den Prozentsatz der verbleibenden Kapazität und den Prozentsatz der als Speicher zu verwendenden Gesamtkapazität aus. (Der verbleibende Speicher wird als nichtflüchtiger Speicher genutzt).

    Achtung:
    - Um nichtflüchtige Intel Optane DC-DIMMs zu konfigurieren, muss die Sicherheit deaktiviert werden und es darf kein Namespace erstellt werden.
    - Die Option „Sicherheit aktivieren“ wird nur unterstützt, sofern der Sicherheitsstatus für alle nichtflüchtigen Intel Optane DC-DIMMs im Server „Deaktiviert“ lautet.
    - Die Optionen „Sicherheit deaktivieren“ und „Sicheres Löschen“ werden nur unterstützt, wenn der Sicherheitsstatus „Gesperrt“ ist und der Verschlüsseltungstext für alle nichtflüchtigen Intel Optane DC-DIMMs im Server identisch ist.
    - Der Intel Optane DC PMEM-Sicherheitsstatus ist nicht im XClarity Administrator-Bestand enthalten. Sie können den Sicherheitsstatus manuell in der UEFI überprüfen.
- **Vorhandene Speicherkonfiguration auf Ziel beibehalten**. Die vorhandene Speicherkonfiguration wird während der Implementierung nicht geändert. Wählen Sie diese

Option aus, wenn die bereits auf dem Zielserver vorhandene Speicherkonfiguration verwendet werden soll.

- **Lokale Festplatte deaktivieren**. (Nur Flex System x240 Rechenknoten) Der integrierte Speichercontroller und die Speicheroption ROM (UEFI und Legacy) werden während der Implementierung deaktiviert. Durch die Deaktivierung des lokalen Plattenlaufwerks wird bei einem SAN-Boot die allgemeine Bootzeit verringert.

E/A-Adapter definieren

Sie können E/A-Porteinstellungen und -Adressierungsmodi festlegen, die bei der Musterimplementierung für die Zielserver übernommen werden sollen.

Zu dieser Aufgabe

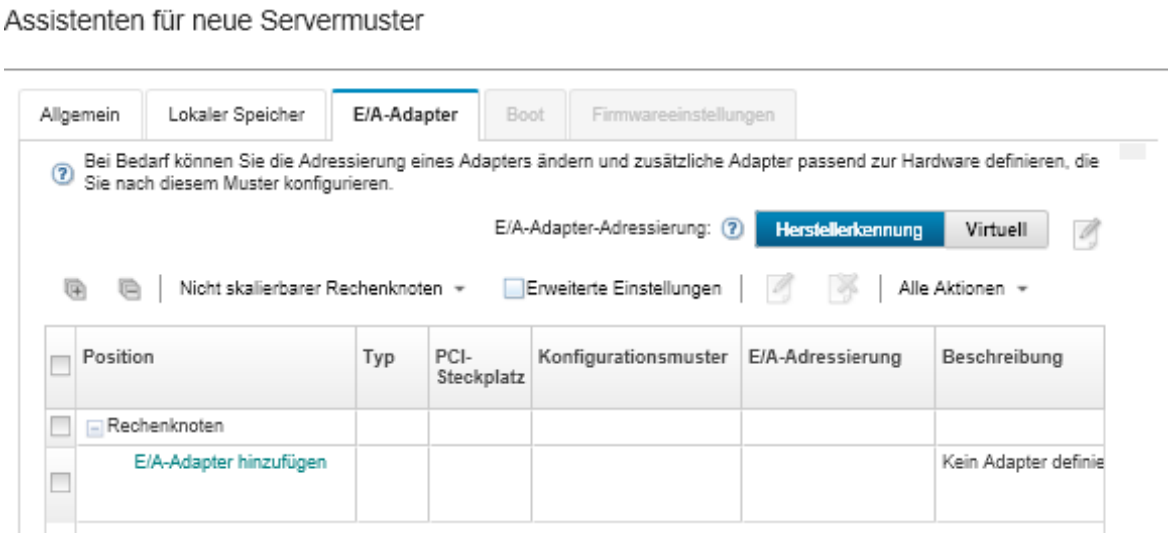
Wenn Sie die Adressen der E/A-Adapter virtualisieren möchten, konfigurieren Sie dieses Muster für die Verwendung der virtuellen Adressierung von E/A-Adaptern.

Wenn Sie ein Muster aus einem vorhandenen Server erstellen, werden einige Adapterinformationen möglicherweise automatisch ermittelt. Sie können zusätzliche E/A-Adaptermuster für die Hardware definieren, die bei der Musterimplementierung auf den Servern vorhanden sein wird. Wenn Sie E/A-Adaptermuster definieren, können Sie Porteinstellungen für den unterstützten Adapter definieren. Bei Verwendung der virtuellen Adressierung des E/A-Adapters können Sie zudem SAN-Bootziele für hinzugefügte Fibre Channel-Adapter definieren (siehe Bootoptionen definieren).

Vorgehensweise

Gehen Sie wie folgt vor, um E/A-Adaptereinstellungen zu definieren.

Schritt 1. Klicken Sie im Neuen Assistent für Servermuster auf die Registerkarte **E/A-Adapter**.



Anmerkung: Weitere Informationen über die E/A-Adapter zeigen Sie an, indem Sie auf **Erweiterte Einstellungen** klicken.

Schritt 2. Wenn Sie ein Servermuster für einen Server in einem Flex System-Gehäuse erstellen, wählen Sie den Adressierungsmodus des E/A-Adapters aus:

- **Herstellerkennung**. Verwenden Sie die vom Hersteller für den Adapter festgelegten WWN- und MAC-Adressen.

- **Virtuell**. Mit der virtuellen Adressierung des E/A-Adapters vereinfachen Sie die LAN- und SAN-Verbindungsverwaltung. Durch die Virtualisierung der E/A-Adressierung wird die Hardware-Herstelleradressenkennung mit virtualisierten Fibre-WWN- und Ethernet-MAC-Adressen neu zugeordnet. Dies kann die Implementierung beschleunigen, da Sie die SAN-Zonenmitgliedschaft vorkonfigurieren und das Failover einstellen können. Damit ist es im Falle eines Hardwareaustauschs nicht mehr erforderlich, die SAN-Zonenzuweisung und die LUN-Maskierungszuordnung neu zu konfigurieren.

  Wenn die virtuelle Adressierung aktiviert ist, werden Ethernet- und Fibre Channel-Adressen standardmäßig und unabhängig von definierten Adaptern zugeordnet. Der Pool, aus dem Ethernet- und Fibre Channel-Adressen zugeordnet werden, ist frei wählbar.

  Sie können die Einstellungen für die virtuelle Adressierung auch bearbeiten. Dazu klicken Sie auf das Symbol **Bearbeiten** ( ) neben den Adressierungsmodi.

  Beschränkung: Virtuelle Adressierung wird nur für Server in einem Flex System-Gehäuse unterstützt. Rack- und Tower-Server werden nicht unterstützt.

Schritt 3. Wenn Sie ein Servermuster für einen Server in einem Flex System-Gehäuse erstellen, wählen Sie eine der folgenden Optionen für Skalierbarkeit aus. Die Zeilen in der Tabelle verändern sich je nach Auswahl.
- Nicht skalierbares Flex System
- Nicht skalierbares Flex System mit zwei Knoten
- Nicht skalierbares Flex System mit vier Knoten

Schritt 4. Wählen Sie die E/A-Adapter aus, die bei der Musterimplementierung auf den Servern installiert sein sollen. So fügen Sie einen Adapter hinzu:

a. Klicken Sie in der Tabelle auf die Verknüpfung **E/A-Adapter hinzufügen**, um das Dialogfenster E/A-Adapter 1 oder LOM hinzufügen zu öffnen.

b. Wählen Sie den PCI-Steckplatz für den Adapter aus.

c. Wählen Sie den Adaptertyp aus der Tabelle aus.

   Anmerkung: Standardmäßig werden in der Tabelle nur E/A-Adapter aufgeführt, die derzeit in den verwalteten Servern installiert sind. Um alle unterstützten E/A-Adapter anzuzeigen, klicken Sie auf **Alle unterstützten Adapter**.

d. Wählen Sie das initiale Anschlussmuster aus, das bei der Musterimplementierung allen Ports in der Portgruppe zugeordnet werden soll.

   Mit *Anschlussmustern* können Sie die vom Server übernommenen Porteinstellungen ändern. Diese initialen Anschlussmuster werden zugeordnet, wenn der Adapter zum ersten Mal hinzugefügt wird. Nachdem der Adapter hinzugefügt wurde, können Sie auf der Seite „E/A-Adapter“ den einzelnen Ports unterschiedliche Muster zuordnen.

   Sie können ein Anschlussmuster erstellen. Klicken Sie dazu auf das Symbol **Erstellen** ( ). Sie können auch ein Anschlussmuster basierend auf einem vorhandenen Muster erstellen. Klicken Sie dazu auf das Symbol **Bearbeiten** ( ).

   Weitere Informationen über Anschlussmuster finden Sie unter Anschlusseinstellungen definieren.

e. Klicken Sie auf **Hinzufügen**, um das Anschlussmuster zur Tabelle auf der Seite „E/A-Adapter“ hinzuzufügen.

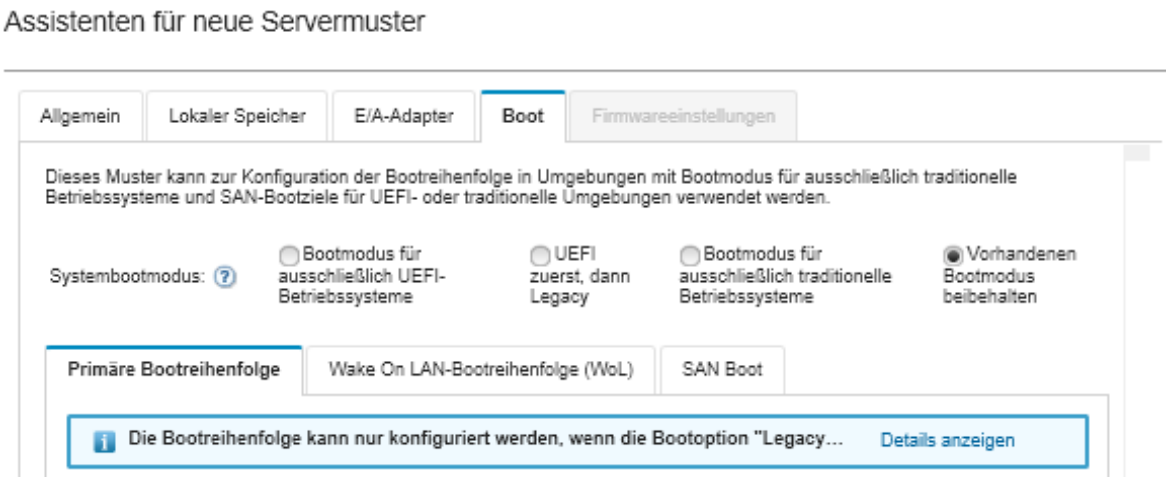
Bootoptionen definieren

Sie können die bei der Bereitstellung des Musters auf die Zielserver angewendete Bootreihenfolge definieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Bootoptionsmuster zu erstellen:

Schritt 1. Klicken Sie im Assistenten für neue Servermuster auf die Registerkarte **Boot**.



Schritt 2. Wählen Sie einen der folgenden Systembootmodi aus:

- **Bootmodus für ausschließlich UEFI-Betriebssysteme**. Wählen Sie diese Option aus, um einen Server zu konfigurieren, der UEFI (Unified Extensible Firmware Interface) unterstützt. Wenn Sie UEFI-fähige Betriebssysteme starten, kann diese Option durch die Deaktivierung von Legacy-Option für ROMs die Startzeit verkürzen.

  Wenn das Muster von einem Thinksystem Server übernommen wird, können Sie die Bootreihenfolge auf der Registerkarte **Primäre Bootreihenfolge** festlegen. Sie können die Bootreihenfolge beibehalten, die auf dem Server festgelegt ist, auf dem das Muster implementiert werden soll, oder die Bootreihenfolge der Bootoptionen nach Ihren Anforderungen konfigurieren. Die Bootpriorität von Booteinheiten in einer Einheitengruppe (Bootoption) wird jedoch nicht unterstützt.

- **UEFI zuerst, dann Legacy**. Wählen Sie diese Option aus, um einen Server so zu konfigurieren, dass er zuerst per UEFI startet. Wenn hierbei ein Fehler auftritt, versucht der Server, im Legacy-Modus zu starten.

  Wenn das Muster von einem Thinksystem Server übernommen wird, können Sie die Bootreihenfolge auf der Registerkarte **Primäre Bootreihenfolge** festlegen. Sie können die Bootreihenfolge beibehalten, die auf dem Server festgelegt ist, auf dem das Muster implementiert werden soll, oder die Bootreihenfolge der Bootoptionen nach Ihren Anforderungen konfigurieren. Die Bootpriorität von Booteinheiten in einer Einheitengruppe (Bootoption) wird jedoch nicht unterstützt.

- **Bootmodus für ausschließlich traditionelle Betriebssysteme**. Wählen Sie diese Option aus, wenn Sie einen Server konfigurieren wollen, dessen Betriebssystem den Start über eine Legacy-Firmware (BIOS) erfordert. Wählen Sie diese Option nur aus, wenn Sie Betriebssysteme starten, die nicht UEFI-fähig sind.

  Tipp: Wenn Sie den Bootmodus „Nur Legacy“ auswählen (wodurch sich die Bootzeit erheblich verkürzt), können Sie keine FoD-Tasten (Feature On Demand) aktivieren.

  Wenn Sie diese Option auswählen, können Sie Folgendes angeben:

  – **Primäre Bootreihenfolge**. Sie können die Bootreihenfolge behalten, die auf dem Server, auf dem das Muster bereitgestellt wird, vorhanden ist. Sie können außerdem die „Bootmodus für

ausschließlich traditionelle Betriebssysteme“-Bootreihenfolge festlegen und die Reihenfolge der Boot-Optionen definieren.

  - **Wake-on-LAN-Bootreihenfolge (WoL)**. Sie können die aktuelle WoL-Bootreihenfolge behalten, die auf dem Server, auf dem das Muster bereitgestellt wird, vorhanden ist. Sie können außerdem die „Bootmodus für ausschließlich traditionelle Betriebssysteme“-Bootreihenfolge festlegen und die Reihenfolge der WoL-Boot-Optionen definieren.

- **Vorhandenen Bootmodus beibehalten**. Wählen Sie diese Option aus, um die vorhandenen Einstellungen auf dem Zielserver beizubehalten. Bei der Bereitstellung des Musters werden keine Änderungen an der Bootreihenfolge vorgenommen.

Schritt 3. Wählen Sie die Registerkarte **SAN-Boot** aus, um ein Bootzielmuster auszuwählen und Booteinheiten anzugeben.

Anmerkung: Wenn Sie Fibre Channel-Adapter definieren und die virtuelle Adressierung bei der Definition der E/A-Adapter aktiviert ist, können Sie primäre und sekundäre SAN-Bootziele für die Fibre Channel-Adapter festlegen. Sie können mehrere WWPNs (Worldwide Port Name) und LUN-Kennungen (Logical Unit Number) für die Storage-Ziele angeben.

Firmwareeinstellungen definieren

Sie können Baseboard Management Controller- und UEFI-Firmwareeinstellungen festlegen, die bei der Musterimplementierung für die Zielserver übernommen werden sollen.

Zu dieser Aufgabe

Die Firmwareeinstellungen sind in Kategorien mit ähnlichen Einstellungen zusammengefasst. Sie können für jede Kategorie ein *Kategoriemuster* mit einheitlichen Firmwareeinstellungen erstellen, die in mehreren Servermustern wiederverwendet werden können. Die meisten Firmwareeinstellungen lassen sich sowohl direkt per Baseboard Management Controller und UEFI als auch mithilfe von Kategoriemustern konfigurieren. Welche Firmwareeinstellungen verfügbar sind, hängt vom Servertyp, der Flex System-Umgebung und dem Funktionsumfang des Servermusters ab.

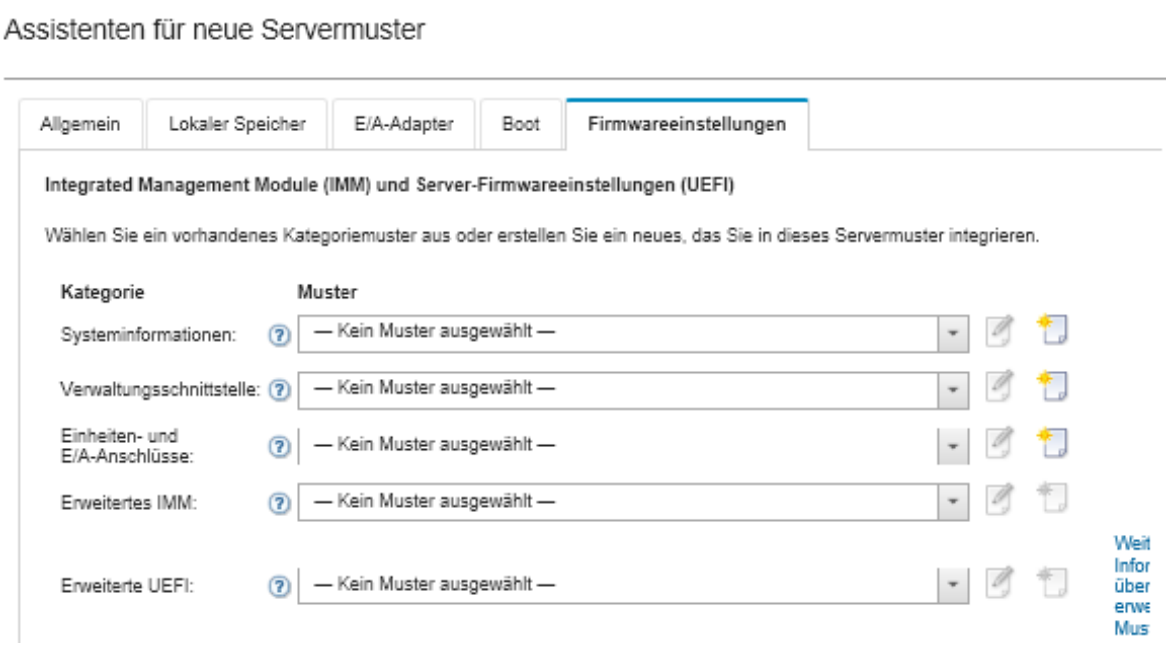
Kategoriemuster können vordefiniert, benutzerdefiniert oder von vorhandenen Servern übernommen werden:

- *Erweiterte Kategoriemuster* werden für einige E/A-Adapterports, erweiterte UEFI- und Baseboard Management-Controller(BMC)-Einstellungen verwendet, die vom angegebenen verwalteten Server übernommen und dynamisch erstellt werden. Wenn Sie ein Servermuster von einem vorhandenen Server erstellen, generiert Lenovo XClarity Administrator diese Muster. Erweiterte Kategoriemuster können nicht manuell erstellt werden, aber Sie können die Muster nach der Erstellung bearbeiten.
- *Benutzerdefinierte Kategoriemuster* werden von Ihnen erstellt und umfassen Systeminformationen, Verwaltungsschnittstellen, Einheiten und E/A-Ports, Fibre Channel-Bootziele und E/A-Adapterports.

Vorgehensweise

Gehen Sie wie folgt vor, um Firmwareeinstellungen zu definieren.

Schritt 1. Klicken Sie im Assistenten für neue Servermuster auf die Registerkarte **Firmwareeinstellungen**.



Schritt 2. Wählen Sie den Kategoriemustertyp mit den Einstellungen, die Sie definieren möchten, aus.

- **Systeminformationen**. Mit diesem Kategoriemuster definieren Sie die automatische Systemnamengenerierung, Kontaktnamen und Standorte. Weitere Informationen über Systeminformationsmuster finden Sie unter Systeminformationseinstellungen definieren.
- **Verwaltungsschnittstellen**. Mit diesem Kategoriemuster definieren Sie die automatische Hostnamengenerierung, Zuordnung von IP-Verwaltungsadressen sowie Einstellungen für DNS (Domain Name System) und Internetverbindungsgeschwindigkeit. Weitere Informationen über Verwaltungsschnittstellenmuster finden Sie unter Verwaltungsschnittstelleneinstellungen definieren.
- **Einheiten und E/A-Ports**. Mit diesem Kategoriemuster definieren Sie Konsolenumleitungen und COM-Ports, PCIe-Geschwindigkeit, integrierte Einheiten, die Adapteroption „ROM“ und die Option „ROM Execution Order“. Weitere Informationen über Einheiten- und E/A-Anschlussmuster finden Sie unter Einheiten- und E/A-Anschlusseinstellungen definieren.
- **Erweitertes BMC**. Mit diesem Kategoriemuster definieren Sie weitere Baseboard Management-Controller-Einstellungen. Die erweiterten Management-Controller-Muster werden automatisch generiert, wenn Sie ein Servermuster von einem vorhandenen Server erstellen. Erweiterte Management-Controller-Muster können nicht manuell erstellt werden. Weitere Informationen über Verwaltungsschnittstellenmuster finden Sie unter Erweiterte Management-Controller-Einstellungen definieren.
- **Erweitertes UEFI**. Mit diesem Kategoriemuster definieren Sie weitere UEFI-Einstellungen (UEFI - Unified Extensible Firmware Interface). Die erweiterten UEFI-Muster werden automatisch generiert, wenn Sie ein Servermuster von einem vorhandenen Server erstellen. Erweiterte UEFI-Muster können nicht manuell erstellt werden. Weitere Informationen über Verwaltungsschnittstellenmuster finden Sie unter Erweiterte UEFI-Einstellungen definieren.

Schritt 3. Legen Sie ein neues Kategoriemuster an. Klicken Sie dazu auf das Symbol **Erstellen** ( ) neben dem Kategoriemustertyp.

Sie können ein vorhandenes Kategoriemuster auch bearbeiten. Markieren Sie dazu ein bestimmtes Muster in der Dropdown-Liste und klicken Sie auf das Symbol **Bearbeiten** ( ) neben dem Kategoriemustertyp. Zudem können Sie ein vorhandenes Kategoriemuster kopieren, indem Sie das Muster bearbeiten und dann auf **Speichern unter** klicken, um das Muster unter einem anderen Namen zu speichern.

Systeminformationseinstellungen definieren

Indem Sie ein Systeminformationsmuster erstellen, können Sie Systemname, Kontakt sowie Positionsinformationen definieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Systeminformationsmuster zu erstellen:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Systeminformationsmuster** und klicken Sie auf das Symbol **Erstellen** ( ).

Tipp: Indem Sie auf das Symbol **Erstellen** neben dem Abschnitt **System Information** klicken, können Sie über die Seite Firmwareeinstellungen des Assistenten Neues Servermuster ein neues Systeminformationsmuster erstellen.

Schritt 4. Geben Sie im Dialog Neues Systeminformationsmuster die folgenden Informationen an.

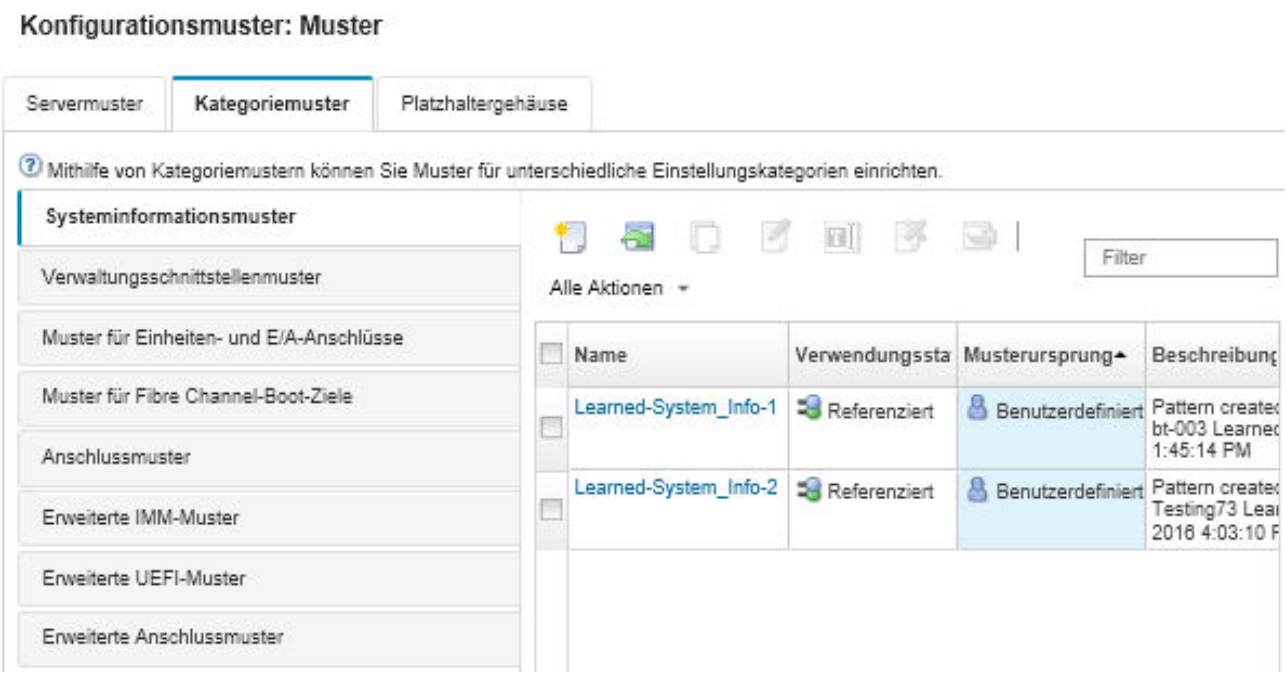
- Geben Sie einen Namen und eine Beschreibung für das Muster ein.
- Wählen Sie aus, ob Systemnamen automatisch generiert werden. Wenn Sie auf **Benutzerdefiniert** klicken, können Sie angeben, wie Namen beim Bereitstellen des Musters generiert werden sollen. Wenn Sie auf **Deaktivieren** klicken, bleiben die Systemnamen der Server beim Bereitstellen des Musters unverändert. Bei den meisten Einheiten wird der Name durch den Baseboard Management Controller auf 256 englische Zeichen begrenzt. Automatisch generierte Namen werden auf 256 Zeichen gekürzt.
- Geben Sie die Position und die Person an, die für diesen Server kontaktiert werden soll.

  Anmerkung: Wenn SNMP aktiviert ist, müssen Sie einen Kontakt und die Systemposition angeben.

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

Ergebnisse

Das neue Muster wird unter der Registerkarte **Systeminformationsmuster** auf der Seite Konfigurationsmuster: Kategoriemuster angezeigt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Ändern der aktuellen Mustereinstellungen über einen Klick auf das Symbol **Bearbeiten** ( ).
- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Verwaltungsschnittstelleneinstellungen definieren

Durch die Erstellung eines Verwaltungsschnittstellenmusters können Sie Hostname, IP-Adresse, DNS (Domain Name System), Schnittstellengeschwindigkeit und Portzuweisungen für die Verwaltungsschnittstelle definieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Verwaltungsschnittstellenmuster zu erstellen.

Anmerkung: Duplexeinstellungen werden von Servermustern nicht unterstützt.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Verwaltungsschnittstellenmuster** und klicken Sie auf das Symbol **Erstellen** ( ).

Tipp: Indem Sie auf das Symbol **Erstellen** ( ) neben dem Abschnitt **Verwaltungsschnittstelle** klicken, können Sie über die Seite „Firmwareeinstellungen“ des Assistenten Neues Servermuster ein neues Verwaltungsschnittstellenmuster erstellen.

Schritt 4. Geben Sie im Dialog Neues Verwaltungsschnittstellenmuster die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für das Muster ein.

- Klicken Sie auf die Registerkarte **Hostname** und wählen Sie aus, ob Hostnamen automatisch generiert werden. Wenn Sie auf **Benutzerdefiniert** klicken, können Sie angeben, wie Namen beim Bereitstellen des Musters generiert werden sollen. Wenn Sie auf **Deaktivieren** klicken, bleiben die Hostnamen der Server beim Bereitstellen des Musters unverändert.

  Hostnamen werden durch den Baseboard Management Controller auf 63 englische Zeichen begrenzt. Automatisch generierte Namen werden auf 63 Zeichen gekürzt.
- Klicken Sie auf die Registerkarte **IP-Verwaltungsadressen** und konfigurieren Sie IPv4- und IPv6-Adresseneinstellungen.

  Bei **IPv4**-Adressen können Sie eine der folgenden Optionen auswählen:
  - **Dynamische IP-Adresse von DHCP-Server anfordern**.
  - **Zuerst von DHCP**. Wenn die Anfrage nicht erfolgreich ist, wird eine statische IP-Adresse aus dem Adresspool abrufen.
  - **Eine statische IP-Adresse aus dem Adresspool abrufen.**

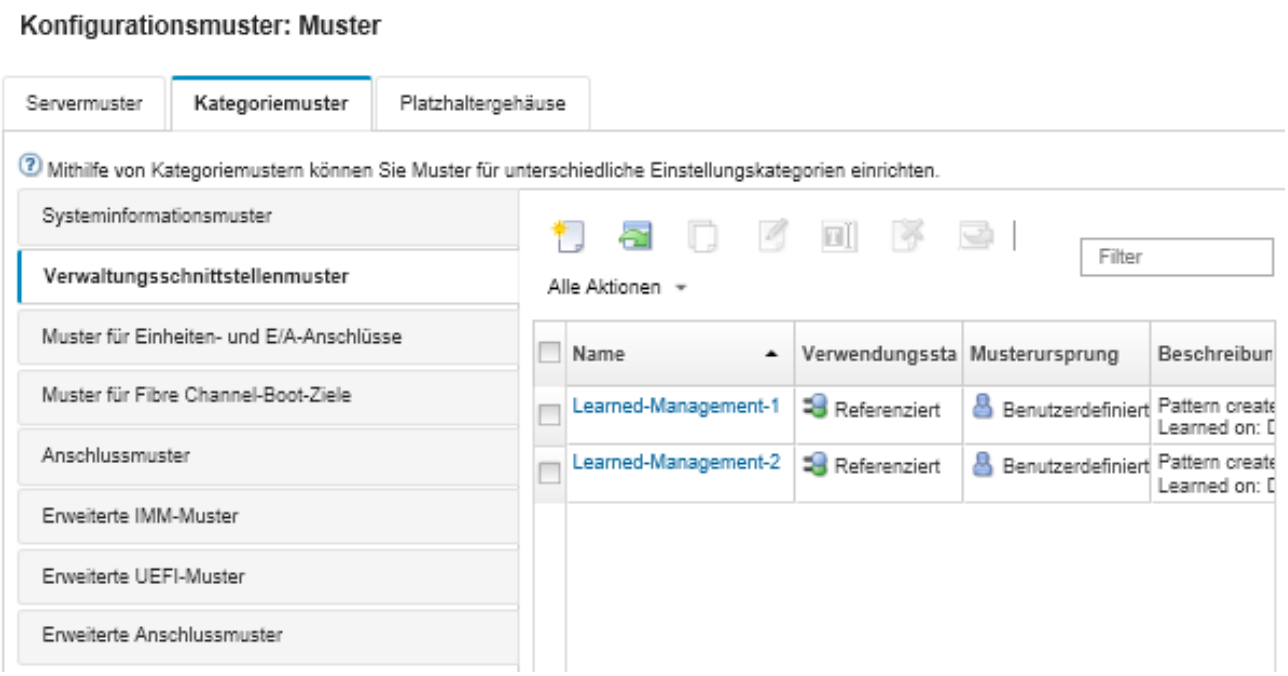
  Bei **IPv6**-Adressen können Sie Folgendes auswählen:
  - **Automatische zustandslose Adresskonfiguration verwenden**.
  - **Eine dynamische IP-Adresse von einem DHCP-Server anfordern**.
  - **Eine statische IP-Adresse aus dem Adresspool abrufen**.

  Aktivieren oder deaktivieren Sie auf der Registerkarte **Domain Name System (DNS)** die DDNS-Option (Dynamic Domain Name Service). Wenn Sie DDNS aktivieren, können Sie eine der folgenden Optionen auswählen:
  - Domänenname von DHCP-Server abrufen.
  - Geben Sie einen Domänennamen an.
- Klicken Sie auf die Registerkarte **Einstellungen für Schnittstelle** und legen Sie die Maximum Transmission Unit (MTU) fest. Der Standardwert ist 1500.
- Klicken Sie auf die Registerkarte **Portzuordnungen** und geben Sie die Portnummern für die folgenden Protokolle, Anwendungen und Dienste an:
  - HTTP
  - HTTPS
  - Telnet-Befehlszeilenschnittstelle
  - SSH-Befehlszeilenschnittstelle
  - SNMP-Agent
  - SNMP-Traps
  - Remote-Steuerungskonsole
  - CIM over HTTP
  - CIM over HTTPS

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

Ergebnisse

Das neue Muster wird unter der Registerkarte **Verwaltungsschnittstellenmuster** auf der Seite Konfigurationsmuster: Kategoriemuster angezeigt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Ändern der aktuellen Mustereinstellungen über einen Klick auf das Symbol **Bearbeiten** ( ).
- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Einheiten- und E/A-Anschlusseinstellungen definieren

Indem Sie ein Muster für Einheiten- und Ein-/Ausgangsanschlüsse erstellen, können Sie eine Konsolenumleitung aktivieren und die Eigenschaften des COM 1-Anschlusses aktivieren und definieren.

Vorgehensweise

So erstellen Sie ein Muster für Einheiten- und Ein-/Ausgangsanschlüsse.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Einheiten- und E/A-Anschlussmuster** und klicken Sie auf das Symbol **Erstellen** ( ).

Tipp: Indem Sie auf das Symbol **Erstellen** ( ) neben dem Abschnitt **Einheiten- und Ein-/Ausgangsanschlüsse** klicken, können Sie über die Seite Firmwareeinstellungen des Assistenten Neues Servermuster ein neues Einheiten- und E/A-Anschlussmuster erstellen.

Schritt 4. Geben Sie im Dialog Neues Einheiten- und E/A-Anschlussmuster die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für das Muster ein.
- Aktivieren oder deaktivieren Sie die Konsolenumleitung. Wenn Sie die Konsolenumleitung aktivieren, können Sie auswählen, ob Sie die folgenden Optionen aktivieren oder deaktivieren:
  - **Serial over LAN**.

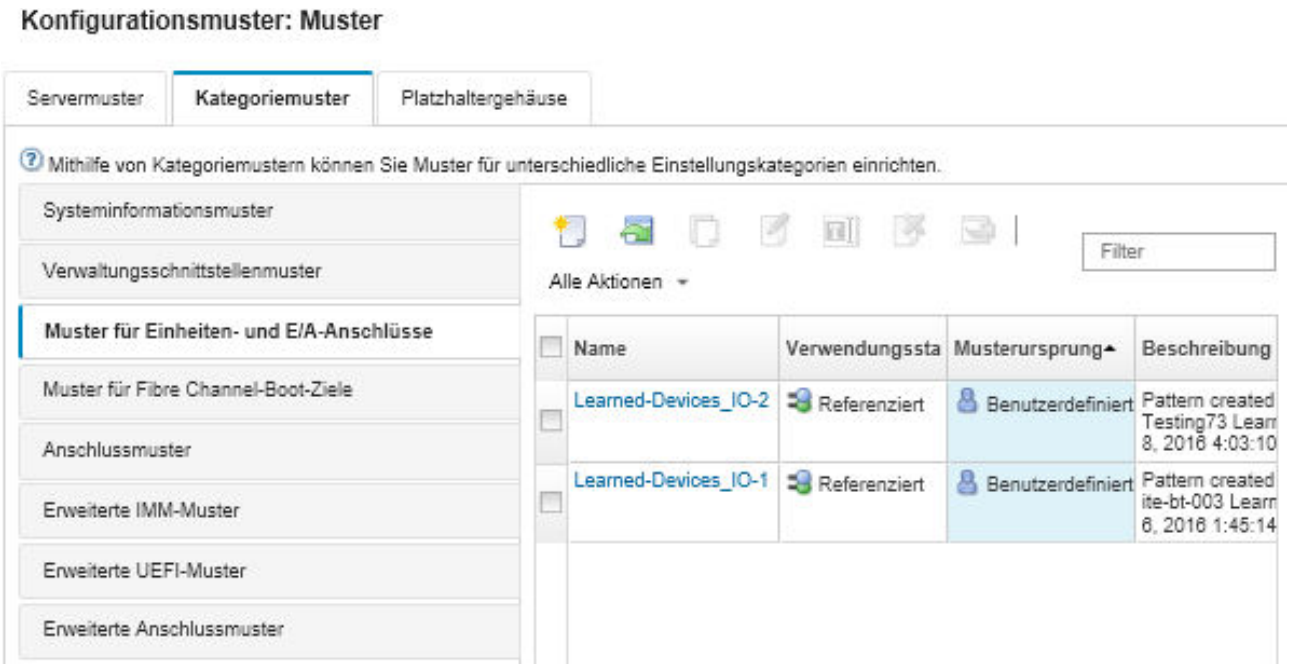
- **Serviceprozessorumleitung**. Wenn Sie die Serviceprozessorumleitung aktivieren, können Sie COM-Port 1 oder 2 für den optionalen seriellen Legacy-Datenport verwenden. Beachten Sie, dass COM-Port 1 immer verwendet wird, wenn diese Option deaktiviert ist.Sie können auch einen der folgenden CLI-Modi auswählen:
  - Deaktivieren
  - Mit benutzerdefinierter Tastenfolge aktiviert
  - Mit EMS-kompatibler Tastenfolge aktivieren

- Wählen Sie aus, ob die COM-Anschlüsse 1 und 2 aktiviert sind. Wenn Sie die COM-Anschlüsse aktivieren, geben Sie die folgenden Einstellungen an:
  - Baudrate
  - Datenbits
  - Parität
  - Bits stoppen
  - Textemulation
  - Aktiv nach Bootvorgang
  - Flusssteuerung

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

Ergebnisse

Das neue Muster wird unter der Registerkarte **Einheiten- und E/A-Anschlussmuster** auf der Seite Konfigurationsmuster: Kategoriemuster angezeigt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Ändern der aktuellen Mustereinstellungen über einen Klick auf das Symbol **Bearbeiten** ( ).
- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Fibre Channel-Bootziel-Einstellungen definieren

Über die Erstellung eines Fibre Channel-Bootziel-Musters können Sie den Server für das Booten über eine SAN-Einheit (Storage Area Network) statt über die lokale Festplatte konfigurieren.

Vorgehensweise

So erstellen Sie ein Fibre Channel-Bootziel-Muster.

Einschränkung: Fibre Channel-Bootziele werden nur für Flex-Rechenknoten unterstützt. Eigenständige Rack- und Tower-Server werden nicht unterstützt.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Fibre Channel-Bootziel-Muster** und dann auf das Symbol **Erstellen** ( ).

Schritt 4. Geben Sie im Dialog Neues Muster für Fibre Channel-Boot-Ziele die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für das Muster ein.
- Geben Sie eine oder mehrere WWPN-Adressen und LUN-Kennungen zur Verwendung als primäre Bootziele an. Außerdem können Sie eine oder mehrere optionale WWPN-Adressen und LUN-Kennungen als sekundäre Bootziele angeben.

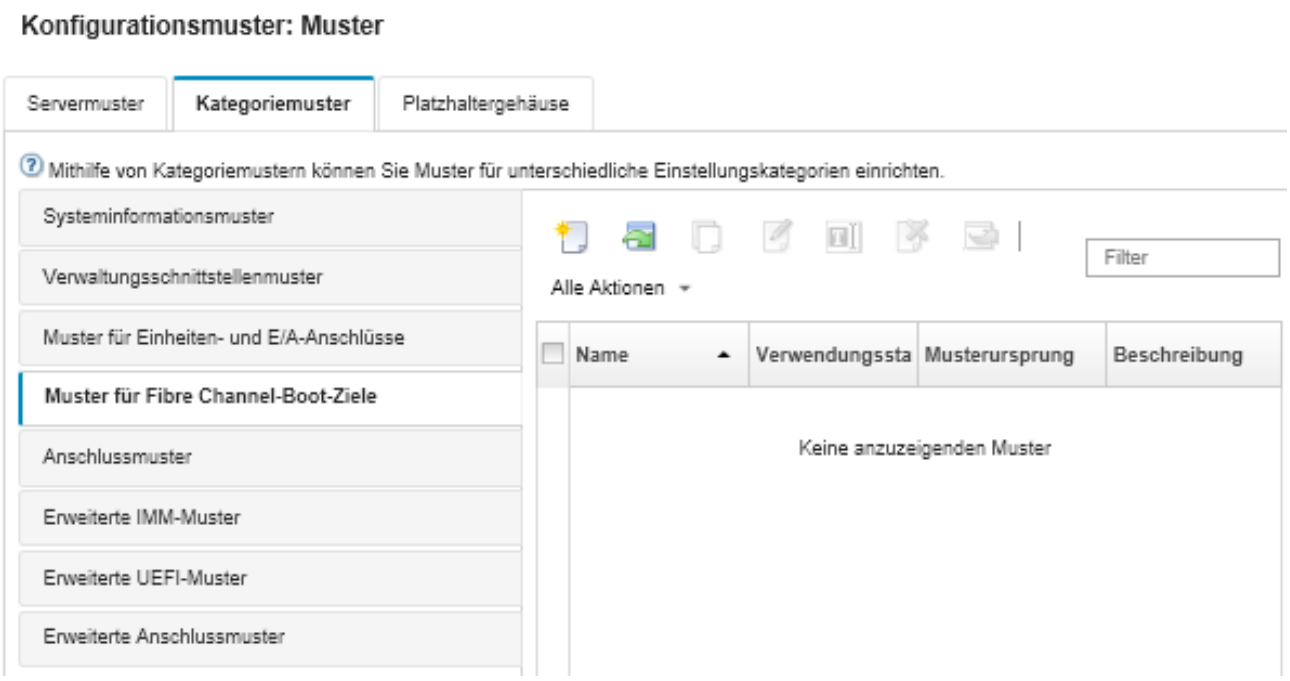
  Sie können beispielsweise die primären Storage-Pfade als primäre Ziele angeben und die sekundären Storage-Pfade als sekundäre Ziele hinzufügen. Durch die Verwendung unterschiedlicher Zielgruppen in verschiedenen Servermustern können Sie die SAN-Auslastung während des gleichzeitigen Bootens von mehreren Hosts verteilen.

  Tipp: Wenn Sie `00:00:00:00:00:00:00:00` für den WWPN angeben, versucht XClarity Administrator, über das erste erkannte Ziel zu booten.

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

Ergebnisse

Das neue Muster wird unter der Registerkarte **Fibre Channel-Bootziel-Muster** auf der Seite Konfigurationsmuster: Kategoriemuster angezeigt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Ändern der aktuellen Mustereinstellungen über einen Klick auf das Symbol **Bearbeiten** ( ).
- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Anschlusseinstellungen definieren

Sie können typische Anschlusseinstellungen für einen bestimmten E/A-Adaptertyp definieren, indem Sie ein Anschlussmuster erstellen.

Zu dieser Aufgabe

Sie können in Anschlussmustern Netzwerkeinstellungen verwenden, um interne Ports für den Switch zu konfigurieren. Sie können die Anschlussmuster nicht dazu verwenden, interne globale Einstellungen des Switchs zu konfigurieren (z. B. VLAN-IDs, globaler UFP-Modus, globaler CEE-Modus und globale FIPs). Bevor Sie die Anschlussmuster bereitstellen, müssen Sie die globalen Einstellungen mit den folgenden Regeln manuell konfigurieren, die mit den Einstellungen für die internen Ports kompatibel sind, die Sie bereitstellen möchten. Sie können Anschlussmuster außerdem nicht zur Konfiguration des PVID-Taggings verwenden. Lesen Sie die mit Ihrem Server gelieferte Dokumentation, um die Kompatibilität zwischen den globalen Einstellungen und den internen Porteinstellungen und die Konfiguration dieser Einstellungen für den Switch zur überprüfen.

- Stellen Sie sicher, dass **globalCEEState** die Einstellung „Ein“ hat, wenn PFC konfiguriert ist.
- Stellen Sie sicher, dass **globalCEEState** die Einstellung „Ein“ hat, wenn vport auf den „FCoE“ -Modus festgelegt ist.
- Stellen Sie sicher, dass **globalCEEState** die Einstellung „Ein“ hat und **globalFIPsState** die Einstellung „Ein“ hat, wenn PIPs konfiguriert sind.

- Stellen Sie sicher, dass **globalUFPMode** die Einstellung „Aktiviert“ hat, wenn der interne Portmodus des Switches auf den „UFP“-Modus festgelegt ist.
- Stellen Sie sicher, dass die VLAN-ID erstellt wird, bevor Sie einen Port zu einem bestimmten VLAN hinzufügen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein E/A-Adapterportmuster zu erstellen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Anschlussmuster** und klicken Sie auf das Symbol **Erstellen** ( ).

Tipp: Sie können ein neues Anschlussmuster über die Seite E/A-Adapter hinzufügen erstellen, indem Sie auf das **Erstellen**-Symbol ( ) neben dem Abschnitt **Initiales Anschlussmuster** klicken.

Schritt 4. Geben Sie im Dialog Neues Anschlussmuster die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für das Muster ein.
- Geben Sie die folgenden Adapter- und Anschlusskompatibilitätseinstellungen an. Bei der Zuordnung von Mustern zu Adaptern und Anschlüssen werden die Mustereinstellungen auf Basis der Kompatibilität mit dem Zieladapter oder Zielanschluss gefiltert.
  - Zieladaptertyp
  - Zielanschlussbetriebsmodus inklusive:
    - pNIC-Modus
    - vNIC Virtual Fabric-Mode
    - vNIC schalterunabhängiger Modus
    - vNIC Unified Fabric-Protokollmodus

    Diese Einstellungen aktivieren die NIC-Virtualisierung. Siehe NIC-Virtualisierung in Flex System Fabric-Lösungen für weitere Informationen.
  - Zielanschlussprotokolle, z. B.:
    - Nur Ethernet
    - Ethernet und FCoE
    - Ethernet und iSCSI
  - Erweitertes Anschlusseinstellungsmuster, das zur Konfiguration weiterer, vom Server erhaltener Anschlusseinstellungen verwendet wird
- Wenn Sie den Zielanschlussbetriebsmodus auf **pNIC-Modus** festlegen, wenden Sie, wenn möglich, die entsprechenden Einstellungen auf die internen Flex-Switch-Ports an. Wenn ausgewählt, können Sie zusätzliche VLAN-Einstellungen und erweiterte Einstellungen konfigurieren:
  - Geben Sie das Protokoll für den Zielanschluss an.
  - Wenn Sie das Zielanschlussprotokoll auf **Ethernet und FCoE** festlegen, wählen Sie optional die Priorität 2-ID aus und geben diese an.
- Wenn Sie den Zielanschluss-Betriebsmodus auf **vNIC Virtual Fabric-Modus** festlegen, konfigurieren Sie die physischen Funktionseinstellungen inkl. Typ und VLAN-Tag pro Anschluss.
- Wenn Sie den Zielanschluss-Betriebsmodus auf **vNIC schalterunabhängiger Modus** festlegen, geben Sie den Typ, die Mindestbandbreite und den VLAN-Tag für jede aktivierte Funktion an. Sie können auch entsprechende Einstellungen auf interne Flex-Switch-Anschlüsse

anwenden. Wenn ausgewählt, können Sie zusätzliche interne Switch-Ports und erweiterte Einstellungen konfigurieren:

- Geben Sie das Standard-LAN an, das nur vom Betriebssystem zum Senden von Paketen ohne Tagging verwendet wird.
- Geben Sie eine durch Kommas getrennte Liste von VLANs an.
- Wählen Sie die Option aus, um die manuelle Steuerung zu konfigurieren und die Trigger anzugeben.
- Wählen Sie die Option aus, um den Flusssteuerungstyp inkl. der folgenden Einstellungen zu konfigurieren
  - Vorhandene Ablaufsteuerung beibehalten
  - Prioritätsbasierte Ablaufsteuerung
  - Ablaufsteuerung auf Verbindungsebene

  Weitere Informationen zu diesen Flusssteuerungstypen finden Sie in der Dokumentation Ihres Flex-Switches.

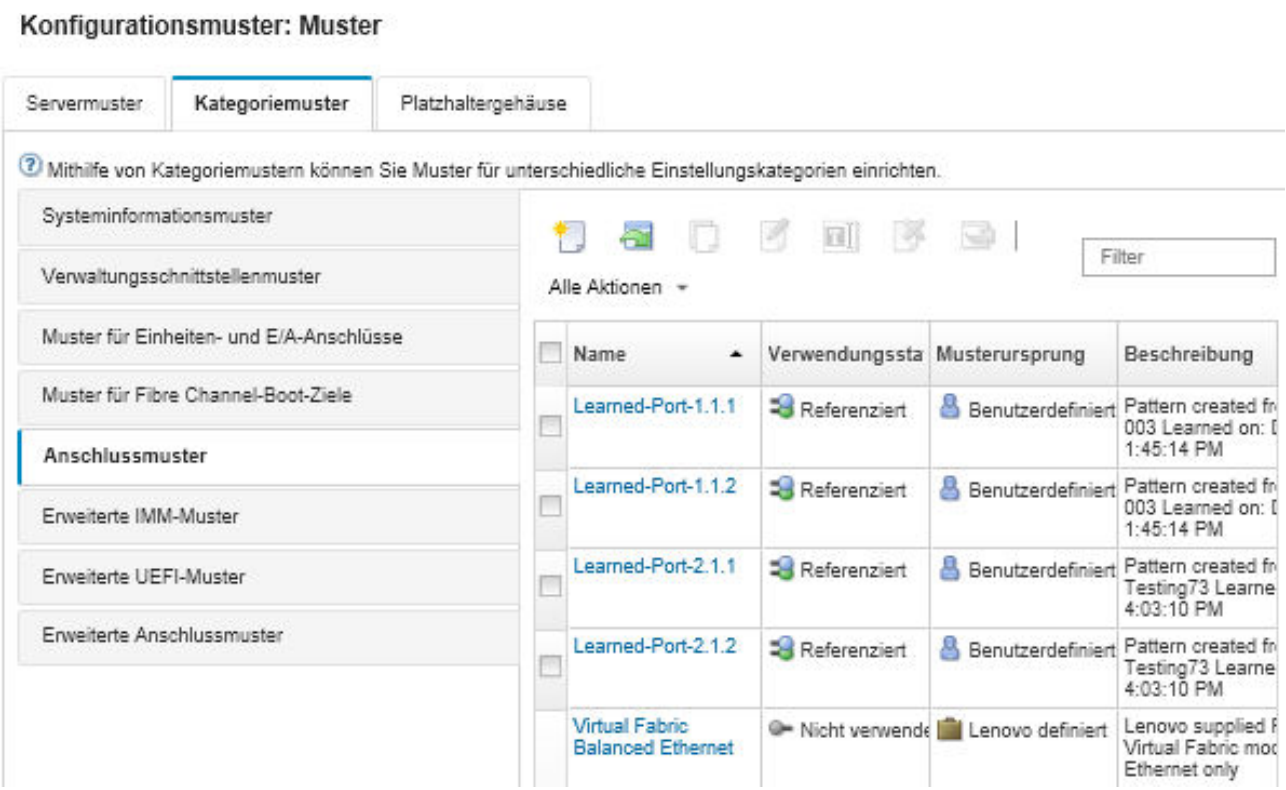
- Wenn Sie den Zielanschlussbetriebsmodus auf **Unified Fabric-Protokoll vNIC-Modus** festlegen, wenden Sie die entsprechenden Einstellungen auf die internen Flex-Switch-Ports an. Wenn ausgewählt, können Sie zusätzliche UFP-Funktionen und erweiterte Einstellungen konfigurieren:
  - Geben Sie den QoS-Modus (Bandbreite oder Priorität) an.
  - Aktivieren Sie das Standard-VLAN-ID-Tagging und geben Sie den Modus, die Mindestbandbreite und den VLAN-Tag für jede aktivierte Funktion an.
  - Wählen Sie die Option aus, um Fehler auf Ebene 2 und die Anzahl der Trigger für jede Funktion anzugeben.
  - Geben Sie für den QoS-Bandbreitenmodus den Ablaufsteuerungstyp an (prioritätsbasiert, Verbindungsebene oder vorhandene Ablaufsteuerung).
  - Geben Sie für den QoS-Bandbreitenmodus an, ob Priorität 4 aktiviert ist, wenn iSCSI ausgewählt ist.

  Anmerkung: Stellen Sie sicher, dass der globale Failover den Wert „Ein“ hat, wenn Sie Failovertrigger definieren.

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

Ergebnisse

Das neue Muster wird unter der Registerkarte **Anschlussmuster** auf der Seite Konfigurationsmuster: Kategoriemuster angezeigt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Ändern der aktuellen Mustereinstellungen über einen Klick auf das Symbol **Bearbeiten** ( ).
- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Erweiterte Management-Controller-Einstellungen definieren

Die erweiterten Baseboard Management-Controller-Einstellungen werden vom angegebenen verwalteten Server übernommen und dynamisch erstellt. Diese Muster werden von Lenovo XClarity Administrator erstellt, wenn Sie ein Servermuster von einem vorhandenen Server übernehmen. Erweiterte Management-Controller-Muster können nicht manuell erstellt werden, aber Sie können bereits erstellte Muster kopieren und ändern.

Vorbereitende Schritte

Anmerkung: Die IMM-Wärmeeinstellung kann mit der Einstellung des UEFI-Betriebsmodus kollidieren. Wenn es zu Konflikten kommt, überschreiben die UEFI-Einstellungen die IMM-Einstellungen beim Neustart des Geräts, und alle Wärmeeinstellungen, die Sie in einem erweiterten Baseboard-Management-Controller-Muster definieren, werden nicht berücksichtigt. Um das Problem zu beheben, entfernen Sie entweder die Einstellung aus dem erweiterten Baseboard-Management-Controller-Muster oder wählen Sie eine Einstellung, die nicht mit der aktuellen UEFI-Betriebsmoduseinstellung kollidiert.

Vorgehensweise

Gehen Sie wie folgt vor, um erweiterte Management-Controller-Muster zu ändern.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Erweiterte BMC-Muster**.

Schritt 4. Wählen Sie das zu ändernde Muster aus und klicken Sie auf das Symbol **Bearbeiten** ().

Schritt 5. Ändern Sie die entsprechenden Felder.

Sie können die Einstellungen auswählen, die in das Kategoriemuster einbezogen werden sollen. Klicken Sie dazu auf die Einstellungen **Einschließen/Ausschließen**.

- Klicken Sie zur Konfiguration der DNS-Einstellungen auf **Netzwerkeinstellungen-Schnittstelle → DNS-Konfiguration**. Sie können DNS aktivieren, das IP-Protokoll auswählen und bis zu drei IPv4- oder IPv6-Adressen angeben und die Ermittlung von XClarity Administrator-IP-Adressen aktivieren.

  Anmerkung: Für Flex System Einheiten können Sie nur die IP-Adresse konfigurieren, die zur Ermittlung des XClarity Administrator-Servers verwendet werden soll.

- Klicken Sie zur Konfiguration der NTP-Einstellungen auf **Netzwerkeinstellungen-Schnittstelle → Integrated Module NTP-Einstellung**. Sie können den Hostnamen für bis zu vier NTP-Server und die Frequenz angeben.

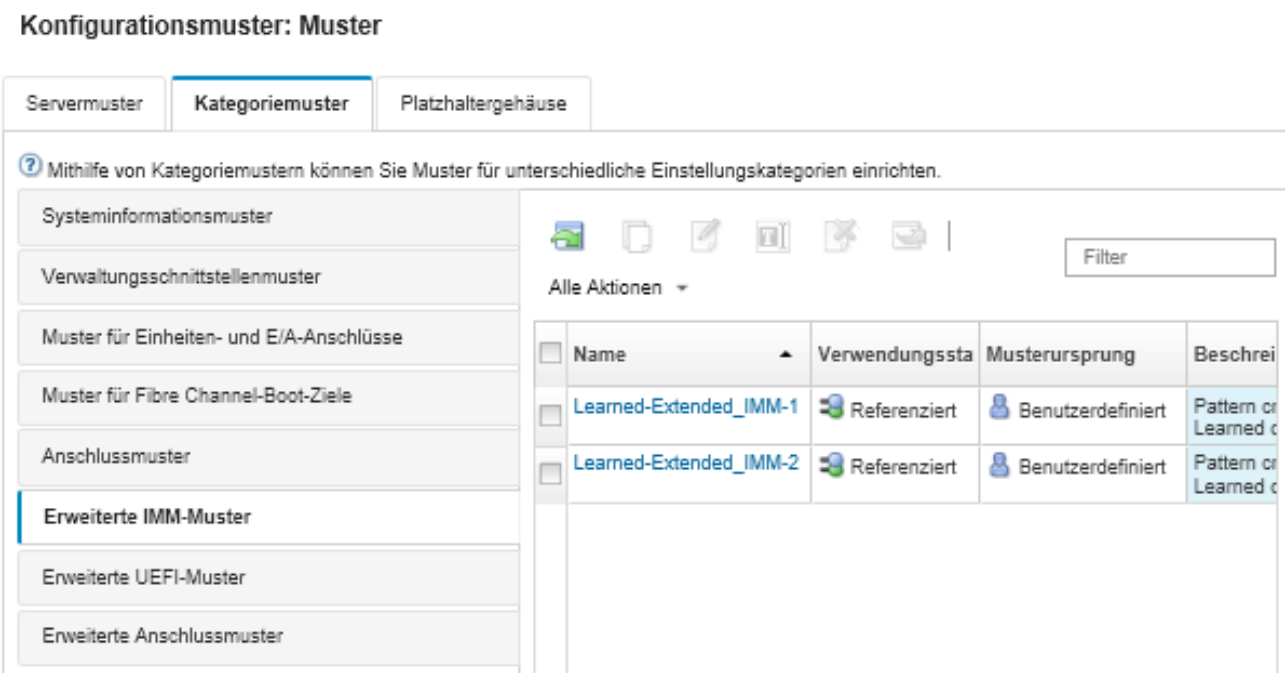
  Anmerkung: Für Flex System Einheiten können Sie keine NTP-Einstellungen konfigurieren.

- (Nur Rack-Server) Um Daten- und Zeiteinstellungen anzuzeigen, klicken Sie auf **Allgemeine Einstellungen → Integrated Module-Zeiteinstellungen**. Sie können die Zeitzone (UTC-Abweichung) angeben, die Sommerzeit aktivieren oder deaktivieren und auswählen, ob UTC oder die Ortszeit auf dem Host verwendet werden soll.
- Klicken Sie zum Ändern der Sicherheitseinstellungen von Benutzeraccounts auf **Accountsicherheitskonfiguration**.

Schritt 6. Klicken Sie auf **Speichern**, um die Änderungen für das aktuelle Kategoriemuster zu speichern. Sie können auch auf **Speichern unter** klicken, um die Änderungen unter einem neuen Konfigurationsmuster zu speichern.

Ergebnisse

Das geänderte Kategoriemuster wird auf der Registerkarte **Erweiterte BMC-Muster** auf der Seite „Konfigurationsmuster: Kategoriemuster“ aufgeführt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Erweiterte UEFI-Einstellungen definieren

Die erweiterten UEFI-Einstellungen (UEFI - Unified Extensible Firmware Interface) werden vom angegebenen verwalteten Server übernommen und dynamisch erstellt. Diese Muster werden von Lenovo XClarity Administrator erstellt, wenn Sie ein Servermuster von einem vorhandenen Server übernehmen. Erweiterte UEFI-Muster können nicht manuell erstellt werden, aber Sie können bereits erstellte Muster kopieren und ändern.

Zu dieser Aufgabe

Die folgenden erweiterten UEFI-Muster werden von Lenovo XClarity Administrator vordefiniert, um Ihre Server für spezielle Umgebungen zu optimieren.

- **ESXi-Installationsoptionen**
- **Effizienz – Schwerpunkt Leistung**
- **Effizienz – Schwerpunkt Stromersparnis**
- **Maximale Leistung**
- **Minimaler Stromverbrauch**

Anmerkungen:

- Eine Änderung der UEFI-Sicherheitseinstellungen (einschließlich der Konfiguration von Secure Boot, Trusted Platform Module (TPM) und der Richtlinie zu physischer Präsenz) wird von den erweiterten UEFI-Mustern nicht unterstützt.
- Sie können das UEFI-Administratorkennwort für ausgewählte ThinkSystem und ThinkAgile Server über die Seite „Server“ ändern, indem Sie auf **Alle Aktionen → Sicherheit → UEFI-Administrator** klicken. Lenovo XClarity Controller Firmwareversion 20A ist erforderlich.

Vorgehensweise

Gehen Sie wie folgt vor, um erweiterte UEFI-Muster zu ändern.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Erweiterte UEFI-Muster**.

Schritt 4. Wählen Sie das zu ändernde Muster aus und klicken Sie auf das Symbol **Bearbeiten** ( ).

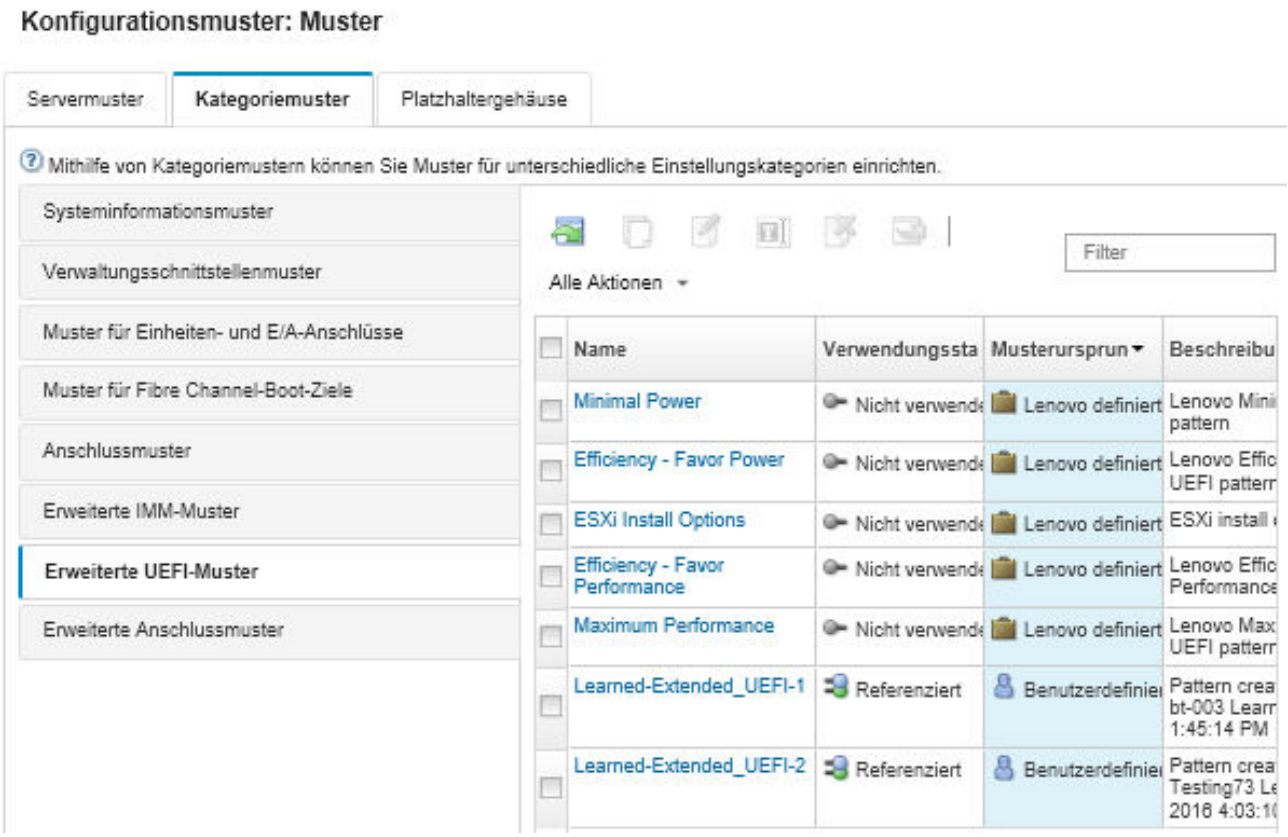
Schritt 5. Ändern Sie die entsprechenden Felder.

Sie können die Einstellungen auswählen, die in das Kategoriemuster einbezogen werden sollen. Klicken Sie dazu auf die Einstellungen **Einschließen/Ausschließen**.

Schritt 6. Klicken Sie auf **Speichern**, um die Änderungen für das aktuelle Kategoriemuster zu speichern. Sie können auch auf **Speichern unter** klicken, um die Änderungen unter einem neuen Konfigurationsmuster zu speichern.

Ergebnisse

Das geänderte Kategoriemuster wird auf der Registerkarte **Erweiterte UEFI-Muster** auf der Seite „Konfigurationsmuster: Kategoriemuster“ aufgeführt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).

- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ().
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Einstellungen für erweiterten Anschluss definieren

Die erweiterten Porteinstellungen werden vom angegebenen verwalteten Server übernommen und dynamisch erstellt. Diese Muster werden von Lenovo XClarity Administrator erstellt, wenn Sie ein Servermuster von einem vorhandenen Server übernehmen. Erweiterte Anschlussmuster können nicht manuell erstellt werden, aber Sie können bereits erstellte Muster kopieren und ändern.

Zu dieser Aufgabe

XClarity Administrator bietet das folgende vordefinierte erweiterte Anschlussmuster:

- **Gleichmäßiges Ethernet für Virtual Fabric**. Von Lenovo unterstütztes Anschlussmuster für den Virtual Fabric-Modus vNIC (nur Ethernet).

Einige Einstellungen für Mellanox und Broadcom E/A-Adapter auf Einheitenebene müssen für alle Ports auf denselben Wert festgelegt werden. Wenn die Einstellungen auf verschiedenen Ports auf unterschiedliche Werte festgelegt werden, werden die Einstellungen für einen Port verwendet und die Einstellungen für andere Ports sind nicht konform. Um das Problem mit der Nichtkonformität zu beheben, wählen Sie denselben Wert für diese Einstellungen auf der Einheitenebene aus.

Bei Mellanox E/A-Adaptern müssen die folgenden Einstellungen für alle Ports auf denselben Wert festgelegt werden.
- Erweiterte Energieeinstellungen
- Angekündigte virtuelle PCI-Funktionen
- Leistungsbegrenzer für Steckplätze
- Virtualisierungsmodus

Bei Broadcom E/A-Adaptern müssen die folgenden Einstellungen für alle Ports auf denselben Wert festgelegt werden.
- Zeitlimitüberschreitung bei Bannermeldungen
- Bandbreitenlimit
- Bandbreitenlimit gültig
- Bandbreitenreservierung
- Bandbreitenreservierung gültig
- PME-Funktion aktivieren
- Maximale Anzahl von PF-MSI-X-Vektoren
- Multifunktionsmodus
- Anzahl der MSI-X-Vektoren pro VF
- Anzahl der VF pro PF
- Options-ROM
- SR-IOV
- RDMA unterstützen

Vorgehensweise

Gehen Sie wie folgt vor, um erweiterte Anschlussmuster zu ändern.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Erweiterte Anschlussmuster**.

Schritt 4. Wählen Sie das zu ändernde Muster aus und klicken Sie auf das Symbol **Bearbeiten** ().

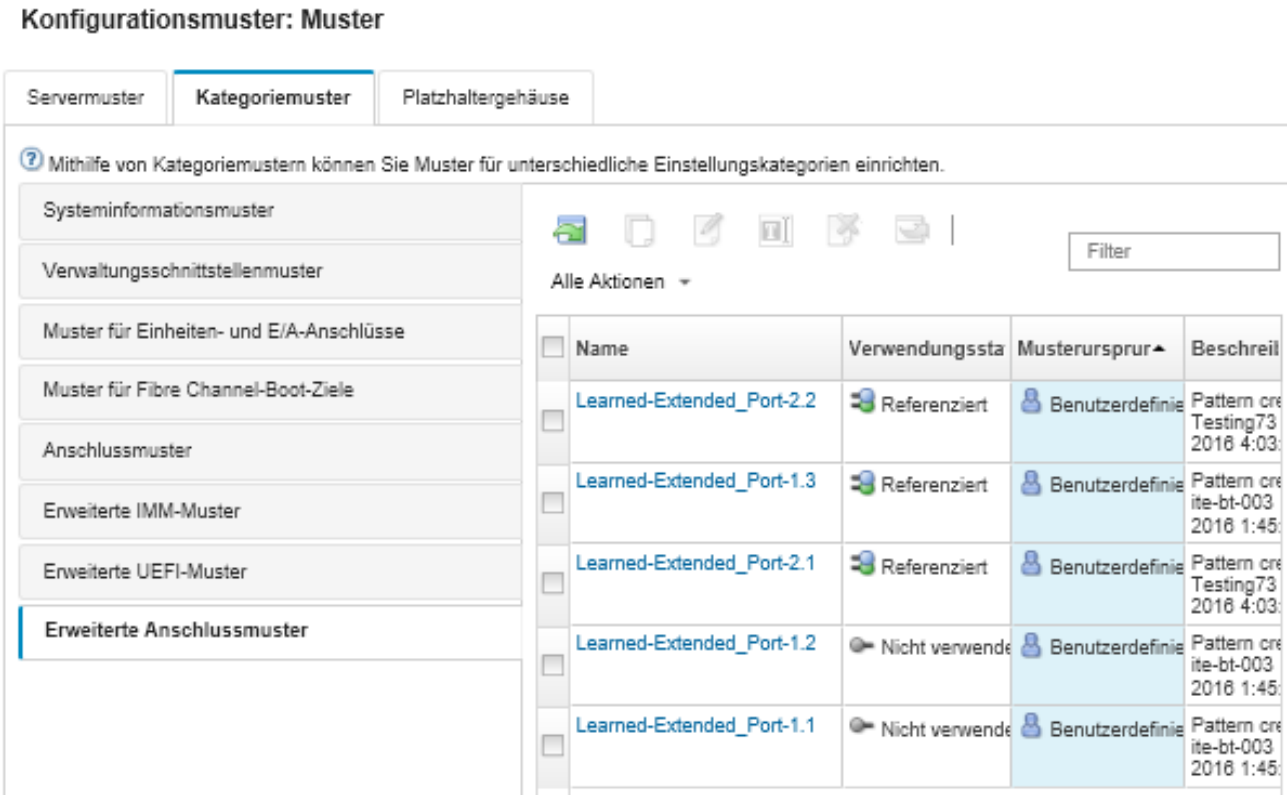
Schritt 5. Ändern Sie die entsprechenden Felder.

Sie können die Einstellungen auswählen, die in das Kategoriemuster einbezogen werden sollen. Klicken Sie dazu auf die Einstellungen **Einschließen/Ausschließen**.

Schritt 6. Klicken Sie auf **Speichern**, um die Änderungen für das aktuelle Kategoriemuster zu speichern. Sie können auch auf **Speichern unter** klicken, um die Änderungen unter einem neuen Konfigurationsmuster zu speichern.

Ergebnisse

Das geänderte Kategoriemuster wird auf der Registerkarte **Erweiterte Anschlussmuster** auf der Seite „Konfigurationsmuster: Kategoriemuster“ aufgeführt:



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Erweiterte SR635/SR655 BIOS-Einstellungen definieren

Die erweiterten SR635/SR655 BIOS-Einstellungen werden von einem bestimmten verwalteten Server ermittelt und dynamisch erstellt. Lenovo XClarity Administrator erstellt diese Muster, wenn Sie ein Servermuster von einem vorhandenen ThinkSystem SR635 oder SR655 Server erstellen. Erweiterte SR635/SR655 BIOS-Muster können nicht manuell erstellt werden, aber Sie können bereits erstellte Muster kopieren und ändern.

Vorgehensweise

Gehen Sie wie folgt vor, um erweiterte SR635/SR655 BIOS-Muster zu ändern.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Lasche **Erweiterte SR635/SR655 BIOS-Muster**.

Schritt 4. Wählen Sie das zu ändernde Muster aus und klicken Sie auf das Symbol **Bearbeiten** ( ).

Schritt 5. Ändern Sie die entsprechenden Felder.

Sie können die Einstellungen auswählen, die in das Kategoriemuster einbezogen werden sollen. Klicken Sie dazu auf die Einstellungen **Einschließen/Ausschließen**.

Schritt 6. Klicken Sie auf **Speichern**, um die Änderungen für das aktuelle Kategoriemuster zu speichern. Sie können auch auf **Speichern unter** klicken, um die Änderungen unter einem neuen Konfigurationsmuster zu speichern.

Ergebnisse

Das geänderte Kategoriemuster wird auf der Registerkarte **Erweiterte SR635/SR655 BIOS-Muster** auf der Seite „Konfigurationsmuster: Kategoriemuster“ aufgeführt:

Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Erweiterte ThinkServer CPlus BIOS-Einstellungen definieren

Die erweiterten ThinkServer CPlus BIOS-Einstellungen werden von einem bestimmten verwalteten Server ermittelt und dynamisch erstellt. Lenovo XClarity Administrator erstellt diese Muster, wenn Sie ein Servermuster von einem vorhandenen ThinkServer CPlus Server erstellen. Erweiterte ThinkServer CPlus BIOS-Muster können nicht manuell erstellt werden, aber Sie können bereits erstellte Muster kopieren und ändern.

Vorgehensweise

Gehen Sie wie folgt vor, um erweiterte ThinkServer CPlus BIOS-Muster zu ändern.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Kategoriemuster**.

Schritt 3. Klicken Sie auf die vertikale Registerkarte **Erweiterte ThinkServer CPlus BIOS-Muster**.

Schritt 4. Wählen Sie das zu ändernde Muster aus und klicken Sie auf das Symbol **Bearbeiten** ( ).

Schritt 5. Ändern Sie die entsprechenden Felder.

Sie können die Einstellungen auswählen, die in das Kategoriemuster einbezogen werden sollen. Klicken Sie dazu auf die Einstellungen **Einschließen/Ausschließen**.

Schritt 6. Klicken Sie auf **Speichern**, um die Änderungen für das aktuelle Kategoriemuster zu speichern. Sie können auch auf **Speichern unter** klicken, um die Änderungen unter einem neuen Konfigurationsmuster zu speichern.

Ergebnisse

Das geänderte Kategoriemuster wird auf der Registerkarte **Erweiterte ThinkServer CPlus BIOS-Muster** der Seite Konfigurationsmuster: Kategoriemuster aufgeführt:

Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Kategoriemuster ausführen:

- Kopieren eines vorhandenen Musters über einen Klick auf das Symbol **Kopieren** ( ).
- Löschen eines Musters über einen Klick auf das Symbol **Löschen** ( ).
- Umbenennen eines Musters über einen Klick auf das Symbol **Umbenennen** ( ).
- Export und Import von Mustern (siehe Server- und Kategoriemuster exportieren und importieren).

Servermuster für einen Server bereitstellen

Sie können ein Servermuster für einen oder mehrere verwaltete Server implementieren. Sie können auch ein Servermuster für eine oder mehrere leere Positionen in einem von Lenovo XClarity Administrator verwalteten Gehäuse oder in einem Platzhaltergehäuse implementieren. Durch die Implementierung eines Servermusters vor der Installation des Servers werden IP-Verwaltungsadressen sowie virtuelle Ethernet- oder Fibre Channel-Adressen reserviert, zudem werden die Netzwerkeinstellungen für die internen Switch-Ports mithilfe von Push übertragen.

Vorbereitende Schritte

Lesen Sie die Hinweise zur Serverkonfiguration, bevor Sie ein Servermuster auf Ihren verwalteten Einheiten anwenden (siehe Servermuster für einen Server bereitstellen).

Vorgehensweise

Gehen Sie wie folgt vor, um ein Serverprofil für einen verwalteten Server zu implementieren.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Servermuster**.

Schritt 3. Wählen Sie das zu implementierende Servermuster aus und klicken Sie auf das Symbol **Implementieren** ( ).

Im angezeigten Dialogfenster Servermuster implementieren wird das ausgewählte Servermuster in der Liste **Zu implementierendes Muster** aufgeführt.

Schritt 4. Bestimmen Sie, wann die Konfigurationen aktiviert werden sollen:

- **Vollständig**. Damit wird der Server unverzüglich eingeschaltet oder neu gestartet, um Server-, BMC- und UEFI-Konfigurationen zu aktivieren.
- **Teilweise**. (Standard) Damit werden Management-Controller-Konfigurationen unverzüglich aktiviert, aber die Aktivierung von Server- und UEFI-Konfigurationen wird auf den nächsten Neustart des Servers verschoben. Für eine vollständige Profilaktivierung muss der Server manuell eingeschaltet oder neu gestartet werden.

  Anmerkung: Bei der Bereitstellung von Servermustern, die nur IMM-Einstellungen enthalten (einschließlich Systeminformationen, Verwaltungsschnittstelle und erweiterte BMC-Kategoriemuster), muss der Server nicht neu gestartet werden.
- **Verzögert**. Damit wird ein Profil für Server-, Management-Controller- und UEFI-Konfigurationen generiert, jedoch werden die Konfigurationseinstellungen auf dem Server nicht aktiviert. Für eine vollständige Profilaktivierung muss das Serverprofil durch einen Neustart des Servers manuell aktiviert werden.

Anmerkung: Die Netzwerkeinstellungen für die internen Switch-Ports werden direkt nach der Implementierung und unabhängig von der konfigurierten Aktivierung mithilfe von Push an den Switch übertragen.

Schritt 5. Wählen Sie mindestens einen Server oder eine leere Gehäuseposition aus, für die das Servermuster implementiert werden soll.

Anmerkung: Um eine Liste der leeren Gehäusepositionen anzuzeigen, wählen Sie **Leere Positionen anzeigen**.

Schritt 6. Klicken Sie auf **Implementieren**. Im angezeigten Dialogfenster wird der Implementierungsstatus für jede ausgewählte Position aufgeführt.

Schritt 7. Klicken Sie erneut auf **Implementieren**, um den Implementierungsprozess zu starten.

Anmerkung: Die Implementierung kann einige Minuten dauern. Im Rahmen der Implementierung wird ein Serverprofil erstellt und den ausgewählten Servern oder Gehäusepositionen zugeordnet.

Schritt 8. Klicken Sie auf **Schließen**.

Nach dieser Aufgabe

Sie können den Implementierungsfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken. Sie können ebenfalls die Serverprofilerstellung überwachen, indem Sie auf **Bereitstellung → Serverprofile** klicken. Nach abgeschlossener Implementierung prüfen Sie die generierten Serverprofile und erfassen die IP-Verwaltungsadressen sowie alle virtualisierten Ethernet- oder Fibre Channel-Adressen.

Wenn Sie ein Servermuster für einen vorhandenen Server implementiert und Folgendes ausgewählt haben:

- Bei der Aktivierungsoption **Vollständig** wird ein Serverprofil für jeden Server erstellt, die Konfiguration wird an jeden Server übermittelt und jeder Server wird zur Aktivierung der Konfigurationsänderungen neu gestartet.
- Bei der Aktivierungsoption **Teilweise** wird ein Serverprofil für jeden Server erstellt und die Konfiguration wird an jeden Server übermittelt. Jeder Server muss manuell eingeschaltet oder neu gestartet werden, um die Konfigurationsänderungen vollständig zu aktivieren (siehe Einen Server ein- und ausschalten).
- Bei der Aktivierungsoption **Verzögert** wird ein Serverprofil für jeden Server erstellt. Das Serverprofil muss auf dem Server manuell aktiviert werden (siehe Ein Serverprofil aktivieren).

Nachdem Sie ein Servermuster für eine leere Position in einem verwalteten Gehäuse oder einem Platzhaltergehäuse implementiert haben, die Rechenknoten physisch in den entsprechenden Gehäusepositionen installiert sind und anschließend von Lenovo XClarity Administrator ermittelt und verwaltet werden, müssen Sie das Serverprofil auf den neu installierten Rechenknoten implementieren und aktivieren (siehe Ein Serverprofil aktivieren).

Wenn ein oder mehrere Server nach der Implementierung eines neuen Servermusters auf diese Server nicht starten, ist das Problem möglicherweise, dass die Booteinstellungen mit den standardmäßigen Booteinstellungen des Servermusters überschrieben wurden. Bei Betriebssystemen, die im UEFI-Modus installiert wurden, sind im Rahmen der Wiederherstellung der Standardeinstellungen möglicherweise weitere Konfigurationsschritte erforderlich, um die Bootkonfiguration wiederherzustellen. Beispiele für die Wiederherstellung der Boot-Einstellungen auf Windows- oder Linux-Servern finden Sie unter Booteinstellungen nach der Servermusterimplementierung wiederherstellen.

Ein Servermuster ändern

Sie können die folgenden Konfigurationsänderungen an einem vorhandenen Servermuster vornehmen. Wurde das ursprüngliche Servermuster auf Servern implementiert (und verwendet), können Sie das geänderte Servermuster auf allen oder einigen Servern erneut implementieren.

Zu dieser Aufgabe

Anmerkung: Falls das geänderte Servermuster auf einigen Servern nicht erneut implementiert werden soll, bleibt diesen Servern weiterhin das ursprüngliche Servermuster zugeordnet.

Durch die Bearbeitung des Servermusters können Sie eine einheitliche Konfiguration von einem zentralen Ort aus steuern und die ursprünglichen virtuellen Adresszuordnungen beibehalten.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Servermuster zu ändern.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Servermuster**.

Schritt 3. Wählen Sie das zu ändernde Servermuster aus und klicken Sie auf das Symbol **Bearbeiten** ( ). Der Assistent zum Bearbeiten von Servermustern wird angezeigt.

Schritt 4. Geben Sie den Namen des Musters und eine Beschreibung ein.

Schritt 5. Wählen Sie die lokale Speicherkonfiguration aus, die bei der Bereitstellung dieses Musters auf einem Server angewendet wird. Klicken Sie auf **Weiter**.

Informationen zu den lokalen Speichereinstellungen finden Sie unter Lokalen Speicher definieren.

Schritt 6. **Optional:** Ändern Sie die E/A-Adapteradressierung und definieren Sie zusätzliche E/A-Adapter zur Anpassung an die Hardware, die Sie vermutlich mit diesem Muster konfigurieren werden. Klicken Sie auf **Weiter**.

Informationen zu den E/A-Adaptereinstellungen finden Sie unter E/A-Adapter definieren.

Schritt 7. Definieren Sie die Bootreihenfolge, die bei der Bereitstellung dieses Musters auf einem Server angewendet wird. Klicken Sie auf **Weiter**.

Informationen zu Einstellungen für SAN-Bootziele finden Sie unter Bootoptionen definieren.

Schritt 8. Ausgewählte Firmwareeinstellungen aus der Liste vorhandener Kategoriemuster.

Sie können neue Kategoriemuster erstellen. Klicken Sie dazu auf das Symbol **Erstellen** ( ).

Weitere Informationen zu Firmwareeinstellungen finden Sie unter Firmwareeinstellungen definieren.

Schritt 9. Klicken Sie auf **Speichern**, um die Konfigurationsänderungen für das aktuelle Servermuster zu speichern. Sie können auch auf **Speichern unter** klicken, um die Konfigurationsänderungen unter einem neuen Servermuster zu speichern.

Schritt 10. Wählen Sie aus, ob die Änderungen für das aktuelle Servermuster oder ein neues Servermuster gespeichert werden sollen.

- Klicken Sie auf **Speichern**, um die Änderungen für das aktuelle Servermuster zu speichern. Führen Sie im Dialogfenster „Muster speichern und erneut bereitstellen“ die folgenden Schritte aus:
  1. Bestimmen Sie, wann die Konfigurationen aktiviert werden sollen.
     - **Vollständig**. Damit wird der Server unverzüglich eingeschaltet oder neu gestartet, um Server-, BMC- und UEFI-Konfigurationen zu aktivieren.
     - **Teilweise**. (Standard) Damit werden Management-Controller-Konfigurationen unverzüglich aktiviert, aber die Aktivierung von Server- und UEFI-Konfigurationen wird

auf den nächsten Neustart des Servers verschoben. Für eine vollständige Profilaktivierung muss der Server manuell eingeschaltet oder neu gestartet werden.

Anmerkung: Bei der Bereitstellung von Servermustern, die nur IMM-Einstellungen enthalten (einschließlich Systeminformationen, Verwaltungsschnittstelle und erweiterte BMC-Kategoriemuster), muss der Server nicht neu gestartet werden.

Anmerkung: Die Netzwerkeinstellungen für die internen Switch-Ports werden direkt nach der Implementierung und unabhängig von der konfigurierten Aktivierung mithilfe von Push an den Switch übertragen.

2. Wählen Sie die Zielserver aus, auf denen die Konfigurationsänderungen erneut implementiert werden sollen. Sie können alle Server, auf denen das ursprünglichen Servermuster implementiert wurde, oder nur einige davon auswählen.
3. Klicken Sie auf **Erneut bereitstellen**.

- Klicken Sie auf **Speichern unter**, um die Änderungen für ein neues Servermuster zu speichern. Informationen zum Implementieren des neues Musters finden Sie unter Servermuster für einen Server bereitstellen.

Server- und Kategoriemuster exportieren und importieren

Wenn Sie mehrere Lenovo XClarity Administrator-Instanzen haben, können Sie Server- und Kategoriemuster aus einer XClarity Administrator-Instanz exportieren und in eine andere XClarity Administrator-Instanz importieren.

Zu dieser Aufgabe

Sie können nur Server- und Kategoriemuster exportieren. Richtlinien, Adresspools und Profile können nicht exportiert werden. Bei exportierten Mustern wird jede Zuordnung zu referenzierten Adresspools aufgehoben. Um die Adresspools in einem importierten Muster zu verwenden, bearbeiten Sie das Muster und ordnen diesem die Pools vom XClarity Administrator zu, in den der Import erfolgte.

Anmerkung: Wenn Sie Servermuster exportieren, werden die zugeordneten Kategoriemuster ebenfalls exportiert.

Vorgehensweise

- So exportieren Sie ein oder mehrere Muster:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.
  2. Klicken Sie auf die Registerkarte **Servermuster** oder **Kategoriemuster**.
  3. Wählen Sie eines oder mehrere Muster für den Export aus.
  4. Klicken Sie auf das Symbol **Exportieren** ( ).
  5. Klicken Sie auf **Exportieren**, um die Muster zu exportieren.
  6. Speichern Sie die Musterdatendatei auf dem lokalen System.

     Anmerkung: Wenn ein exportiertes Muster Adresspools referenziert, werden solche Referenzen aus dem exportierten Muster entfernt, damit bei einem Import dieses Musters in eine andere XClarity Administrator-Instanz keine Konflikte entstehen. Nach dem Import des Musters können Sie dieses bearbeiten und die gewünschten Adresspools wieder zuordnen.
- So importieren Sie ein oder mehrere Muster:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.

2. Klicken Sie auf das Symbol **Importieren** (), um die Muster zu importieren. Das Dialogfenster „Muster importieren“ wird angezeigt.
3. Klicken Sie auf **Datei auswählen** und wählen Sie die zu importierende Musterdatendatei aus. Wiederholen Sie diesen Schritt für weitere Musterdatendateien.
4. Klicken Sie auf **Importieren**, um die ausgewählten Dateien zu importieren.

   Die angezeigte Zusammenfassung enthält eine Liste mit importierten Mustern, umbenannten Mustern (aufgrund von Namenskonflikten) und übersprungenen Mustern (da diese bereits vorhanden waren).

Mit Serverprofilen arbeiten

Ein *Serverprofil* ist eine Instanz eines Servermusters, die auf einen bestimmten Server angewendet wird. Wenn ein Servermuster für einen oder mehrere Server implementiert wird, werden Serverprofile automatisch generiert und zugeordnet. Für jeden Zielserver wird ein Serverprofil erstellt. Jedes Serverprofil enthält die spezielle Konfiguration für einen einzelnen Server sowie eindeutige Informationen über diesen (z. B. zugeordneter Name, IP- und MAC-Adressen).

Zu dieser Aufgabe

Das Serverprofil wird während des Baseboard Management Controller-Starts aktiviert. Sie können zwischen folgenden Optionen wählen:
- Starten Sie den Server nach der Musterimplementierung neu, um das Serverprofil unverzüglich zu aktivieren.
- Verzögern Sie die Aktivierung bis zum nächsten Neustart.
- Verzögern Sie die Aktivierung, bis Sie das Serverprofil manuell aktivieren.

Mehrere Serverprofile können die Einstellungen eines einzelnen Servermusters übernehmen. Nachdem ein Servermuster für einen oder mehrere Server implementiert wurde, können auch Konfigurationsänderungen schnell für mehrere Server übernommen werden. Dazu bearbeiten Sie das übergeordnete Servermuster sowie die Kategoriemuster. Die abhängigen Serverprofile werden automatisch aktualisiert und erneut für die zugeordneten Server implementiert. Durch eine Änderung des Servermusters können Sie über einen einzigen Verwaltungspunkt für eine einheitliche Konfiguration sorgen.

Wenn Sie einen vorhandenen Server ersetzen oder einen vorab bereitgestellten Server in einer leeren Position in einem Gehäuse installieren, muss das Serverprofil für diesen neuen Server aktiviert werden, um die Konfigurationsänderungen zu übernehmen.

Anmerkung: Sie können ein Servermuster für mehrere Server implementieren, mehrere Muster können jedoch nicht für einen einzelnen Server implementiert werden.

Es gibt mehrere Möglichkeiten, um das einem Server zugeordnete Serverprofil zu ändern. Dies ist vom Grund der Änderung abhängig.

- Server verschieben oder einem anderen Zweck zuführen:
  1. Deaktivieren Sie das derzeitige Serverprofil auf dem entsprechenden Server (siehe Ein Serverprofil deaktivieren).
  2. Implementieren Sie das neue Servermuster für den neuen Server (siehe Servermuster für einen Server bereitstellen).
- Ersatzserver anstelle eines ausgefallenen Servers verwenden:
  1. Deaktivieren Sie das derzeitige Serverprofil für den ausgefallenen Server (siehe Ein Serverprofil deaktivieren).
  2. Aktivieren Sie dasselbe Serverprofil für den Ersatzserver (siehe Ein Serverprofil aktivieren).

3. Sobald der ausgefallene Server wiederhergestellt ist, können Sie diese Schritte wiederholen und so die Profilzuordnung wieder wechseln.

- Hardware von ausgefallenem Server austauschen:
  1. Deaktivieren Sie das derzeitige Serverprofil für den ausgefallenen Server (siehe Ein Serverprofil deaktivieren).
  2. Tauschen Sie den ausgefallenen Server aus.
  3. Aktivieren Sie dasselbe Serverprofil für den neuen Server (siehe Ein Serverprofil aktivieren).

Wichtig:

- Bei Verwendung der virtuellen Adresszuordnung behält der Server die zugeordnete virtuelle MAC- oder WWN-Adresse, bis er ausgeschaltet wird. Wenn Sie ein Profil mit aktivierter virtueller Adresszuordnung deaktivieren, wird das Kontrollkästchen **Server ausschalten** automatisch ausgewählt. Stellen Sie zur Vermeidung von Adresskonflikten sicher, dass der ursprüngliche Server ausgeschaltet ist, bevor Sie das inaktive Profil für einen anderen Server aktivieren.
- Wenn Sie ein Profil löschen, das nicht vor Kurzem erstellt wurde, werden die virtuellen MAC- und WWN-Adressen *nicht* aus dem Adressenpool freigegeben. Siehe Serverprofil löschen für weitere Informationen.
- Die Einstellungen auf einem Server können nicht mehr konform mit dem jeweiligen Serverprofil sein, wenn Einstellungen ohne den Einsatz von Konfigurationsmustern geändert werden oder während der Implementierung ein Fehler aufgetreten ist, beispielsweise ein Fehler bei der Firmware oder eine ungültige Einstellung. Sie können den Konformitätsstatus jedes Servers über die Seite „Konfigurationsmuster: Serverprofile“ ermitteln.

Ein Serverprofil aktivieren

Sie können ein Serverprofil für einen verwalteten Server aktivieren, der ausgetauscht, neu zugewiesen oder neu installiert wurde.

Zu dieser Aufgabe

Wenn Sie einen vorhandenen Server ersetzen oder einen vorab bereitgestellten Server in einer leeren Position in einem Gehäuse installieren, muss das Serverprofil für diesen neuen Server aktiviert werden, um die Konfigurationsänderungen zu übernehmen.

Wichtig:

- Bei Verwendung der virtuellen Adresszuordnung behält der Server die zugeordnete virtuelle MAC- oder WWN-Adresse, bis er ausgeschaltet wird. Wenn Sie ein Profil mit aktivierter virtueller Adresszuordnung deaktivieren, wird das Kontrollkästchen **Server ausschalten** automatisch ausgewählt. Stellen Sie zur Vermeidung von Adresskonflikten sicher, dass der ursprüngliche Server ausgeschaltet ist, bevor Sie das inaktive Profil für einen anderen Server aktivieren.
- Wenn Sie ein Profil löschen, das nicht vor Kurzem erstellt wurde, werden die virtuellen MAC- und WWN-Adressen *nicht* aus dem Adressenpool freigegeben. Siehe Serverprofil löschen für weitere Informationen.
- Die Einstellungen auf einem Server können nicht mehr konform mit dem jeweiligen Serverprofil sein, wenn Einstellungen ohne den Einsatz von Konfigurationsmustern geändert werden oder während der Implementierung ein Fehler aufgetreten ist, beispielsweise ein Fehler bei der Firmware oder eine ungültige Einstellung. Sie können den Konformitätsstatus jedes Servers über die Seite „Konfigurationsmuster: Serverprofile“ ermitteln.

Vorgehensweise

So aktivieren Sie ein Serverprofil:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverprofile**. Die Seite Konfigurationsmuster: Serverprofile wird angezeigt.

Schritt 2. Wählen Sie das zu aktivierende Serverprofil.

Tipps: Der aktuelle Status der Serverprofile wird in der Spalte **Profilstatus** angezeigt. Sie können Serverprofile aktivieren, die den Aktivierungsstatus „deaktiv“ oder „Anstehend“ haben.

Schritt 3. Klicken Sie auf das Symbol **Serverprofil aktivieren** ( ).

Schritt 4. Klicken Sie auf **Activate**.

Wenn das Profil im Status „Ausstehend“, „Aktiv“ oder „Aktiv ausgefallen“ ist, können Sie auswählen, wann die Implementierung aktiviert werden soll:

- **Vollständig**. Damit wird der Server unverzüglich eingeschaltet oder neu gestartet, um Server-, BMC- und UEFI-Konfigurationen zu aktivieren.
- **Teilweise**. (Standard) Damit werden Management-Controller-Konfigurationen unverzüglich aktiviert, aber die Aktivierung von Server- und UEFI-Konfigurationen wird auf den nächsten Neustart des Servers verschoben. Für eine vollständige Profilaktivierung muss der Server manuell eingeschaltet oder neu gestartet werden.

  Anmerkung: Bei der Bereitstellung von Servermustern, die nur IMM-Einstellungen enthalten (einschließlich Systeminformationen, Verwaltungsschnittstelle und erweiterte BMC-Kategoriemuster), muss der Server nicht neu gestartet werden.

wenn das Serverprofil zum ersten Mal aktiviert wird, wechselt der Status des Profils zu „Aktiv“. Nachdem die Konformität überprüft wurde, wechselt der Status zu „Konformität“ oder „Nicht kompatibel“.

Ergebnisse

Der Status des Serverprofils auf der Seite „Konfigurationsmuster: Serverprofile“ ändert sich zu „Aktiv“.

Konfigurationsmuster: Serverprofile

Serverprofile bilden die spezielle Konfiguration für einen einzelnen Server ab.

Alle Aktionen | Alle Systeme | Filter

Profil	Server	Rack-Name/Einheit	Gehäuse/Position	Profilstatus	Muster
noop-profile1	ite-bt-217	C11 / Einheit 31	Chassis094 / Position 1	Aktiv	noop
noop-profile10	ite-bv-1507	C11 / Einheit 31	Chassis094 / Position 8	Aktiv	noop
noop-profile100	ite-cc-1431l	C12 / Einheit 21	Chassis113 / Position 4:1	Aktiv	noop
noop-profile101	ite-cc-1431u	C12 / Einheit 21	Chassis113 / Position 4:2	Ausstehende Aktivierung	noop
noop-profile102	ite-cc-1351l	C12 / Einheit 21	Chassis113 / Position 5:1	Ausstehende Aktivierung	noop

Ein Serverprofil deaktivieren

Sie können die Serverprofilzuordnung eines Servers oder einer Gehäuseposition aufheben, indem Sie das Profil deaktivieren.

Vorgehensweise

So deaktivieren Sie ein Serverprofil:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverprofile**. Die Seite Konfigurationsmuster: Serverprofile wird angezeigt.

Schritt 2. Wählen Sie das zu deaktivierende Serverprofil aus.

Tipp: Der aktuelle Status des Serverprofils wird in der Spalte **Profilstatus** angezeigt.

Schritt 3. Klicken Sie auf das Symbol **Serverprofil deaktivieren** ().

Schritt 4. Wählen Sie eine der folgenden Deaktivierungsoptionen aus:

- **IMM-ID-Einstellungen zurücksetzen**. Setzt die über das Profil konfigurierten Identitätseinstellungen zurück (einschließlich Baseboard Management Controller-Hostname, Einheitenname oder der Verwaltungsschnittstelle zugewiesene statische IP-Adressen). Nur die Einstellungen, die über das zugeordnete Servermuster konfiguriert wurden, werden zurückgesetzt.

  Anmerkung: Bei Servern mit statisch zugewiesenen IP-Adressen aktiviert diese Option den DHCP-Modus. Wenn im Netzwerk kein DHCP-Server aktiviert ist, muss der Server manuell mit einer gültigen statischen IP-Adresse konfiguriert werden. Converged-, NeXtScale- und System x-Rack- und -Tower-Server müssen manuell mit XClarity Administrator neu verwaltet werden.
- **Server ausschalten**. Server ausschalten. Wenn der Server wieder eingeschaltet ist, werden die Zuweisungen für virtuelle Adressen auf die fest integrierten Standardwerte zurückgesetzt.
- **Deaktivierung erzwingen**. Deaktiviert das Serverprofil auch dann, wenn der Server entfernt wurde oder nicht erreichbar ist.
- **Einstellungen für den internen Switch-Anschluss zurücksetzen**. Setzt die über das Profil konfigurierten Einstellungen für den internen Switch-Anschluss auf die Standardwerte zurück, einschließlich Deaktivieren des UFP-Modus und Entfernen zugeordneten Member-vports von VLAN-Definitionen. Nur die Einstellungen, die über das zugeordnete Servermuster konfiguriert wurden, werden zurückgesetzt.

  Diese Option ist standardmäßig deaktiviert.

  Wählen Sie diese Option aus, um die Switch-Ports in einem Status zu belassen, in dem das Serverprofil dann für einen anderen Server implementiert werden kann, ohne dass Einstellungen mit der vorherigen Switch-Port-Konfiguration in Konflikt stehen.

Schritt 5. Klicken Sie auf **Deaktivieren**.

Ergebnisse

Der Status des Serverprofils auf der Seite „Konfigurationsmuster: Serverprofile“ ändert sich zu „Deaktiv“.

Anmerkung: Wenn XClarity Administrator nicht mit dem Management-Controller kommunizieren kann (beispielsweise aufgrund eines fehlerhaften Status oder eines Neustartes des Management-Controllers), schlägt die Deaktivierung des Serverprofils fehl. Es wird nicht deaktiviert. Wenn dieser Fall eintritt, versuchen Sie die Deaktivierung erneut und wählen Sie die Option „Deaktivierung erzwingen“ aus. Der zuvor zugewiesene Server ist weiterhin mit der über das Profil zugewiesenen Identität und den Adresszuweisungen konfiguriert. Der Server muss manuell heruntergefahren und aus der Infrastruktur entfernt werden, um Adresskonflikte zu vermeiden.

Serverprofil löschen

Sie können nur Serverprofile löschen, die deaktiviert wurden.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die zu löschenden Serverprofile deaktiviert sind (siehe Ein Serverprofil deaktivieren).

Vorgehensweise

Gehen Sie wie folgt vor, um ein Serverprofil zu löschen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverprofile**. Die Seite Konfigurationsmuster: Serverprofile wird angezeigt.

Schritt 2. Wählen Sie das Serverprofil aus, das sich deaktivierten Status befindet.

Tipp: Der aktuelle Status des Serverprofils wird in der Spalte **Profilstatus** angezeigt.

Schritt 3. Klicken Sie auf das Symbol für **Löschen** ( ).

Anmerkung: Wenn Sie das zuletzt erstellte Profil löschen, wird eine virtuelle MAC- oder WWN-Adresse aus dem Adressenpool freigegeben. Wenn Sie ein Profil löschen, das nicht vor Kurzem erstellt wurde, werden die virtuellen MAC- und WWN-Adressen *nicht* aus dem Adressenpool freigegeben.

Mit Platzhaltergehäuse arbeiten

Über die Definition eines *Platzhaltergehäuses* als Ziel für das Servermuster können Sie vorab Server, die zu einem späteren Zeitpunkt in einem Flex System-Gehäuse installiert werden, implementieren.

Zu dieser Aufgabe

Wenn Sie ein Servermuster für ein Platzhaltergehäuse implementieren, erstellt Lenovo XClarity Administrator ein Serverprofil für alle 14 Serverpositionen im Flex System-Gehäuse und reserviert die IP-Verwaltungsadressen sowie die virtuellen Ethernet- oder Fibre Channel-Adressen für die Server.

Das Platzhaltergehäuse bündelt alle Serverprofile, sodass mit dem Eintreffen der Hardware auch das Platzhaltergehäuse implementiert werden kann, um die Serverprofile auf den physischen Server zu aktivieren (anstatt alle 14 Serverprofile einzeln zu implementieren). Jeder Server muss für eine vollständige Aktivierung des Serverprofils neu gestartet werden.

Ein Platzhaltergehäuse erstellen

Sie können ein Platzhaltergehäuse erstellen, das vor der Installation der Hardware bereitgestellt werden kann. Das Bereitstellen von Rechenknoten im Gehäuse reserviert IP-Verwaltungsadressen und virtuelle Ethernet- oder Fibre Channel-Adressen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Platzhaltergehäuse zu erstellen:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Platzhaltergehäuse**.

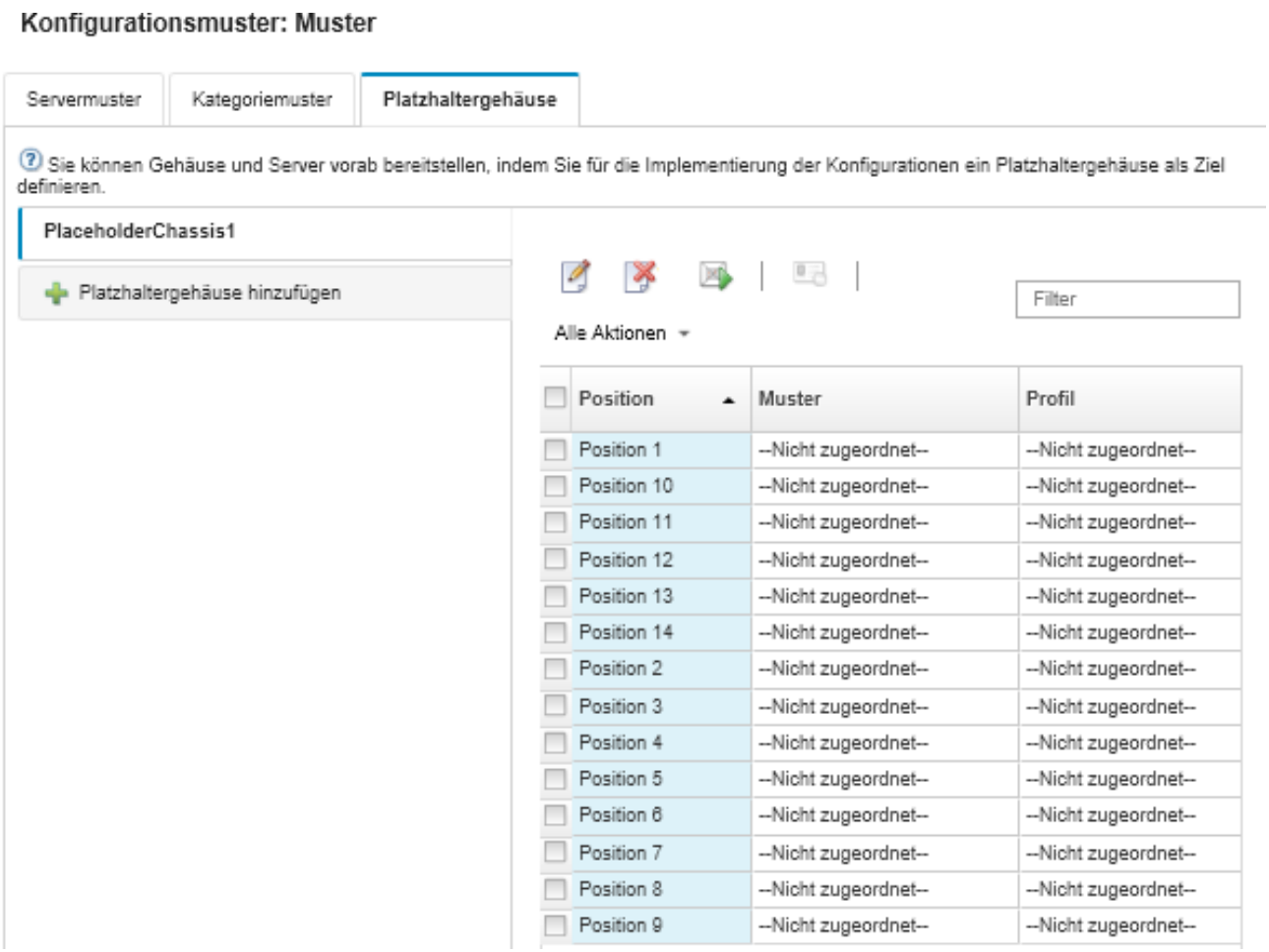
Schritt 3. Klicken Sie auf die vertikale Registerkarte **Platzhaltergehäuse hinzufügen**.

Schritt 4. Geben Sie Name und Beschreibung des Platzhaltergehäuses ein.

Schritt 5. Klicken Sie auf **Hinzufügen**.

Nach dieser Aufgabe

Für das neue Platzhaltergehäuse wird auf der Seite Konfigurationsmuster: Platzhaltergehäuse eine vertikale Registerkarte hinzugefügt.



Auf dieser Seite können Sie die folgenden Aktionen für ein ausgewähltes Platzhaltergehäuse ausführen:

- Bereitstellen des Platzhaltergehäuses über einen Klick auf das **Bereitstellen**-Symbol ( ).
- Ändern von Platzhaltergehäusename und -beschreibung über einen Klick auf das **Bearbeiten**-Symbol ( ).
- Bereitstellen eines Servermusters für das Platzhaltergehäuse (siehe Ein Servermuster für ein Platzhaltergehäuse implementieren).
- Deaktivieren des Serverprofils über ein Platzhaltergehäuse (siehe Ein Serverprofil deaktivieren).
- Löschen von Platzhaltergehäusen über einen Klick auf das **Löschen**-Symbol ( ).

Ein Servermuster für ein Platzhaltergehäuse implementieren

Sie können ein Servermuster für jede Position eines Platzhaltergehäuses implementieren. Sie können ein Servermuster implementieren, bevor dieServer im Flex System-Gehäuse installiert sind. Dann wird für jede Serverposition im Gehäuse ein Serverprofil erstellt und die IP-Verwaltungsadressen sowie die virtuellen Ethernet- oder Fibre Channel-Adressen werden reserviert.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Serverprofil für ein Platzhaltergehäuse zu implementieren.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Servermuster**.

Schritt 3. Wählen Sie das Servermuster aus, das Sie für das Platzhaltergehäuse implementieren möchten.

Schritt 4. Klicken Sie auf das Symbol **Implementieren** (). Das Dialogfenster Servermuster implementieren wird mit einer Liste der verfügbaren Gehäuse und Platzhaltergehäuse geöffnet.

Schritt 5. Wählen Sie **Verzögert** aus der Liste **Aktivierung** aus.

Schritt 6. Klicken Sie auf **Leere Positionen anzeigen**.

Schritt 7. Wählen Sie mindestens eine Platzhaltergehäuseposition aus, für die das Servermuster implementiert werden soll.

Schritt 8. Klicken Sie auf **Implementieren**. Im angezeigten Dialogfenster wird der Implementierungsstatus für jede ausgewählte Position aufgeführt.

Schritt 9. Klicken Sie erneut auf **Implementieren**, um den Implementierungsprozess zu starten.

Ein Serverprofil wird erstellt und jeder ausgewählten Position im Platzhaltergehäuse zugeordnet.

Anmerkung: Die Implementierung kann einige Minuten dauern.

Schritt 10. Klicken Sie auf **Schließen**.

Nach dieser Aufgabe

Sie können den Implementierungsfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken. Sie können ebenfalls die Serverprofilerstellung überwachen, indem Sie auf **Bereitstellung → Serverprofile** klicken. Nach abgeschlossener Implementierung prüfen Sie die generierten Serverprofile und erfassen die IP-Verwaltungsadressen sowie alle virtualisierten Ethernet- oder Fibre Channel-Adressen.

Nachdem das Flex System-Gehäuse physisch im Rack installiert ist und anschließend von XClarity Administrator ermittelt und verwaltet wird, können Sie das Platzhaltergehäuse implementieren, um alle Server im Gehäuse einzurichten (siehe Ein Servermuster für ein Platzhaltergehäuse implementieren).

Ein Platzhaltergehäuse implementieren

Nachdem Sie ein Platzhaltergehäuse vorkonfiguriert haben, indem Sie für dieses ein Servermuster implementiert und anschließend das tatsächliche Gehäuse ermittelt und verwaltet haben, können Sie nun das Platzhaltergehäuse implementieren und die tatsächlichen Rechenknoten konfigurieren.

Vorgehensweise

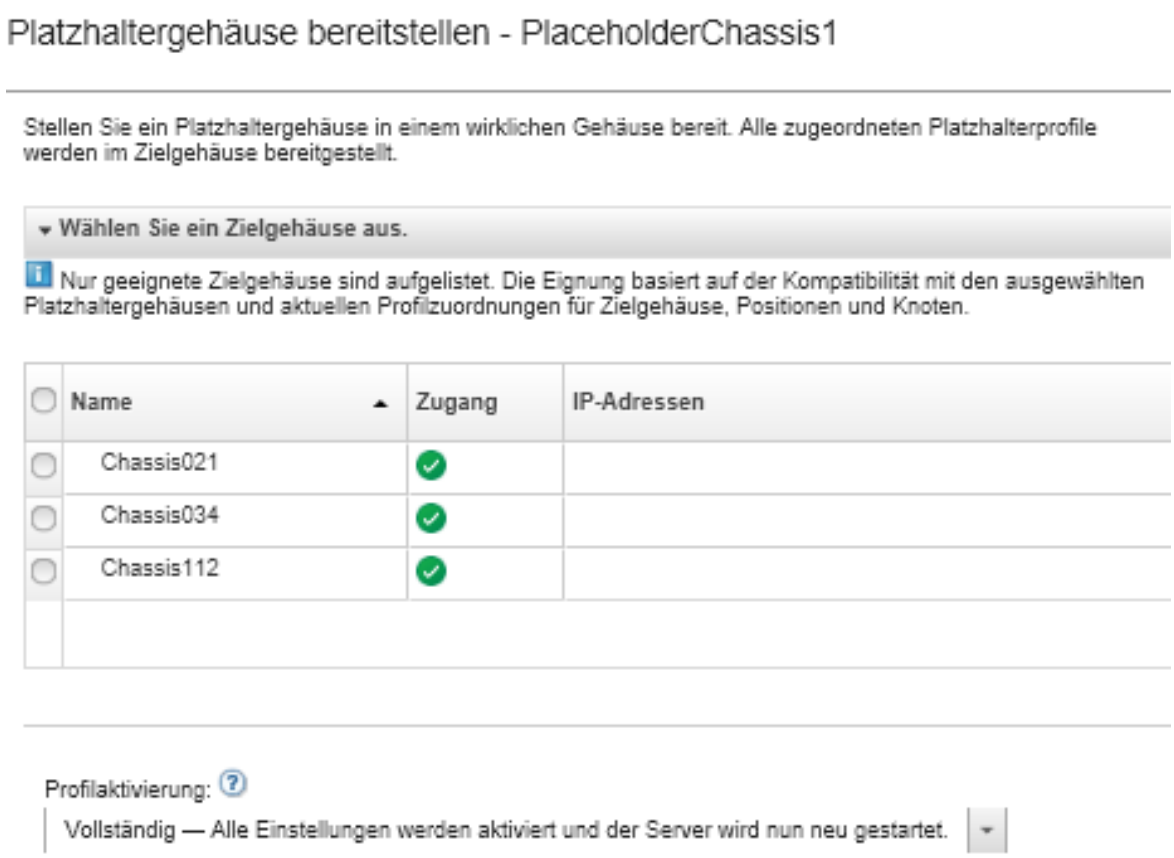
Gehen Sie wie folgt vor, um ein Platzhaltergehäuse zu implementieren:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverkonfigurationsmuster**. Die Seite Serverkonfigurationsmuster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Platzhaltergehäuse**.

Schritt 3. Wählen Sie die vertikale Registerkarte für das zu implementierende Platzhaltergehäuse aus.

Schritt 4. Klicken Sie auf das Symbol **Platzhaltergehäuse implementieren** (), um das Dialogfenster Platzhaltergehäuse bereitstellen anzuzeigen.



Schritt 5. Bestimmen Sie, wann die Konfigurationen aktiviert werden sollen:

Anmerkung: Die Netzwerkeinstellungen für die internen Switch-Ports werden direkt nach der Implementierung und unabhängig von der konfigurierten Aktivierung mithilfe von Push an den Switch übertragen.

- **Vollständig**. Damit wird der Server unverzüglich eingeschaltet oder neu gestartet, um Server-, BMC- und UEFI-Konfigurationen zu aktivieren.
- **Teilweise**. (Standard) Damit werden Management-Controller-Konfigurationen unverzüglich aktiviert, aber die Aktivierung von Server- und UEFI-Konfigurationen wird auf den nächsten Neustart des Servers verschoben. Für eine vollständige Profilaktivierung muss der Server manuell eingeschaltet oder neu gestartet werden.

  Anmerkung: Bei der Bereitstellung von Servermustern, die nur IMM-Einstellungen enthalten (einschließlich Systeminformationen, Verwaltungsschnittstelle und erweiterte BMC-Kategoriemuster), muss der Server nicht neu gestartet werden.

Schritt 6. Klicken Sie auf **Activate**.

Speicheradapter auf Standardwerte zurücksetzen

Sie können lokale Speicheradapter für einen oder mehrere Server auf in ihre werkseitigen Voreinstellungen zurücksetzen.

Zu dieser Aufgabe

Achtung: Diese Aktion löscht alle Daten auf den lokalen Speicheradaptern.

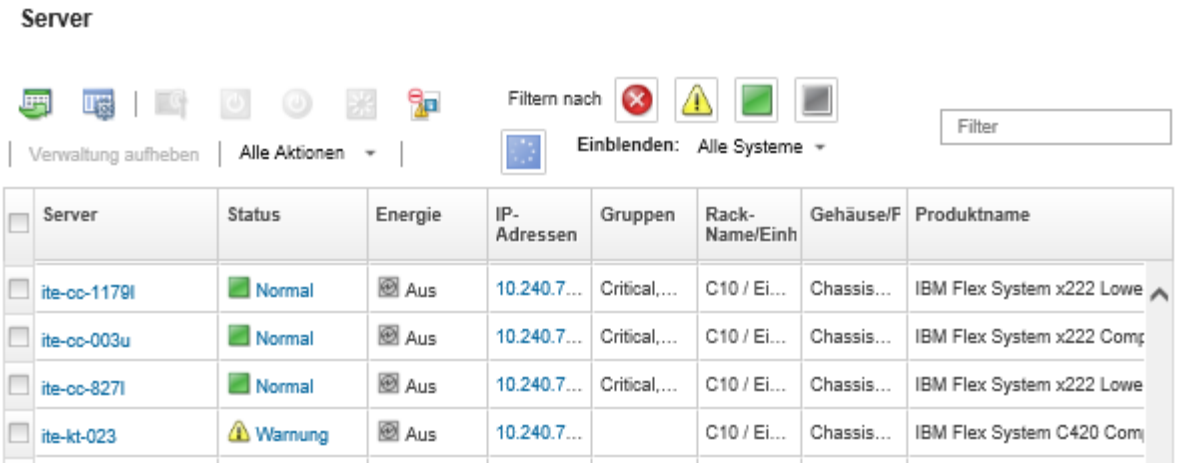
Wenn der Server ausgeschaltet ist und RAID-Verbindung unterstützt wird, wird der Server zur Systemkonfiguration gebootet, um lokalen Festplatten- und SSD-Adapter zurückzusetzen.

Vorgehensweise

Führen Sie diese Schritte aus, um die RAID-Konfiguration für einen oder mehrere Server zu löschen.

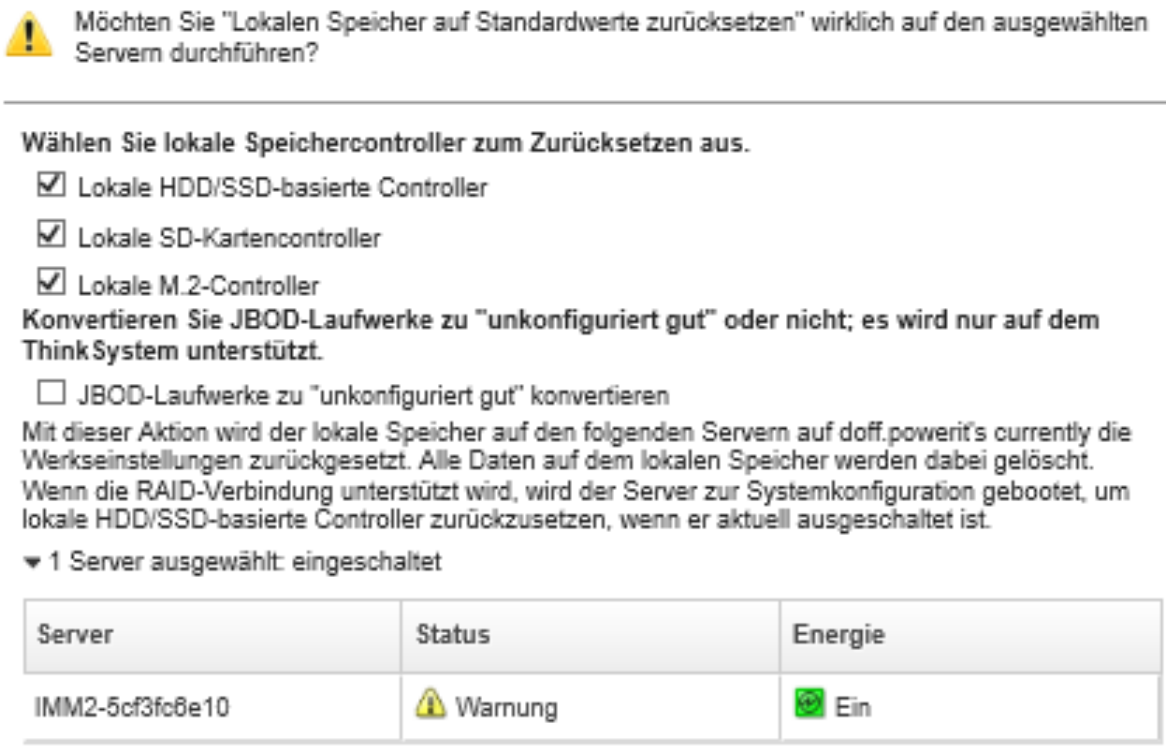
Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rack-Server und Rechenknoten).

Sie können die Tabellenspalten sortieren, um den Server, den Sie verwalten möchten, schneller zu finden. Außerdem können Sie in der Dropdownliste **Alle Systeme** einen Servertyp auswählen und im Feld **Filter** einen Text eingeben (beispielsweise den Namen oder die IP-Adresse), um die anzuzeigenden Server auszuwählen.



Schritt 2. Einen oder mehrere Server auswählen

Schritt 3. Wählen Sie **Alle Aktionen → Service → Lokalen Speicher auf Standardwerte zurücksetzen** aus. Ein Dialogfenster wird angezeigt, in dem zur Eingabe zusätzlicher Informationen aufgefordert wird.



Schritt 4. Wählen Sie die lokalen Speicheradapter zum Zurücksetzen aus.

Schritt 5. : (Nur ThinkSystem-Server) Wählen Sie aus, dass JBOD-Laufwerke zu „unkonfiguriert gut“ konvertiert werden.

Schritt 6. Klicken Sie auf **Speicher zurücksetzen**.

Speicher konfigurieren

Sie können permanenten Speicher für nichtflüchtige Intel® Optane™ DC-DIMMs ver- und entschlüsseln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um nichtflüchtigen Speicher zu ver- und zu entschlüsseln.

Schritt 1. Klicken Sie im XClarity Administrator-Menü auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rack-Server und Rechenknoten).

Schritt 2. Wählen Sie einen oder mehrere zu konfigurierende Server aus.

Schritt 3. Klicken Sie zum Anzeigen des Dialogfensters Intel Optane PMEM-Vorgang auf **Alle Aktionen → Sicherheit → Intel Optane PMEM-Vorgang**.

Schritt 4. Wählen Sie den auszuführenden Sicherheitsvorgang aus.

- **Sicherheit aktivieren**. In den nichtflüchtigen Speicherbereich geschriebene Daten werden mithilfe des angegebenen Verschlüsseltungstexts verschlüsselt.

  Wichtig: Notieren Sie sich den Verschlüsseltungstext. Der Verschlüsseltungstext ist erforderlich, um die Deaktivierung der Sicherheit zu autorisieren oder den Verschlüsseltungstext zu löschen.
- **Sicherheit deaktivieren**. In den nichtflüchtigen Speicherbereich geschriebene Daten werden nicht verschlüsselt.

Daten, die bereits in den nichtflüchtigen Speicherbereich geschrieben wurden, bleiben verschlüsselt und können weiterhin aufgerufen werden.

Anmerkung: Diese Aktion ist nur bei aktivierter Sicherheit und festgelegtem Verschlüsseltungstext verfügbar. Sie müssen den Vorgang mit dem aktuellen Verschlüsseltungstext autorisieren. Sie können die Sicherheit für mehrere DIMMs in der Einheit nur deaktivieren, wenn für alle DIMMs derselbe Verschlüsseltungstext genutzt wird.

- **Sicheres Löschen**. Damit löschen Sie den Verschlüsseltungstext, mit dem die im nichtflüchtigen Speicherbereich gespeicherten Daten verschlüsselt wurden. Auf diese Weise wird sichergestellt, dass die Daten nicht wiederherstellbar sind.

  Anmerkung: Diese Aktion ist nur bei aktivierter Sicherheit und festgelegtem Verschlüsseltungstext verfügbar. Sie müssen den Vorgang mit dem aktuellen Verschlüsseltungstext autorisieren.

- **Sicheres Löschen ohne Passphrase**. Löscht sicher alle Daten, die im persistenten Speicher der angegebenen DIMMs auf dem Gerät gespeichert sind. Nach dem sicheren Löschen sind keine Daten mehr wiederherstellbar.

  Anmerkung: Diese Aktion ist nur verfügbar, wenn die Sicherheit deaktiviert ist und keine Passphrase erforderlich ist.

Schritt 5. Geben Sie bei Bedarf die Passphrase an und bestätigen Sie sie.

Schritt 6. Klicken Sie auf **OK**.

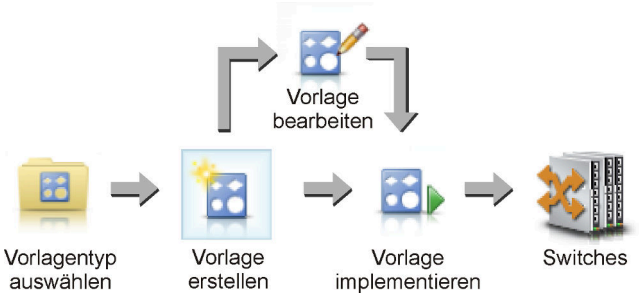
Kapitel 12. Switches mithilfe von Konfigurationsvorlagen konfigurieren

Sie können mithilfe von Vorlagen schnell mehrere CNOS-RackSwitches über einen einzelnen Satz definierter Konfigurationseinstellungen bereitstellen.

Zu dieser Aufgabe

Sie können Switch-Konfigurationsvorlagen in XClarity Administrator verwenden, um globale Einstellungen, Portkanäle, virtuelle LANs, VLAGs (Virtual Link Aggregation Groups) und Spine-Leaf-Topologien auf verwalteten Switches zu konfigurieren. Derzeit werden nur RackSwitches mit CNOS unterstützt.

In der folgenden Abbildung wird der Ablauf der Konfiguration von verwalteten RackSwitches dargestellt.



1. **Wählen Sie einen Vorlagentyp aus.**

   Eine *Switch-Konfigurationsvorlage* gruppiert ähnliche Switch-Einstellungen. Sie können folgende Typen an Switch-Konfigurationsvorlagen erstellen.
   - **Global**. Konfiguriert globale Einstellungen, einschließlich Systemeigenschaften, systemeigenen VLAN-Tags und L2-Schnittstellen.
   - **Portkanal**. Konfiguriert allgemeine und erweiterte Einstellungen für Portkanäle und entfernt Ports aus einem Portkanal und löscht einen Portkanal.
   - **Spine-Leaf**. Implementiert eine Spine-Leaf-Konfiguration in einer vorhandenen Topologie.
   - **Virtuelles LAN (VLAN)**. Konfiguriert VLAN-Einstellungen und -Eigenschaften und löscht ein VLAN.
   - **VLAG (Virtual Link Aggregation Group)**. Konfiguriert allgemeine, erweiterte und Peer-VLAG-Einstellungen und erstellt und löscht eine VLAG-Instanz.
2. **Erstellen Sie eine Vorlage.**

   Sie können mehrere Switch-Konfigurationsvorlagen erstellen, um so die verschiedenen, in Ihrem Rechenzentrum verwendeten Konfigurationen abzubilden. Verwenden Sie Switch-Konfigurationsvorlagen, damit Sie eine einheitliche Switch-Konfiguration von einem zentralen Ort aus steuern können.

   Weitere Informationen zum Erstellen von Switch-Konfigurationsvorlagen finden Sie unter Switch-Konfigurationsvorlage erstellen.
3. **Implementieren Sie die Vorlage auf einem oder mehreren Switches.**

   Sie können ein Servermuster auf einem oder mehreren einzelnen RackSwitches mit CNOS implementieren.

   Weitere Informationen zum Implementieren einer Switch-Konfiguration Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.
4. **Bearbeiten Sie eine Vorlage.**

Wenn Sie eine Switch-Konfigurationsvorlage bearbeiten, werden die aktualisierten Einstellungen nicht automatisch für alle Switches übernommen, auf denen die ursprüngliche Vorlage implementiert wurde. Geänderte Vorlagen müssen manuell erneut implementiert werden. Auf der Verlaufseite werden die Einstellungen jeder Implementierung nachverfolgt.

Einstellungen für die Standardserverkonfiguration festlegen

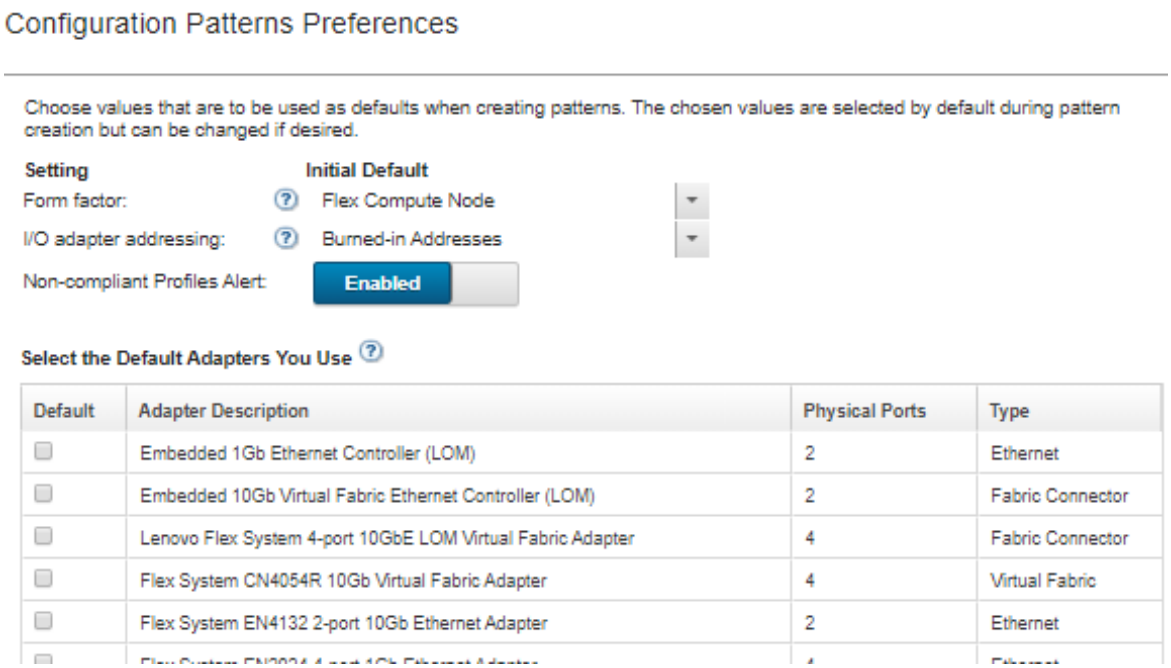
Sie können Werte definieren, die standardmäßig bei der Erstellung von Serverkonfigurationsmustern ausgewählt werden. Die Werte können während der Erstellung der Servermuster geändert werden.

Vorgehensweise

Gehen Sie wie folgt vor, um Einstellungen für die Standardserverkonfiguration festzulegen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung** und dann auf das Hilfesymbol (?) hinter **Konfigurationsmuster**, um die Seite Konfigurationsmuster: Erste Schritte aufzurufen.

Schritt 2. Klicken Sie auf **Einstellung für Konfigurationsmuster festlegen**, um das Dialogfeld Einstellung für Konfigurationsmuster anzuzeigen.



Schritt 3. Wählen Sie die Abmessungen für den Standardserver aus.

Schritt 4. Wählen Sie den Adressierungsmodus für den Standard-E/A-Adapter aus.

- **Herstellerkennung**. Verwenden Sie die vom Hersteller für den Adapter festgelegten WWN- und MAC-Adressen.
- **Virtuell**. Mit der virtuellen Adressierung des E/A-Adapters vereinfachen Sie die LAN- und SAN-Verbindungsverwaltung. Durch die Virtualisierung der E/A-Adressierung wird die Hardware-Herstelleradressenkennung mit virtualisierten Fibre-WWN- und Ethernet-MAC-Adressen neu zugeordnet. Dies kann die Implementierung beschleunigen, da Sie die SAN-Zonenmitgliedschaft vorkonfigurieren und das Failover einstellen können. Damit ist es im Falle eines Hardwareaustauschs nicht mehr erforderlich, die SAN-Zonenzuweisung und die LUN-Maskierungszuordnung neu zu konfigurieren.

Wenn die virtuelle Adressierung aktiviert ist, werden Ethernet- und Fibre Channel-Adressen standardmäßig und unabhängig von definierten Adaptern zugeordnet. Der Pool, aus dem Ethernet- und Fibre Channel-Adressen zugeordnet werden, ist frei wählbar.

Sie können die Einstellungen für die virtuelle Adressierung auch bearbeiten. Dazu klicken Sie auf das Symbol **Bearbeiten** () neben den Adressierungsmodi.

Beschränkung: Virtuelle Adressierung wird nur für Server in einem Flex System-Gehäuse unterstützt. Rack- und Tower-Server werden nicht unterstützt.

Schritt 5. Aktivieren oder deaktivieren Sie das Auslösen einen Alerts, wenn die Konfigurationseinstellungen eines Servers nicht mit dem zugewiesenen Serverkonfigurationsprofil übereinstimmen.

Alerts werden nur für die Nichtkonformität mit einem aktiven Profil ausgelöst (im ZUGEWIESENEN- oder FEHLERAUSLÖSENDEN-Status).

Wenn die Konfiguration des Servers wieder mit dem Serverprofil übereinstimmt oder das Serverprofil nicht zugewiesen ist, wird der Profil-Alert über die Nichtkonformität gelöscht.

Schritt 6. Wählen einen oder mehrere Standard-E/A-Adapter aus, die Sie als bevorzugte Adapter in den Auswahllisten verwenden möchten.

Schritt 7. Klicken Sie auf **Speichern**.

Switch-Konfigurationsvorlage erstellen

Wenn Sie eine Switch-Konfigurationsvorlage erstellen, definieren Sie die Einstellungen für einen bestimmten Konfigurationstyp.

Vorbereitende Schritte

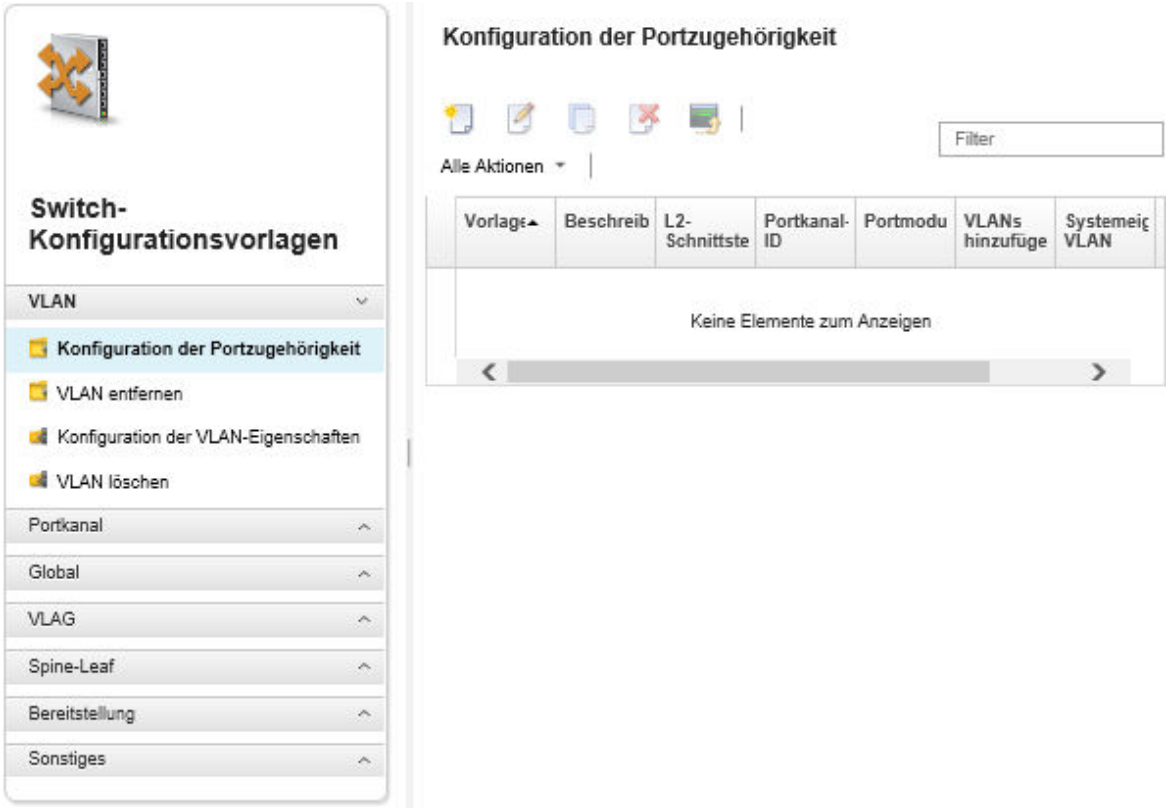
Berücksichtigen Sie vor der Erstellung einer Switch-Konfigurationsvorlage die folgenden Aspekte:

- Ermitteln Sie Switch-Gruppen mit den gleichen Hardwareoptionen, die identisch konfiguriert werden sollen. Sie können eine Switch-Konfigurationsvorlage verwenden, um dieselben Konfigurationseinstellungen auf mehrere Switches anzuwenden und so über einen zentralen Ort eine gemeinsame Konfiguration umzusetzen.
- Geben Sie die Aspekte der Konfiguration an, die angepasst werden sollen (z. B. globale, Portkanal- oder VLAN-Einstellungen).

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Switch-Konfigurationsvorlage zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.



Schritt 2. Wählen Sie im linken Navigationsbereich den Typ der zu erstellenden Vorlage aus.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ), um das Dialogfenster „Neue Vorlage erstellen“ anzuzeigen.

Die in diesem Dialogfenster aufgeführten Felder hängen vom Typ der Vorlage ab.

Schritt 4. Klicken Sie auf **Speichern**, um die Vorlage zu speichern, oder klicken Sie auf **Speichern und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Nach dieser Aufgabe

Wenn Sie auf **Speichern und implementieren** klicken, wird die Seite „Switch-Vorlage implementieren“ angezeigt. Über diese Seite können Sie die Switch-Konfigurationsvorlage auf bestimmten Switches implementieren.

Klicken Sie auf **Speichern**, um die Switch-Konfigurationsvorlage auf der Seite „Switch-Konfigurationsvorlagen“ zu speichern. Auf dieser Seite können Sie die folgenden Aktionen für ausgewählte Servermuster ausführen:

- Klicken Sie in der Spalte „Name“ auf den Vorlagennamen, um Informationen zur Vorlage anzuzeigen.
- Um eine aggregierte Liste aller Vorlagen anzuzeigen, klicken Sie auf **Andere → Alle Vorlagen**.
- Implementieren Sie die Vorlage (siehe Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren).
- Kopieren Sie eine Vorlage und ändern Sie diese, indem Sie auf das Symbol **Kopieren** klicken ( ).

- Bearbeiten Sie die Vorlage, indem Sie auf das Symbol **Bearbeiten** klicken ( ).

  Anmerkung: Änderungen an der Vorlage werden *nicht automatisch* erneut auf Switches implementiert, auf denen die ursprüngliche Vorlage implementiert war.

- Benennen Sie das Muster um, indem Sie auf das Symbol **Umbenennen** klicken ( ).
- Löschen Sie das Muster, indem Sie auf das Symbol **Löschen** klicken ( ).

Einstellungen für VLAN-Portzugehörigkeit definieren

Mit der Konfigurationsvorlage für die VLAN-Portzugehörigkeit können Sie einem oder mehreren VLANs (für Trunking) physische Ports und Portkanäle hinzufügen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Konfigurationsvorlage für die VLAN-Portzugehörigkeit zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAN → Konfiguration der Portzugehörigkeit** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

Wichtig: Sie müssen eine physische L2-Schnittstelle oder Portkanal-IDs angeben.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie mindestens eine gültige physische L2-Schnittstelle an. Sie können eine durch Komma getrennte Liste der Schnittstellen, einen durch Bindestrich getrennten ID-Bereich oder eine Kombination aus beiden angeben. Beispiel:
  - Ethernet 1/10
  - Ethernet 1/3, 5, 7, 9
  - Ethernet1/5-10, 21-32
  - Ethernet 2/2-5, 7, 9, 11-13
- Geben Sie mindestens eine gültige Portkanal-IDs (Port-Aggregator-Schnittstellen) an. Sie können eine Liste von Zahlen, die jeweils durch ein Komma getrennt sind, einen Bereich von Zahlen, die jeweils durch einen Bindestrich getrennt sind, oder eine Kombination aus beiden angeben. Die Werte und Bereiche können Zahlen von 1 bis 4096 sein, z. B.:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Legen Sie fest, ob der Port Datenverkehr mit oder ohne Tags akzeptiert. Es kann einen der folgenden Werte aufweisen.
  - **access**. Der Port übernimmt den Datenverkehr für ein einzelnes VLAN.
  - **trunk**. (Standard) Der Port übernimmt den Datenverkehr für alle VLANs, auf die der Switch zugreifen kann.
- Legen Sie mindestens eine VLAN-ID fest, die der Liste der VLAN-Zugehörigkeiten des Ports hinzugefügt werden soll. Sie können eine Liste von Zahlen, die jeweils durch ein Komma getrennt sind, einen Bereich von Zahlen, die jeweils durch einen Bindestrich getrennt sind, oder eine Kombination aus beiden angeben. Die Werte und Bereiche können Zahlen von 1 bis 4096 sein, z. B.:
  - 10
  - 3,5,7,9

– 5-10,21-32
– 2-5,7,9,11-13

Anmerkungen:

– Wenn der Portmodus auf „access“ gesetzt ist, wird nur die erste VLAN-ID verwendet. Beispielsweise wird im Bereich `2-4,5,10-20` nur `2`verwendet.
– CNOS reserviert standardmäßig die VLAN-IDs 4000 bis 4095. Wenn reservierte VLAN-IDs (von CNOS oder einem anderen Benutzer) verwendet werden, kann dies dazu führen, dass die Switch-Konfigurationsimplementierung fehlschlägt.

- Geben Sie eine systemeigene VLAN-ID an, mit der Datenverkehr ohne Tags markiert wird. Dies kann eine Zahl zwischen 1 und 4096 sein.

  Anmerkungen:
  – Dieses Feld ist nur gültig, wenn der Portmodus auf „trunk“ festgelegt ist.
  – Wenn er nicht angegeben ist oder sich die ID außerhalb der End-State-VLANs auf einem Port befindet, lässt der Port den Datenverkehr ohne Tags nicht zu.
- Wählen Sie **VLANs erstellen** aus, um die VLAN-IDs zu erstellen, die derzeit auf dem Ziel-Switch fehlen.

  Wenn ein Port zu einem VLAN gehört, das nicht erstellt wurde, bleibt der Port weiterhin Mitglied dieses VLANs, der Datenverkehr, der mit dieser VLAN-ID markiert ist und den Port erreicht, darf jedoch nicht übergeben werden.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

VLAN-Eigenschaften definieren

Sie können erweiterte VLAN-Eigenschaften mit der Vorlage für die Konfiguration von VLAN-Eigenschaften konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die Konfiguration von VLAN-Eigenschaften zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAN → Konfiguration der VLAN-Eigenschaften** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie eine VLAN-ID an, auf die die Änderungen angewendet werden sollen. Dies kann eine Zahl zwischen 1 und 4095 sein.

  Anmerkung: CNOS reserviert standardmäßig die VLAN-IDs 4000 bis 4095. Wenn reservierte VLAN-IDs (von CNOS oder einem anderen Benutzer) verwendet werden, kann dies dazu führen, dass die Switch-Konfigurationsimplementierung fehlschlägt.
- Geben Sie einen benutzerdefinierten Namen für das VLAN an.

- Legen Sie fest, ob das VLAN aktiv (aktiviert) oder ausgesetzt (deaktiviert) ist.
- Legen Sie fest, ob das Fluten von IP-Multicast-Daten (IPMC) im Ziel-VLAN über IPv4- oder IPv6-Schnittstellen gesteuert (aktiviert) wird. Es kann einen der folgenden Werte aufweisen.
  - **Deaktivieren**. IPv4 und IPv6 sind deaktiviert.
  - **Aktivieren**. IPv4 und IPv6 sind aktiviert.
  - **IPv4 deaktivieren**.
  - **IPv4 aktivieren**
  - **IPv6 deaktivieren**
  - **IPv6 aktivieren**

  Diese Aktion ist additiv, d. h., wenn „IPv4 aktivieren“ zusätzlich zu „Deaktivieren“ implementiert wird, führt dies zu „IPv4 aktivieren“, erfolgt die Implementierung jedoch zusätzlich zu „IPv6 aktivieren“, führt dies zu „Aktivieren“. Für die Deaktivierungsoptionen gilt das Umgekehrte.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

VLAN-Einstellungen entfernen

Sie können Schnittstellen aus VLANs mit der Vorlage „VLAN Remove“ entfernen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die VLAN-Entfernung zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAN → VLAN entfernen** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

Wichtig: Sie müssen eine physische L2-Schnittstelle oder Portkanal-IDs angeben.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie mindestens eine gültige physische L2-Schnittstelle an. Sie können eine durch Komma getrennte Liste der Schnittstellen, einen durch Bindestrich getrennten ID-Bereich oder eine Kombination aus beiden angeben. Beispiel:
  - Ethernet 1/10
  - Ethernet 1/1, 3, 5, 7
  - Ethernet 1/1-10, 21-30
  - Ethernet 2/1-5, 7, 9, 11-13
- Geben Sie mindestens eine gültige Portkanal-IDs (Port-Aggregator-Schnittstellen) an. Sie können eine Liste von Zahlen, die jeweils durch ein Komma getrennt sind, einen Bereich von Zahlen, die jeweils durch einen Bindestrich getrennt sind, oder eine Kombination aus beiden angeben. Die Werte und Bereiche können Zahlen von 1 bis 4096 sein, z. B.:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

- Geben Sie mindestens eine VLAN-ID an, die aus der Liste der VLAN-Portzugehörigkeit entfernt werden soll. Sie können eine Liste von Zahlen, die jeweils durch ein Komma getrennt sind, einen Bereich von Zahlen, die jeweils durch einen Bindestrich getrennt sind, oder eine Kombination aus beiden angeben. Die Werte und Bereiche können Zahlen von 1 bis 4096 sein, z. B.:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

  Anmerkung: Wenn der Portmodus auf „access“ gesetzt ist, bewirkt das Entfernen des VLANs, dass der Port zu VLAN 1 führt.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

VLANs löschen

Sie können VLAN-Konfigurationen mithilfe der Vorlage „VLAN löschen“ aus dem Switch entfernen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Vorlage „VLAN löschen“ zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAN → VLAN löschen** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie mindestens eine VLAN-ID an, die aus der Liste der VLAN-Portzugehörigkeit entfernt werden soll. Sie können eine Liste von Zahlen, die jeweils durch ein Komma getrennt sind, einen Bereich von Zahlen, die jeweils durch einen Bindestrich getrennt sind, oder eine Kombination aus beiden angeben. Die Werte und Bereiche können Zahlen von 1 bis 4096 sein, z. B.:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

  Anmerkung: Sie können keine reservierten VLAN-IDs löschen.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Allgemeine Einstellungen für den Portkanal definieren

Sie können Port-Aggregatoren erstellen und den Aggregatoren Ports hinzufügen, indem Sie eine allgemeine Konfigurationsvorlage für den Portkanal verwenden.

Wenn der Portkanal Ports aufweist und einige dieser Ports Teil der Vorlage sind, werden deren Eigenschaften mit den Einstellungen der Vorlage aktualisiert, wenn die Vorlage implementiert wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die allgemeine Konfiguration des Portkanals zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Portkanal → Allgemeine Konfiguration** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie mindestens eine gültige physische L2-Schnittstelle an. Sie können eine durch Komma getrennte Liste der Schnittstellen, einen durch Bindestrich getrennten ID-Bereich oder eine Kombination aus beiden angeben. Beispiel:
  - Ethernet 1/10
  - Ethernet 1/3, 5, 7, 9
  - Ethernet1/5-10, 21-32
  - Ethernet 2/2-5, 7, 9, 11-13
- Geben Sie zu erstellende oder zu aktualisierende Portkanal-ID (Port-Aggregator-Schnittstelle) an. Dies kann eine Zahl zwischen 1 und 4095 sein.
- Geben Sie den LACP (Link Aggregation Control Protocol)-Portmodus an. Es kann einen der folgenden Werte aufweisen.
  - **Aktiv**. (Standard) LACP wird ohne Bedingungen aktiviert.
  - **Passiv**. LACP wird nur bei Erkennung einer LCAP-Einheit aktiviert.
  - **Static**. Deaktiviert LCAP.

  Anmerkung: Im selben Aggregator kann sowohl „Aktiv“ als auch „Passiv“ verwendet werden, „Statisch“ hingegen nicht.
- Geben Sie die LACP-Portpriorität an. Dies kann eine Zahl zwischen 1 und 65535 sein.

  Anmerkung: Die LACP-Port-ID setzt sich aus der Priorität des LACP-Ports und der Portnummer zusammen.
- Geben Sie den LACP-Timeout-Modus an, bevor LCAP in den Einzelmodus wechselt. Es kann einen der folgenden Werte aufweisen.
  - **Lang**. (Standard) 90 Sekunden
  - **Kurz**. 3 Sekunden

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Erweiterte Einstellungen für den Portkanal definieren

Sie können erweiterte Einstellungen für den Portkanal mithilfe der Vorlage für die erweiterte Konfiguration des Portkanals konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die erweiterte Konfiguration des Portkanals zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Portkanal → Erweiterte Konfiguration** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie eine zu aktualisierende Portkanal-ID (Port-Aggregator-Schnittstelle) an. Dies kann eine Zahl zwischen 1 und 4095 sein.
- Legen Sie fest, ob einzelne Ports aktiv bleiben sollen, wenn LACP fehlschlägt. Es kann einen der folgenden Werte aufweisen.
  - **Aktiv**. (Standard) LACP wird ohne Bedingungen aktiviert.
  - **Aussetzen**. Deaktiviert LACP.
- Geben Sie die Mindestanzahl der Links an, die aktiv sein müssen, damit der Portkanal als aktiv betrachtet wird. Dies kann eine Zahl zwischen 1 und 32 sein.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Portkanäle löschen

Mit der Vorlage „Portkanal löschen“ können Sie Portkanäle aus dem Switch entfernen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Vorlage „Portkanal löschen“ zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Portkanal → Portkanal löschen** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie mindestens eine gültige Portkanal-ID (Port-Aggregator-Schnittstellen) an, die gelöscht werden soll. Sie können eine Liste von Zahlen, die jeweils durch ein Komma getrennt sind, einen Bereich von Zahlen, die jeweils durch ein Komma getrennt sind, oder eine Kombination aus beiden angeben. Die Werte und Bereiche können Zahlen von 1 bis 4096 sein, z. B.:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Allgemeine Switch-Einstellungen definieren

Sie können allgemeine Switch-Eigenschaften mithilfe der Vorlage für die globale generische Konfiguration konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die globale generische Konfiguration von Switches zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Global → Generische Konfiguration** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie die LACP-Systempriorität an, die zum Generieren der LACP-System-ID verwendet wird. Dies kann eine Zahl zwischen 1 und 65535 sein.
- Legen Sie fest, wo das systemeigene VLAN-Tagging aktiviert werden soll. Es kann einen der folgenden Werte aufweisen.
  - **Eingang und Ausgang**
  - **Nur Ausgang**

  Anmerkung: Diese Eigenschaft wird von CNOS 10.10.1 und höher unterstützt.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Globale L2-Schnittstelleneinstellungen definieren

Sie können VLAN-Tagging-Eigenschaften auf L2-Schnittstellen mithilfe der Konfigurationsvorlage für die L2-Schnittstelle konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die L2-Schnittstellenkonfiguration zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Global → Konfiguration der L2-Schnittstelle** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie mindestens eine gültige physische L2-Schnittstelle an. Sie können eine durch Komma getrennte Liste der Schnittstellen, einen durch Bindestrich getrennten ID-Bereich oder eine Kombination aus beiden angeben. Beispiel:
  - Ethernet 1/10

  - Ethernet 1/3, 5, 7, 9
  - Ethernet1/5-10, 21-32
  - Ethernet 2/2-5, 7, 9, 11-13
- Legen Sie fest, wo das systemeigene VLAN-Tagging aktiviert werden soll. Es kann einen der folgenden Werte aufweisen.
  - **Eingang und Ausgang**
  - **Nur Ausgang**

  Anmerkung: Diese Eigenschaft wird von CNOS 10.10.1 und höher unterstützt.
- Legen Sie fest, ob die Unterstützung für Tunnelling (QinQ) aktiviert oder deaktiviert werden soll.

  Anmerkung: Diese Eigenschaft wird von CNOS 10.10.1 und höher unterstützt.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Einstellungen für Peer-VLAG definieren

Sie können erweiterte VLAG-Peers mit der Vorlage für die VLAG-Peer-Konfiguration konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die VLAG-Peer-Konfiguration zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAG → Peer-Konfiguration** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Wählen Sie aus, ob die VLAG aktiviert oder deaktiviert werden soll.
- Füllen Sie die folgenden Felder für Peer 1 und Peer 2 aus. Die Felder für beide Peers müssen ausgefüllt werden.
  - Geben Sie die IIPv4- oder die IPv6-Adresse des VLAG-Peers an, der für die Integritätsprüfung verwendet werden soll.
  - Geben Sie die ID des Portkanals an, der zwischen den beiden Peers verwendet wird. Dies kann eine Zahl zwischen 1 und 4095 sein.
  - Geben Sie die VRF an, die für die Integritätsprüfung verwendet wird (z. B. Verwaltung, Standard oder customVRF).

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Einstellungen der VLAG-Instanz definieren

Sie können eine VLAG-Instanz mit der Vorlage für die VLAG-Instanz-Konfiguration erstellen oder aktualisieren. Eine VLAG-Instanz ist ein Gerät, das mit beiden Switches verbunden ist (in der Regel über eine Portzusammenlegung), dem das VLAG als ein einzelnes Gerät angezeigt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die VLAG-Instanzkonfiguration zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAG → Instanzkonfiguration** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie die VLAG-ID an. Dies kann eine Zahl zwischen 1 und 64 sein.
- Geben Sie die ID des Portkanals an, der mit Peer 1 und Peer 2 verbunden ist. Hierbei kann es sich um eine Zahl von 1 bis 4095 handeln.
- Legen Sie fest, ob die VLAG-Instanz aktiviert oder deaktiviert werden soll.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Erweiterte VLAG-Einstellungen definieren

Sie können erweiterte Vlag-Eigenschaften mit der Vorlage für die erweiterte VLAG-Konfiguration konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für die erweiterte VLAG-Konfiguration zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAG → Erweiterte Konfiguration** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Legen Sie die Priorität fest, mit der gesteuert wird, welcher Peer primär ist. Dies kann eine Zahl zwischen 1 und 65535 sein.

  Wenn nicht anders angegeben, wird die Standardpriorität des Switches verwendet. Der Standardwert für CNOS ist 0.
- Legen Sie die Karenzzeit (in Sekunden) fest, innerhalb derer die VLAG nach einem gleichzeitigen Neustart online geschaltet werden soll. Dies kann eine Zahl zwischen 240 und 3600 sein.

  Wenn nicht anders angegeben, wird der Switch-Standardwert verwendet. Der Standardwert für CNOS ist 300.

- Legen Sie die Ebenen-ID zur Unterscheidung von VLAG-Setups im selben Netzwerk fest. Dies kann eine Zahl zwischen 1 und 512 sein.
- Legen Sie das Intervall für die vLAG-Startverzögerung fest, das verwendet wird, um den Aufruf von Ports nach dem erneuten Laden von Peers zu verzögern. Dies kann eine Zahl zwischen 0 und 3600 sein.

  Wenn nicht anders angegeben, wird der Switch-Standardwert verwendet. Der Standardwert für CNOS ist 120.
- Legen Sie die Anzahl der VLAG-Keep-Alive-Versuche (unbeantwortete Hello-Nachrichten) an, bevor die VLAG fehlschlägt. Dies kann eine Zahl zwischen 1 und 24 sein.

  Wenn nicht anders angegeben, wird der Switch-Standardwert verwendet. Der Standardwert für CNOS ist 3.
- Legen Sie das Intervall zwischen VLAG-Keep-Alive-Versuchen (in Sekunden) fest. Dies kann eine Zahl zwischen 2 und 300 sein.

  Wenn nicht anders angegeben, wird der Switch-Standardwert verwendet. Der Standardwert für CNOS ist 5.
- VLAG-Keep-Alive-Wiederholungsversuche (in Sekunden) fest. Dies kann eine Zahl zwischen 1 und 300 sein.

  Wenn nicht anders angegeben, wird der Switch-Standardwert verwendet. Der Standardwert für CNOS ist 30.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Vlag-Instanz löschen

Sie können eine VLAG-Instanz mit der Vorlage „VLAG-Instanz löschen“ erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Vorlage „VLAG-Instanz löschen“ zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **VLAG → Instanz löschen** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie die eindeutige ID der VLAG-Instanz an. Dies kann eine Zahl zwischen 1 und 64 sein.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Spine-Leaf-Topologie definieren

Sie können die physische Topologie überprüfen und eine SpineLeaf (L3 Fabric)-Konfiguration auf verwalteten Switches mithilfe der Vorlage für den Spine-Leaf-Topologie-Assistenten implementieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Vorlage für den Spine-Leaf-Topologie-Assistenten zu erstellen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf den **Spine-Leaf → Topologie-Assistenten** und dann auf das Symbol **Erstellen** ( ).

Schritt 3. Geben Sie im Dialogfenster Neue Vorlage die folgenden Informationen an.

- Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
- Geben Sie die AS-Nummer (Autonomous System Number, ASN) für das Border Gateway Protocol (BGP) an, das auf dem Switch ausgeführt wird. Hierbei kann es sich um eine Zahl zwischen 1 und 4294967295 handeln.

  Anmerkung: Diese wird von CNOS 10.9.3 und höher unterstützt.
- Legen Sie fest, ob einzelne Links zwischen Switches zugelassen werden sollen.

  In der Regel treten bei der Implementierung Fehler auf, wenn nicht mindestens zwei Links zwischen Spine- und Leaf-Switch vorhanden sind.

Schritt 4. Klicken Sie auf **Erstellen**, um die Vorlage zu speichern, oder klicken Sie auf **Erstellen und implementieren**, um die Vorlage zu speichern und sofort auf einem oder mehreren verwalteten RackSwitches zu implementieren.

Informationen zum Implementieren von Vorlagen finden Sie unter Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren.

Switch-Konfigurationsvorlagen auf einem Ziel-Switch implementieren

Sie können VLAN-Porteinstellungen definieren, indem Sie eine Vorlage für die VLAN-Portkonfiguration erstellen.

Zu dieser Aufgabe

Es gibt drei Typen der Implementierung:

- **Normal**. Implementiert Switch-Konfigurationseinstellungen auf einem oder mehreren RackSwitches in einer grundlegend mehrstufigen Architektur.
- **VLAG**. Implementiert Switch-Konfigurationseinstellungen auf genau zwei Switches, die eine VLAG (Virtual Link Aggregation Group)-Architektur unterstützen. Die Switches müssen das gleiche Modell und dieselbe Softwareversion haben.
- **Spine-Leaf**. Implementierungsvorlagen für einen oder mehrere Spine- und Leaf-Switches.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Switch-Konfigurationsvorlage auf einem oder mehreren verwalteten Switches zu implementieren.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Wählen Sie eine oder mehrere zu implementierende Switch-Konfigurationsvorlagen aus.

Schritt 3. Klicken Sie auf das Symbol **Implementieren** (), um das Dialogfenster „Vorlage implementieren“ anzuzeigen.

Schritt 4. Wählen Sie einen oder mehrere Switches aus, auf denen die Vorlagen implementiert werden sollen.

Es werden nur Switches aufgelistet, die mit den ausgewählten Vorlagen kompatibel sind.

Schritt 5. Klicken Sie auf **Implementieren**. Im angezeigten Dialogfenster wird der Implementierungsstatus für jeden ausgewählten Switch aufgeführt.

Schritt 6. Klicken Sie erneut auf **Implementieren**, um den Implementierungsprozess zu starten.

Anmerkung: Die Implementierung kann einige Minuten dauern.

Nach dieser Aufgabe

Sie können den Implementierungsverlauf anzeigen (siehe Verlauf der Switch-Konfigurationsimplementierung anzeigen).

Verlauf der Switch-Konfigurationsimplementierung anzeigen

Sie können Informationen über Switch-Konfigurationsvorlagen anzeigen, die auf verwalteten Switches implementiert wurden, darunter Vorlagenname und -typ, Zeitstempel sowie die Switches, auf denen die Implementierung erfolgte. Jede Implementierung enthält einen Snapshot der Vorlage zum Implementierungszeitpunkt.

Vorgehensweise

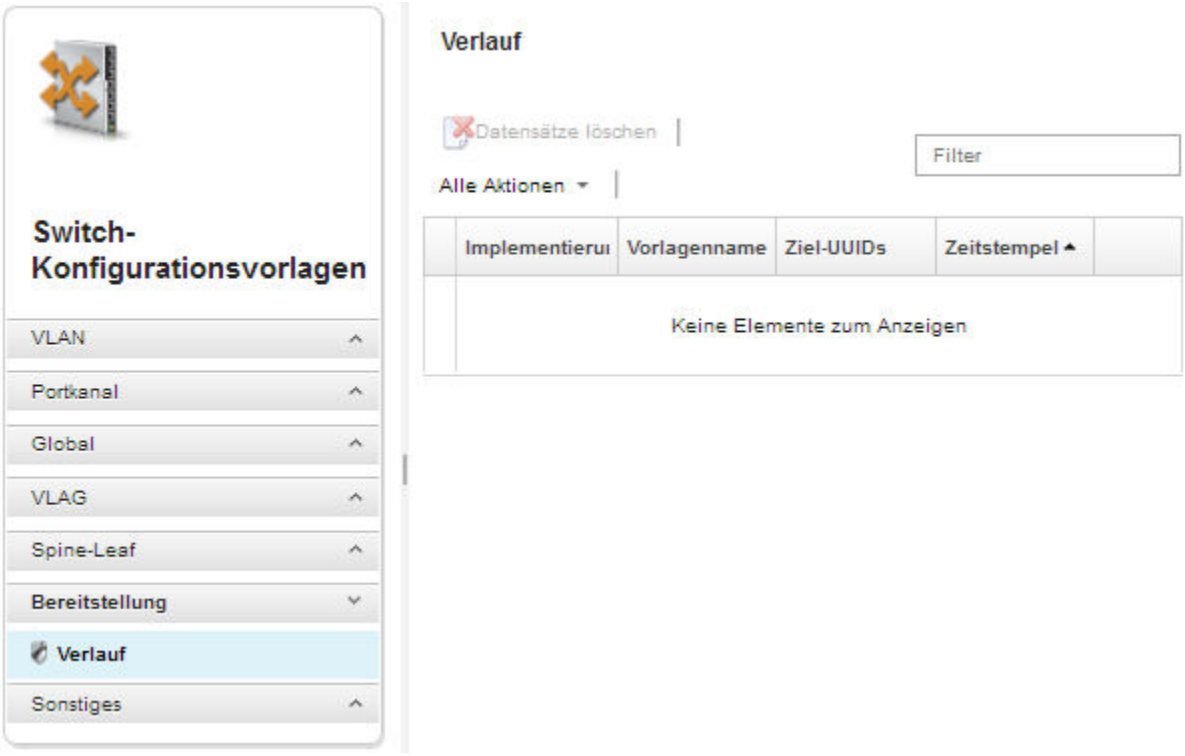
Führen Sie die folgenden Schritte aus, um den Verlauf der Switch-Konfigurationsimplementierung anzuzeigen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Switch-Konfigurationsvorlagen**. Die Seite „Switch-Konfigurationsvorlagen“ wird angezeigt.

Schritt 2. Blenden Sie **Implementierung** ein und klicken Sie im linken Navigationsbereich auf **Verlauf**, um eine Tabelle mit implementierten Vorlagen anzuzeigen.

Die Spalte **Status** gibt an, ob die Konfigurationsimplementierung erfolgreich war. Sie kann einen der folgenden Status haben:

- **Erfolgreich**. Die Konfigurationsimplementierung auf allen Ziel-Switches wurde erfolgreich abgeschlossen.
- **Warnung**. Die Konfigurationsimplementierung auf mindestens einem Ziel-Switch wurde mit Warnungen abgeschlossen.
- **Fehlgeschlagen**. Die Konfigurationsimplementierung auf mindestens einem Ziel-Switch ist fehlgeschlagen.



Nach dieser Aufgabe

- Zeigen Sie die Informationen zu jeder implementierten Vorlage an, einschließlich dessen, was implementiert wurde und ob es erfolgreich abgeschlossen wurde oder ein Fehler aufgetreten ist, indem Sie auf den Namen der Vorlage in der Tabelle klicken.
- Löschen Sie den Implementierungsverlauf, indem Sie eine Implementierung auswählen und auf das Symbol **Löschen** klicken ( ).

Kapitel 13. Firmware auf verwalteten Einheiten aktualisieren

Über die Lenovo XClarity Administrator-Webschnittstelle können Sie Firmwareaktualisierungen für verwaltete Einheiten wie Gehäuse, Server, Speichersysteme und Switches herunterladen, installieren und verwalten. Sie können Firmwarekonformitätsrichtlinien für verwaltete Einheiten zuweisen. So können Sie sicherstellen, dass die Firmware auf diesen Einheiten konform bleibt. Wenn die überprüften Firmwareversionen nicht den vorgeschlagenen vordefinierten Richtlinien entsprechen, können Sie außerdem Firmwarekonformitätsrichtlinien erstellen und bearbeiten.

Weitere Informationen:
- XClarity Administrator: Effizienz bei der Aktualisierung von Firmware steigern
- Lenovo ThinkSystem Firmware- und Treiberaktualisierung Best Practices
- XClarity Administrator: Bare Metal zu Cluster
- XClarity Administrator: Firmwareaktualisierungen
- XClarity Administrator: Firmwaresicherheitsaktualisierungen bereitstellen

Vorbereitende Schritte

Das Aktualisieren der Firmware und das Aktualisieren der Einheitentreiber sind separate Prozesse in XClarity Administrator; es besteht keine Verbindung zwischen diesen Prozessen. XClarity Administrator sorgt nicht für Kompatibilität zwischen Firmware und Einheitentreibern auf verwalteten Einheiten, obwohl es empfohlen wird, die Einheitentreiber gleichzeitig mit der Firmware zu aktualisieren.

Zu dieser Aufgabe

Anmerkung: Zur Aktualisierung der Firmware ist kein Betriebssystem erforderlich. Stellen Sie bei Bare-Metal-Servern sicher, dass der Server vor der Aktualisierung der Firmware ausgeschaltet wird.

Sie können Firmwareaktualisierungen für die folgenden verwalteten Einheiten übernehmen und verwalten.
- **Gehäuse**. CMM-Aktualisierungen
- **ThinkAgile-, ThinkSystem-, System x-, Converged-, Flex System- und NeXtScale-Server**. Baseboard Management Controller-, UEFI-, DSA-, Mezzanine- und Adapteraktualisierungen
- **RackSwitch und Flex System-Switches**
- **Lenovo Storage und ThinkSystem DM-Speichereinheiten**
- **IBM TS4300 Bandbibliothekseinheiten**

Firmware für die folgenden Einheiten kann nicht über XClarity Administrator aktualisiert werden.

- **ThinkServer-Server**. Lesen Sie die im Lieferumfang des Servers enthaltene Dokumentation, um Informationen zur Aktualisierung der Firmware zu erhalten.
- **Flex Power Systems-Rechenknoten**. Es sind verschiedene Methoden zur Aktualisierung der Firmware von Flex Power Systems-Rechenknoten verfügbar. Siehe IBM Flex System p260/p460 Rechenknoten Online -dokumentation für weitere Informationen. Der Prozess für andere Flex Power Systems-Rechenknoten ist identisch.
- **Flex-Switches im gestapelten Modus oder im geschützten Modus**. Sie können *keine* Firmware für gestapelte Switches aktualisieren. Die Aktualisierung von Firmware ist für alle gestapelten Switches deaktiviert.
- **Flex-Switches**. Wenn Sie den folgenden Switch verwenden, lesen Sie die im Lieferumfang des Switches enthaltene Dokumentation, um Informationen zur Aktualisierung der Firmware zu erhalten.
  - Cisco Nexus B22 Fabric Extender

Vorgehensweise

In der folgenden Abbildung wird der Ablauf der Aktualisierung von Firmware auf verwalteten Einheiten dargestellt.

Schritt 1. **Repository für Firmwareaktualisierungen verwalten**

Das *Firmwareaktualisierungs-Repository* enthält einen Katalog mit den verfügbaren Aktualisierungen und Aktualisierungspaketen, die auf verwalteten Einheiten übernommen werden können.

Der *Katalog* enthält Informationen zu Firmwareaktualisierungen, die derzeit für die von XClarity Administrator unterstützten Einheiten verfügbar sind. Der Katalog organisiert die Firmwareaktualisierungen nach Einheitentyp. Wenn Sie den Katalog aktualisieren, ruft XClarity Administrator Informationen zu den neuesten verfügbaren Firmwareaktualisierungen von der Lenovo Website ab (einschließlich der Dateien metadata.xml oder .json und readme.txt) und speichert die Informationen im Firmwareupdate-Repository. Die Nutzdatendatei (.exe) wird nicht heruntergeladen. Weitere Informationen zum Aktualisieren des Katalogs finden Sie unter Produktkatalog aktualisieren.

Wenn neue Firmwareaktualisierungen verfügbar sind, müssen Sie die Aktualisierungspakete erst herunterladen, bevor Sie die Firmware auf den verwalteten Geräten aktualisieren können. Beim Aktualisieren des Katalogs werden nicht automatisch Aktualisierungspakete heruntergeladen. Die Tabelle **Produktkatalog** auf der Seite Repository für Firmwareaktualisierungen zeigt, welche Aktualisierungspakete heruntergeladen werden und welche zum Download verfügbar sind.

Zum Herunterladen von Firmwareaktualisierungen stehen Ihnen folgende Optionen zur Verfügung:

- **Firmwareaktualisierungs-Repository-Pakete**

  Firmwareaktualisierungs-Repository-Pakete sind Sammlungen der neuesten Firmware, die zur gleichen Zeit wie die XClarity Administrator-Version für die meisten unterstützten Einheiten sowie eine aktualisierte Standard-Firmwarekonformitätsrichtlinie verfügbar ist. Diese Repository-Pakete werden importiert und über die Seite Verwaltungsserver aktualisieren übernommen. Wenn Sie ein Firmwareaktualisierungs-Repository-Paket übernehmen, wird jede im Aktualisierungspaket enthaltene Aktualisierung zum Repository für Firmwareaktualisierungen hinzugefügt und eine Standardfirmwarekonformitätsrichtlinie wird automatisch für alle verwaltenden Einheiten erstellt. Sie können diese vordefinierte Richtlinie kopieren, aber nicht ändern.

  Die folgenden Repositorypakete sind verfügbar.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle CMMs und Flex System-Switches.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle RackSwitch-Switches und Lenovo Storage-Einheiten.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle Convergend HX Series-, Flex System-, NeXtScale- und System x-Server.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle ThinkAgile- und ThinkSystem-Server.

- **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle ThinkAgile und ThinkSystem V2-Server.
- **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle ThinkAgile und ThinkSystem V3 Server.

In der Spalte **Downloadstatus** auf der Seite Verwaltungsserver aktualisieren können Sie ermitteln, ob Firmwareaktualisierungs-Repository-Pakete im Repository gespeichert sind. Die Spalte enthält einen der folgenden Werte:

- **Heruntergeladen**. Das Firmwareaktualisierungs-Repository-Paket ist im Repository gespeichert.
- **Nicht heruntergeladen**. Das Firmwareaktualisierungs-Repository-Paket ist verfügbar, aber nicht im Repository gespeichert.

- **UpdateXpress System Packs (UXSPs)**

  Anmerkung: Bei Servern mit XCC2 werden diese Pakete als Firmwarepakete bezeichnet. *Paket* wird in den Paketnamen und vordefinierten Richtliniennamen verwendet.

  UXSPs enthalten die neuesten Firmware- und Einheitentreiberaktualisierungen, geordnet nach Betriebssystem. Wenn Sie UXSPs herunterladen, lädt XClarity Administrator das UXSP basierend auf der Version im Katalog herunter und speichert die Aktualisierungspakete im Repository für Firmwareaktualisierungen. Wenn Sie ein UXSP herunterladen, wird jede Firmwareaktualisierung im UXSP zum Firmwareupdate-Repository hinzugefügt und auf der Registerkarte **Einzelne Aktualisierungen** aufgeführt. Eine Standard-Firmwarekonformitätsrichtlinie wird automatisch für alle verwaltbaren Einheiten mit den folgenden Namen erstellt. Sie können diese vordefinierte Richtlinie kopieren, aber nicht ändern.
  - *{uxsp-version}-{date}-{server-short-name}***-UXSP** (z. B. `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (z. B. `22a.0-kaj92va-SR650V3-bundle`)

  Anmerkung: Wenn Sie UXSPs über die Seite Firmwareaktualisierungen: Repository herunterladen oder importieren, werden nur Firmwareaktualisierungen heruntergeladen und im Repository gespeichert. Einheitentreiberaktualisierungen werden verworfen. Weitere Informationen zum Herunterladen oder Importieren von Windows-Einheitentreiberaktualisierungen mithilfe von UXSPs finden Sie unter BS-Einheitentreiber-Repository verwalten.

  Anhand der Spalte **Downloadstatus** auf der Registerkarte **Einzelne Aktualisierungen** der Seite Firmwareaktualisierungen: Repository können Sie ermitteln, ob UXSPs im Repository für Firmwareaktualisierungen gespeichert sind. Die Spalte enthält einen der folgenden Werte:

  - **Heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist im Repository gespeichert.
  - *x* **von** *y* **heruntergeladen**. Es sind nur einige Firmwareaktualisierungen des Aktualisierungspakets im Repository gespeichert. Die Zahlen in Klammern geben die Anzahl der verfügbaren Aktualisierungen und die Anzahl gespeicherten Aktualisierungen an oder es liegen keine Aktualisierungen für den speziellen Einheitentyp vor.
  - **Nicht heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist verfügbar, aber nicht im Repository gespeichert.

- **Einzelne Firmwareaktualisierungen**

  Sie können einzelne Firmwareaktualisierungspakete auf einmal herunterladen. Wenn Sie Firmwareaktualisierungspakete herunterladen, lädt XClarity Administrator die Aktualisierung basierend auf der Version im Katalog herunter und speichert das Aktualisierungspaket im

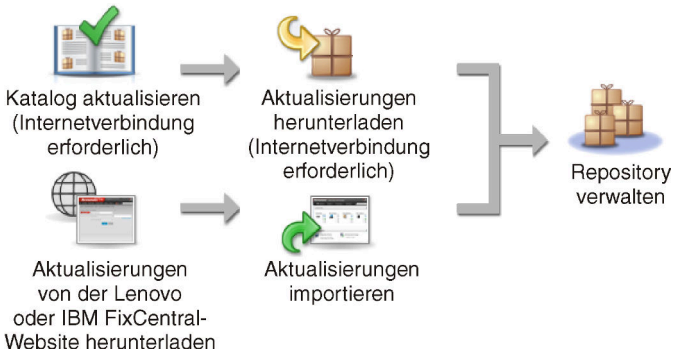
Repository für Firmwareaktualisierungen. Sie können dann mit den Aktualisierungspaketen Firmwarekonformitätsrichtlinien für die verwalteten Einheiten erstellen.

Anmerkung: Die Kernfirmwareaktualisierungen (z. B. für Management-Controller, UEFI und pDSA) sind betriebssystemunabhängig. Firmwareaktualisierungspakete für die Betriebssysteme RHEL 6 und SLES 11 werden zur Aktualisierung von Rechenknoten und Rack-Servern verwendet. Weitere Informationen zu den für die verwalteten Server verwendeten Firmwareaktualisierungspaketen finden Sie unter Firmwareaktualisierungen werden heruntergeladen.

Anhand der Spalte **Downloadstatus** auf der Registerkarte **Einzelne Aktualisierungen** der Seite Firmwareaktualisierungen: Repository können Sie ermitteln, ob bestimmte *Firmwareaktualisierungen* im Repository für Firmwareaktualisierungen gespeichert sind. Die Spalte enthält die folgenden Werte.

- **Heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist im Repository gespeichert.
- *x* **von** *y* **heruntergeladen**. Es sind nur einige Firmwareaktualisierungen des Aktualisierungspakets im Repository gespeichert. Die Zahlen in Klammern geben die Anzahl der verfügbaren Aktualisierungen und die Anzahl gespeicherten Aktualisierungen an oder es liegen keine Aktualisierungen für den speziellen Einheitentyp vor.
- **Nicht heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist verfügbar, aber nicht im Repository gespeichert.

XClarity Administrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und Firmwareaktualisierungen herunterzuladen. Wenn keine Internetverbindung besteht, können Sie die Dateien manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Administrator-Host über einen Webbrowser herunterladen und die Dateien dann in das Firmwareupdate-Repository importieren.



Wenn Sie Firmwareaktualisierungen manuell in XClarity Administrator importieren, müssen diese alle erforderlichen Nutzlast- (Image und MIB), Metadaten-, Änderungsprotokoll- und Readme-Dateien enthalten. Beispiele:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Achtung:

- Importieren Sie nur diese erforderlichen Dateien. Importieren Sie keine anderen Dateien, die sich möglicherweise auf den Websites mit Firmware-Downloads befinden.

- Wenn Sie keine XML-Datei in das Aktualisierungspaket einbeziehen, wird die Aktualisierung nicht importiert.
- Wenn Sie nicht alle zur Aktualisierung erforderlichen Daten einbeziehen, zeigt das Repository die Aktualisierung als nicht heruntergeladen an. Dies bedeutet, dass sie teilweise importiert ist. Sie können dann die fehlenden Dateien importieren, indem Sie sie auswählen und importieren.
- Die Kernfirmwareaktualisierungen (z. B. für Management-Controller, UEFI und pDSA) sind betriebssystemunabhängig. Firmwareaktualisierungspakete für die Betriebssysteme RHEL 6 und SLES 11 werden zur Aktualisierung von Rechenknoten und Rack-Servern verwendet. Weitere Informationen zu den für die verwalteten Server verwendeten Firmwareaktualisierungspaketen finden Sie unter Firmwareaktualisierungen werden heruntergeladen.

Weitere Informationen zu Firmwareaktualisierungen finden Sie unter Repository für Firmwareaktualisierungen verwalten.

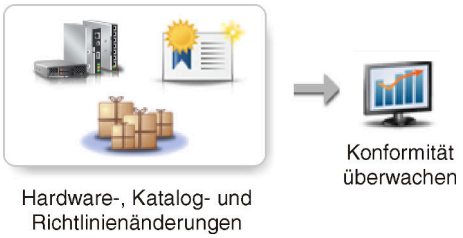
Schritt 2. **(Optional) Firmwarekonformitätsrichtlinien erstellen und zuweisen**

Firmwarekonformitätsrichtlinien stellen sicher, dass die Firmware auf bestimmten verwalteten Einheiten auf dem neuesten Stand ist, indem die Einheiten gekennzeichnet werden, die Ihre Aufmerksamkeit erfordern. Jede Firmwarekonformitätsrichtlinie identifiziert, welche Einheiten überwacht werden und welche Firmwareversion installiert werden muss, damit die Einheiten konform bleiben. Sie können die Konformität auf Einheiten- oder Firmwarekomponentenebene festlegen. XClarity Administrator verwendet die Richtlinien, um den Status von verwalteten Einheiten sicherzustellen und nicht konforme Einheiten zu erkennen.

Wenn Sie eine Firmwarekonformitätsrichtlinie erstellen, können Sie die folgenden Einheiten von XClarity Administrator markieren lassen:
- Die Firmware auf der Einheit ist niedriger
- Die Firmware auf der Einheit stimmt nicht mit der Version aus der Firmwarekonformitätsrichtlinie überein

XClarity Administrator enthält eine vordefinierte Firmwarekonformitätsrichtlinie namens **Neueste Firmware im Repository**. Wenn neue Firmware heruntergeladen oder in das Repository importiert wird, wird diese Richtlinie so aktualisiert, dass die neuesten verfügbaren Versionen der Firmware im Repository enthalten sind.

Nachdem der Einheit eine Firmwarekonformitätsrichtlinien zugewiesen wurde, überprüft XClarity Administrator bei Änderungen des Bestands oder des Repositorys für Firmwareaktualisierungen den Konformitätsstatus jeder Einheit. Wenn die Firmware auf einer Einheit mit der zugewiesenen Richtlinie nicht konform ist, zeigt XClarity Administrator die Einheit auf der Seite Firmwareaktualisierungen: Übernehmen/Aktivieren entsprechend der in der Firmware-Konformitätsrichtlinie angegebenen Regel, als nicht konform an.



Sie können beispielsweise eine Firmwarekonformitätsrichtlinie erstellen, die die Basisversion für die auf den ThinkSystem SR850 Einheiten installierte Firmware definiert, und diese Firmwarekonformitätsrichtlinie dann allen verwalteten ThinkSystem SR850 Einheiten zuordnen.

Wenn das Repository für Firmwareaktualisierungen aktualisiert und eine neue Firmwareaktualisierung hinzugefügt wird, sind die Rechenknoten möglicherweise nicht mehr konform. Wenn dies der Fall ist, aktualisiert XClarity Administrator die Seite Firmwareaktualisierungen: Übernehmen/Aktivieren, um zu zeigen, dass die Einheiten nicht konform sind, und generiert einen Alert.

Anmerkung: Sie können festlegen, dass Alerts für Einheiten angezeigt oder ausgeblendet werden, die die Anforderungen der ihnen zugewiesenen Firmwarekonformitätsrichtlinien nicht erfüllen (siehe Globale Einstellungen der Firmwareaktualisierungen konfigurieren). Alerts sind standardmäßig ausgeblendet.

Weitere Informationen zu Firmwarekonformitätsrichtlinien finden Sie unter Firmwarekonformitätsrichtlinien erstellen und zuordnen.

Schritt 3. **Übernehmen und Aktivieren von Aktualisierungen**

XClarity Administrator wendet Firmwareaktualisierungen nicht automatisch auf verwalteten Einheiten an. Zum Aktualisieren von Firmware müssen Sie die Aktualisierung auf ausgewählten Einheiten manuell übernehmen und aktivieren. Folgende Möglichkeiten stehen zur Übernahme der Firmware zur Verfügung.

- **Paket-Firmwareaktualisierungen unter Verwendung von Konformitätsrichtlinien übernehmen**

  Sie können Firmwareaktualisierungen für *alle* Komponenten in den ausgewählten Einheiten gemäß der zugeordneten Firmwarekonformitätsrichtlinie mithilfe eines Paket-Images übernehmen, das die entsprechenden Firmwareaktualisierungspakete enthält.

  Der Paket-Aktualisierungsprozess aktualisiert zuerst den Baseboard Management Controller und UEFI Außerband. Wenn diese Aktualisierungen abgeschlossen sind, erstellt der Prozess basierend auf dem Maschinentyp ein Paketimage der verbleibenden Firmware in der Konformitätsrichtlinie. Anschließend wird das Image vom Prozess an die ausgewählte Einheit angehängt und die Einheit wird zum Booten des Images neu gestartet. Das Image wird automatisch ausgeführt, um die verbleibenden Aktualisierungen durchzuführen.

  Achtung: Ausgewählte Einheiten werden vor dem Start des Aktualisierungsprozesses ausgeschaltet. Vergewissern Sie sich, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf einen anderen Server verschoben wurden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.

  Anmerkungen:

  – Das Übernehmen von Paket-Firmwareaktualisierungen wird nur für ThinkSystem SR635 und SR655 Server unterstützt.
  – Das Anwenden von Paket-Firmwareaktualisierungen wird nur für IPv4-Adressen unterstützt. IPv6-Adressen werden nicht unterstützt.
  – Stellen Sie sicher, dass jede Zieleinheit mindestens einmal auf das BS gebootet wurde, um die vollständigen Bestandsinformationen abzurufen.
  – Zur Verwendung der Funktion für Paket-Aktualisierungen ist die Baseboard Management Controller-Firmware v2.94 oder höher erforderlich.
  – Es werden nur Firmwareaktualisierungen aus Repository-Paketen oder einzelne Firmwareaktualisierungen verwendet. UpdateXpress System Packs (UXSPs) werden nicht unterstützt.

- Es werden nur heruntergeladene Firmwareaktualisierungen angewendet. Aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Firmwareaktualisierungen herunter (siehe Produktkatalog aktualisieren und Firmwareaktualisierungen werden heruntergeladen).

  Anmerkung: Bei der Erstinstallation von XClarity Administrator sind der Produktkatalog und das Repository leer.
- Die Konformitätsprüfung wird nur für Baseboard Management Controller und UEFI in ThinkSystem SR635 und SR655 Servern unterstützt. XClarity Administrator versucht jedoch, Firmwareaktualisierungen auf allen verfügbaren Hardwarekomponenten zu übernehmen.
- Aktualisierungen werden gemäß der zugeordneten Firmwarekonformitätsrichtlinie übernommen. Sie können nicht nur einen Teil der Komponenten aktualisieren.
- XClarity Administrator v3.2 oder höher ist erforderlich, um Firmwareaktualisierungen für Lenovo XClarity Provisioning Manager (LXPM), LXPM Windows-Treiber oder LXPM Linux-Treiber auf ThinkSystem SR635 und SR655 Servern zu übernehmen.
- Baseboard Management Controller- und UEFI-Aktualisierungen werden übersprungen, wenn die aktuell installierte Version höher als die zugeordnete Konformitätsrichtlinie ist.
- Firmwarekonformitätsrichtlinien müssen erstellt und den Einheiten zugeordnet werden, auf denen Sie die Firmwareaktualisierungen übernehmen möchten. Siehe Firmwarekonformitätsrichtlinien erstellen und zuordnen für weitere Informationen.
- Die ausgewählten Einheiten werden vor dem Start des Aktualisierungsprozesses ausgeschaltet. Vergewissern Sie sich, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf einen anderen Server verschoben wurden.

- **Ausgewählte Firmwareaktualisierungen mit oder ohne Konformitätsrichtlinien übernehmen**

  Sie können Firmwareaktualisierungen für ausgewählte Komponenten und Einheiten gemäß der zugeordneten Firmwarekonformitätsrichtlinie mithilfe der entsprechenden Firmwareaktualisierungspakete übernehmen. Darüber hinaus können Sie auch Firmwareaktualisierungen, bei denen es sich um eine spätere Version als die aktuell installierte handelt, auf ausgewählten Komponenten und Einheiten übernehmen, ohne die Konformitätsrichtlinien zu verwenden.

  Sie können außerdem Aktualisierungen für alle Komponenten in einer bestimmten Einheit übernehmen. Sie können auch nur einen Teil der Komponenten in den ausgewählten Einheiten aktualisieren, beispielsweise Baseboard Management Controller oder UEFI.

  Um die Firmwareaktualisierungen zu aktivieren, müssen die Einheiten neu gestartet werden. (Beachten Sie, dass der Neustart einer Einheit zu einer Unterbrechung führt.) Sie können die Einheiten im Rahmen des Aktualisierungsprozesses neu starten (*sofortige Aktivierung*) oder Sie warten, bis ein Wartungsfenster für den Neustart verfügbar ist (*verzögerte Aktivierung*). In diesem Fall müssen Sie die Einheit manuell neu starten, damit die Aktualisierung in Kraft tritt.

  Wenn Sie die Aktualisierung der Firmware auf einer verwalteten Einheit auswählen, treten die folgenden Schritte auf.

  1. XClarity Administrator sendet die Firmwareaktualisierungen (z. B. für Management-Controller, UEFI und DSA) zur Einheit.
  2. Wenn die Einheit neu gestartet wird, sind die Firmwareaktualisierungen auf der Einheit aktiviert.
  3. Für Server sendet XClarity Administrator Aktualisierungen für optionale Komponenten (z. B. Netzwerkadapter und Festplattenlaufwerke). XClarity Administrator übernimmt diese Aktualisierungen und der Server wird neu gestartet.

4. Wenn Sie die Einheit neu starten oder die sofortige Aktivierung auswählen, werden die Aktualisierungen für die optionalen Komponenten aktiviert.

Anmerkungen:

- Wenn Sie Aktualisierungen mithilfe von Konformitätsrichtlinien übernehmen, muss eine Firmwarekonformitätsrichtlinie erstellt und jeder Zieleinheit zugeordnet werden. Siehe Firmwarekonformitätsrichtlinien erstellen und zuordnen für weitere Informationen.
- Wenn Sie ein Firmwareaktualisierungspaket mit Aktualisierungen für verschiedene Komponenten installieren, werden alle Komponenten, für die das Aktualisierungspaket übernommen wird, aktualisiert.
- Aktualisierungen für CMM und Flex-Switches werden immer sofort aktiviert. Dies gilt auch dann, wenn Sie die verzögerte Aktivierung auswählen.

Wenn Sie Aktualisierungen für eine Gruppe von Einheiten ausführen, führt XClarity Administrator die Aktualisierungen in der folgenden Reihenfolge aus.

- Gehäuse-CMM
- RackSwitch- und Flex System-Switches
- Flex-Rechenknoten, Rack- und Tower-Server
- Lenovo Storage-Einheit

Achtung: Bevor Sie versuchen, Firmwareaktualisierungen auf verwalteten Einheiten zu übernehmen, müssen Sie sicherstellen, dass Sie die folgenden Aktionen ausgeführt haben.

- Lesen Sie die Hinweise zur Firmwareaktualisierung, bevor Sie versuchen, die Firmware auf verwalteten Einheiten zu aktualisieren (siehe Hinweise zur Firmwareaktualisierung).
- Einheiten, bei denen keine Aktualisierungen unterstützt werden, sind in der Ansicht zunächst ausgeblendet. Nicht unterstützte Einheiten können nicht für Aktualisierungen ausgewählt werden.
- Standardmäßig werden alle erkannten Komponenten als verfügbar für die Übernahme von Aktualisierungen aufgelistet. Möglicherweise verhindert jedoch eine ältere Firmwareversion, dass eine Komponente im Bestand aufgeführt wird bzw. dass vollständige Versionsinformationen angezeigt werden. Um alle zur Übernahme verfügbaren richtlinienbasierten Pakete aufzulisten, klicken Sie auf **Alle Aktionen → Globale Einstellungen** und wählen **Erweiterter Support für Einheiten mit einer älteren Version** aus. Mit dieser Option wird für die nicht erkannten Einheiten in der Spalte „Installierte Version“ „Weitere verfügbare Software“ aufgeführt. Siehe Globale Einstellungen der Firmwareaktualisierungen konfigurieren für weitere Informationen.

  Anmerkungen:

  - Die globalen Einstellungen können bei laufenden Aktualisierungen für verwaltete Einheiten nicht geändert werden.
  - Das Generieren der zusätzlichen Optionen dauert einige Minuten. Nach kurzer Zeit müssen Sie möglicherweise auf das Symbol **Aktualisieren** () klicken, um die Tabelle zu aktualisieren.
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.
- Stellen Sie sicher, dass das Repository für Firmwareaktualisierungen die Firmwarepakete enthält, die Sie implementieren möchten. Ist dies nicht der Fall, so aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Firmwareaktualisierungen herunter (siehe Produktkatalog aktualisieren und Firmwareaktualisierungen werden heruntergeladen).

Anmerkung: Bei der Erstinstallation von XClarity Administrator sind der Produktkatalog und das Repository leer.

Wenn Sie erforderliche Firmware installieren möchten, stellen Sie sicher, dass die erforderliche Firmware ebenfalls in das Repository heruntergeladen wird.

In einigen Fällen können mehrere Versionen für die Aktualisierung der Firmware erforderlich sein, dann müssen alle Versionen in das Repository heruntergeladen werden. Beispielsweise müssen Sie für eine Aktualisierung des skalierbaren IBM FC5022 SAN-Switches von v7.4.0a auf v8.2.0a zuerst v8.0.1-pha, dann v8.1.1 und abschließend v8.2.0a installieren. Alle drei Versionen müssen im Repository sein, um den Switch auf v8.2.0a zu aktualisieren.

- Um die Firmwareaktualisierungen zu aktivieren, müssen die Einheiten normalerweise neu gestartet werden. Wenn Sie die Einheit 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 einen anderen Server verschoben wurden.

Weitere Informationen zum Installieren von Aktualisierungen finden Sie unter Firmwareaktualisierungen anwenden und aktivieren.

Hinweise zur Firmwareaktualisierung

Bevor Sie mit der Aktualisierung von Firmware für verwaltete Einheiten mit Lenovo XClarity Administrator beginnen, lesen Sie die folgenden wichtigen Hinweise.

- Allgemeine Hinweise
- CMM-Hinweise
- Hinweise zum Baseboard Management Controller
- Hinweise zur ThinkSystem Einheit
- Hinweise zur Flex System Einheit
- Hinweise zum Speicher

Allgemeine Hinweise

- **Mindestens erforderliche Firmwareversion.**

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

  Anmerkung: Weitere Informationen über die Unterstützung von E/A-Einheiten und bekannte Einschränkungen finden Sie in der Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator.

- **Aktualisieren Sie alle Komponenten auf die Version, die im Repository für Firmwareaktualisierungen enthalten ist.**

  Da Firmwareaktualisierungen für Flex System-Komponenten gemeinsam getestet und freigegeben werden, sollten Sie für alle Komponenten in einem Flex System-Gehäuse dieselbe Firmwareversion beibehalten. Aus diesem Grund ist es wichtig, die Firmware auf allen Komponenten im Gehäuse im selben Wartungsfenster zu aktualisieren. XClarity Administrator übernimmt die ausgewählten Aktualisierungen automatisch in der richtigen Reihenfolge.

- **LXPM Linux-Treiber und LXPM Windows-Treiber sind beim Herunterladen von UXSPs nicht enthalten.**

Lenovo XClarity Provisioning Manager (LXPM) Linux- und Windows-Treiber sind nicht in UpdateXpress System Packs (UXSPs) enthalten. Zum Übernehmen dieser Aktualisierungspakete auf Ihren Einheiten müssen Sie entweder die aktuellen Firmwareupdate-Repository-Pakete oder die einzelnen Pakete manuell herunterladen und eine Firmwarekonformitätsrichtlinie erstellen, um diese Pakete einzubeziehen.

- **Einige Firmwareaktualisierungen setzen außerdem eine Mindestversion des Einheitentreibers voraus**

  Bevor Sie Adapter- und E/A-Firmwareaktualisierungen auf einem Server übernehmen, müssen Sie möglicherweise den Einheitentreiber auf eine Firmware-Mindestversion aktualisieren. Im Allgemeinen sind Firmwareaktualisierungen nicht auf bestimmte Einheitentreiberversionen angewiesen. Lesen Sie die Readme-Datei der Firmwareaktualisierung, um sich über entsprechende Abhängigkeiten zu informieren. Aktualisieren Sie die Einheitentreiber in Ihrem Betriebssystem, bevor Sie die Firmware aktualisieren. XClarity Administrator aktualisiert die Einheitentreiber in Ihrem Betriebssystem nicht.

- **XClarity Administrator vor der Firmwareaktualisierung neu starten**

  Wenn vorherige Versuche der Firmwareaktualisierung fehlgeschlagen sind, starten Sie XClarity Administrator vor der Aktualisierung der Firmware neu. Durch einen Warmstart des Verwaltungsservers wird sichergestellt, dass der für die Firmwareaktualisierung verwendete Systemaccount auf den verwalteten Einheiten synchronisiert ist.

- **Firmwareaktualisierungen sorgen für Unterbrechungen und erfordern, dass Workloads auf Einheiten ausgesetzt werden müssen.**

  Die Durchführung von Firmwareaktualisierungen auf verwalteten Einheiten sorgt dann für Unterbrechungen, wenn Sie sich für die direkte Aktivierung und Aktualisierung entscheiden. Sie müssen die Einheiten vor der Aktualisierung der Firmware mit sofortiger Aktivierung stilllegen.

  Wenn Sie Firmware auf Servern aktualisieren, werden die Server heruntergefahren und zur Aktualisierung von Einheitentreibern für Adapter, Plattenlaufwerke und Solid-State-Laufwerke mit einem Wartungsbetriebssystem gestartet.

  Die Flex-Switches in einem Gehäuse werden nacheinander aktualisiert und werden während des Firmwareaktualisierungsprozesses neu gestartet. Das Implementieren von redundanten Datenwegen reduziert die Unterbrechungen. Es kann jedoch trotzdem während der Firmwareaktualisierung zu einer kurzen Unterbrechung der Netzwerkverbindungen kommen.

- **Verwenden Sie XClarity Administrator nicht, um die Firmware auf dem Server zu aktualisieren, auf denen XClarity Administrator ausgeführt wird.**

  Wenn XClarity Administrator auf einem Hypervisor-Host ausgeführt wird, der auf einem verwaltenden Server ausgeführt wird, verwenden Sie nicht XClarity Administrator, um Firmware auf diesem Server zu aktualisieren. Wenn Firmwareaktualisierungen mit sofortiger Aktivierung übernommen werden, zwingt XClarity Administrator den Zielserver zu einem Neustart. Dabei werden auch der Hypervisor-Host und XClarity Administrator neu gestartet. Bei einer verzögerten Aktivierung wird bei einem Neustart des Zielsystems nur ein Teil der Firmware übernommen.

CMM-Hinweise

- **Setzen Sie die CMMs virtuell wieder ein, bevor Sie Firmware aktualisieren.**

  Wenn Sie CMMs mit der Firmwareversion-Stackversion 1.3.2.1 2PET12K bis 2PET12Q aktualisieren, die seit mehr als drei Wochen ausgeführt werden und die sich in einer Konfiguration mit zwei CMMs befinden, müssen Sie die primären und Standby-CMMs vor einer Firmwareaktualisierung virtuell erneut einsetzen (siehe Ein CMM virtuell neu einsetzen).

Hinweise zum Baseboard Management Controller

- **Mindestens erforderliche BMC-Version für den Status „Ausstehende Aktivierung“**

Um den Status „Ausstehende Aktivierung“ anzeigen zu können, muss die folgende Firmwareversion auf dem primären BMC (Baseboard Management Controller) des Servers installiert sein.
  - **IMM2**: TCOO46F, TCOO46E oder höher (abhängig von der Plattform)
  - **XCC**: CDI328M, PSI316N, TEI334I oder höher (abhängig von der Plattform)

- **Für den primären Management-Controller und UEFI-Firmwarepartitionen übernommene Aktualisierungen.**

  Baseboard Management-Controller- (BMC) und UEFI-Aktualisierungen können unabhängig für die primären Firmwarepartitionen und Firmwaresicherungspartitionen des Management-Controllers und für UEFI angewendet werden.

  Sie können Management-Controller- und UEFI-Aktualisierungen auch nur für die primären Firmwarepartitionen auf dem Server übernehmen. Standardmäßig ist der Controller so konfiguriert, dass die Management-Controller-Sicherungspartition mit der primären Management-Controller-Partition synchronisiert wird, nachdem der primäre Management-Controller zufriedenstellend ausgeführt wurde und die neue Version zur Hochstufung der Sicherung bereit ist. Allerdings ist Management-Controller standardmäßig nicht zur Synchronisierung der UEFI-Sicherungspartition konfiguriert. Daher sollten Sie auf dem Management-Controller eine der folgenden Möglichkeiten nutzen:

  - Aktivieren Sie die automatische Synchronisation der UEFI-Sicherungspartition.

    Dadurch wird sichergestellt, dass die primäre Partition und die Sicherungspartitionen dieselbe Firmwareversion ausführen (und das die UEFI-Firmware-Sicherungskopie mit der Management-Controller-Firmware konform ist).
  - Deaktivieren Sie die automatische Synchronisation der Management-Controller-Sicherungspartition.

    Diese Vorgehensweise wird nicht empfohlen. Sie gibt Ihnen jedoch die vollständige Kontrolle über die Firmwareversionen der Management-Controller und von UEFI. Sie müssen die Management-Controller- und UEFI-Firmware jedoch für beide Partitionen manuell aktualisieren.

  Sie verwenden Firmwarekonformitätsrichtlinien, um die auf den einzelnen Einheiten zu übernehmenden Aktualisierungen zu ermitteln. Weitere Informationen zu den Firmwarekonformitätsrichtlinien finden Sie unter Firmwarekonformitätsrichtlinien erstellen und zuordnen.

  Anmerkung: Wenn der Management-Controller und die UEFI für die automatische Synchronisierung der Sicherungsfirmware mit der primären Firmware konfiguriert sind, muss XClarity Administrator die Sicherungsgruppe nicht mehr aktualisieren. In diesem Fall können Sie die Aktualisierungen für die Sicherungsgruppe beim Übernehmen von Aktualisierungen für einen Server löschen oder diese aus der Firmwarekonformitätsrichtlinie entfernen.

- **Es besteht die Möglichkeit, dass es nach dem Zurücksetzen von Management-Controllern zu VMware vSphere ESXi-Systemausfällen kommt (violette Diagnoseanzeige).**

  Wenn Sie VMware vSphere ESXi auf einem Server ausführen, stellen Sie sicher, dass die folgenden VMware ESXi-Mindestversionen vor der Aktualisierung von Firmware auf dem Server installiert sind:

  - Wenn Sie VMware vSphere ESXi 5.0 ausführen, installieren Sie mindestens Version 5.0u2 (Update 2)
  - Wenn Sie VMware vSphere ESXi 5.1 ausführen, installieren Sie mindestens Version 5.1u1 (Update 1)

  Wenn Sie die Mindestversionen nicht installieren, kann es beim Zurücksetzen des Management-Controllers zu einem VMware vSphere ESXi-Systemausfall kommen (violette Diagnoseanzeige). Dies gilt auch dann, wenn die Management-Controller-Firmware übernommen und aktiviert ist.

  Anmerkung: Dieses Problem betrifft nicht ESXi v5.5.

Hinweise zur ThinkSystem Einheit

- **Für ThinkSystem SE350 Server, auf denen eine ältere XCC-Firmwareversion als 20A ausgeführt wird, muss der IPMI-over-KCS-Zugriff manuell im Baseboard Management Controller aktiviert werden, damit der BMC sicher mit XClarity Administrator kommunizieren kann.**

  Auf ThinkSystem SE350 Servern ist IPMI-over-KCS standardmäßig deaktiviert. Für ThinkSystem SE350 Server mit XCC-Firmwareversion 20A oder höher aktiviert XClarity Administrator IPMI-over-KCS automatisch während einer Firmwareaktualisierung und deaktiviert es, nachdem die Firmwareaktualisierung abgeschlossen ist. Für ThinkSystem SE350 Server, auf denen eine ältere XCC-Firmwareversion als 20A ausgeführt wird, müssen Sie diese Option allerdings manuell über die Lenovo XClarity Controller-Benutzerschnittstelle aktivieren. Navigieren Sie dafür zu **BMC-Konfiguration → Sicherheit → IPMI-over-KCS-Zugriff**.

- Für ThinkSystem SR635 und SR655 Server gelten die folgenden Einschränkungen.
  - Es wird nur die sofortige Aktivierung unterstützt. Verzögerte Aktivierung und priorisierte Aktivierung werden nicht unterstützt.
  - Für XClarity Administrator v3.1.1 und höher können Sie die Funktion für Paket-Aktualisierungen verwenden, um alle Komponenten auf ThinkSystem SR635 und SR655 Servern zu aktualisieren, einschließlich Baseboard Management Controller, UEFI, Plattenlaufwerken und E/A-Zusatzeinrichtungen.

    Achtung: Ausgewählte Einheiten werden vor dem Start des Aktualisierungsprozesses ausgeschaltet. Vergewissern Sie sich, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf einen anderen Server verschoben wurden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.

    Anmerkungen:

    - Das Übernehmen von Paket-Firmwareaktualisierungen wird nur für ThinkSystem SR635 und SR655 Server unterstützt.
    - Das Anwenden von Paket-Firmwareaktualisierungen wird nur für IPv4-Adressen unterstützt. IPv6-Adressen werden nicht unterstützt.
    - Stellen Sie sicher, dass jede Zieleinheit mindestens einmal auf das BS gebootet wurde, um die vollständigen Bestandsinformationen abzurufen.
    - Zur Verwendung der Funktion für Paket-Aktualisierungen ist die Baseboard Management Controller-Firmware v2.94 oder höher erforderlich.
    - Es werden nur Firmwareaktualisierungen aus Repository-Paketen oder einzelne Firmwareaktualisierungen verwendet. UpdateXpress System Packs (UXSPs) werden nicht unterstützt.
    - Es werden nur heruntergeladene Firmwareaktualisierungen angewendet. Aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Firmwareaktualisierungen herunter (siehe Produktkatalog aktualisieren und Firmwareaktualisierungen werden heruntergeladen).

      Anmerkung: Bei der Erstinstallation von XClarity Administrator sind der Produktkatalog und das Repository leer.
    - Die Konformitätsprüfung wird nur für Baseboard Management Controller und UEFI in ThinkSystem SR635 und SR655 Servern unterstützt. XClarity Administrator versucht jedoch, Firmwareaktualisierungen auf allen verfügbaren Hardwarekomponenten zu übernehmen.
    - Aktualisierungen werden gemäß der zugeordneten Firmwarekonformitätsrichtlinie übernommen. Sie können nicht nur einen Teil der Komponenten aktualisieren.

  - XClarity Administrator v3.2 oder höher ist erforderlich, um Firmwareaktualisierungen für Lenovo XClarity Provisioning Manager (LXPM), LXPM Windows-Treiber oder LXPM Linux-Treiber auf ThinkSystem SR635 und SR655 Servern zu übernehmen.
  - Baseboard Management Controller- und UEFI-Aktualisierungen werden übersprungen, wenn die aktuell installierte Version höher als die zugeordnete Konformitätsrichtlinie ist.
  - Firmwarekonformitätsrichtlinien müssen erstellt und den Einheiten zugeordnet werden, auf denen Sie die Firmwareaktualisierungen übernehmen möchten. Siehe Firmwarekonformitätsrichtlinien erstellen und zuordnen für weitere Informationen.
  - Die ausgewählten Einheiten werden vor dem Start des Aktualisierungsprozesses ausgeschaltet. Vergewissern Sie sich, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf einen anderen Server verschoben wurden.

  Sie können auch die herkömmliche Aktualisierungsfunktion verwenden, um Firmwareaktualisierungen nur auf dem Baseboard Management Controller und UEFI zu übernehmen.
- Für XClarity Administrator v3.0:
  - Verwaltungsdaten werden nicht ordnungsgemäß aktualisiert, wenn die Firmware von 20A auf 20B oder 20C aktualisiert wird. Um dieses Problem zu umgehen, müssen Sie entweder die Verwaltung der Einheiten aufheben und sie dann wieder erneut verwalten oder XClarity Administrator neu starten.
  - Ein Downgrade von Firmwareaktualisierungen wird nicht unterstützt.

- **Firmwareaktualisierungen werden auf ThinkSystemserver-Servern mit DHCPv6 oder statisch zugewiesenen IPv6-Adressen nicht unterstützt.**

  Wenn Sie IPv6-Adressierung auf ThinkSystem Servern verwenden, werden Firmwareaktualisierungen nur für die IPv6-Link-Local-Adresse (LLA) und die statuslosen Adressen unterstützt.
- **Wenn Sie die Firmware auf Version 20D aktualisieren, müssen Sie UEFI und XCC zusammen aktualisieren.**

  UEFI und Lenovo XClarity Controller (XCC) müssen für Version 20D zusammen aktualisiert werden. Wenn XCC aktualisiert wird, und UEFI nicht, oder umgekehrt, führt dies zu Problemen.

Hinweise zur Flex System Einheit

- **Stellen Sie sicher, dass die zu aktualisierenden Flex-Switches eingeschaltet sind,**
- **Wählen Sie die sofortige Aktivierung beim Aktualisieren von Rechenknoten mit Management-Controller-Firmwareversionen von Flex System 1.3.2 oder niedriger aus.**

  Wenn Sie die Flex System 1.3.2, 2nd Quarter-Version für einen Rechenknoten übernehmen, müssen Sie die *sofortige Aktivierung* auswählen, um den Rechenknoten zu aktualisieren. Die sofortige Aktivierung zwingt den Rechenknoten während des Aktualisierungsprozesses zum Neustart.
- **Flex-Switches müssen mit einer IP-Adresse konfiguriert werden, die für XClarity Administrator erreichbar ist.**

  Dem Ziel-Flex-Switch muss eine IP-Adresse zugeordnet werden, mit der XClarity Administrator kommunizieren kann. Nur so kann XClarity Administrator die Firmwareaktualisierung herunterladen und anwenden.
- **Unterstützung von Aktualisierungen auf skalierbaren Komplexen, beispielsweise x480 X6- und x880 X6-Knoten.**

  Aktualisierungsunterstützung auf skalierbaren Knoten wie den Flex System x480 X6 und x880 X6 Rechenknoten ist auf Konfigurationen begrenzt, bei denen der Komplex als *einzelne Partition* konfiguriert ist, die alle Rechenknoten enthält, die Teil des Komplexes mit mehreren Knoten sind. Sie können nicht XClarity Administrator verwenden, um einen Komplex mit mehreren Partitionen zu aktualisieren.

Wenn Sie eine Firmwarekonformitätsrichtlinie zu einer Partition zuweisen, die mehrere Server in einem skalierbaren Komplex (z. B. Flex System x480 X6 und x880 X6 Rechenknoten) umfasst, aktualisiert XClarity Administrator standardmäßig die Firmware auf allen Management-Controllern und UEFIs jedes Servers in der Partition. Wenn Sie jedoch nur eine Teilmenge der Komponenten innerhalb der Partition auswählen, aktualisiert XClarity Administrator die Firmware nur für die ausgewählten Komponenten der Partition.

- **Bevor Sie den CMM2 auf v1.30 (1AON06C) oder höher aktualisieren, müssen Flex-Switches die Level 3-Version von Enhanced Configuration and Management (EHCM L3) ausführen**

  CMM2 und die Flex-Switches kommunizieren über das EHCM-Protokoll. XClarity Administrator benötigt dieses Protokoll zur Aktualisierung der Flex-Switches. Wenn Sie einen CMM2 auf v1.30 (1AON06C) oder höher aktualisieren, prüft XClarity Administrator, ob die Flex-Switches die EHCM L3 ausführen. Wenn dies nicht der Fall ist, wird die CMM-Aktualisierung mit einer Warnung beenden. Die Warnung informiert darüber, dass die Flex-Switches zuerst auf eine Version aktualisiert werden müssen, die EHCM-L3 unterstützt. Sie können diese Überprüfung bei der Aktualisierung der CMM-Firmware über die Auswahl von **Aktualisierung bereits konformer Komponenten versuchen** außer Kraft setzen.

  Achtung: Im Moment ist für Flex System EN6131-Ethernet-Switches und IB6131 InfiniBand Switches keine Firmwareversion mit Unterstützung von EHCM L3 verfügbar. Nach der Aktualisierung des CMM2 auf Firmware v1.30 (1AON06C) oder höher können Sie daher XClarity Administrator nicht mehr zur Aktualisierung dieser Switches verwenden. Nutzen Sie stattdessen die Management-Controller-Webschnittstelle oder die Befehlszeilenschnittstelle für das Gehäuse, um den Switch zu aktualisieren.

Flex System-Switch	Version	Releasedatum
CN4093	7.8.4.0	Juni 2014
EN4023	6.0.0	April 2015
EN4093	7.8.4.0	Juni 2014
EN4093R	7.8.4.0	Juni 2014
EN6132	Nicht verfügbar	Nicht verfügbar
FC3171	9.1.3.02.00	Juni 2014
FC5022	7.4.0b1	März 2016
IB6132	Nicht verfügbar	Nicht verfügbar
SI4091	7.8.4.0	Juni 2014
SI4093	7.8.4.0	Juni 2014

  Anmerkung: Der Skalierbarer EN2092 1 Gb Ethernet-Switch erfordert kein EHCM L3 und unterliegt daher nicht dieser Einschränkung.

Hinweise zum Speicher

- **Hinweise zu ThinkSystem DM Speichereinheiten**

  Um die Firmware auf ThinkSystem DM Speichereinheiten zu aktualisieren, muss auf den Einheiten v9.7 oder höher ausgeführt werden.

  Ein Downgrade wird nur für Nebenversionen unterstützt. Sie können z. B. ein Downgrade von Version 9.7P11 auf 9.7P9 durchführen, aber nicht von Version 9.8 auf 9.7.

  So laden Sie Firmware für Speichereinheiten der ThinkSystem DM-Serie herunter:

  – Eine oder mehrere Speichereinheiten der ThinkSystem DM-Serie müssen von XClarity Administrator verwaltet werden.

- Jede Speichereinheit der ThinkSystem DM-Serie muss eine Berechtigung für Hardwareservice und -unterstützung haben.
- Sie müssen auf der Seite „Firmwareaktualisierungen: Repository“ das Land angeben, in dem sich die Speichereinheiten der ThinkSystem DM-Serie befinden. Für Einheiten in den folgenden Ländern kann nur verschlüsselte Firmware heruntergeladen werden: Armenien, Weißrussland, China, Kuba, Iran, Kasachstan, Kirgisistan, Nordkorea, Russland, Sudan, Syrien.

- **Plattenlaufwerke müssen den Status „JBOD“, „Online“, „Bereit“ oder „Nicht konfiguriert (gut)“ aufweisen.**

  Um die Firmware auf Plattenlaufwerken zu aktualisieren, muss der RAID-Status „JBOD“, „Online“, „Bereit“ oder „Nicht konfiguriert (gut)“ lauten. Andere Status werden nicht unterstützt. Um den RAID-Status für ein Plattenlaufwerk zu bestimmen, rufen Sie die Seite „Inventar“ für die Einheit auf, erweitern Sie den Abschnitt **Einheiten** und überprüfen Sie die Spalte **RAID-Status** für dieses Plattenlaufwerk (siehe Die Details eines verwalteten Servers anzeigen).

- **Die Firmwareversion erkennt keine Plattenlaufwerke und Solid-State-Laufwerke.**

  XClarity Administrator erkennt nur die installierte Firmwareversion und führt eine Konformitätsprüfung für Plattenlaufwerke und Solid-State-Laufwerke (SSDs) durch, die an einen MegaRAID- oder NVMe-Adapter angeschlossen sind. Andere angehängte Laufwerke arbeiten möglicherweise mit einer Firmwareversion, die nicht unterstützt wird oder keine Meldungen der Firmwareversion unterstützt. Wenn ausgewählt, werden jedoch Firmwareaktualisierungen für diese Plattenlaufwerke übernommen.

- **NVMe-Firmware wird auch dann angewendet, wenn sie nicht mit einer Zielkomponente erkannt wird**

  Auf der Seite „Übernehmen/Aktivieren“ wird die NVMe-Firmwareversion für Solid-State-Laufwerke (SSDs) aufgelistet. Da für erkannte NVMe-Einheiten keine Zielfirmwareaktualisierung ermittelt wird, wird beim Versuch der Aktualisierung des Zielsystems eine Warnung angezeigt. Allerdings wird die HDD-/SSD-Aktualisierung auch dann übernommen, wenn es nicht mit einer Zielkomponente erkannt wird. Die NVMe-Firmware wird also trotzdem aktualisiert.

- **Zum Übernehmen des Aktualisierungspakets ServeRAID-M5115-Controller PSoC3 von XClarity Administrator muss mindestens die Version 68 installiert sein.**

  Die Aktualisierung ServeRAID M5115 PSoC3 (Programmable System-on-Chip) von einer niedrigeren Version als 68 aus muss kontrolliert erfolgen.

  Tipp: Sie können die Codeversion für ServeRAID M5115 PSoC3 anzeigen, indem Sie sich an der CMM-Webschnittstelle anmelden und die **Firmware**-Registerkarte für den Zielrechenknoten auswählen. Wählen Sie dann die Erweiterungskarte für den ServeRAID M5115-Adapter aus. Die PSoc3-Codeversion ist der GENERISCHE Firmwaretyp.

  Für installierte Versionen, die niedriger als 68 sind, können Sie XClarity Administrator nicht zur Aktualisierung nutzen. Stattdessen müssen Sie die folgenden Schritte über die Chassis Management Module (CMM)- Webschnittstelle oder über die Befehlszeilenschnittstelle (CLI) ausführen:

  - **Über die CMM-Webschnittstelle:**
    1. Melden Sie sich an der Webschnittstelle für das Chassis Management Module (CMM) an.
    2. Klicken Sie im Hauptmenü auf **Service und Support → Erweitert**.
    3. Klicken Sie auf die Registerkarte **Servicerücksetzung**.
    4. Wählen Sie einen entsprechenden Rechenknoten aus, indem Sie auf das Optionsfeld klicken.
    5. Wählen Sie über die Auswahlschaltfläche **Zurücksetzen** die Option **Virtuell erneut einsetzen** aus.
    6. Klicken Sie zur Bestätigung auf **OK**.
  - **Über die CMM-CLI**:
    - Melden Sie sich per SSH-Schnittstelle (Secure Shell) am CMM an.

– Geben Sie den folgenden Befehl ein, um ein virtuelles Neueinsetzen auszuführen:
  `'service -vr -T blade[x]`

  (*x* ist die Positionsnummer des Rechenknotens, der neu eingesetzt werden soll).

Sobald das System wieder eingeschaltet ist, starten Sie das Betriebssystem und aktualisieren Sie das ServeRAID M5115 PSoC3 mithilfe des extrahierten eingebetteten Aktualisierungspakets. Gehen Sie wie folgt vor, um das eingebettete Paket zu extrahieren.

– **Mit Microsoft Windows:**

  Öffnen Sie das Aktualisierungspaket (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe) und wählen Sie Auf Festplatte extrahieren aus. Wählen Sie anschließend den Pfad aus, in den das eingebettete Paket extrahiert werden soll.

– **Mit Linux:**

  Führen Sie den folgenden Befehl aus:

  `lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x`

  (*x* ist der Pfad, in den das eingebettete Paket extrahiert werden soll).

Repository für Firmwareaktualisierungen verwalten

Das *Firmwareaktualisierungs-Repository* enthält einen Katalog mit den verfügbaren Aktualisierungen und Aktualisierungspaketen, die auf verwalteten Einheiten übernommen werden können.

Zu dieser Aufgabe

Der *Katalog* enthält Informationen zu Firmwareaktualisierungen, die derzeit für die von XClarity Administrator unterstützten Einheiten verfügbar sind. Der Katalog organisiert die Firmwareaktualisierungen nach Einheitentyp. Wenn Sie den Katalog aktualisieren, ruft XClarity Administrator Informationen zu den neuesten verfügbaren Firmwareaktualisierungen von der Lenovo Website ab (einschließlich der Dateien metadata.xml oder .json und readme.txt) und speichert die Informationen im Firmwareupdate-Repository. Die Nutzdatendatei (.exe) wird nicht heruntergeladen. Weitere Informationen zum Aktualisieren des Katalogs finden Sie unter Produktkatalog aktualisieren.

Wenn neue Firmwareaktualisierungen verfügbar sind, müssen Sie die Aktualisierungspakete erst herunterladen, bevor Sie die Firmware auf den verwalteten Geräten aktualisieren können. Beim Aktualisieren des Katalogs werden nicht automatisch Aktualisierungspakete heruntergeladen. Die Tabelle **Produktkatalog** auf der Seite Repository für Firmwareaktualisierungen zeigt, welche Aktualisierungspakete heruntergeladen werden und welche zum Download verfügbar sind.

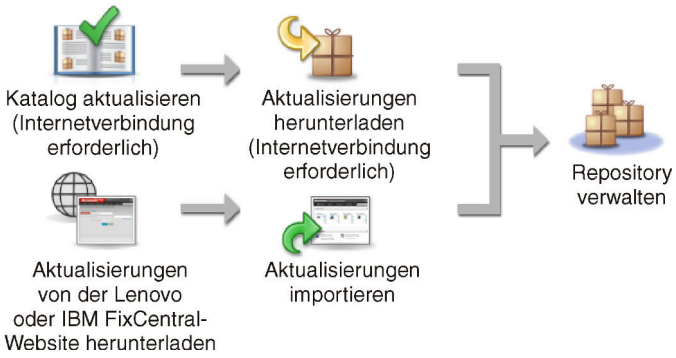
Zum Herunterladen von Firmwareaktualisierungen stehen Ihnen folgende Optionen zur Verfügung:

- **Firmwareaktualisierungs-Repository-Pakete**. Repository-Pakete enthalten die neuesten verfügbaren Firmwareaktualisierungen für alle unterstützten Einheiten sowie eine aktualisierte Standard-Firmwarekonformitätsrichtlinie. Diese Repository-Pakete werden importiert und über die Seite Verwaltungsserver aktualisieren übernommen.
- **UpdateXpress System Packs (UXSPs)**. UXSPs enthalten die neuesten Firmware- und Einheitentreiberaktualisierungen, geordnet nach Betriebssystem. Wenn Sie UXSPs über die Seite Firmwareaktualisierungen: Repository herunterladen, werden nur Firmwareaktualisierungen heruntergeladen und im Repository gespeichert. Einheitentreiberaktualisierungen sind davon ausgeschlossen.

  Anmerkung: Bei Servern mit XCC2 werden diese Pakete als Firmware*pakete* bezeichnet.

- **Einzelne Firmwareaktualisierungen**. Sie können einzelne Firmwareaktualisierungspakete auf einmal herunterladen, je nach der Version, die im Katalog aufgeführt ist.

XClarity Administrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und Firmwareaktualisierungen herunterzuladen. Wenn keine Internetverbindung besteht, können Sie die Dateien manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Administrator-Host über einen Webbrowser herunterladen und die Dateien dann in das Firmwareupdate-Repository importieren.



Wenn Sie Firmwareaktualisierungen manuell in XClarity Administrator importieren, müssen diese alle erforderlichen Nutzlast- (Image und MIB), Metadaten-, Änderungsprotokoll- und Readme-Dateien enthalten. Beispiele:
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Achtung:

- Importieren Sie nur diese erforderlichen Dateien. Importieren Sie keine anderen Dateien, die sich möglicherweise auf den Websites mit Firmware-Downloads befinden.
- Wenn Sie keine XML-Datei in das Aktualisierungspaket einbeziehen, wird die Aktualisierung nicht importiert.
- Wenn Sie nicht alle zur Aktualisierung erforderlichen Daten einbeziehen, zeigt das Repository die Aktualisierung als nicht heruntergeladen an. Dies bedeutet, dass sie teilweise importiert ist. Sie können dann die fehlenden Dateien importieren, indem Sie sie auswählen und importieren.
- Die Kernfirmwareaktualisierungen (z. B. für Management-Controller, UEFI und pDSA) sind betriebssystemunabhängig. Firmwareaktualisierungspakete für die Betriebssysteme RHEL 6 und SLES 11 werden zur Aktualisierung von Rechenknoten und Rack-Servern verwendet. Weitere Informationen zu den für die verwalteten Server verwendeten Firmwareaktualisierungspaketen finden Sie unter Firmwareaktualisierungen werden heruntergeladen.

Nachdem die Firmwareaktualisierungen im Repository heruntergeladen wurden, werden zu jeder Aktualisierung Informationen bereitgestellt, darunter Veröffentlichungsdatum, Größe, Richtliniennutzung und Schweregrad. Der Schweregrad zeigt die Auswirkungen und die Dringlichkeit für die Übernahme der Aktualisierung an. So können Sie ermitteln, wie Ihre Umgebung möglicherweise betroffen ist.
- **Erste Version**. Dies ist die erste Version der Firmware.
- **Kritisch**. Die Firmwareversion enthält dringende Fixes für Probleme mit Datenverlusten, der Sicherheit oder der Stabilität.
- **Empfohlen**. Die Firmwareversion enthält wichtige Fixes für vermutlich auftretende Problem.
- **Nicht kritisch**. Die Firmwareversion enthält untergeordnete Fixes, Leistungsverbesserungen und Textänderungen.

Anmerkungen:

- Der Schweregrad wird im Verhältnis zur zuvor veröffentlichten Version der Aktualisierung bewertet. Beispiel: Ist die installierte Firmware v1.01, die Aktualisierung v1.02 Kritisch und die Aktualisierung v1.03 Empfohlen, so bedeutet dies, dass die Aktualisierung von 1.02 auf 1.03 empfohlen ist und die Aktualisierung von v1.01 auf v1.03 kritisch ist – denn diese ist kumulativ (v1.03 umfasst die kritischen Fixes aus v1.02).
- In speziellen Fällen kann eine Aktualisierung nur für einen bestimmten Computertyp oder ein Betriebssystem empfohlen oder kritisch sein. Weitere Informationen finden Sie in den Versionshinweisen.

Vorgehensweise

So zeigen Sie im Produktkatalog verfügbare Firmwareaktualisierungen an:

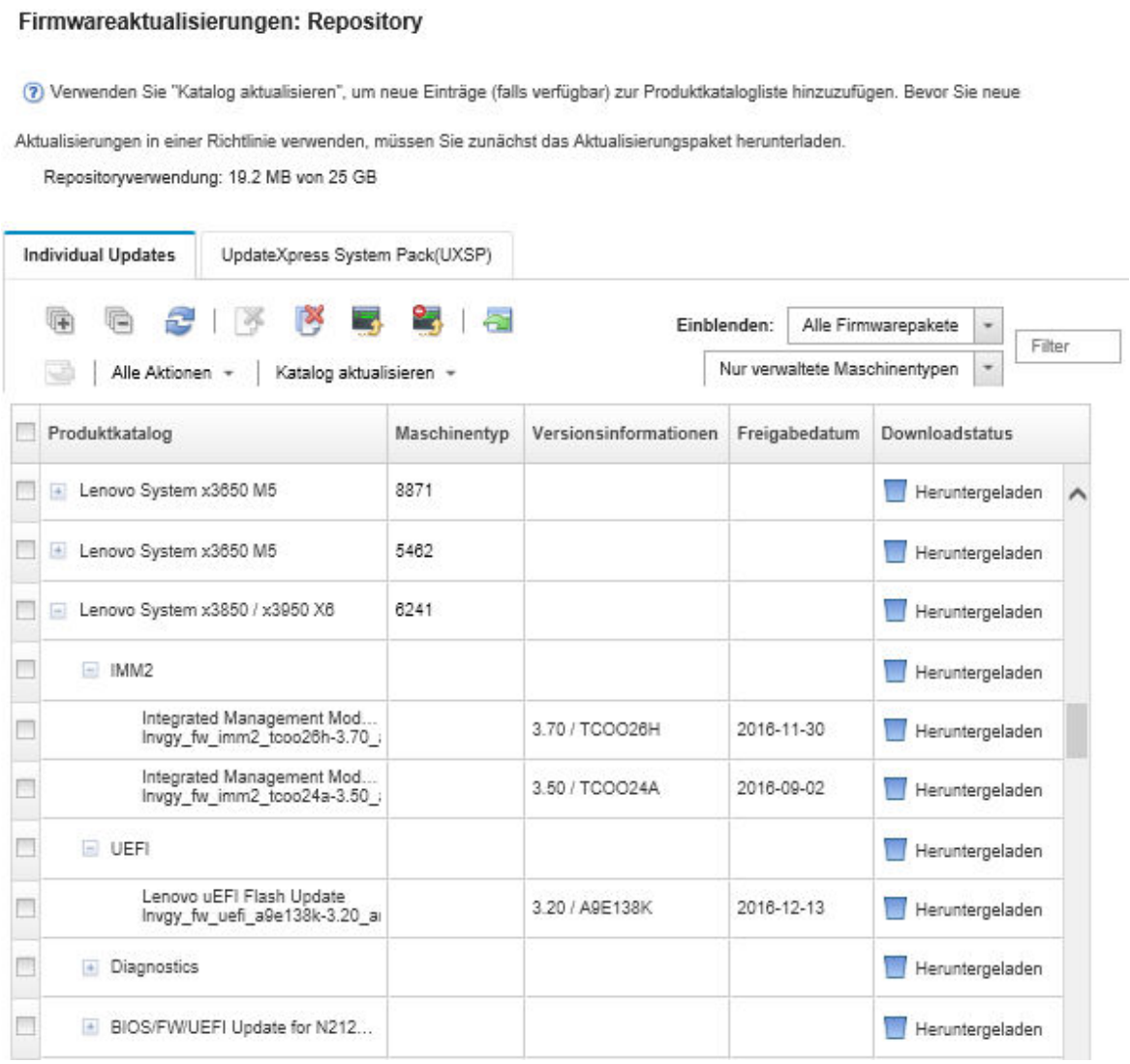
Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Repository**. Die Seite Repository für Firmwareaktualisierungen wird mit einer Liste verfügbarer Firmwareaktualisierungspakete angezeigt (nach Einheitentyp zusammengefasst).

Schritt 2. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen**, um Informationen zu den verfügbaren Firmwareaktualisierungspaketen anzuzeigen, oder klicken Sie auf die Registerkarte **UpdateXpress System Packs (UXSPs)**, um Informationen zu den verfügbaren UXSPs anzuzeigen.

Schritt 3. Erweitern Sie eine Einheit und Einheitenkomponenten, um die Aktualisierungspakete und Firmwareaktualisierungen für die Einheiten aufzulisten.

Sie können die Tabellenspalten sortieren und auf das Symbol **Alle erweitern** ( ) und **Alle ausblenden** ( ) klicken, um bestimmte Firmwareaktualisierungen zu suchen. Darüber hinaus können Sie die Liste der angezeigten Einheiten und Firmwareaktualisierungen filtern, indem Sie eine Option im Menü **Anzeigen** auswählen, um nur die Firmwareaktualisierungen eines bestimmten Zeitraums, Firmwareaktualisierungen für alle Servertypen oder nur für verwaltete Servertypen anzuzeigen, oder indem Sie Text im Feld **Filter** eingeben. Beachten Sie, dass bei der Suche nach bestimmten Einheiten, nur die Einheiten aufgeführt sind; Firmwareaktualisierungen sind nicht unter dem Einheitennamen aufgeführt.

Anmerkung: Für Server sind bestimmte Aktualisierungspakete auf Basis des Servertyps verfügbar. Wenn Sie einen Server erweitern, werden beispielsweise die Flex System x240 Rechenknoten-Aktualisierungspakete angezeigt, die speziell für diesen Rechenknoten verfügbar sind.



Ergebnisse

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Aktualisieren Sie die Seite mit den aktuellen Firmwareaktualisierungsinformationen im Katalog, indem Sie auf das Symbol **Aktualisieren** ( ) klicken.
- Rufen Sie die neuesten Informationen zu den verfügbaren Aktualisierungen ab, indem Sie auf **Katalog aktualisieren** klicken.Das Abrufen der Informationen kann einige Minuten dauern. Siehe Produktkatalog aktualisieren für weitere Informationen.
- Fügen Sie Firmwareaktualisierungen zum Repository hinzu, indem Sie Aktualisierungspakete oder Aktualisierungen im Produktkatalog auswählen und anschließend auf das Symbol **Herunterladen** ( ) klicken. Wenn die Firmwareaktualisierungen heruntergeladen und zum Repository hinzugefügt sind, ändert sich der Status zu „Heruntergeladen“.

  Anmerkung: XClarity Administrator muss mit dem Internet verbunden sein, um Aktualisierungen über die XClarity Administrator-Benutzerschnittstelle abzurufen. Wenn es nicht mit dem Internet verbunden ist, können Sie Aktualisierungen importieren, die Sie zuvor heruntergeladen haben.

Weitere Informationen zum Herunterladen von Aktualisierungen finden Sie im Abschnitt Firmwareaktualisierungen werden heruntergeladen.

- Importieren Sie Firmwareaktualisierungen, die manuell auf eine Arbeitsstation mit Netzwerkzugriff auf XClarity Administrator heruntergeladen haben, indem Sie eine oder mehrere Aktualisierungen auswählen und anschließend auf das Symbol **Importieren** () klicken.Weitere Informationen zum Importieren von Aktualisierungen finden Sie im Abschnitt Firmwareaktualisierungen werden heruntergeladen.
- Halten Sie die aktuell laufenden Firmware-Downloads an, indem Sie eine oder mehrere Aktualisierungen auswählen und anschließend auf das Symbol **Download abbrechen** () klicken.Durch das Abbrechen von Downloads werden *alle* laufenden Firmware-Downloads abgebrochen. Sie können den detaillierten Fortschritt eines bestimmten Firmware-Downloads im Jobprotokoll überwachen und stoppen (siehe Jobs überwachen).
- Löschen Sie Aktualisierungspakete oder einzelne Aktualisierungen aus dem Repository (siehe Firmwareaktualisierungen löschen).
- Sie können Firmwareaktualisierungen, die im Firmwareupdate-Repository vorhanden sind, auf ein lokales System exportieren (siehe Firmwareaktualisierungen exportieren und importieren).

Remote-Repository für Firmwareaktualisierungen verwenden

Standardmäßig verwendet Lenovo XClarity Administrator ein lokales (internes) Repository zum Speichern von Firmwareaktualisierungen. Sie können Speicherplatz freigeben, der für das lokale XClarity Administrator Repository zur Verfügung steht, indem Sie eine angehängte Remote-Freigabe über das SSH File System (SSHFS) als Remote-Repository verwenden. Sie können dann Firmwareaktualisierungsdateien direkt aus dem Remote-Repository verwenden, um die Firmwarekonformität auf Ihren Einheiten zu erhalten.

Vorbereitende Schritte

Auf der Remote-Freigabe können nur Firmwareaktualisierungen gespeichert werden. Windows-Einheitentreiber und XClarity Administrator-Aktualisierungen können nur im lokalen Aktualisierungs-Repository gespeichert werden.

Stellen Sie sicher, dass der SFTP-Service an Port 22 auf dem Remote-Freigabe-Server geöffnet ist. Die Baseboard Management Controller müssen auf diesen Port zugreifen können.

Die Remote-Freigabe wird als SFTP-Server verwendet, wenn sie als Firmware-Repository verwendet wird. Stellen Sie sicher, dass SFTP bei der Aktualisierung der SSHD-Konfiguration nicht deaktiviert wird.

Zu dieser Aufgabe

Wenn Sie die Position des Firmwareaktualisierungs-Repositorys ändern, können Sie festlegen, dass alle Firmwareaktualisierungen aus dem ursprünglichen Repository in das neue Repository kopiert werden.

Die Firmwareaktualisierungsdateien im ursprünglichen Repository werden nach dem Wechseln der Positionen *nicht* automatisch gelöscht.

Wenn XClarity Administrator eine Schreib- und Leseberechtigung für das Remote-Repository hat, ist das Verhalten dasselbe wie bei der Verwendung des lokalen Repositorys. Wenn XClarity Administrator jedoch nur eine Leseberechtigung hat, können Sie den Katalog nicht aktualisieren oder Aktualisierungen in das Repository herunterladen oder importieren.

Dasselbe Remote-Repository kann von mehreren XClarity Administrator-Instanzen gemeinsam genutzt werden. Wenn jedoch eine XClarity Administrator-Instanz das Repository ändert, werden die anderen XClarity Administrator-Instanzen nicht automatisch benachrichtigt. Sie müssen das Repository aktualisieren,

um die neuesten Details zu erhalten. Um das Repository zu aktualisieren, klicken Sie auf der Seite Firmwareaktualisierungen: Repository auf **Alle Aktionen → Repository aktualisieren**.

Anmerkung: Seien Sie vorsichtig beim Löschen von Firmwareaktualisierungen und UXSPs, wenn sich das Firmwareaktualisierungs-Repository auf einer Remote-Freigabe befindet, die von mehreren XClarity Administrator-Instanzen verwendet wird.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Remote-Firmwareaktualisierungs-Repository zu verwenden.

Schritt 1. Fügen Sie eine Remote-Freigabe zu XClarity Administrator hinzu (siehe Remote-Freigaben verwalten).

Schritt 2. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Repository**. Die Seite Repository für Firmwareaktualisierungen wird angezeigt.

Schritt 3. Klicken Sie auf **Alle Aktionen → Repository-Position tauschen**, um das Dialogfeld „Repository-Position tauschen“ anzuzeigen.

Schritt 4. Wählen Sie die gerade erstellte Remote-Freigabe aus der Dropdown-Liste **Repository-Position** aus.

Schritt 5. Wählen Sie optional **Aktuelles Repository bereinigen** aus, um Firmwareaktualisierungsdateien aus der aktuellen Repository-Position zu löschen.

Schritt 6. Wählen Sie optional **Aktualisierungspakete aus aktuellem Repository in neues Repository kopieren** aus, um die Firmwareaktualisierungsdateien in die neue Repository-Position zu kopieren, bevor die Repository-Position gewechselt wird.

Standardmäßig werden Firmwareaktualisierungsdateien, die in der neuen Position vorhanden sind, nicht kopiert, sondern übersprungen. In der Dropdown-Liste **Regeln überschreiben** können Sie optional festlegen, dass alle vorhandenen Dateien oder nur vorhandene Dateien mit einer anderen Größe oder einem anderen Änderungsdatum überschrieben werden.

Schritt 7. Klicken Sie auf **OK**.

Es wird ein Job erstellt, um Firmwareaktualisierungspakete in das neue Repository zu kopieren. Sie können den Jobfortschritt überwachen, indem Sie in der XClarity Administrator-Menüleiste auf **Überwachung → Jobs** klicken.

Produktkatalog aktualisieren

Der Produktkatalog enthält Informationen zu allen Firmwareaktualisierungen, die derzeit für die von Lenovo XClarity Administrator unterstützten Einheiten verfügbar sind (inkl. Gehäuse, Server und Flex-Switches).

Vorbereitende Schritte

Zur Aktualisierung des Produktkatalogs ist eine Internetverbindung erforderlich.

Die Aktualisierung des Katalogs kann mehrere Minuten in Anspruch nehmen.

Zu dieser Aufgabe

Wenn Sie den Katalog aktualisieren, ruft XClarity Administrator Informationen zu den neuesten verfügbaren Firmwareaktualisierungen von der Lenovo XClarity Unterstützungswebsite ab und speichert die Informationen im Repository für Firmwareaktualisierungen.

Die Aktualisierung des Katalogs fügt nur Informationen zu verfügbaren Firmwareaktualisierungen zum Repository hinzu. Sie lädt keine Aktualisierungspakete herunter. Sie müssen die Firmwareaktualisierungen herunterladen, um die Aktualisierungen für die Installation bereitzustellen. Weitere Informationen zum Herunterladen von Aktualisierungen finden Sie im Abschnitt Firmwareaktualisierungen werden heruntergeladen.

Vorgehensweise

So aktualisieren Sie den Produktkatalog:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Repository**. Die Seite Repository für Firmwareaktualisierungen wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen**, um Informationen zu einzelnen Firmwareaktualisierungspaketen abzurufen, oder klicken Sie auf die Registerkarte **UpdateXpress System Pack (UXSP)**, um Informationen zu UXSPs abzurufen.

Schritt 3. Klicken Sie auf **Katalog aktualisieren** und anschließend auf eine der folgenden Optionen, um Informationen zu den neuesten verfügbaren Firmwareaktualisierungen zu erhalten.

- **Ausgewählte aktualisieren – Nur aktuelle Version**. Ruft Informationen zur aktuellen Version von Firmwareaktualisierungen ab, die für die ausgewählten Einheiten verfügbar sind.
- **Alle aktualisieren – Nur aktuelle Version**. Ruft Informationen zur aktuellen Version von Firmwareaktualisierungen ab, die für alle Einheiten verfügbar sind.
- **Ausgewählte aktualisieren**. Ruft Informationen zu allen Versionen von Firmwareaktualisierungen ab, die für die ausgewählten Einheiten verfügbar sind.
- **Alle aktualisieren**. Ruft Informationen zu allen Versionen von allen Firmwareaktualisierungen ab, die für die unterstützten Einheiten verfügbar sind.

Tipp: Sie können den Produktkatalog aktualisieren und die aktuelle Firmware in einem Schritt herunterladen. Klicken Sie dazu auf **Alle Aktionen → Aktualisieren und aktuelle für alle verwalteten Einheiten herunterladen** oder **Alle Aktionen → Aktualisieren und aktuelle für ausgewählte Einheiten herunterladen**.

Firmwareaktualisierungen werden heruntergeladen

Je nach Internetzugriff können Sie Firmwareaktualisierungen im Repository für Firmwareaktualisierungen herunterladen oder importieren. Bevor Sie die Firmware auf Verwaltungseinheiten aktualisieren können, müssen die Firmwareaktualisierungen im Repository für Firmwareaktualisierungen verfügbar sein.

Vorbereitende Schritte

Stellen Sie vor dem Herunterladen von Firmware sicher, dass alle von Lenovo XClarity Administrator benötigten Ports und Internetadressen verfügbar sind. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit und Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn ein Einheitentyp nicht im Repository für Firmwareaktualisierungen aufgelistet ist, müssen Sie zuerst eine Einheit dieses Typs verwalten, bevor Sie eine einzelne Firmwareaktualisierung für diesen Einheitentyp herunterladen oder importieren können.

Wichtig:

- Für XClarity Administrator v1.1.1 und niedriger müssen Sie die Firmwareaktualisierungen für Lenovo Hardware manuell von Lenovo Website zu Support für Rechenzentrum herunterladen und importieren.
- XClarity Administrator kann keine Aktualisierungen für RackSwitch-Switches und Lenovo Speichereinheiten der DE, DX und SS Serien von der Lenovo Website in das Firmwareaktualisierungs-

Repository herunterladen. Stattdessen müssen Sie diese Aktualisierungen von der Lenovo Website auf eine Workstation mit Netzwerkzugriff auf den XClarity Administrator-Host herunterladen oder *Firmwareaktualisierungs-Repository-Pakete*, die alle verfügbaren Firmwareaktualisierungen enthalten, herunterladen und anwenden.

- Für Internet Explorer sowie Microsoft Edge-Webbrowser besteht ein Upload-Limit von 4 GB. Wenn die Datei, die Sie importieren, größer als 4 GB ist, können Sie einen anderen Webbrowser verwenden (z. B. Chrome oder Firefox).
- So laden Sie Firmware für Speichereinheiten der ThinkSystem DM-Serie herunter:
  - Eine oder mehrere Speichereinheiten der ThinkSystem DM-Serie müssen von XClarity Administrator verwaltet werden.
  - Jede Speichereinheit der ThinkSystem DM-Serie muss eine Berechtigung für Hardwareservice und -unterstützung haben.
  - Sie müssen auf der Seite „Firmwareaktualisierungen: Repository“ das Land angeben, in dem sich die Speichereinheiten der ThinkSystem DM-Serie befinden. Für Einheiten in den folgenden Ländern kann nur verschlüsselte Firmware heruntergeladen werden: Armenien, Weißrussland, China, Kuba, Iran, Kasachstan, Kirgisistan, Nordkorea, Russland, Sudan, Syrien.

Zu dieser Aufgabe

Zum Herunterladen von Firmwareaktualisierungen stehen Ihnen folgende Optionen zur Verfügung:

- **Firmwareaktualisierungs-Repository-Pakete**

  Firmwareaktualisierungs-Repository-Pakete sind Sammlungen der neuesten Firmware, die zur gleichen Zeit wie die XClarity Administrator-Version für die meisten unterstützten Einheiten sowie eine aktualisierte Standard-Firmwarekonformitätsrichtlinie verfügbar ist. Diese Repository-Pakete werden importiert und über die Seite Verwaltungsserver aktualisieren übernommen. Wenn Sie ein Firmwareaktualisierungs-Repository-Paket übernehmen, wird jede im Aktualisierungspaket enthaltene Aktualisierung zum Repository für Firmwareaktualisierungen hinzugefügt und eine Standardfirmwarekonformitätsrichtlinie wird automatisch für alle verwaltenden Einheiten erstellt. Sie können diese vordefinierte Richtlinie kopieren, aber nicht ändern.

  Die folgenden Repositorypakete sind verfügbar.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle CMMs und Flex System-Switches.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle RackSwitch-Switches und Lenovo Storage-Einheiten.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle Convergend HX Series-, Flex System-, NeXtScale- und System x-Server.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle ThinkAgile- und ThinkSystem-Server.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle ThinkAgile und ThinkSystem V2-Server.
  - **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Enthält Firmwareaktualisierungen für alle ThinkAgile und ThinkSystem V3 Server.

  In der Spalte **Downloadstatus** auf der Seite Verwaltungsserver aktualisieren können Sie ermitteln, ob Firmwareaktualisierungs-Repository-Pakete im Repository gespeichert sind. Die Spalte enthält einen der folgenden Werte:

  - **Heruntergeladen**. Das Firmwareaktualisierungs-Repository-Paket ist im Repository gespeichert.

– **Nicht heruntergeladen**. Das Firmwareaktualisierungs-Repository-Paket ist verfügbar, aber nicht im Repository gespeichert.

- **UpdateXpress System Packs (UXSPs)**

  Anmerkung: Bei Servern mit XCC2 werden diese Pakete als Firmwarepakete bezeichnet. *Paket* wird in den Paketnamen und vordefinierten Richtliniennamen verwendet.

  UXSPs enthalten die neuesten Firmware- und Einheitentreiberaktualisierungen, geordnet nach Betriebssystem. Wenn Sie UXSPs herunterladen, lädt XClarity Administrator das UXSP basierend auf der Version im Katalog herunter und speichert die Aktualisierungspakete im Repository für Firmwareaktualisierungen. Wenn Sie ein UXSP herunterladen, wird jede Firmwareaktualisierung im UXSP zum Firmwareupdate-Repository hinzugefügt und auf der Registerkarte **Einzelne Aktualisierungen** aufgeführt. Eine Standard-Firmwarekonformitätsrichtlinie wird automatisch für alle verwaltbaren Einheiten mit den folgenden Namen erstellt. Sie können diese vordefinierte Richtlinie kopieren, aber nicht ändern.
  – *{uxsp-version}-{date}-{server-short-name}***-UXSP** (z. B. `v1.50-2017-11-22- SD530-UXSP`)
  – *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (z. B. `22a.0-kaj92va-SR650V3-bundle`)

  Anmerkung: Wenn Sie UXSPs über die Seite Firmwareaktualisierungen: Repository herunterladen oder importieren, werden nur Firmwareaktualisierungen heruntergeladen und im Repository gespeichert. Einheitentreiberaktualisierungen werden verworfen. Weitere Informationen zum Herunterladen oder Importieren von Windows-Einheitentreiberaktualisierungen mithilfe von UXSPs finden Sie unter BS-Einheitentreiber-Repository verwalten.

  Anhand der Spalte **Downloadstatus** auf der Registerkarte **Einzelne Aktualisierungen** der Seite Firmwareaktualisierungen: Repository können Sie ermitteln, ob UXSPs im Repository für Firmwareaktualisierungen gespeichert sind. Die Spalte enthält einen der folgenden Werte:

  – **Heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist im Repository gespeichert.
  – *x* **von** *y* **heruntergeladen**. Es sind nur einige Firmwareaktualisierungen des Aktualisierungspakets im Repository gespeichert. Die Zahlen in Klammern geben die Anzahl der verfügbaren Aktualisierungen und die Anzahl gespeicherten Aktualisierungen an oder es liegen keine Aktualisierungen für den speziellen Einheitentyp vor.
  – **Nicht heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist verfügbar, aber nicht im Repository gespeichert.

- **Einzelne Firmwareaktualisierungen**

  Sie können einzelne Firmwareaktualisierungspakete auf einmal herunterladen. Wenn Sie Firmwareaktualisierungspakete herunterladen, lädt XClarity Administrator die Aktualisierung basierend auf der Version im Katalog herunter und speichert das Aktualisierungspaket im Repository für Firmwareaktualisierungen. Sie können dann mit den Aktualisierungspaketen Firmwarekonformitätsrichtlinien für die verwalteten Einheiten erstellen.

  Anmerkung: Die Kernfirmwareaktualisierungen (z. B. für Management-Controller, UEFI und pDSA) sind betriebssystemunabhängig. Firmwareaktualisierungspakete für die Betriebssysteme RHEL 6 und SLES 11 werden zur Aktualisierung von Rechenknoten und Rack-Servern verwendet. Weitere Informationen zu den für die verwalteten Server verwendeten Firmwareaktualisierungspaketen finden Sie unter Firmwareaktualisierungen werden heruntergeladen.

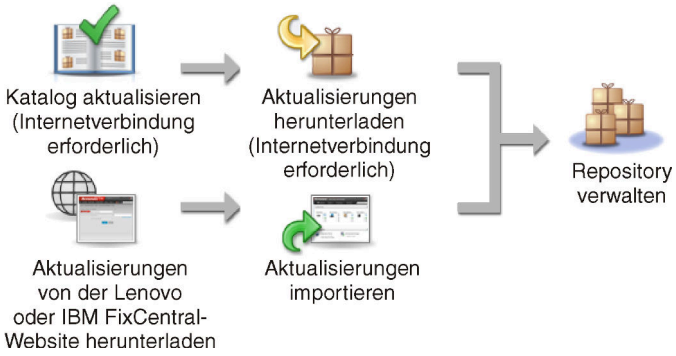
  Anhand der Spalte **Downloadstatus** auf der Registerkarte **Einzelne Aktualisierungen** der Seite Firmwareaktualisierungen: Repository können Sie ermitteln, ob bestimmte *Firmwareaktualisierungen* im Repository für Firmwareaktualisierungen gespeichert sind. Die Spalte enthält die folgenden Werte.

  – **Heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist im Repository gespeichert.

- *x* **von** *y* **heruntergeladen**. Es sind nur einige Firmwareaktualisierungen des Aktualisierungspakets im Repository gespeichert. Die Zahlen in Klammern geben die Anzahl der verfügbaren Aktualisierungen und die Anzahl gespeicherten Aktualisierungen an oder es liegen keine Aktualisierungen für den speziellen Einheitentyp vor.
- **Nicht heruntergeladen**. Das gesamte Aktualisierungspaket oder die einzelne Firmwareaktualisierung ist verfügbar, aber nicht im Repository gespeichert.

Wenn Sie XClarity Administrator installieren oder auf eine neue Version aktualisieren, sollten Sie als bewährte Vorgehensweise das aktuelle Repository-Paket herunterladen, um sicherzustellen, dass Sie über die aktuellen Firmwareaktualisierungen verfügen. Anschließend können Sie einen wiederkehrenden Job für die Aktualisierung des Katalogs planen, um nach einzelnen Aktualisierungen zu suchen, die seit dem letzten Repository-Paket im Web veröffentlicht wurden, und diese Aktualisierungen anschließend nacheinander elektronisch herunterzuladen.

XClarity Administrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und Firmwareaktualisierungen herunterzuladen. Wenn keine Internetverbindung besteht, können Sie die Dateien manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Administrator-Host über einen Webbrowser herunterladen und die Dateien dann in das Firmwareupdate-Repository importieren.



Wenn Sie Firmwareaktualisierungen manuell in XClarity Administrator importieren, müssen diese alle erforderlichen Nutzlast- (Image und MIB), Metadaten-, Änderungsprotokoll- und Readme-Dateien enthalten. Beispiele:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Anmerkung: Die Kernfirmwareaktualisierungen (z. B. für Management-Controller, UEFI und pDSA) sind betriebssystemunabhängig. Firmwareaktualisierungspakete für die Betriebssysteme RHEL 6 und SLES 11 werden zur Aktualisierung von Rechenknoten und Rack-Servern verwendet.

Wenn das Repository zu mehr als 50 % voll ist, wird eine Nachricht auf der Seite angezeigt. Wenn das Repository zu mehr als 85 % voll ist, wird eine weitere Nachricht auf der Seite angezeigt. Um den im Repository verwendeten Speicherplatz zu reduzieren, können Sie nicht verwendete Imagedateien und Richtlinien entfernen. Sie können nicht verwendete Firmwarekonformitätsrichtlinien und die zugeordneten Firmwarepakete entfernen, indem Sie auf **Bereitstellung → Konformitätsrichtlinien** klicken, mindestens eine zu löschende Richtlinien auswählen und dann auf **Aktionen → Alle Richtlinien und Firmwarepakete löschen** klicken.

Die folgende Tabelle fasst die Unterschiede zwischen dem Abrufen von Firmwareaktualisierungspaketen, UXSPs und einzelnen Firmwareaktualisierungspaketen zusammen.

Aktualisierungspaket	Benutzeroberflächen-seite für das Herunterladen und Importieren von Dateien	Webseite für das manuelle Herunterladen von Dateien	Wurde das Repository für Firmwa-reaktuali-sierungen aktuali-siert?	Wird die Firmwarekon-formitätsrichtli-nie automatisch aktualisiert?
Firmwareaktualisie-rungs-Repository-Pakete	Seite „Verwaltungsserver aktualisieren“ **Anmerkung:** Sie müssen das Repository-Paket importieren und dann anwenden.	Website zum Herunterladen von XClarity Administrator	Ja	Ja
UpdateXpress System Packs	Seite „Firmwareaktualisierun-gen: Repository“, Registerkarte **UpdateXpress System Packs (UXSPs)**	Webseite für Lenovo XClarity Essentials UpdateXpress	Ja	Ja
Firmwareaktualisierun-gen	Seite „Firmwareaktualisierun-gen: Repository“, Registerkarte **Einzelne Aktualisierungen**	Lenovo Website zu Support für Rechenzentrum **Anmerkungen:** Verwenden Sie den Website zu Fix Central für die folgenden Einheiten: • Flex System x220 Typen 2585 und 7906 • Flex System x222 Rechenknoten Typen 2589 und 7916 • Flex System x240 Typen 7863, 8737, 8738 und 8956 • Flex System x280 / x480 / x880 X6 Typen 4259 und 7903 • Flex System x440 Typen 2584 und 7917	Ja	Es werden keine

Vorgehensweise

So laden Sie eine oder mehrere Firmwareaktualisierungen herunter:

- So importieren Sie eines oder mehrere *Firmwareupdate-Repository-Pakete*:
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Verwaltungsserver aktualisieren**, um die Seite Aktualisierung des Verwaltungsservers anzuzeigen.
  2. Herunterladen der neuesten Repository-Pakete:
     - Wenn XClarity Administrator mit dem Internet verbunden ist:
       a. Rufen Sie Informationen über die neuesten Aktualisierungen ab, indem Sie auf **Katalog aktualisieren → Alle aktualisieren – nur aktuelle Version** klicken. Neue Aktualisierungen für Verwaltungsserver und Firmwareaktualisierungs-Repository-Pakete werden in der Tabelle auf der Seite „Aktualisierung des Verwaltungsservers“ aufgeführt.

Die Aktualisierung des Repositorys kann mehrere Minuten in Anspruch nehmen.

Anmerkung: Beim Aktualisieren des Repositorys werden nicht automatisch Nutzdatendateien heruntergeladen. Nur die Metadaten- und Readme-Dateien werden heruntergeladen.

b. Wählen Sie die Firmwareaktualisierungs-Repository-Pakete aus, die Sie herunterladen möchten.

Tipp: Prüfen Sie, ob die ausgewählten Pakete in der Spalte **Typ** „Zusatzpakete“ haben.

c. Klicken Sie auf das Symbol **Ausgewählte herunterladen** (). Wenn das Herunterladen abgeschlossen ist, ändert sich der **Downloadstatus** für die Software-Updates zu „Heruntergeladen“.

– Wenn XClarity Administrator nicht mit dem Internet verbunden ist:

a. Laden Sie die Firmwareaktualisierungs-Repository-Pakete von der Website zum Herunterladen von XClarity Administrator auf eine Arbeitsstation herunter, die über eine Netzwerkverbindung zum XClarity Administrator-Host verfügt.

b. Klicken Sie auf der Seite Aktualisierung des Verwaltungsservers auf das Symbol **Importieren** ().

c. Klicken Sie auf **Dateien auswählen** und wählen Sie die Position der Pakete im Repository für Firmwareaktualisierungen auf der Arbeitsstation aus.

d. Wählen Sie alle Paketdateien aus und klicken Sie auf **Öffnen**.

Sie müssen die Metadatendatei (.xml oder .json) sowie das Image oder die Nutzlastdatei (.zip, .bin, .uxz oder .tgz), die Änderungshistoriendatei (.chg) und die Readme-Datei (.txt) für die Aktualisierung importieren. Alle ausgewählten und nicht in der Metadatendatei angegebenen Dateien werden gelöscht. Wenn Sie keine Metadatendatei auswählen, wird die Aktualisierung nicht importiert.

e. Klicken Sie auf **Importieren**.

Wenn der Import abgeschlossen ist, werden die Pakete im Repository für Firmwareaktualisierungen in der Tabelle auf der Seite Aktualisierung des Verwaltungsservers aufgeführt. Der **Downloadstatus** der einzelnen Aktualisierungen ist „Heruntergeladen“.

3. Wählen Sie die Pakete im Repository für Firmwareaktualisierungen aus, die Sie für das Repository für Firmwareaktualisierungen installieren möchten.

Anmerkung: Prüfen Sie, ob der **Downloadstatus** den Wert „Heruntergeladen“ hat und ob der **Typ** den Wert „Patch“ hat.

4. Klicken Sie auf das Symbol **Aktualisierung durchführen** (), um die Pakete im Repository für Firmwareaktualisierungen zum Repository hinzuzufügen.
5. Warten Sie einige Minuten auf den Abschluss der Aktualisierung und den Neustart von XClarity Administrator.
6. Prüfen Sie, ob die Aktualisierung abgeschlossen ist, indem Sie den Webbrowser aktualisieren.

Wenn sie abgeschlossen ist, wird die Seite Aktualisierung des Verwaltungsservers angezeigt. Der Wert in der Spalte **Angewendeter Status** ändert sich in „Angewendet“.

7. Löschen Sie den Cache des Webbrowsers.

- So laden Sie eine oder mehrere *UXSPs* herunter.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → Firmwareaktualisierungen: Repository**, um die Seite Repository für Firmwareaktualisierungen anzuzeigen.
2. Klicken Sie auf die Registerkarte **UpdateXpress System Packs (UXSPs)**.

3. Laden Sie die aktuellen UXSPs herunter:
   - Wenn XClarity Administrator mit dem Internet verbunden ist:

     Um den Katalog zu aktualisieren und die aktuellen UXSPs für alle verwalteten Einheiten herunterzuladen, klicken Sie auf **Alle Aktionen → Aktualisieren und aktuelle für alle verwalteten Einheiten herunterladen**.

     Um den Katalog zu aktualisieren und die aktuellen UXSPs für ausgewählte Einheiten herunterzuladen:

     a. Erweitern Sie die Einheit, um die Liste der verfügbaren UXSPs anzuzeigen.
     b. Wählen Sie ein oder mehrere UXSPs aus, die heruntergeladen werden sollen.
     c. Klicken Sie auf **Alle Aktionen → Aktualisieren und aktuelle für ausgewählte Einheiten herunterladen**.

        Wenn der Download abgeschlossen ist, ändert sich der **Downloadstatus** für die ausgewählten UXSPs in „Heruntergeladen“.
   - Wenn XClarity Administrator nicht mit dem Internet verbunden ist:

     a. Laden Sie die UXSPs von der Webseite für Lenovo XClarity Essentials UpdateXpress auf eine Arbeitsstation herunter, die über eine Netzwerkverbindung zum XClarity Administrator-Host verfügt.
     b. Klicken Sie von XClarity Administrator auf das Symbol **Importieren** ().
     c. Klicken Sie auf **Dateien auswählen** und wählen Sie die Position der UXSPs auf der Arbeitsstation aus.
     d. Wählen Sie alle Paketdateien aus und klicken Sie auf **Öffnen**.

        Sie müssen die Metadatendatei (.xml oder .json) sowie das Image oder die Nutzlastdatei (.zip, .bin, .uxz oder .tgz), die Änderungshistoriendatei (.chg) und die Readme-Datei (.txt) für die Aktualisierung importieren. Alle ausgewählten und nicht in der Metadatendatei angegebenen Dateien werden gelöscht. Wenn Sie keine Metadatendatei auswählen, wird die Aktualisierung nicht importiert.
     e. Klicken Sie auf **Importieren**.

        Wenn der Import abgeschlossen ist, werden die Pakete im Repository für Firmwareaktualisierungen in der Tabelle auf der Seite „Aktualisierung des Verwaltungsservers“ aufgeführt. Der Downloadstatus der einzelnen Aktualisierungen ist „Heruntergeladen“.

- So laden Sie ein oder mehrere *Firmwareaktualisierungspakete* herunter.
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → Firmwareaktualisierungen: Repository**, um die Seite Repository für Firmwareaktualisierungen anzuzeigen.
  2. Wählen Sie beim Herunterladen von Firmware für Speichereinheiten der ThinkSystem DM-Serie das Land aus, in dem sich die Speichereinheiten befinden.
  3. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen**.
  4. Laden Sie die neuesten einzelnen Firmwareaktualisierungen herunter:
     - Wenn XClarity Administrator mit dem Internet verbunden ist:

       Um den Katalog zu aktualisieren und die aktuelle Firmware für alle verwalteten Einheiten herunterzuladen, klicken Sie auf **Alle Aktionen → Aktualisieren und aktuelle für alle verwalteten Einheiten herunterladen**.

       Um den Katalog zu aktualisieren und die aktuelle Firmware für ausgewählte Einheiten herunterzuladen:

a. Erweitern Sie die Einheit, um die Liste der verfügbaren Firmwareaktualisierungen anzuzeigen.
b. Wählen Sie ein oder mehrere Firmwareaktualisierungen aus, die heruntergeladen werden sollen.

   Tipp: Ein Aktualisierungspaket kann aus mehreren Firmwareaktualisierungen bestehen. Wenn Sie eine Firmwareaktualisierung herunterladen, können Sie das gesamte Aktualisierungspaket oder nur einzelne Aktualisierungen herunterladen. Sie können außerdem mehrere Pakete gleichzeitig herunterladen.
c. Klicken Sie auf **Alle Aktionen → Aktualisieren und aktuelle für ausgewählte Einheiten herunterladen**.

   Wenn das Herunterladen abgeschlossen ist, ändert sich der **Downloadstatus** für die ausgewählten Firmwareaktualisierungen zu „Heruntergeladen“.

– Wenn XClarity Administrator nicht mit dem Internet verbunden ist:

a. Laden Sie die Firmwareaktualisierungspakete von Lenovo Website zu Support für Rechenzentrum auf eine Arbeitsstation herunter, die über eine Netzwerkverbindung zum XClarity Administrator-Host verfügt.

   Laden Sie für die folgenden Server Firmwareaktualisierungen für das SLES 11-Betriebssystem vom Website zu Fix Central herunter:

   – Flex System x220 Typen 2585 und 7906
   – Flex System x222 Rechenknoten Typen 2589 und 7916
   – Flex System x240 Typen 7863, 8737, 8738 und 8956
   – Flex System x280 / x480 / x880 X6 Typen 4259 und 7903
   – Flex System x440 Typen 2584 und 7917

   Laden Sie für alle anderen Server Firmwareaktualisierungen für das RHEL 6-Betriebssystem vom Lenovo XClarity Unterstützungswebsite herunter.
b. Klicken Sie von XClarity Administrator auf das Symbol **Importieren** ().
c. Klicken Sie auf **Dateien auswählen** und wählen Sie die Position der Firmwareaktualisierungen auf der Arbeitsstation aus.
d. Wählen Sie alle Paketdateien aus und klicken Sie auf **Öffnen**.

   Sie müssen die Metadatendatei (.xml oder .json) sowie das Image oder die Nutzlastdatei (.zip, .bin, .uxz oder .tgz), die Änderungshistoriendatei (.chg) und die Readme-Datei (.txt) für die Aktualisierung importieren. Alle ausgewählten und nicht in der Metadatendatei angegebenen Dateien werden gelöscht.

   Achtung:

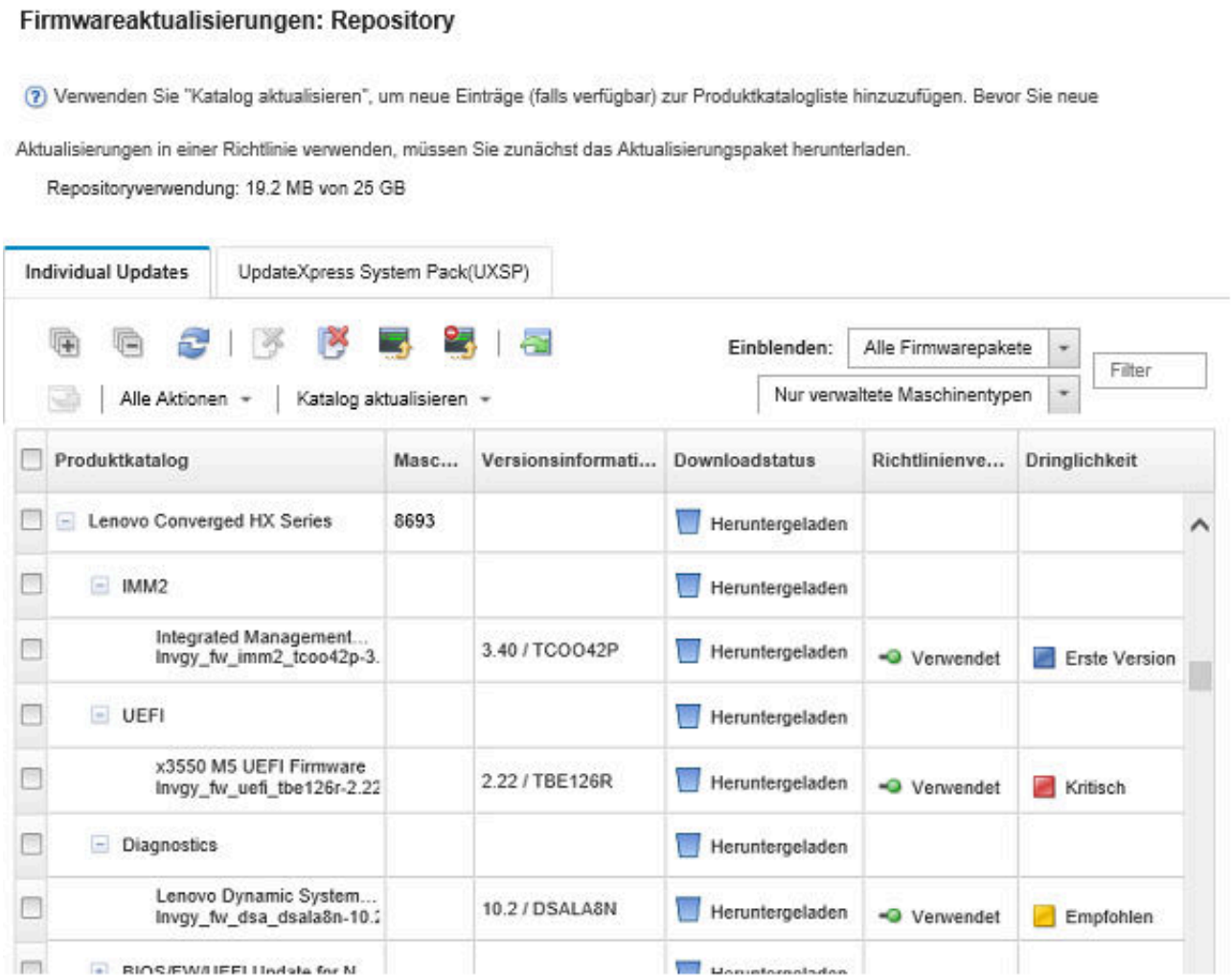
   – Importieren Sie nur diese erforderlichen Dateien. Importieren Sie keine anderen Dateien, die sich möglicherweise auf den Websites mit Firmware-Downloads befinden.
   – Wenn Sie keine XML-Datei in das Aktualisierungspaket einbeziehen, wird die Aktualisierung nicht importiert.
   – Wenn Sie nicht alle zur Aktualisierung erforderlichen Daten einbeziehen, zeigt das Repository die Aktualisierung als nicht heruntergeladen an. Dies bedeutet, dass sie teilweise importiert ist. Sie können dann die fehlenden Dateien importieren, indem Sie sie auswählen und importieren.
   – Die Kernfirmwareaktualisierungen (z. B. für Management-Controller, UEFI und pDSA) sind betriebssystemunabhängig. Firmwareaktualisierungspakete für die Betriebssysteme RHEL 6 und SLES 11 werden zur Aktualisierung von Rechenknoten und Rack-Servern verwendet. Weitere Informationen zu den für die verwalteten Server verwendeten

Firmwareaktualisierungspaketen finden Sie unter Firmwareaktualisierungen werden heruntergeladen.

e. Klicken Sie auf **Importieren**.

Das Aktualisieren des Katalogs und Herunterladen der Firmwareaktualisierungen kann einige Minuten dauern. Wenn die Aktualisierungen heruntergeladen und im Repository gespeichert wurden, wird die Zeile im Produktkatalog hervorgehoben und die Spalte **Downloadstatus** ändert sich zu „Heruntergeladen“.

Anmerkung: Der Maschinentyp für einige Switches wird möglicherweise als Hexadezimalzahl angezeigt.



Nach dieser Aufgabe

Sie können die maximale Größe des Aktualisierungs-Repositorys (inkl. Firmwareaktualisierungen, BS-Einheitentreiber und Verwaltungsserveraktualisierungen) auf der Seite Firmware-Repository konfigurieren, indem Sie auf **Alle Aktionen → Globale Einstellungen** klicken. Die Mindestgröße ist 50 GB. Die maximale Größe hängt vom Festplattenspeicherplatz des lokalen Systems ab.

Firmwareaktualisierungen exportieren und importieren

Sie können im Repository vorhandene einzelne Firmwareaktualisierungen und UpdateXpress System Packs (UXSPs) in das lokale System exportieren.

Zu dieser Aufgabe

Nur Firmwareaktualisierungen, die im Repository vorhanden sind, können exportiert werden. Stellen Sie sicher, dass der Downloadstatus der ausgewählten Firmwareaktualisierungen „Heruntergeladen“ lautet.

Alle Dateien, die mit der Firmwareaktualisierung zusammenhängen, werden exportiert, darunter auch die Aktualisierungsimagedatei oder Nutzlastdatei (.zip, .bin, .uxz oder .tgz), die Metadatendatei (.xml oder .json), die Änderungshistoriendatei (.chg) und die Readme-Datei (.txt).

Achtung: Ändern Sie nicht die Namen der Firmwareaktualisierungsdateien.

Vorgehensweise

- So exportieren Sie Firmwareaktualisierungen:
  1. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen** oder auf die Registerkarte **UpdateXpress System Packs (UXSPs)**.
  2. Wählen Sie eine oder mehrere Firmwareaktualisierungen aus.
  3. Klicken Sie auf das Symbol **Exportieren** ( ).
- So importieren Sie Firmwareaktualisierungen:

  Sie können Dateien importieren, die Sie manuell aus Lenovo XClarity Administrator exportiert haben, und Dateien, die Sie manuell aus dem Internet heruntergeladen haben. Siehe Firmwareaktualisierungen werden heruntergeladen für weitere Informationen.

Firmwareaktualisierungen löschen

Sie können Firmwareaktualisierungen und UpdateXpress System Packs (UXSPs) aus dem Repository für Firmwareaktualisierungen löschen.

Vorbereitende Schritte

Stellen Sie sicher, dass alle geplanten oder laufenden Aktualisierungsjobs für eine Firmwarekonformitätsrichtlinie mit den zu löschenden Firmwareaktualisierungen abgeschlossen oder abgebrochen sind (siehe Jobs überwachen).

Stellen Sie vor dem Löschen sicher, dass die Aktualisierung nicht in einer Firmwarekonformitätsrichtlinie verwendet wird. Sie können keine Firmwareaktualisierungspakete löschen, die gerade in einer oder mehreren Firmwarekonformitätsrichtlinien verwendet werden.

Beim Löschen eines UXSP wird auch die Firmwarekonformitätsrichtlinie gelöscht, die automatisch für diese UXSP erstellt wurde.

Anmerkung: Seien Sie vorsichtig beim Löschen von Firmwareaktualisierungen und UXSPs, wenn das Firmwareaktualisierungs-Repository eine Remote-Freigabe ist, die von mehreren XClarity Administrator-Instanzen verwendet wird.

Vorgehensweise

So löschen Sie eine oder mehrere Firmwareaktualisierungen aus dem Repository für Firmwareaktualisierungen:

Schritt 1. Heben Sie die Zuordnungen für alle Firmwarekonformitätsrichtlinien auf, die Firmwareaktualisierungen enthalten, welche von allen verwalteten Einheiten gelöscht werden sollen.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Übernehmen/ Aktivieren**. Die Seite Firmwareaktualisierungen: anwenden/aktivieren wird angezeigt.

b. Klicken Sie auf „Keine Zuordnung“ oder wählen Sie eine andere Firmwarekonformitätsrichtlinie in der Spalte **Zugeordnete Richtlinie** für die verwalteten Einheiten aus, die die Firmwarekonformitätsrichtlinie verwenden.

Schritt 2. Löschen Sie alle benutzerdefinierten Firmwarekonformitätsrichtlinien, die zu löschende Firmwareaktualisierungen enthalten, oder geben Sie für die Firmwarekonformitätsrichtlinien an, dass die zu löschenden Firmwareaktualisierungen entfernt werden sollen.

a. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Konformitätsrichtlinien**. Die Seite Firmwareaktualisierungen: Konformitätsrichtlinien wird angezeigt.

b. Wählen Sie die Firmwarekonformitätsrichtlinie und dann das Symbol für **Löschen** ( ) aus, um die Richtlinie zu löschen oder klicken Sie auf das Symbol für **Bearbeiten** ( ), um die Firmwareaktualisierungen aus der Richtlinie zu entfernen.

Schritt 3. Löschen Sie die Firmwareaktualisierungen.

- **Einzelne Firmwareaktualisierungen**
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Repository**. Die Seite Repository für Firmwareaktualisierungen wird angezeigt.
  2. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen**.
  3. Wählen Sie eine oder mehrere zu löschende Firmwareaktualisierungen aus.
  4. Klicken Sie auf das **Nur Images löschen**-Symbol ( ), um nur das Image oder die Nutzlastdatei (.zip, .bin, .uxz oder .tgz) zu löschen. Informationen zur Aktualisierung bleibt vorhanden. So können Sie die Aktualisierung problemlos erneut herunterladen. Oder klicken Sie auf das Symbol **Vollständige Aktualisierungspakete löschen** ( ), um die vollständigen Aktualisierungspakete, einschließlich der Image- oder Nutzdatendatei, der Datei für den Änderungsverlauf (.chg), der readme-Datei (.txt) und der Metadaten-Datei (. xml oder .json) zu löschen.

  Wenn Sie eine Firmwareaktualisierung löschen, werden die Nutzlastdateien entfernt. Die Metadatendatei mit Informationen zur Aktualisierung bleibt jedoch vorhanden, sodass Sie die Aktualisierung bei Bedarf problemlos erneut herunterladen können. Der **Downloadstatus** ändert sich in „Nicht heruntergeladen“.

- **UXSPs**
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Repository**. Die Seite Repository für Firmwareaktualisierungen wird angezeigt.
  2. Klicken Sie auf die Registerkarte **UpdateXpress System Pack (UXSP)**.
  3. Wählen Sie ein oder mehrere zu löschende UXSPs aus.
  4. Klicken Sie auf das Symbol **UXSP und zugehörige Richtlinie löschen** ( ), um die vollständigen UXSPs zu löschen, einschließlich Image- oder Nutzdatendatei, Änderungshistoriendatei (.chg), Readme-Datei (.txt) und Metadatendatei (.xml oder .json) sowie alle zugehörigen Firmwarekonformitätsrichtlinien.

  Wenn die ausgewählten UXSPs Richtlinien zugeordnet sind, die verwendet werden (d. h. Einheiten zugeordnet sind), wird das Dialogfenster zum Löschen von UXSP, Richtlinie und Aktualisierungspaketen angezeigt. Geben Sie an, ob die zugeordneten Richtlinien zusätzlich

zum UXSP und den Richtlinien mit aufgehobener Zuordnung gelöscht werden sollen, und klicken Sie auf **OK**.

Firmwarekonformitätsrichtlinien erstellen und zuordnen

Firmwarekonformitätsrichtlinien stellen sicher, dass die Firmware auf bestimmten verwalteten Einheiten auf dem neuesten Stand ist, indem die Einheiten gekennzeichnet werden, die Ihre Aufmerksamkeit erfordern. Jede Firmwarekonformitätsrichtlinie identifiziert, welche Einheiten überwacht werden und welche Firmwareversion installiert werden muss, damit die Einheiten konform bleiben. Sie können die Konformität auf Einheiten- oder Firmwarekomponentenebene festlegen. XClarity Administrator verwendet die Richtlinien, um den Status von verwalteten Einheiten sicherzustellen und nicht konforme Einheiten zu erkennen.

Vorbereitende Schritte

Wenn Sie eine Firmwarekonformitätsrichtlinie erstellen, wählen Sie die Zielaktualisierungsversion zur Anwendung auf die Einheiten aus, die der Richtlinie zugeordnet werden sollen. Achten Sie darauf, dass sich die Firmwareaktualisierungen für die Zielversion im Aktualisierungs-Repository befinden, bevor Sie die Richtlinie erstellen (siehe Firmwareaktualisierungen werden heruntergeladen).

Wenn ein Einheitentyp nicht im Repository für Firmwareaktualisierungen aufgelistet ist, müssen Sie zuerst eine Einheit dieses Typs verwalten, bevor Sie die kompletten Firmwareaktualisierungen zur Erstellung von Konformitätsrichtlinien für die Einheiten dieses Typs herunterladen oder importieren.

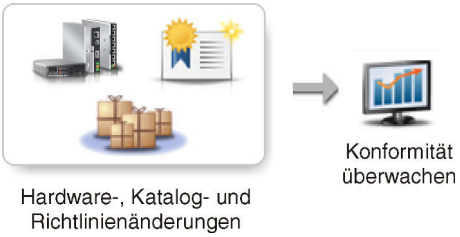
Zu dieser Aufgabe

Wenn Sie eine Firmwarekonformitätsrichtlinie erstellen, können Sie die folgenden Einheiten von XClarity Administrator markieren lassen:

- Die Firmware auf der Einheit ist niedriger
- Die Firmware auf der Einheit stimmt nicht mit der Version aus der Firmwarekonformitätsrichtlinie überein

XClarity Administrator enthält eine vordefinierte Firmwarekonformitätsrichtlinie namens **Neueste Firmware im Repository**. Wenn neue Firmware heruntergeladen oder in das Repository importiert wird, wird diese Richtlinie so aktualisiert, dass die neuesten verfügbaren Versionen der Firmware im Repository enthalten sind.

Nachdem der Einheit eine Firmwarekonformitätsrichtlinien zugewiesen wurde, überprüft XClarity Administrator bei Änderungen des Bestands oder des Repositorys für Firmwareaktualisierungen den Konformitätsstatus jeder Einheit. Wenn die Firmware auf einer Einheit mit der zugewiesenen Richtlinie nicht konform ist, zeigt XClarity Administrator die Einheit auf der Seite Firmwareaktualisierungen: Übernehmen/Aktivieren entsprechend der in der Firmware-Konformitätsrichtlinie angegebenen Regel, als nicht konform an.



Sie können beispielsweise eine Firmwarekonformitätsrichtlinie erstellen, die die Basisversion für die auf den ThinkSystem SR850 Einheiten installierte Firmware definiert, und diese Firmwarekonformitätsrichtlinie dann allen verwalteten ThinkSystem SR850 Einheiten zuordnen. Wenn das Repository für Firmwareaktualisierungen aktualisiert und eine neue Firmwareaktualisierung hinzugefügt wird, sind die

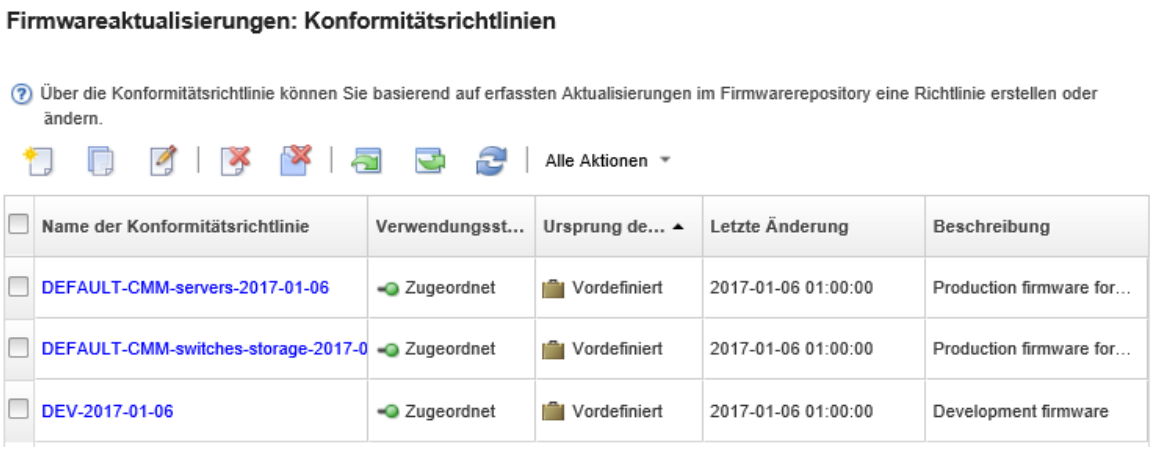
Rechenknoten möglicherweise nicht mehr konform. Wenn dies der Fall ist, aktualisiert XClarity Administrator die Seite Firmwareaktualisierungen: Übernehmen/Aktivieren, um zu zeigen, dass die Einheiten nicht konform sind, und generiert einen Alert.

Anmerkung: Sie können festlegen, dass Alerts für Einheiten angezeigt oder ausgeblendet werden, die die Anforderungen der ihnen zugewiesenen Firmwarekonformitätsrichtlinien nicht erfüllen (siehe Globale Einstellungen der Firmwareaktualisierungen konfigurieren). Alerts sind standardmäßig ausgeblendet.

Vorgehensweise

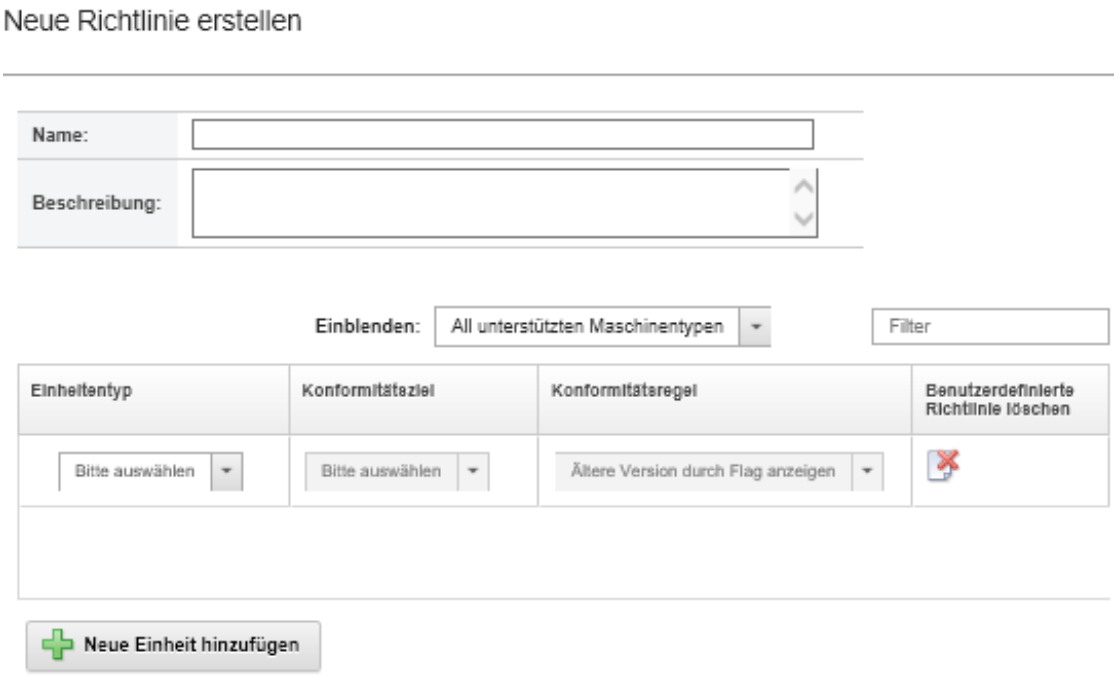
Führen Sie die folgenden Schritte aus, um eine Firmwarekonformitätsrichtlinie zu erstellen und zuzuordnen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Konformitätsrichtlinien**. Die Seite Konformitätsrichtlinie wird mit einer Liste aller vorhandenen Firmwarekonformitätsrichtlinien angezeigt.



Schritt 2. Erstellen Sie eine Firmwarekonformitätsrichtlinie.

1. Wählen Sie das Symbol **Erstellen** ( ) aus, um das Dialogfeld Neue Richtlinie erstellen anzuzeigen.



2. Geben Sie den Namen und die Beschreibung für die Firmwarekonformitätsrichtlinie ein.
3. Füllen Sie Tabelle basierend auf den folgenden Kriterien für jede Einheit aus.
   - **Einheitentyp**. Wählen Sie einen Typ von Einheit oder Komponente aus, für den diese Richtlinie übernommen werden soll.

     Tipp: Wenn Sie einen Server auswählen, wird die Konformitätsversion auf der UXSP-Ebene umgesetzt. Sie können jedoch auch den Server erweitern und bestimmte Firmwareversionen für die einzelnen Komponenten festlegen (beispielsweise Baseboard Management-Controller oder UEFI).
   - **Konformitätsziel**. Geben Sie das Konformitätsziel für die zutreffenden Zieleinheiten und Unterkomponenten an.

     Bei Servern können Sie einen der folgenden Werte auswählen.

     – **Standard**. Ändert das Konformitätsziel für jede Unterkomponente auf den Standardwert (z. B. zur aktuellen Firmware im Repository für diese Zieleinheit).

     – **Nicht aktualisieren**. Ändert das Konformitätsziel für jede Unterkomponente zu „Nicht aktualisieren“.

     Für Einheiten ohne Unterkomponenten (z. B. CMMs, Switches oder Speichereinheiten) oder Unterkomponenten in einem Server können Sie einen der folgenden Werte auswählen.

     – <*firmware_level*>. Gibt die Basis-Firmwareversion an.

     – **Nicht aktualisieren**. Gibt an, dass die Firmware nicht aktualisiert werden soll. Beachten Sie, dass die Firmware auf dem Sicherungs-Management-Controller nicht standardmäßig aktualisiert wird.

     Anmerkung: Wenn Sie die Standardwerte für eine Unterkomponente auf einem Server ändern, ändert sich das Konformitätsziel für diesen Zielserver zu **Angepasst**.
   - **Konformitätsregel**. Geben Sie an, wann eine Einheit in der Spalte **Installierte Version** in Firmware-Updates: Übernehmen/Aktivieren als nicht konform markiert wird.

     – **Ältere Version durch Flag anzeigen**. Wenn die auf einer Einheit installierte Firmwareversion niedriger als in der Firmwarekonformitätsrichtlinie angegeben ist, wird die Einheit als nicht konform markiert. Wenn Sie beispielsweise einen Netzwerkadapter in einem Rechenknoten ersetzen und die Firmware auf diesem Netzwerkadapter niedriger als die Version in der Firmwarekonformitätsrichtlinie ist, wird der Rechenknoten als nicht konform gekennzeichnet.

     – **Bei nicht exakter Übereinstimmung durch Flag anzeigen**. Wenn die auf einer Einheit installierte Firmwareversion nicht exakt der Firmwarekonformitätsrichtlinie entspricht, wird die Einheit als nicht konform markiert. Wenn Sie beispielsweise einen Netzwerkadapter in einem Rechenknoten ersetzen und die Firmware auf diesem Netzwerkadapter von der Version in der Firmwarekonformitätsrichtlinie abweicht, wird der Rechenknoten als nicht konform gekennzeichnet.

     – **Kein Flag**. Einheiten, die nicht konform sind, werden nicht gekennzeichnet.
4. **Optional:** Erweitern Sie den Systemtyp, um jedes Update im Paket anzuzeigen und die Firmwareversion für das Konformitätsziel auszuwählen oder wählen Sie „Nicht aktualisieren“ aus, um die Aktualisierung der Firmware auf dieser Einheit zu verhindern.
5. Klicken Sie auf **Erstellen**.

   Die Firmwarekonformitätsrichtlinie wird in der Tabelle auf der Seite Firmwareaktualisierungen: Konformitätsrichtlinie aufgeführt. Die Tabelle zeigt den Nutzungsstatus, den Ursprung der Richtlinie (benutzerdefiniert oder vordefiniert) und das letzte Änderungsdatum an.

Schritt 3. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**. Die Seite Firmwareaktualisierungen: anwenden/aktivieren wird mit einer Liste der verwalteten Einheiten angezeigt.

Schritt 4. Ordnen Sie die Firmwarekonformitätsrichtlinie Einheiten zu.

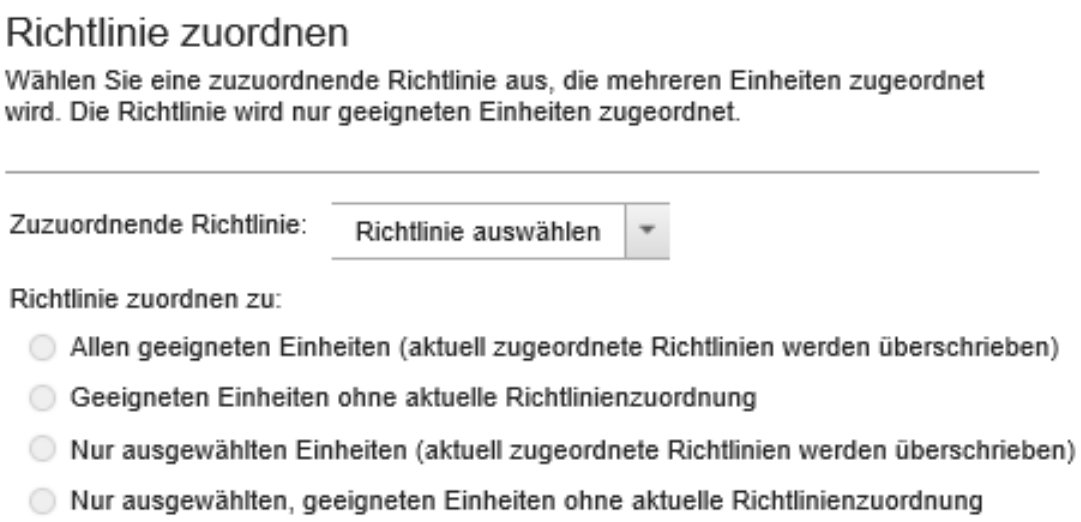
- **Für eine einzelne Einheit**

  Wählen Sie im Dropdown-Menü in der Spalte **Zugeordnete Konformitätsrichtlinie** eine Richtlinie für jede Einheit aus.

  Sie können aus einer Liste von Firmwarekonformitätsrichtlinien auswählen, die für die jeweilige Einheit anwendbar sind. Wenn der Einheit aktuell keine Richtlinie zugeordnet ist, wird die zugeordnete Richtlinie auf **Keine Zuordnung** festgelegt. Wenn keine Richtlinien für die Einheit anwendbar sind, wird die zugeordnete Richtlinie auf **Keine anwendbaren Richtlinien** festgelegt.

- **Für mehrere Einheiten**

  1. **Optional:** Wählen Sie eine oder mehrere Einheiten aus, zu denen Sie eine Firmwarekonformitätsrichtlinie zuweisen möchten.
  2. Klicken Sie auf das Symbol **Richtlinie zuordnen** ( ), um den Richtlinie zuordnen-Dialog anzuzeigen.

  3. Wählen Sie im Dropdown-Menü **Zuzuweisende Richtlinie** eine Firmwarekonformitätsrichtlinie aus.

     Sie können aus einer Liste von Firmwarekonformitätsrichtlinien auswählen, die für die ausgewählten Einheiten anwendbar sind. Wenn vor dem Öffnen des Dialogs keine Einheiten ausgewählt wurden, werden alle Richtlinien aufgelistet.

     Um die Zuordnung einer Richtlinie aufzuheben, wählen Sie **Keine Zuordnung** aus.

  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 Einheitenkriterium aus.
     - **Ohne zugewiesene Richtlinie**
     - **Nicht-konform (die aktuell zugeordnete Richtlinie wird überschrieben)**
     - **Konform (die aktuell zugeordnete Richtlinie wird überschrieben)**
     - **Nicht überwacht (die aktuell zugeordnete Richtlinie wird überschrieben)**

– **Andere (die aktuell zugeordnete Richtlinie wird überschrieben)** Dies gilt für Einheiten, die sich in einem anderen Status befinden, z. B. im Status „Ausstehend“, denen Daten fehlen oder die nicht für Aktualisierungen unterstützt werden. Bewegen Sie den Mauszeiger über das Hilfesymbol (), um eine Liste der geeigneten Einheiten anzuzeigen.

Anmerkung: Die Kriterien **Nicht überwacht** und **Andere** werden nur aufgelistet, wenn es Einheiten in diesen Status gibt.

6. Klicken Sie auf **OK**.

   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

Nachdem Sie eine Firmwarekonformitätsrichtlinie erstellt haben, führen Sie die folgenden Aktionen für eine ausgewählte Firmwarekonformitätsrichtlinie aus:

- Zeigen Sie Richtliniendetails an, einschließlich einer Liste der zugeordneten Einheiten, indem Sie auf den Richtliniennamen in der Tabelle klicken.
- Erstellen Sie ein Duplikat einer ausgewählten Richtlinie, indem Sie auf das Symbol **Kopieren** () klicken.
- Benennen Sie eine Richtlinie um oder ändern Sie sie, indem Sie auf das Symbol **Bearbeiten** () klicken. Sie können keine vordefinierten Firmwarekonformitätsrichtlinien oder Richtlinien bearbeiten, die verwalteten Einheiten zugeordnet sind.

  Wenn Sie eine zugewiesene Richtlinie so ändern, dass sie nicht mehr auf bestimmte zugewiesene Einheiten angewendet ist, wird die Zuordnung der Richtlinie zu diesen Einheiten automatisch aufgehoben.

  Sie können die vordefinierte **Aktuelle Firmwarerichtlinie** nicht umbenennen oder ändern.
- Löschen Sie eine ausgewählte Firmwarekonformitätsrichtlinie, indem Sie auf das Symbol **Richtlinie löschen** () klicken, oder löschen Sie die ausgewählte Firmwarekonformitätsrichtlinie und alle zugehörigen Firmwareaktualisierungen für die Richtlinie, indem Sie auf das Symbol **Alle Richtlinien und Firmwarepakete löschen** () klicken.Sie können die Richtlinie auch dann löschen, wenn sie einer Einheit zugeordnet ist.

  Wenn Sie eine Richtlinie löschen, die einer Einheit zugeordnet ist, wird die Zuordnung der Richtlinie vor dem Löschen entfernt.

  Die vordefinierte **Aktuelle Firmwarerichtlinie** kann nicht gelöscht werden. Sie können die Richtlinie jedoch deaktivieren, indem Sie auf das Symbol **Globale Einstellungen** () klicken und dann die Option **Aktuelle Firmwarerichtlinie deaktivieren** auswählen. Wenn diese Option ausgewählt ist, wird die Zuordnung der aktuellen Firmwarerichtlinie mit verwalteten Einheiten aufgehoben und die Richtlinie wird nicht mehr aktualisiert, damit sie die neuesten verfügbaren Firmwareversionen im Repository enthält.
- Exportieren Sie eine ausgewählte Richtlinie zu einem lokalen System, indem Sie die Richtlinien auswählen und auf das Symbol **Exportieren** () klicken. Sie können die Richtlinien in einer anderen XClarity Administrator-Instanz importieren, indem Sie auf das Symbol **Importieren** () klicken.

Nachdem Sie eine Firmwarekonformitätsrichtlinie erstellt haben, können Sie die Richtlinie zu einer bestimmten Einheit zuordnen (siehe Firmwarekonformitätsrichtlinien erstellen und zuordnen) und Aktualisierungen für diese Einheit übernehmen und aktivieren (siehe Firmwareaktualisierungen anwenden und aktivieren).

Einheiten, die nicht konform sind, identifizieren

Wenn eine Firmwarekonformitätsrichtlinie einer verwalteten Einheit zugeordnet wurde, können Sie ermitteln, ob die Firmware auf dieser Einheit mit dieser Richtlinie konform ist.

Vorgehensweise

Um festzustellen, ob die Firmware auf einer Einheit mit der zugewiesenen Firmwarekonformitätsrichtlinie konform ist, klicken Sie auf der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**, um die Seite Firmwareaktualisierung: Konformitätsrichtlinie anzuzeigen. Überprüfen Sie die Spalte **Installierte Versionen** für die Einheit.

Die Spalte **Installierte Versionen** enthält einen der folgenden Werte:

- **Firmwareversion**. Die auf der Einheit installierte Firmwareversion ist mit der zugewiesenen Richtlinie konform.
- **Konform**. Die auf der Einheit installierte Firmwareversion ist mit der zugewiesenen Richtlinie konform.
- **Nicht konform**. Die auf der Einheit installierte Firmwareversion ist nicht mit der zugewiesenen Richtlinie konform.
- **Keine Konformitätsrichtlinie festgelegt**. Der Einheit ist keine Firmwarekonformitätsrichtlinie zugeordnet.

Sie können auf das Symbol **Aktualisieren** ( ) klicken, um den Inhalt der Spalte **Installierte Version** zu aktualisieren.

Globale Einstellungen der Firmwareaktualisierungen konfigurieren

Globale Einstellungen dienen als Standardeinstellungen, wenn Firmwareaktualisierungen übernommen werden.

Zu dieser Aufgabe

Über die Seite „Globale Einstellungen“ können Sie die folgenden Einstellungen konfigurieren:
- Erweiterter Support für Einheiten mit einer älteren Version
- Alerts für Einheiten, die mit den zugeordneten Richtlinien nicht konform sind
- Automatische Zuordnung einer Firmwarekonformitätsrichtlinie zu einer Einheit, die über keine zugeordnete Richtlinie verfügt
- Nichtkonformitätsstatus für Einheiten mit einer Firmwarekomponente, die kein zugeordnetes Ziel in der Firmwarekonformitätsrichtlinie hat

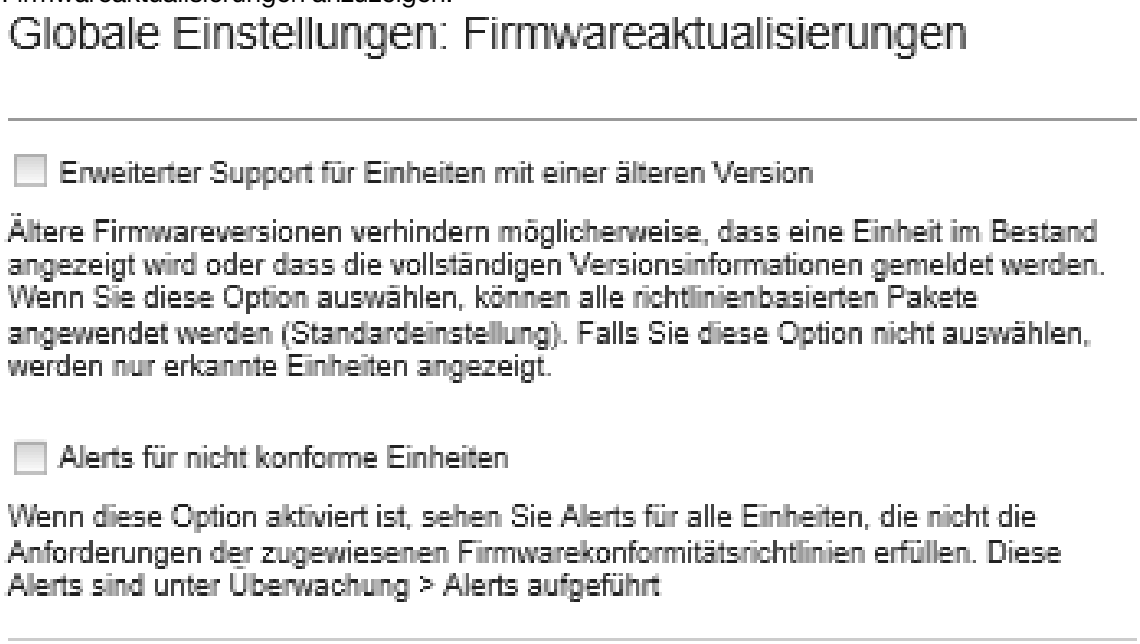
Vorgehensweise

So konfigurieren Sie die globalen Einstellungen, die für alle Server verwendet werden:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**. Die Seite Firmwareaktualisierungen: anwenden/aktivieren wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Aktualisierung mit Richtlinie** oder **Aktualisierung ohne Richtlinie**.

Schritt 3. Klicken Sie auf **Alle Aktionen → Globale Einstellungen**, um das Dialogfeld Globale Einstellungen: Firmwareaktualisierungen anzuzeigen.



Schritt 4. Wählen Sie optional die folgenden Optionen.

- Wählen Sie **Erweiterter Support für Einheiten mit einer älteren Version** aus, um den Bestand und vollständige Versionsinformationen für alle Einheiten anzuzeigen, selbst wenn die Firmware eine ältere ist oder die Einheit im Bestand fehlt.
- Wählen Sie **Alerts für nicht konforme Einheiten** aus, um auf der Seite „Alerts“ Alerts für Einheiten anzuzeigen, die die Anforderungen ihrer zugewiesenen Firmwarekonformitätsrichtlinien nicht erfüllen. Alerts werden auf der Seite „Alerts“ standardmäßig ausgeblendet. Weitere Informationen finden Sie unter Aktive Alerts anzeigen.
- Wählen Sie **Automatische Richtlinienzuordnung deaktivieren** aus, um die automatische Zuordnung einer Firmware-Konformitätsrichtlinie zu einer Einheit, die über keine zugeordnete Richtlinie verfügt, zu deaktivieren. Wenn diese Option nicht ausgewählt ist, werden die Firmware-Konformitätsrichtlinien Einheiten ohne Richtlinie zugewiesen, wenn XClarity Administrator neu gestartet wird oder wenn Sie eine neue Einheit verwalten.
- Wählen Sie **Nichtkonformität für Firmware ohne Ziel melden** aus, um Einheiten als nicht konform zu markieren, wenn eine Firmwareversion kein zugeordnetes Ziel in der Firmwarekonformitätsrichtlinie hat. Wenn diese Option nicht ausgewählt ist, werden Einheiten ohne Ziele als konform gekennzeichnet.

Schritt 5. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Firmwareaktualisierungen anwenden und aktivieren

Lenovo XClarity Administrator wendet Firmwareaktualisierungen nicht automatisch auf verwalteten Einheiten an. Sie können auswählen, ob Firmwareaktualisierungen mit oder ohne Konformitätsrichtlinien angewendet werden.

Vorbereitende Schritte

Wenn Sie Konformitätsrichtlinien verwenden, können Sie Aktualisierungen für mehrere Einheiten gleichzeitig planen. XClarity Administrator aktualisiert Einheiten automatisch in der richtigen Reihenfolge. Der CMM wird zuerst aktualisiert. Danach folgen die Switches, Server und Speichereinheiten.

Es können nur heruntergeladene Firmwareaktualisierungen angewendet werden.

Wenn Sie eine Firmwareaktualisierung ausführen, startet XClarity Administrator oder mehrere Jobs, um die Aktualisierung durchzuführen.

Während die Firmwareaktualisierung läuft, ist die Zieleinheit gesperrt. Sie können keine anderen Verwaltungsaufgaben auf der Zieleinheit starten, bis der Aktualisierungsprozess abgeschlossen ist.

Nachdem eine Firmwareaktualisierung auf eine Einheit angewendet wurde, sind möglicherweise einer oder mehrere Neustarts erforderlich, um die Firmwareaktualisierung vollständig zu aktivieren. Sie können auswählen, ob die Einheit zur Aktivierung sofort oder verzögert neu gestartet werden soll. Sie können die Aktivierung auch priorisieren. Wenn Sie den sofortigen Neustart wählen, minimiert XClarity Administrator die Anzahl der erforderlichen Neustarts. Wenn Sie die verzögerte Aktivierung wählen, werden die Aktualisierungen beim nächsten Neustart der Einheit aktiviert. Wenn Sie die priorisierte Aktivierung auswählen, werden die Aktualisierungen auf dem Baseboard Management Controller sofort aktiviert. Alle anderen Firmwareaktualisierungen werden das nächste Mal aktiviert, wenn die Einheit neu gestartet wird.

Sie können ausgewählte Firmware auf 50 Einheiten gleichzeitig aktualisieren. Wenn Sie ausgewählte Firmware auf mehr als 50 Einheiten aktualisieren möchten, werden die verbleibenden Einheiten in die Warteschlange gestellt. Eine in der Warteschlange befindliche Einheit wird aus der Warteschlange mit „ausgewählten Firmwareaktualisierungen“ entfernt, wenn entweder die Aktivierung auf einer aktualisierten Einheit abgeschlossen ist oder eine aktualisierte Einheit in den ausstehenden Wartungsmodus versetzt wird (wenn auf dieser Einheit ein Neustart erforderlich ist). Wenn eine Einheit, die sich im ausstehenden Wartungsmodus befindet, neu gestartet wird, bootet die Einheit in den Wartungsmodus und setzt den Aktualisierungsprozess fort, auch wenn die maximale Anzahl an Firmware-Aktualisierungen bereits ausgeführt wird.

Sie können Paket-Firmware auf max. 10 Einheiten gleichzeitig aktualisieren. Wenn Sie Paket-Firmware auf mehr als 10 Einheiten aktualisieren möchten, werden die verbleibenden Einheiten in die Warteschlange gestellt. Eine in der Warteschlange befindliche Einheit wird aus der Warteschlange mit „Paket-Firmwareaktualisierungen“ entfernt, wenn die Aktivierung auf einer Einheit abgeschlossen ist, auf der eine Paket-Firmwareaktualisierung durchgeführt wurde.

Achtung: Bei Red Hat® Enterprise Linux (RHEL) v7 und höher setzt ein Neustart des Betriebssystems über einen grafischen Modus den Server standardmäßig aus. Bevor Sie die Aktionen **Normal neu starten** oder **Sofort neu starten** von XClarity Administrator ausführen können, müssen Sie beim Betriebssystem manuell das Ausschalteverhalten des Netzschalters konfigurieren. Anweisungen hierzu finden Sie im Abschnitt Red Hat-Handbuch zur Datenmigration und -Verwaltung: Ändern des Verhaltens beim Drücken des Netzschalters im grafischen Zielmodus.

Anmerkung: Der XClarity Administrator aktiviert automatisch die LAN über USB-Schnittstelle.

Paket-Firmwareaktualisierungen unter Verwendung von Konformitätsrichtlinien übernehmen

Wenn Lenovo XClarity Administrator eine verwaltete Einheit als nicht konform erkennt, können Sie manuell die Firmwareaktualisierungen für *alle* Komponenten in ausgewählten ThinkSystem SR635 und SR655 Servern, die nicht mit der zugeordneten Firmwarekonformitätsrichtlinie konform sind, mithilfe eines Paket-Images übernehmen, das die entsprechenden Firmwareaktualisierungspakete enthält. Das *Paketimage* wird während des Aktualisierungsprozesses erstellt, indem alle Firmwareaktualisierungspakete aus der Konformitätsrichtlinie gesammelt werden.

Vorbereitende Schritte

- Lesen Sie die Hinweise zur Firmwareaktualisierung, bevor Sie versuchen, die Firmware auf verwalteten Einheiten zu aktualisieren (siehe Hinweise zur Firmwareaktualisierung).

- Einheiten, bei denen keine Aktualisierungen unterstützt werden, sind in der Ansicht zunächst ausgeblendet. Nicht unterstützte Einheiten können nicht für Aktualisierungen ausgewählt werden.
- Standardmäßig werden alle erkannten Komponenten als verfügbar für die Übernahme von Aktualisierungen aufgelistet. Möglicherweise verhindert jedoch eine ältere Firmwareversion, dass eine Komponente im Bestand aufgeführt wird bzw. dass vollständige Versionsinformationen angezeigt werden. Um alle zur Übernahme verfügbaren richtlinienbasierten Pakete aufzulisten, klicken Sie auf **Alle Aktionen → Globale Einstellungen** und wählen **Erweiterter Support für Einheiten mit einer älteren Version** aus. Mit dieser Option wird für die nicht erkannten Einheiten in der Spalte „Installierte Version“ „Weitere verfügbare Software“ aufgeführt. Siehe Globale Einstellungen der Firmwareaktualisierungen konfigurieren für weitere Informationen.

  Anmerkungen:

  – Die globalen Einstellungen können bei laufenden Aktualisierungen für verwaltete Einheiten nicht geändert werden.

  – Das Generieren der zusätzlichen Optionen dauert einige Minuten. Nach kurzer Zeit müssen Sie möglicherweise auf das Symbol **Aktualisieren** () klicken, um die Tabelle zu aktualisieren.
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.
- Das Übernehmen von Paket-Firmwareaktualisierungen wird nur für ThinkSystem SR635 und SR655 Server unterstützt.
- Das Anwenden von Paket-Firmwareaktualisierungen wird nur für IPv4-Adressen unterstützt. IPv6-Adressen werden nicht unterstützt.
- Stellen Sie sicher, dass jede Zieleinheit mindestens einmal auf das BS gebootet wurde, um die vollständigen Bestandsinformationen abzurufen.
- Zur Verwendung der Funktion für Paket-Aktualisierungen ist die Baseboard Management Controller-Firmware v2.94 oder höher erforderlich.
- Es werden nur Firmwareaktualisierungen aus Repository-Paketen oder einzelne Firmwareaktualisierungen verwendet. UpdateXpress System Packs (UXSPs) werden nicht unterstützt.
- Es werden nur heruntergeladene Firmwareaktualisierungen angewendet. Aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Firmwareaktualisierungen herunter (siehe Produktkatalog aktualisieren und Firmwareaktualisierungen werden heruntergeladen).

  Anmerkung: Bei der Erstinstallation von XClarity Administrator sind der Produktkatalog und das Repository leer.
- Die Konformitätsprüfung wird nur für Baseboard Management Controller und UEFI in ThinkSystem SR635 und SR655 Servern unterstützt. XClarity Administrator versucht jedoch, Firmwareaktualisierungen auf allen verfügbaren Hardwarekomponenten zu übernehmen.
- Aktualisierungen werden gemäß der zugeordneten Firmwarekonformitätsrichtlinie übernommen. Sie können nicht nur einen Teil der Komponenten aktualisieren.
- XClarity Administrator v3.2 oder höher ist erforderlich, um Firmwareaktualisierungen für Lenovo XClarity Provisioning Manager (LXPM), LXPM Windows-Treiber oder LXPM Linux-Treiber auf ThinkSystem SR635 und SR655 Servern zu übernehmen.
- Baseboard Management Controller- und UEFI-Aktualisierungen werden übersprungen, wenn die aktuell installierte Version höher als die zugeordnete Konformitätsrichtlinie ist.
- Firmwarekonformitätsrichtlinien müssen erstellt und den Einheiten zugeordnet werden, auf denen Sie die Firmwareaktualisierungen übernehmen möchten. Siehe Firmwarekonformitätsrichtlinien erstellen und zuordnen für weitere Informationen.

- Die ausgewählten Einheiten werden vor dem Start des Aktualisierungsprozesses ausgeschaltet. Vergewissern Sie sich, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf einen anderen Server verschoben wurden.

Achtung: Ausgewählte Einheiten werden vor dem Start des Aktualisierungsprozesses ausgeschaltet. Vergewissern Sie sich, dass alle aktiven Workloads entweder beendet wurden, oder – sofern Sie in einer virtuellen Umgebung arbeiten – auf einen anderen Server verschoben wurden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.

Zu dieser Aufgabe

Der Paket-Aktualisierungsprozess aktualisiert zuerst den Baseboard Management Controller und UEFI Außerband. Wenn diese Aktualisierungen abgeschlossen sind, erstellt der Prozess basierend auf dem Maschinentyp ein Paketimage der verbleibenden Firmware in der Konformitätsrichtlinie. Anschließend wird das Image vom Prozess an die ausgewählte Einheit angehängt und die Einheit wird zum Booten des Images neu gestartet. Das Image wird automatisch ausgeführt, um die verbleibenden Aktualisierungen durchzuführen.

Sie können Paket-Firmware auf max. 10 Einheiten gleichzeitig aktualisieren. Wenn Sie Paket-Firmware auf mehr als 10 Einheiten aktualisieren möchten, werden die verbleibenden Einheiten in die Warteschlange gestellt. Eine in der Warteschlange befindliche Einheit wird aus der Warteschlange mit „Paket-Firmwareaktualisierungen“ entfernt, wenn die Aktivierung auf einer Einheit abgeschlossen ist, auf der eine Paket-Firmwareaktualisierung durchgeführt wurde.

Wenn beim Aktualisieren einer Komponente in der Einheit ein Fehler auftritt, aktualisiert der Firmwareaktualisierungsprozess die Firmware der entsprechenden Komponente nicht. Der Firmwareaktualisierungsprozess wird jedoch zur Aktualisierung aller anderen Komponenten in der Einheit und aller anderen Einheiten im aktuellen Firmwareaktualisierungsjob fortgesetzt.

Vorgehensweise

Gehen Sie wie folgt vor, um Firmwareaktualisierungen in Form eines Paketimages auf verwalteten Einheiten durchzuführen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**. Die Seite Firmwareaktualisierungen: anwenden/aktivieren wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Aktualisierung mit Richtlinie**.

Schritt 3. Wählen Sie eine oder mehrere Einheiten und Komponenten aus, für die die Firmwareaktualisierungen übernommen werden sollen.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Einheiten zu erleichtern. Darüber hinaus können Sie die Liste der angezeigten Einheiten filtern, indem Sie eine Option im Menü **Anzeigen** auswählen, um nur Einheiten in einem bestimmten Gehäuse, Rack oder in einer bestimmten Gruppe anzuzeigen, Text im Feld **Filter** eingeben (z. B. einen Namen oder eine IP-Adresse) oder auf eines der folgenden Symbole klicken, um nur Einheiten mit einem bestimmten Status anzuzeigen.

- Symbol **Konforme Einheiten ausblenden** ()
- Symbol **Nicht konformen Einheitenstatus ausblenden** ()
- Symbol **Einheiten ohne zugewiesene Konformitätsrichtlinien ausblenden** ()
- Symbol **Nicht überwachte Einheiten ausblenden** ()

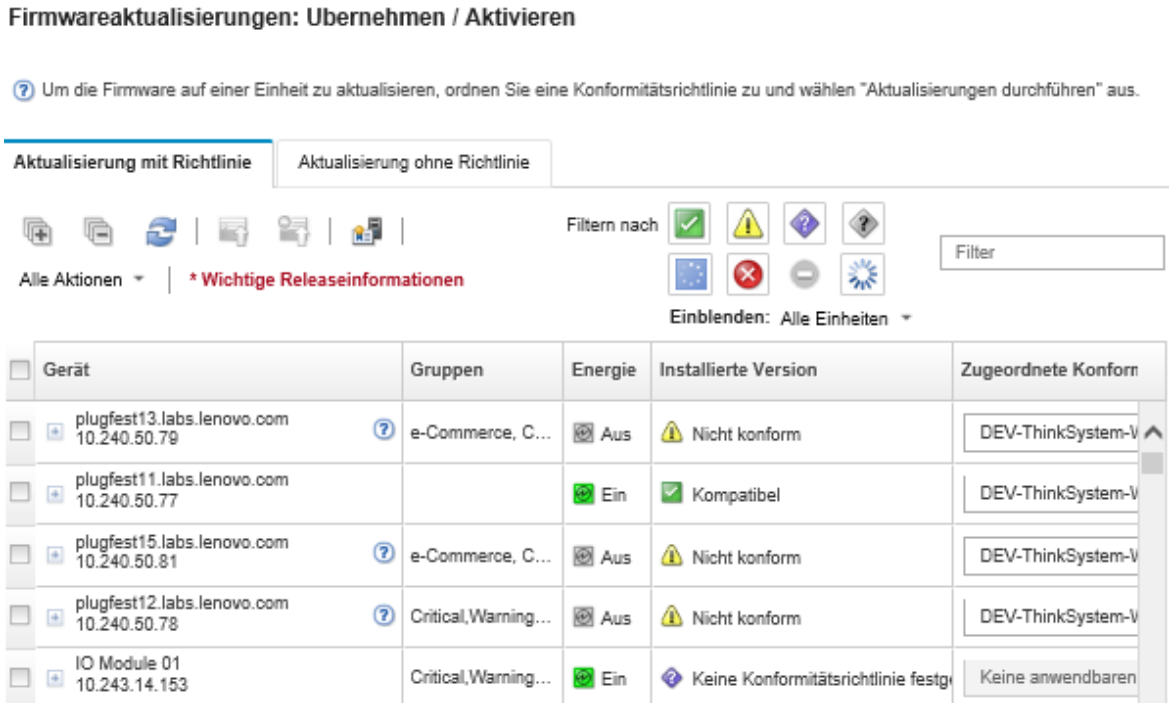
- Symbol **Einheiten mit ausstehender Firmwareaktivierung ausblenden** ( )
- Symbol **Einheiten mit fehlerhafter Konformität ausblenden** ( )
- Symbol **Nicht für Aktualisierung unterstützte Einheiten ausblenden** ( )
- Symbol **Einheiten, die einer Firmwareaktualisierung unterzogen werden, ausblenden** ( )
- **Geräte mit nicht ladbarer Firmware ausblenden** Symbol ( )

Die Spalte **Gruppen** gibt die Gruppen an, zu denen jede Einheit gehört. Sie können den Mauszeiger über die Spalte **Gruppen** bewegen, um eine vollständige Liste der Gruppen nach Gruppentyp abzurufen.

Die Spalte **Installierte Version** gibt die installierte Firmwareversion, den Konformitätsstatus oder den Status der Einheit an.

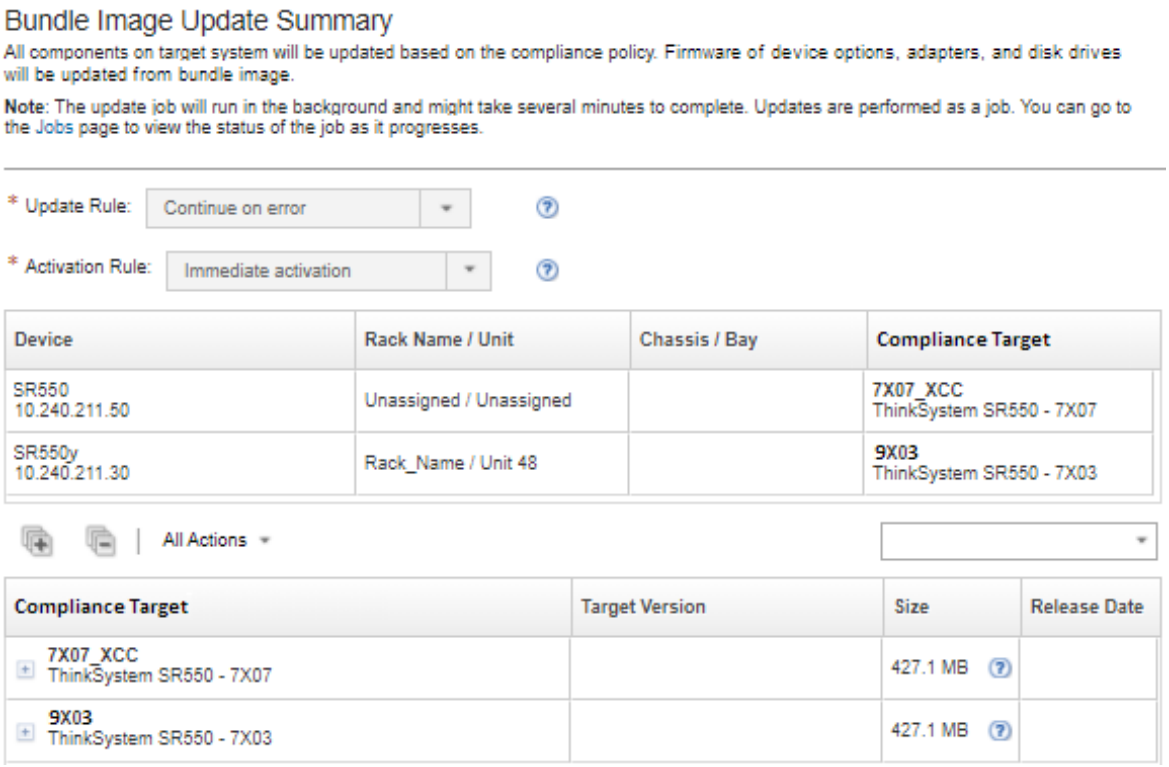
Der Konformitätsstatus kann einer der folgenden sein:
- **Konform**
- **Fehlerhafte Konformität**
- **Nicht konform**
- **Keine Konformitätsrichtlinie festgelegt**
- **Nicht überwacht**

Der Einheitenstatus kann einer der folgenden sein:
- **Aktualisierungen werden nicht unterstützt**
- **Aktualisierung wird ausgeführt**



Schritt 4. Klicken Sie auf das Symbol **Aktualisierung aus Paketimage durchführen** ( ). Das Dialogfenster Zusammenfassung der Paketimage-Aktualisierung wird angezeigt. In diesem Dialogfenster werden

die ausgewählten Einheiten und Firmwareaktualisierungen aufgeführt, die im Paketimage enthalten sind.



Schritt 5. Klicken Sie auf **Aktualisierung aus Paketimage durchführen**, um sofort zu aktualisieren, oder klicken Sie auf **Zeitplan**, um diese Aktualisierung geplant zu einem späteren Zeitpunkt auszuführen.

Nach dieser Aufgabe

Versuchen Sie erneut die Aktualisierung zu übernehmen, wenn der Wechsel zum Wartungsmodus bei einem Server beim Übernehmen einer Firmwareaktualisierung fehlschlägt.

Wenn Aktualisierungen nicht erfolgreich abgeschlossen werden, finden Sie unter Probleme bei Firmwareaktualisierung und Repository in der Onlinedokumentation von XClarity Administrator Informationen zur Fehlerbehebung und Korrekturmaßnahmen.

Sie können über die Seite „Firmwareaktualisierung: Übernehmen/Aktivieren“ die folgenden Aktionen ausführen.

- Exportieren Sie Firmware- und Konformitätsinformationen für jede verwaltete Einheit, indem Sie auf **Alle Aktionen → Ansicht als CSV exportieren** klicken.

  Anmerkung: Die CSV-Datei enthält nur gefilterte Informationen in der aktuellen Ansicht. Informationen, die aus der Ansicht gefiltert und in den Spalten ausgeblendet wurden, werden hier nicht aufgeführt.

- Indem Sie die Einheit auswählen und auf das Symbol **Aktualisierung abbrechen** klicken ( ), können Sie eine laufende Aktualisierung für eine Einheit abbrechen.

  Anmerkung: Sie können Firmwareaktualisierungen in der Warteschlange abbrechen. Nach dem Beginn des Aktualisierungsprozesses kann die Firmwareaktualisierung nur abgebrochen werden, wenn der Aktualisierungsprozess eine Task durchführt, die nicht die Durchführung der Aktualisierung ist, z. B. der Wechsel in den Wartungsmodus oder der Neustart der Einheit.

- Sie können den Status der Firmwareaktualisierung direkt über die Seite Übernehmen/Aktivieren in der Spalte **Status** anzeigen.
- Sie können den Status des Aktualisierungsprozesses im Jobprotokoll überwachen. Klicken Sie im Lenovo XClarity Administrator-Menü auf **Überwachung → Jobs**.

  Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

  Wenn die Firmwareaktualisierungsjobs abgeschlossen sind, können Sie sicherstellen, dass die Einheiten kompatibel sind. Klicken Sie hierzu auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**, um zur Seite Firmwareaktualisierungen: anwenden/aktivieren zu wechseln, und klicken Sie auf das Symbol **Aktualisieren** ( ). Die aktuelle, auf der jeweiligen Einheit aktive Firmwareversion wird in der Spalte **Installierte Version** angezeigt.

Ausgewählte Firmwareaktualisierungen unter Verwendung von Konformitätsrichtlinien übernehmen

Wenn Lenovo XClarity Administrator eine Einheit als nicht konform erkennt, können Sie die Firmwareaktualisierungen für diese verwaltete Einheit manuell übernehmen und aktivieren. Sie können alle für eine Firmwarekonformitätsrichtline geltenden Firmwareaktualisierungen oder nur bestimmte Firmwareaktualisierungen einer Richtlinie übernehmen und aktivieren. Es werden nur heruntergeladene Firmwareaktualisierungen angewendet.

Weitere Informationen:

- XClarity Administrator: Effizienz bei der Aktualisierung von Firmware steigern
- Lenovo ThinkSystem Firmware- und Treiberaktualisierung Best Practices
- XClarity Administrator: Bare Metal zu Cluster
- XClarity Administrator: Firmwareaktualisierungen
- XClarity Administrator: Firmwaresicherheitsaktualisierungen bereitstellen

Vorbereitende Schritte

- Lesen Sie die Hinweise zur Firmwareaktualisierung, bevor Sie versuchen, die Firmware auf verwalteten Einheiten zu aktualisieren (siehe Hinweise zur Firmwareaktualisierung).

- Einheiten, bei denen keine Aktualisierungen unterstützt werden, sind in der Ansicht zunächst ausgeblendet. Nicht unterstützte Einheiten können nicht für Aktualisierungen ausgewählt werden.
- Standardmäßig werden alle erkannten Komponenten als verfügbar für die Übernahme von Aktualisierungen aufgelistet. Möglicherweise verhindert jedoch eine ältere Firmwareversion, dass eine Komponente im Bestand aufgeführt wird bzw. dass vollständige Versionsinformationen angezeigt werden. Um alle zur Übernahme verfügbaren richtlinienbasierten Pakete aufzulisten, klicken Sie auf **Alle Aktionen → Globale Einstellungen** und wählen **Erweiterter Support für Einheiten mit einer älteren Version** aus. Mit dieser Option wird für die nicht erkannten Einheiten in der Spalte „Installierte Version“ „Weitere verfügbare Software“ aufgeführt. Siehe Globale Einstellungen der Firmwareaktualisierungen konfigurieren für weitere Informationen.

  Anmerkungen:

  – Die globalen Einstellungen können bei laufenden Aktualisierungen für verwaltete Einheiten nicht geändert werden.

  – Das Generieren der zusätzlichen Optionen dauert einige Minuten. Nach kurzer Zeit müssen Sie möglicherweise auf das Symbol **Aktualisieren** () klicken, um die Tabelle zu aktualisieren.
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.
- Stellen Sie sicher, dass das Repository für Firmwareaktualisierungen die Firmwarepakete enthält, die Sie implementieren möchten. Ist dies nicht der Fall, so aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Firmwareaktualisierungen herunter (siehe Produktkatalog aktualisieren und Firmwareaktualisierungen werden heruntergeladen).

  Anmerkung: Bei der Erstinstallation von XClarity Administrator sind der Produktkatalog und das Repository leer.

  Wenn Sie erforderliche Firmware installieren möchten, stellen Sie sicher, dass die erforderliche Firmware ebenfalls in das Repository heruntergeladen wird.

  In einigen Fällen können mehrere Versionen für die Aktualisierung der Firmware erforderlich sein, dann müssen alle Versionen in das Repository heruntergeladen werden. Beispielsweise müssen Sie für eine Aktualisierung des skalierbaren IBM FC5022 SAN-Switches von v7.4.0a auf v8.2.0a zuerst v8.0.1-pha, dann v8.1.1 und abschließend v8.2.0a installieren. Alle drei Versionen müssen im Repository sein, um den Switch auf v8.2.0a zu aktualisieren.
- Um die Firmwareaktualisierungen zu aktivieren, müssen die Einheiten normalerweise neu gestartet werden. Wenn Sie die Einheit 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 einen anderen Server verschoben wurden.
- Für ThinkSystem SR635 und SR655 Server können Sie auch diese herkömmliche Aktualisierungsfunktion verwenden, um nur Firmwareaktualisierungen für Baseboard Management Controller und UEFI zu übernehmen. Die Management Controller-Firmwareversion AMBT10M oder höher und die UEFI-Firmwareversion CFE114L oder höher sind erforderlich. Zur Aktualisierung aller Komponenten (einschließlich Management Controller, UEFI, Plattenlaufwerken und E/A-Zusatzeinrichtungen) verwenden Sie die Paket-Aktualisierungsfunktion (siehe Paket-Firmwareaktualisierungen unter Verwendung von Konformitätsrichtlinien übernehmen).

Zu dieser Aufgabe

- Sie können ausgewählte Firmware auf 50 Einheiten gleichzeitig aktualisieren. Wenn Sie ausgewählte Firmware auf mehr als 50 Einheiten aktualisieren möchten, werden die verbleibenden Einheiten in die Warteschlange gestellt. Eine in der Warteschlange befindliche Einheit wird aus der Warteschlange mit „ausgewählten Firmwareaktualisierungen“ entfernt, wenn entweder die Aktivierung auf einer aktualisierten

Einheit abgeschlossen ist oder eine aktualisierte Einheit in den ausstehenden Wartungsmodus versetzt wird (wenn auf dieser Einheit ein Neustart erforderlich ist). Wenn eine Einheit, die sich im ausstehenden Wartungsmodus befindet, neu gestartet wird, bootet die Einheit in den Wartungsmodus und setzt den Aktualisierungsprozess fort, auch wenn die maximale Anzahl an Firmware-Aktualisierungen bereits ausgeführt wird.

- Sie können Firmware übernehmen und aktivieren, die neuer als die installierte Firmware ist.
- Sie können außerdem alle Aktualisierungen für eine bestimmte Einheit übernehmen. Sie können jedoch auch eine Einheit erweitern, um Aktualisierungen für bestimmte Komponenten festzulegen (beispielsweise Baseboard Management Controller oder UEFI).
- Wenn Sie ein Firmwareaktualisierungspaket mit Aktualisierungen für verschiedene Komponenten installieren, werden alle Komponenten, für die das Aktualisierungspaket übernommen wird, aktualisiert.

Vorgehensweise

So übernehmen und aktivieren Sie Aktualisierungen auf verwalteten Einheiten:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**. Die Seite Firmwareaktualisierungen: anwenden/aktivieren wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Aktualisierung mit Richtlinie**.

Schritt 3. Wählen Sie eine oder mehrere Komponenten und Einheiten aus, für die die Firmwareaktualisierungen übernommen werden sollen.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Darüber hinaus können Sie die Liste der angezeigten Einheiten filtern, indem Sie eine Option im Menü **Anzeigen** auswählen, um nur Einheiten in einem bestimmten Gehäuse, Rack oder in einer bestimmten Gruppe anzuzeigen, Text im Feld **Filter** eingeben (z. B. einen Namen oder eine IP-Adresse) oder auf eines der folgenden Symbole klicken, um nur Einheiten mit einem bestimmten Status anzuzeigen.

- Symbol **Konforme Einheiten ausblenden** ()
- Symbol **Nicht konformen Einheitenstatus ausblenden** ()
- Symbol **Einheiten ohne zugewiesene Konformitätsrichtlinien ausblenden** ()
- Symbol **Nicht überwachte Einheiten ausblenden** ()
- Symbol **Einheiten mit ausstehender Firmwareaktivierung ausblenden** ()
- Symbol **Einheiten mit fehlerhafter Konformität ausblenden** ()
- Symbol **Nicht für Aktualisierung unterstützte Einheiten ausblenden** ()
- Symbol **Einheiten, die einer Firmwareaktualisierung unterzogen werden, ausblenden** ()
- **Geräte mit nicht ladbarer Firmware ausblenden** Symbol ()

Die Spalte **Gruppen** gibt die Gruppen an, zu denen jede Einheit gehört. Sie können den Mauszeiger über die Spalte **Gruppen** bewegen, um eine vollständige Liste der Gruppen nach Gruppentyp abzurufen.

Die Spalte **Installierte Version** gibt die installierte Firmwareversion, den Konformitätsstatus oder den Status der Einheit an.

Der Konformitätsstatus kann einer der folgenden sein:

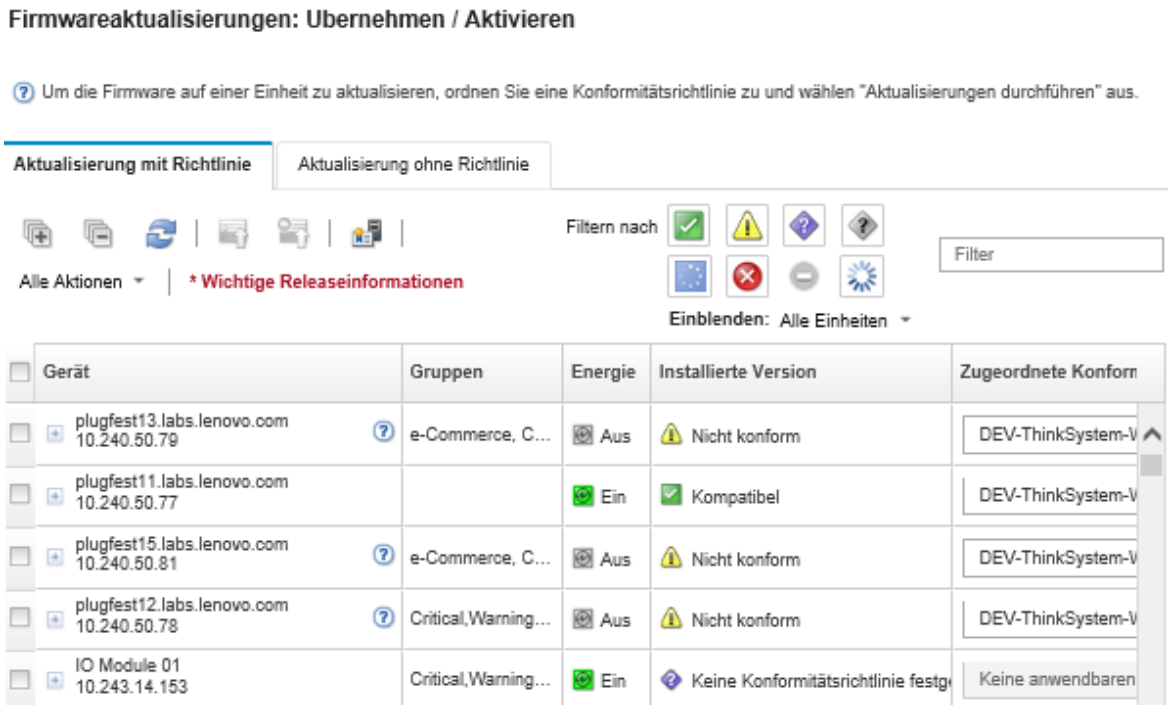
- **Konform**
- **Fehlerhafte Konformität**
- **Nicht konform**
- **Keine Konformitätsrichtlinie festgelegt**
- **Nicht überwacht**

Der Einheitenstatus kann einer der folgenden sein:

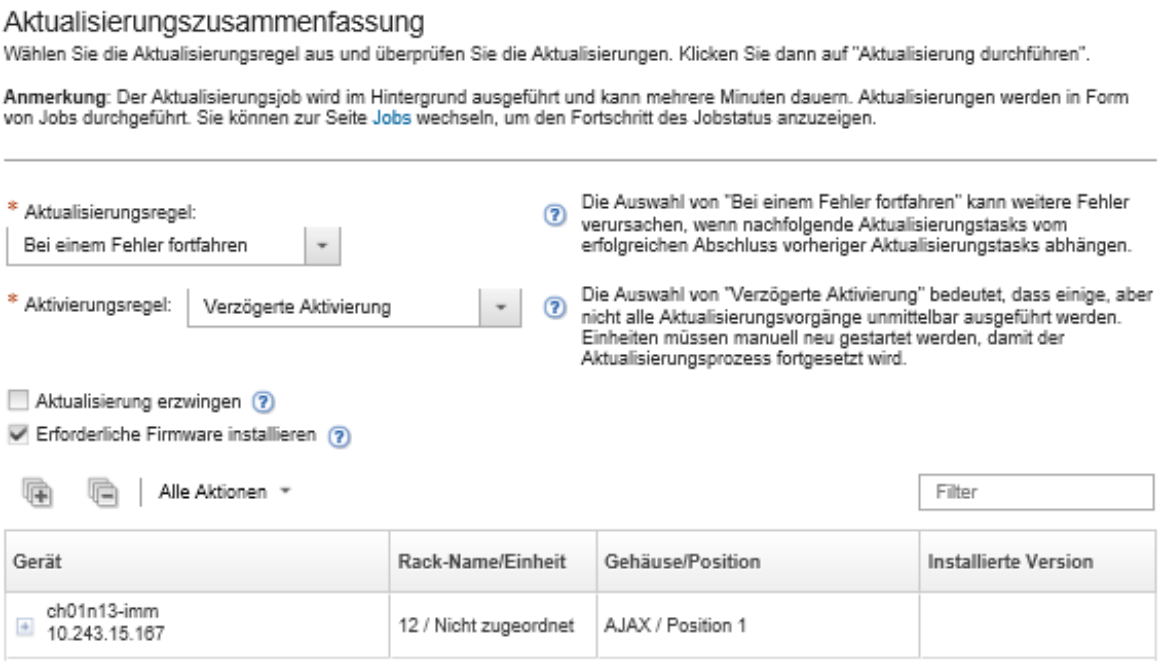
- **Aktualisierungen werden nicht unterstützt**
- **Aktualisierung wird ausgeführt**

Anmerkungen: Wenn die Aktivierung der installierten Firmwareversion aussteht, wird „(ausstehende Aktivierung)“ an die installierte Firmwareversion oder den Konformitätsstatus jeder Einheit angehängt, z. B. „2.20 / A9E12EUS (ausstehende Aktivierung)“. Um den Status „Ausstehende Aktivierung“ anzeigen zu können, muss die folgende Firmwareversion auf dem primären BMC (Baseboard Management Controller) des Servers installiert sein.

- **IMM2**: TCOO46F, TCOO46E oder höher (abhängig von der Plattform)
- **XCC**: CDI328M, PSI316N, TEI334I oder höher (abhängig von der Plattform)



Schritt 4. Klicken Sie auf das Symbol **Aktualisierungen durchführen** ( ). Das Dialogfenster Aktualisierungszusammenfassung wird angezeigt.



Schritt 5. Wählen Sie eine der folgenden Aktualisierungsregeln aus

- **Alle Aktualisierungen bei einem Fehler anhalten.** Wenn bei der Aktualisierung einer der Komponenten (wie einem Adapter oder Management-Controller) in der Zieleinheit ein Fehler auftritt, stoppt die Firmwareaktualisierung für alle ausgewählten Einheiten im aktuellen Firmwareaktualisierungsjob. In diesem Fall wird keine der Aktualisierungen im Aktualisierungspaket für die Einheit übernommen. Die aktuelle, auf allen ausgewählten Systemen installierte Firmware bleibt erhalten.
- **Bei einem Fehler fortfahren**. Wenn beim Aktualisieren einer der Komponenten in der Einheit ein Fehler auftritt, aktualisiert der Firmwareaktualisierungsprozess die Firmware der entsprechenden Komponente nicht. Der Firmwareaktualisierungsprozess wird jedoch zur Aktualisierung aller anderen Komponenten in der Einheit und aller anderen Einheiten im aktuellen Firmwareaktualisierungsjob fortgesetzt.
- **Bei einem Fehler zum nächsten System wechseln**. Wenn beim Aktualisieren einer der Komponenten in der Einheit ein Fehler auftritt, stoppt der Firmwareaktualisierungsprozess alle Versuche, die Firmware für die entsprechende Komponente zu aktualisieren. Die aktuell auf der Einheit installierte Firmware bleibt also bestehen. Der Firmwareaktualisierungsprozess fährt mit der Aktualisierung aller anderen Einheiten im aktuellen Firmwareaktualisierungsjob fort.

Schritt 6. Wählen Sie eine der folgenden Aktivierungsregeln aus:

- **Sofortige Aktivierung**. Während des Aktualisierungsprozesses wird die Einheit möglicherweise mehrmals automatisch neu gestartet, bis der gesamte Prozess abgeschlossen ist. Sorgen Sie dafür, dass alle Anwendungen für die Einheit vor dem Fortfahren beendet sind.
- **Verzögerte Aktivierung**. Es werden einige, aber nicht alle Aktualisierungsvorgänge ausgeführt. Einheiten müssen 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 eine Einheit aus irgendeinem Grund neu startet, wird der verzögerte Aktualisierungsprozess abgeschlossen.

Diese Aktivierungsregel wird nur für Server und Rack-Switches unterstützt. CMMs und Flex-Switches werden unabhängig von dieser Einstellung sofort aktiviert.

Es wird ein Ereignis ausgelöst, wenn der Status zum **Firmware-Wartungsmodus „Ausstehend“** wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.

Der verzögerte Aktualisierungsprozess wird abgeschlossen, wenn die Einheit aus irgendeinem Grund neu gestartet wird (einschließlich eines manuellen Neustarts). Es gibt kein Zeitlimit für den Neustart des Servers.

XClarity Administrator kann Aktualisierungen mit verzögerter Aktivierung für bis zu 50 Einheiten gleichzeitig übernehmen. Wenn Sie versuchen, Aktualisierungen mit verzögerter Aktivierung für mehr als 50 Einheiten anzuwenden, werden die verbleibenden Einheiten in eine Warteschlange gestellt. Eine Einheit verlässt die Warteschlange, wenn sich der Status einer zu aktualisierenden Einheit in den **Firmware-Wartungsmodus „Ausstehend“** ändert.

Wichtig:

- Wenn XClarity Administrator während des Aktualisierungsjobs neu gestartet wird, wird der Aktualisierungsjob mit einem Fehler beendet.
- Wenn ein Server im Status **Firmware-Wartungsmodus „Ausstehend“** neu gestartet wird, während XClarity Administrator nicht aktiv oder nicht erreichbar ist, bootet der Server zur BMU. Da XClarity Administrator jedoch keine Verbindung mit der BMU herstellen kann und es nach 60 Sekunden zu einer Zeitlimitüberschreitung kommt, wird der Stromversorgungsstatus des Systems vom Baseboard Management Controller wiederhergestellt (wird ausgeschaltet, wenn er ausgeschaltet war; wird neu gestartet, wenn er eingeschaltet war).

- **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. Diese Regel wird nur für Server unterstützt.

  Es wird ein Ereignis ausgelöst, wenn der Status zum Firmware-Wartungsmodus „Ausstehend“ wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.

Anmerkung: Wenn die Wake-On-LAN-Bootoption aktiviert ist, kann sie beim Ausschalten des Servers zu Konflikten mit XClarity Administrator führen. Dies gilt auch für Firmwareaktualisierungen, bei denen ein Wake-On-LAN-Client im Netzwerk „Aktivierung durch Magic Packet“-Befehle sendet.

Schritt 7. **Optional:** Wählen Sie **Update 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.

Anmerkung: Sie können ältere Firmwareversionen auf Einheitenoptionen, Adaptern und Laufwerken übernehmen, die das Herabsetzen unterstützen. In der Hardwaredokumentation erfahren Sie, ob Herabsetzen unterstützt wird.

Schritt 8. **Optional:** Deaktivieren Sie **Erforderliche Firmware installieren**, wenn Sie nicht möchten, dass erforderliche Firmware installiert wird. Erforderliche Firmware wird standardmäßig installiert.

Anmerkung: Bei der Verwendung von **Verzögerte Aktivierung** oder **Priorisierte Aktivierung** für erforderliche Firmwareaktualisierungen müssen Sie den Server möglicherweise neu starten, um die erforderliche Firmware zu aktivieren. Nach dem ersten Neustart werden die verbleibenden Firmwareaktualisierungen mit **Sofortige Aktivierung** installiert.

Schritt 9. **Optional:** Wenn Sie **Sofortige Aktivierung** ausgewählt haben, wählen Sie **Hauptspeichertest**, um einen Hauptspeichertest nach Abschluss der Firmware-Aktualisierung durchzuführen, wenn der Server während der Aktualisierung neu gestartet wird.

Diese Option wird für ThinkSystem v1- und v2-Server unterstützt (ausgenommen ThinkSystem Server SR635, SR645, SR655, SR665).

Schritt 10. Klicken Sie auf **Aktualisierung durchführen**, um sofort zu aktualisieren, oder klicken Sie auf **Zeitplan**, um diese Aktualisierung geplant zu einem späteren Zeitpunkt auszuführen.

Bei Bedarf können Sie Stromversorgungsaktionen auf den verwalteten Einheiten durchführen. Die Stromversorgungsaktionen sind hilfreich, wenn **Verzögerte Aktivierung** ausgewählt ist und Sie die Aktualisierungen weiterlaufen lassen möchten, sobald sich die Einheit im Status „Ausstehende Wartung“ befindet. Um eine Stromversorgungsaktion auf einer verwalteten Einheit über diese Seite auszuführen, klicken Sie auf **Alle Aktionen → Stromversorgungsaktionen** und wählen Sie dann eine der folgenden Stromversorgungsaktionen aus.

- **Einschalten**
- **Betriebssystem herunterfahren und ausschalten**
- **Ausschalten**
- **Betriebssystem herunterfahren und neu starten**
- **Neustart**

Nach dieser Aufgabe

Versuchen Sie erneut die Aktualisierung zu übernehmen, wenn der Wechsel zum Wartungsmodus bei einem Server beim Übernehmen einer Firmwareaktualisierung fehlschlägt.

Wenn Aktualisierungen nicht erfolgreich abgeschlossen werden, finden Sie unter Probleme bei Firmwareaktualisierung und Repository in der Onlinedokumentation von XClarity Administrator Informationen zur Fehlerbehebung und Korrekturmaßnahmen.

Sie können über die Seite „Firmwareaktualisierung: Übernehmen/Aktivieren“ die folgenden Aktionen ausführen:

- Exportieren Sie Firmware- und Konformitätsinformationen für jede verwaltete Einheit, indem Sie auf **Alle Aktionen → Ansicht als CSV exportieren** klicken.

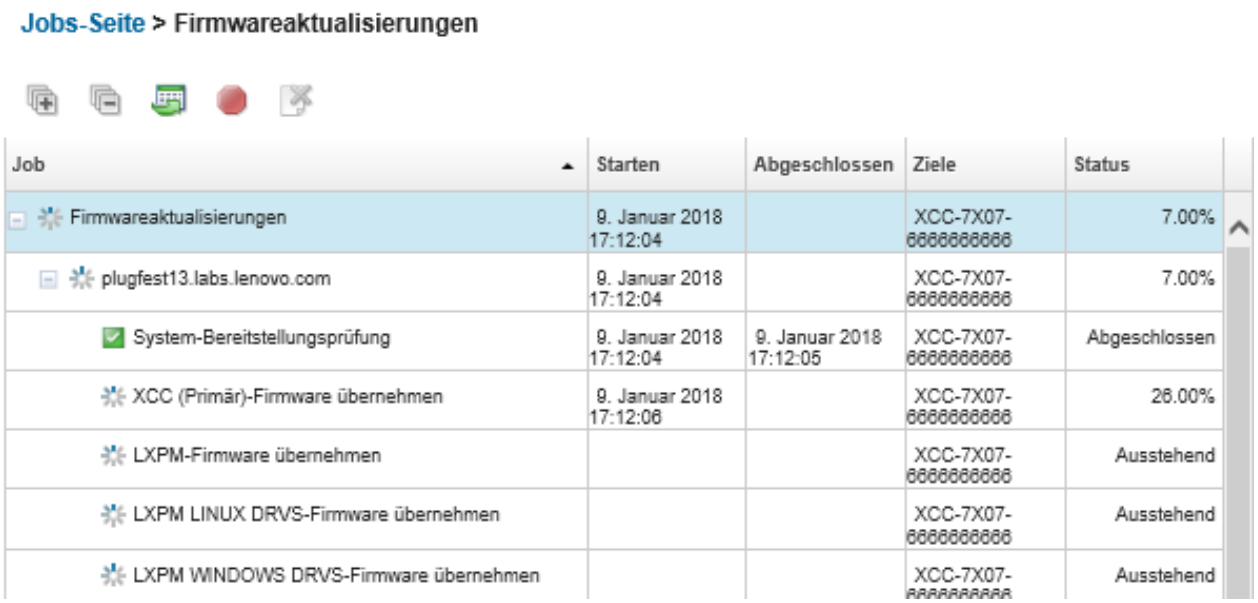
  Anmerkung: Die CSV-Datei enthält nur gefilterte Informationen in der aktuellen Ansicht. Informationen, die aus der Ansicht gefiltert und in den Spalten ausgeblendet wurden, werden hier nicht aufgeführt.

- Indem Sie die Einheit auswählen und auf das Symbol **Aktualisierung abbrechen** klicken (), können Sie eine laufende Aktualisierung für eine Einheit abbrechen.

  Anmerkung: Sie können Firmwareaktualisierungen in der Warteschlange abbrechen. Nach dem Beginn des Aktualisierungsprozesses kann die Firmwareaktualisierung nur abgebrochen werden, wenn der Aktualisierungsprozess eine Task durchführt, die nicht die Durchführung der Aktualisierung ist, z. B. der Wechsel in den Wartungsmodus oder der Neustart der Einheit.

- Sie können den Status der Firmwareaktualisierung direkt über die Seite Übernehmen/Aktivieren in der Spalte **Status** anzeigen.
- Sie können den Status des Aktualisierungsprozesses im Jobprotokoll überwachen. Klicken Sie im Lenovo XClarity Administrator-Menü auf **Überwachung → Jobs**.

  Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.



Wenn die Firmwareaktualisierungsjobs abgeschlossen sind, können Sie sicherstellen, dass die Einheiten kompatibel sind. Klicken Sie hierzu auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**, um zur Seite Firmwareaktualisierungen: anwenden/aktivieren zu wechseln, und klicken Sie auf das Symbol **Aktualisieren** ( ). Die aktuelle, auf der jeweiligen Einheit aktive Firmwareversion wird in der Spalte **Installierte Version** angezeigt.

Ausgewählte Firmwareaktualisierungen ohne die Verwendung von Konformitätsrichtlinien übernehmen

Sie können Firmware, bei der es sich um eine spätere Version als die aktuell installierte handelt, auf einer einzelnen verwalteten Einheit übernehmen und aktivieren, ohne die Konformitätsrichtlinien zu verwenden.

Weitere Informationen:

- XClarity Administrator: Effizienz bei der Aktualisierung von Firmware steigern
- Lenovo ThinkSystem Firmware- und Treiberaktualisierung Best Practices
- XClarity Administrator: Bare Metal zu Cluster
- XClarity Administrator: Firmwareaktualisierungen
- XClarity Administrator: Firmwaresicherheitsaktualisierungen bereitstellen

Vorbereitende Schritte

- Lesen Sie die Hinweise zur Firmwareaktualisierung, bevor Sie versuchen, die Firmware auf verwalteten Einheiten zu aktualisieren (siehe Hinweise zur Firmwareaktualisierung).
- Einheiten, bei denen keine Aktualisierungen unterstützt werden, sind in der Ansicht zunächst ausgeblendet. Nicht unterstützte Einheiten können nicht für Aktualisierungen ausgewählt werden.
- Standardmäßig werden alle erkannten Komponenten als verfügbar für die Übernahme von Aktualisierungen aufgelistet. Möglicherweise verhindert jedoch eine ältere Firmwareversion, dass eine Komponente im Bestand aufgeführt wird bzw. dass vollständige Versionsinformationen angezeigt werden. Um alle zur Übernahme verfügbaren richtlinienbasierten Pakete aufzulisten, klicken Sie auf **Alle Aktionen → Globale Einstellungen** und wählen **Erweiterter Support für Einheiten mit einer älteren Version** aus. Mit dieser Option wird für die nicht erkannten Einheiten in der Spalte „Installierte Version“ „Weitere verfügbare Software“ aufgeführt. Siehe Globale Einstellungen der Firmwareaktualisierungen konfigurieren für weitere Informationen.

Anmerkungen:

- Die globalen Einstellungen können bei laufenden Aktualisierungen für verwaltete Einheiten nicht geändert werden.
- Das Generieren der zusätzlichen Optionen dauert einige Minuten. Nach kurzer Zeit müssen Sie möglicherweise auf das Symbol **Aktualisieren** () klicken, um die Tabelle zu aktualisieren.

- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Wenn gerade Jobs ausgeführt werden, wird der Aktualisierungsjob bis zum Abschluss dieser Jobs in eine Warteschlange gestellt. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.
- Stellen Sie sicher, dass das Repository für Firmwareaktualisierungen die Firmwarepakete enthält, die Sie implementieren möchten. Ist dies nicht der Fall, so aktualisieren Sie den Produktkatalog und laden Sie die entsprechenden Firmwareaktualisierungen herunter (siehe Produktkatalog aktualisieren und Firmwareaktualisierungen werden heruntergeladen).

  Anmerkung: Bei der Erstinstallation von XClarity Administrator sind der Produktkatalog und das Repository leer.

  Wenn Sie erforderliche Firmware installieren möchten, stellen Sie sicher, dass die erforderliche Firmware ebenfalls in das Repository heruntergeladen wird.

  In einigen Fällen können mehrere Versionen für die Aktualisierung der Firmware erforderlich sein, dann müssen alle Versionen in das Repository heruntergeladen werden. Beispielsweise müssen Sie für eine Aktualisierung des skalierbaren IBM FC5022 SAN-Switches von v7.4.0a auf v8.2.0a zuerst v8.0.1-pha, dann v8.1.1 und abschließend v8.2.0a installieren. Alle drei Versionen müssen im Repository sein, um den Switch auf v8.2.0a zu aktualisieren.
- Um die Firmwareaktualisierungen zu aktivieren, müssen die Einheiten normalerweise neu gestartet werden. Wenn Sie die Einheit 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 einen anderen Server verschoben wurden.

Zu dieser Aufgabe

- Sie können ausgewählte Firmware auf 50 Einheiten gleichzeitig aktualisieren. Wenn Sie ausgewählte Firmware auf mehr als 50 Einheiten aktualisieren möchten, werden die verbleibenden Einheiten in die Warteschlange gestellt. Eine in der Warteschlange befindliche Einheit wird aus der Warteschlange mit „ausgewählten Firmwareaktualisierungen“ entfernt, wenn entweder die Aktivierung auf einer aktualisierten Einheit abgeschlossen ist oder eine aktualisierte Einheit in den ausstehenden Wartungsmodus versetzt wird (wenn auf dieser Einheit ein Neustart erforderlich ist). Wenn eine Einheit, die sich im ausstehenden Wartungsmodus befindet, neu gestartet wird, bootet die Einheit in den Wartungsmodus und setzt den Aktualisierungsprozess fort, auch wenn die maximale Anzahl an Firmware-Aktualisierungen bereits ausgeführt wird.
- Sie können Firmware übernehmen und aktivieren, die neuer als die installierte Firmware ist.
- Sie können außerdem alle Aktualisierungen für eine bestimmte Einheit übernehmen. Sie können jedoch auch eine Einheit erweitern, um Aktualisierungen für bestimmte Komponenten festzulegen (beispielsweise Baseboard Management Controller oder UEFI).
- Wenn Sie ein Firmwareaktualisierungspaket mit Aktualisierungen für verschiedene Komponenten installieren, werden alle Komponenten, für die das Aktualisierungspaket übernommen wird, aktualisiert.

Vorgehensweise

So übernehmen und aktivieren Sie Aktualisierungen auf einer verwalteten Einheit:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**. Die Seite Firmwareaktualisierungen: anwenden/aktivieren wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Aktualisierung ohne Richtlinie**.

Schritt 3. Wählen Sie in der Spalte **Spätere Versionen heruntergeladen** die Firmwareversion für jede Einheit aus, die Sie aktualisieren möchten.

Schritt 4. Wählen Sie eine oder mehrere zu aktualisierende Einheiten und Geräte aus.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Darüber hinaus können Sie die Liste der angezeigten Einheiten filtern, indem Sie eine Option im Menü **Anzeigen** auswählen, um nur Einheiten in einem bestimmten Gehäuse, Rack oder in einer bestimmten Gruppe anzuzeigen, Text im Feld **Filter** eingeben (z. B. einen Namen oder eine IP-Adresse) oder auf eines der folgenden Symbole klicken, um nur Einheiten mit einem bestimmten Status anzuzeigen.

- **Komponenten mit einigen späteren Versionen ausblenden** – Symbol ( )
- Symbol **Komponenten ohne spätere Versionen ausblenden** ( )
- Symbol **Nicht für Aktualisierung unterstützte Einheiten ausblenden** ( )
- Symbol **Einheiten, die einer Firmwareaktualisierung unterzogen werden, ausblenden** ( )
- **Geräte mit nicht ladbarer Firmware ausblenden** Symbol ( )

Die Spalte **Gruppen** gibt die Gruppen an, zu denen jede Einheit gehört. Sie können den Mauszeiger über die Spalte **Gruppen** bewegen, um eine vollständige Liste der Gruppen nach Gruppentyp abzurufen.

Die Spalte **Installierte Version** gibt die installierte Firmwareversion, den Konformitätsstatus oder den Status der Einheit an.

Der Konformitätsstatus kann einer der folgenden sein:

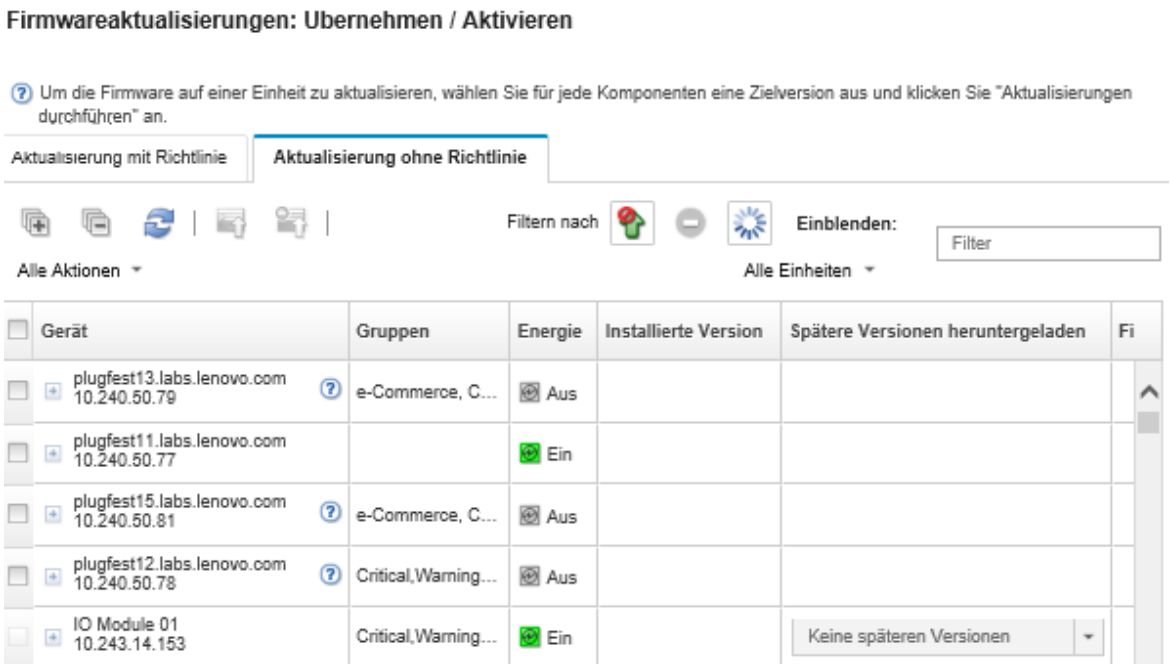
- **Konform**
- **Fehlerhafte Konformität**
- **Nicht konform**
- **Keine Konformitätsrichtlinie festgelegt**
- **Nicht überwacht**

Der Einheitenstatus kann einer der folgenden sein:

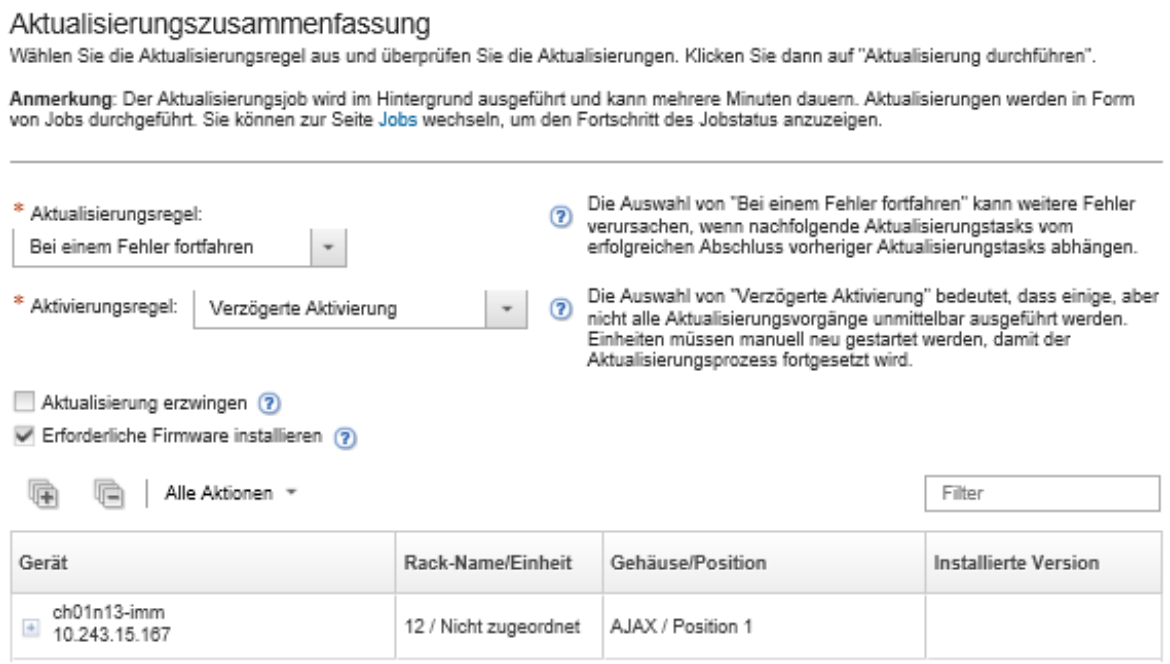
- **Aktualisierungen werden nicht unterstützt**
- **Aktualisierung wird ausgeführt**

Anmerkungen: Wenn die Aktivierung der installierten Firmwareversion aussteht, wird „(ausstehende Aktivierung)“ an die installierte Firmwareversion oder den Konformitätsstatus jeder Einheit angehängt, z. B. „2.20 / A9E12EUS (ausstehende Aktivierung)“. Um den Status „Ausstehende Aktivierung“ anzeigen zu können, muss die folgende Firmwareversion auf dem primären BMC (Baseboard Management Controller) des Servers installiert sein.

- **IMM2**: TCOO46F, TCOO46E oder höher (abhängig von der Plattform)
- **XCC**: CDI328M, PSI316N, TEI334I oder höher (abhängig von der Plattform)



Schritt 5. Klicken Sie auf das Symbol **Aktualisierungen durchführen** ( ). Das Dialogfenster Aktualisierungszusammenfassung wird angezeigt.



Schritt 6. Wählen Sie eine der folgenden Aktualisierungsregeln aus

- **Alle Aktualisierungen bei einem Fehler anhalten.** Wenn bei der Aktualisierung einer der Komponenten (wie einem Adapter oder Management-Controller) in der Zieleinheit ein Fehler auftritt, stoppt die Firmwareaktualisierung für alle ausgewählten Einheiten im aktuellen Firmwareaktualisierungsjob. In diesem Fall wird keine der Aktualisierungen im Aktualisierungspaket für die Einheit übernommen. Die aktuelle, auf allen ausgewählten Systemen installierte Firmware bleibt erhalten.
- **Bei einem Fehler fortfahren**. Wenn beim Aktualisieren einer der Komponenten in der Einheit ein Fehler auftritt, aktualisiert der Firmwareaktualisierungsprozess die Firmware der

entsprechenden Komponente nicht. Der Firmwareaktualisierungsprozess wird jedoch zur Aktualisierung aller anderen Komponenten in der Einheit und aller anderen Einheiten im aktuellen Firmwareaktualisierungsjob fortgesetzt.

- **Bei einem Fehler zum nächsten System wechseln**. Wenn beim Aktualisieren einer der Komponenten in der Einheit ein Fehler auftritt, stoppt der Firmwareaktualisierungsprozess alle Versuche, die Firmware für die entsprechende Komponente zu aktualisieren. Die aktuell auf der Einheit installierte Firmware bleibt also bestehen. Der Firmwareaktualisierungsprozess fährt mit der Aktualisierung aller anderen Einheiten im aktuellen Firmwareaktualisierungsjob fort.

Anmerkung: Wenn die Wake-On-LAN-Bootoption aktiviert ist, kann sie beim Ausschalten des Servers zu Konflikten mit XClarity Administrator führen. Dies gilt auch für Firmwareaktualisierungen, bei denen ein Wake-On-LAN-Client im Netzwerk „Aktivierung durch Magic Packet“-Befehle sendet.

Schritt 7. Wählen Sie eine der folgenden Aktivierungsregeln aus:

- **Sofortige Aktivierung**. Während des Aktualisierungsprozesses wird die Einheit möglicherweise mehrmals automatisch neu gestartet, bis der gesamte Prozess abgeschlossen ist. Sorgen Sie dafür, dass alle Anwendungen für die Einheit vor dem Fortfahren beendet sind.
- **Verzögerte Aktivierung**. Es werden einige, aber nicht alle Aktualisierungsvorgänge ausgeführt. Einheiten müssen 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 eine Einheit aus irgendeinem Grund neu startet, wird der verzögerte Aktualisierungsprozess abgeschlossen.

  Diese Aktivierungsregel wird nur für Server und Rack-Switches unterstützt. CMMs und Flex-Switches werden unabhängig von dieser Einstellung sofort aktiviert.

  Es wird ein Ereignis ausgelöst, wenn der Status zum **Firmware-Wartungsmodus „Ausstehend“** wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.

  Der verzögerte Aktualisierungsprozess wird abgeschlossen, wenn die Einheit aus irgendeinem Grund neu gestartet wird (einschließlich eines manuellen Neustarts). Es gibt kein Zeitlimit für den Neustart des Servers.

  XClarity Administrator kann Aktualisierungen mit verzögerter Aktivierung für bis zu 50 Einheiten gleichzeitig übernehmen. Wenn Sie versuchen, Aktualisierungen mit verzögerter Aktivierung für mehr als 50 Einheiten anzuwenden, werden die verbleibenden Einheiten in eine Warteschlange gestellt. Eine Einheit verlässt die Warteschlange, wenn sich der Status einer zu aktualisierenden Einheit in den **Firmware-Wartungsmodus „Ausstehend“** ändert.

  Wichtig:

  – Wenn XClarity Administrator während des Aktualisierungsjobs neu gestartet wird, wird der Aktualisierungsjob mit einem Fehler beendet.
  – Wenn ein Server im Status **Firmware-Wartungsmodus „Ausstehend“** neu gestartet wird, während XClarity Administrator nicht aktiv oder nicht erreichbar ist, bootet der Server zur BMU. Da XClarity Administrator jedoch keine Verbindung mit der BMU herstellen kann und es nach 60 Sekunden zu einer Zeitlimitüberschreitung kommt, wird der Stromversorgungsstatus des Systems vom Baseboard Management Controller wiederhergestellt (wird ausgeschaltet, wenn er ausgeschaltet war; wird neu gestartet, wenn er eingeschaltet war).

- **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. Diese Regel wird nur für Server unterstützt.

  Es wird ein Ereignis ausgelöst, wenn der Status zum Firmware-Wartungsmodus „Ausstehend“ wechselt, damit Sie wissen, wenn der Server neu gestartet werden muss.

Anmerkung: Wenn die Wake-On-LAN-Bootoption aktiviert ist, kann sie beim Ausschalten des Servers zu Konflikten mit XClarity Administrator führen. Dies gilt auch für Firmwareaktualisierungen, bei denen ein Wake-On-LAN-Client im Netzwerk „Aktivierung durch Magic Packet“-Befehle sendet.

Schritt 8. **Optional:** Wählen Sie **Update 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.

Anmerkung: Sie können ältere Firmwareversionen auf Einheitenoptionen, Adaptern und Laufwerken übernehmen, die das Herabsetzen unterstützen. In der Hardwaredokumentation erfahren Sie, ob Herabsetzen unterstützt wird.

Schritt 9. **Optional:** Deaktivieren Sie **Erforderliche Firmware installieren**, wenn Sie nicht möchten, dass erforderliche Firmware installiert wird. Erforderliche Firmware wird standardmäßig installiert.

Anmerkung: Bei der Verwendung von **Verzögerte Aktivierung** oder **Priorisierte Aktivierung** für erforderliche Firmwareaktualisierungen müssen Sie den Server möglicherweise neu starten, um die erforderliche Firmware zu aktivieren. Nach dem ersten Neustart werden die verbleibenden Firmwareaktualisierungen mit **Sofortige Aktivierung** installiert.

Schritt 10. **Optional:** Wenn Sie **Sofortige Aktivierung** ausgewählt haben, wählen Sie **Hauptspeichertest**, um einen Hauptspeichertest nach Abschluss der Firmware-Aktualisierung durchzuführen, wenn der Server während der Aktualisierung neu gestartet wird.

Diese Option wird für ThinkSystem v1- und v2-Server unterstützt (ausgenommen ThinkSystem Server SR635, SR645, SR655, SR665).

Schritt 11. Klicken Sie auf **Aktualisierung durchführen**, um sofort zu aktualisieren, oder klicken Sie auf **Zeitplan**, um diese Aktualisierung geplant zu einem späteren Zeitpunkt auszuführen.

Bei Bedarf können Sie Stromversorgungsaktionen auf den verwalteten Einheiten durchführen. Die Stromversorgungsaktionen sind hilfreich, wenn **Verzögerte Aktivierung** ausgewählt ist und Sie die Aktualisierungen weiterlaufen lassen möchten, sobald sich die Einheit im Status „Ausstehende Wartung“ befindet. Um eine Stromversorgungsaktion auf einer verwalteten Einheit über diese Seite auszuführen, klicken Sie auf **Alle Aktionen → Stromversorgungsaktionen** und wählen Sie dann eine der folgenden Stromversorgungsaktionen aus.

- **Einschalten**
- **Betriebssystem herunterfahren und ausschalten**
- **Ausschalten**
- **Betriebssystem herunterfahren und neu starten**
- **Neustart**

Nach dieser Aufgabe

Versuchen Sie erneut die Aktualisierung zu übernehmen, wenn der Wechsel zum Wartungsmodus bei einem Server beim Übernehmen einer Firmwareaktualisierung fehlschlägt.

Wenn Aktualisierungen nicht erfolgreich abgeschlossen werden, finden Sie unter Probleme bei Firmwareaktualisierung und Repository in der Onlinedokumentation von XClarity Administrator Informationen zur Fehlerbehebung und Korrekturmaßnahmen.

Sie können über die Seite „Firmwareaktualisierung: Übernehmen/Aktivieren“ die folgenden Aktionen ausführen:

- Exportieren Sie Firmware- und Konformitätsinformationen für jede verwaltete Einheit, indem Sie auf **Alle Aktionen → Ansicht als CSV exportieren** klicken.

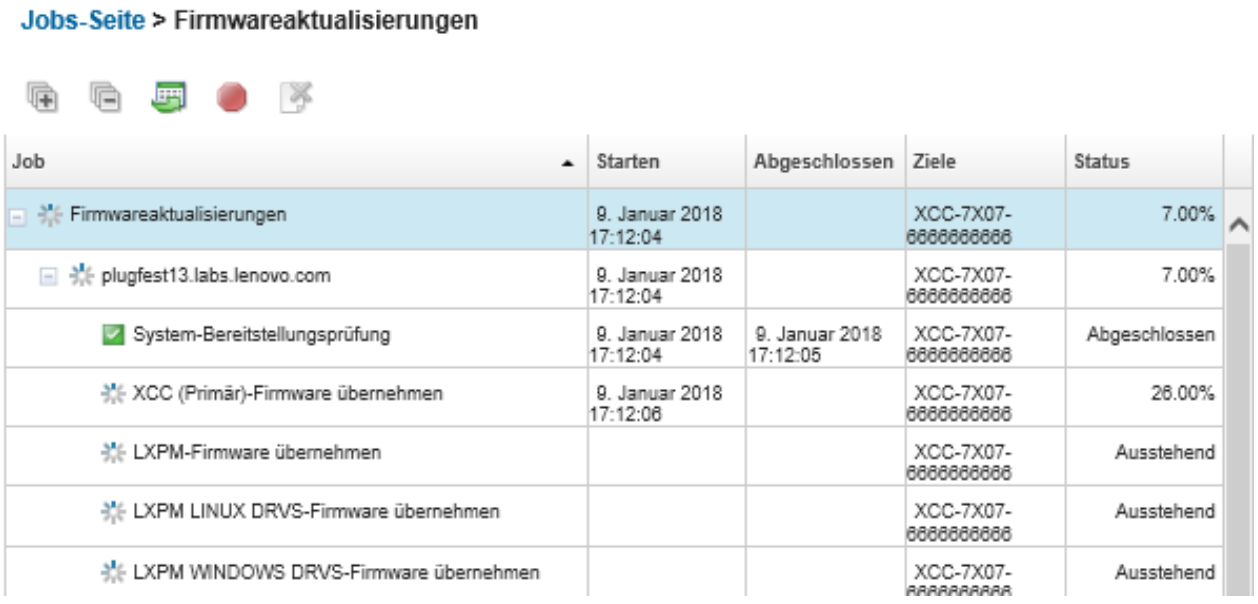
  Anmerkung: Die CSV-Datei enthält nur gefilterte Informationen in der aktuellen Ansicht. Informationen, die aus der Ansicht gefiltert und in den Spalten ausgeblendet wurden, werden hier nicht aufgeführt.

- Indem Sie die Einheit auswählen und auf das Symbol **Aktualisierung abbrechen** klicken ( ), können Sie eine laufende Aktualisierung für eine Einheit abbrechen.

  Anmerkung: Sie können Firmwareaktualisierungen in der Warteschlange abbrechen. Nach dem Beginn des Aktualisierungsprozesses kann die Firmwareaktualisierung nur abgebrochen werden, wenn der Aktualisierungsprozess eine Task durchführt, die nicht die Durchführung der Aktualisierung ist, z. B. der Wechsel in den Wartungsmodus oder der Neustart der Einheit.

- Sie können den Status der Firmwareaktualisierung direkt über die Seite Übernehmen/Aktivieren in der Spalte **Status** anzeigen.
- Sie können den Status des Aktualisierungsprozesses im Jobprotokoll überwachen. Klicken Sie im Lenovo XClarity Administrator-Menü auf **Überwachung → Jobs**.

  Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.



Wenn die Firmwareaktualisierungsjobs abgeschlossen sind, können Sie sicherstellen, dass die Einheiten kompatibel sind. Klicken Sie hierzu auf **Bereitstellung → Firmwareaktualisierungen: anwenden/aktivieren**, um zur Seite Firmwareaktualisierungen: anwenden/aktivieren zu wechseln, und klicken Sie auf das Symbol **Aktualisieren** ( ). Die aktuelle, auf der jeweiligen Einheit aktive Firmwareversion wird in der Spalte **Installierte Version** angezeigt.

Kapitel 14. Windows-Einheitentreiber auf verwalteten Servern aktualisieren

Unter Windows UpdateXpress System Packs (UXSPs) können Sie BS-Einheitentreiber auf implementierten Windows-Betriebssystemen aktualisieren.

Vorbereitende Schritte

Sie müssen die Berechtigungen **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** oder **lxc-hw-admin** haben, um BS-Einheitentreiber verwalten und implementieren und Stromversorgungsaktionen auf verwalteten Servern von den Seiten der Windows-Treiberaktualisierungen durchführen zu können.

Das Aktualisieren der Firmware und das Aktualisieren der Einheitentreiber sind separate Prozesse in XClarity Administrator; es besteht keine Verbindung zwischen diesen Prozessen. XClarity Administrator sorgt nicht für Kompatibilität zwischen Firmware und Einheitentreibern auf verwalteten Einheiten, obwohl es empfohlen wird, die Einheitentreiber gleichzeitig mit der Firmware zu aktualisieren.

Zu dieser Aufgabe

Windows UpdateXpress System Packs (UXSPs) enthalten Windows-Einheitentreiber für unterstützte Windows-Versionen und für Lenovo Server, die Windows unterstützen.

Es werden nur Einheitentreiber für Windows Server 2012 R2 oder höher unterstützt. XClarity Administrator unterstützt nicht die Aktualisierung von Linux- oder VMware-Einheitentreibern.

Informationen zur Installation von Einheitentreibern bei der Implementierung von Betriebssystemen finden Sie unter Betriebssysteme auf Bare-Metal-Servern installieren.

Vorgehensweise

Schritt 1. **Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren**

Lenovo XClarity Administrator verwendet die Windows-Remoteverwaltung (WinRM) über HTTPS oder HTTP, um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen. WinRM muss ordnungsgemäß auf den Zielservern konfiguriert sein, bevor BS-Einheitentreiber aktualisiert werden können (siehe Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren)

Schritt 2. **BS-Einheitentreiber-Repository verwalten**

Das *BS-Einheitentreiber-Repository* enthält einen Katalog der verfügbaren Windows-Einheitentreiber und die Einheitentreiberpakete, die auf die verwalteten Einheiten angewendet werden können.

Der *Katalog* enthält Informationen über alle Windows UpdateXpress System Packs (UXSPs) und Einheitentreiber-Aktualisierungen, die für alle Lenovo Server, die Windows unterstützen, verfügbar sind. Der Katalog organisiert die Einheitentreiber-Aktualisierungen nach Einheitentyp. Wenn Sie den Katalog aktualisieren, ruft XClarity Administrator Informationen zu den neuesten verfügbaren UXSPs von der Lenovo Website zu Support für Rechenzentrum ab (einschließlich der Metadaten-XML-Datei und der Readme-TXT-Dateien) und speichert die Informationen im Repository. Die Nutzdatendatei (.exe) wird nicht heruntergeladen. Weitere Informationen zum Aktualisieren des Katalogs finden Sie unter BS-Einheitentreiber-Katalog aktualisieren.

Sie können Windows UXSPs aus dem Repository herunterladen oder importieren. Windows UXSPs enthalten Windows-Einheitentreiber für unterstützte Windows-Versionen und für Lenovo Server, die Windows unterstützen. UXSPs müssen im Repository verfügbar sein, bevor Sie Windows-Einheitentreiber auf verwalteten Servern aktualisieren können. Weitere Informationen zum Herunterladen von Einheitentreibern finden Sie unter Windows-Einheitentreiber herunterladen .

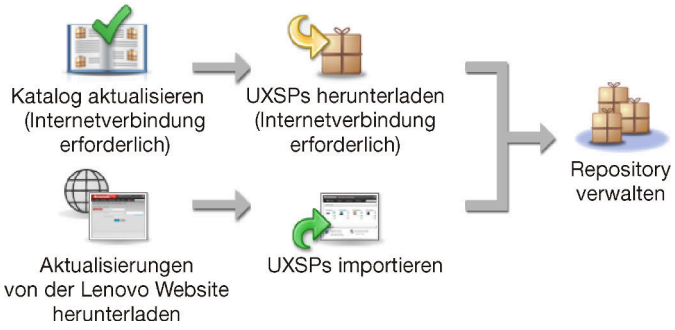
Anhand der Spalte „Downloadstatus“ auf der Registerkarte „Einzelne Aktualisierungen“ der Seite „Windows-Treiberaktualisierungen: Repository“ können Sie ermitteln, ob UXSPs im BS-Einheitentreiber-Repository gespeichert sind. Die Spalte enthält die folgenden Werte.

- **Heruntergeladen**. Das gesamte Paket oder die einzelne Aktualisierung ist im Repository gespeichert.
- ***x* von *y* heruntergeladen**. Es sind nur einige Aktualisierungen des Pakets im Repository gespeichert. Die Zahlen in Klammern geben die Anzahl der verfügbaren Aktualisierungen und die Anzahl gespeicherten Aktualisierungen an oder es liegen keine Aktualisierungen für den speziellen Einheitentyp vor.
- **Nicht heruntergeladen**. Das gesamte Paket oder die einzelne Aktualisierung ist verfügbar, aber nicht im Repository gespeichert.

Anmerkung: Wenn Sie UXSPs über die Seite „Windows-Treiberupdates: Repository“ herunterladen oder importieren, werden nur Einheitentreiber heruntergeladen und im Repository gespeichert. Firmwareaktualisierungen werden verworfen. Informationen zum Herunterladen oder Importieren von Firmwareaktualisierungen finden Sie unter Repository für Firmwareaktualisierungen verwalten.

XClarity Administrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und UXSPs herunterzuladen. Sofern nicht mit dem Internet verbunden, können Sie UXSPs manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Administrator-Host über einen Webbrowser herunterladen. Dieser UXSPs-Download liegt im ZIP-Format vor und enthält alle erforderlichen Einheitentreiberdateien für den UXSP, einschließlich Nutzdatendatei (.exe), Metadatendatei (.xml) und Änderungsprotokolldatei (.chg) sowie Readme-Dateien (.txt).

Anmerkung: Möglicherweise werden Meldungen angezeigt, dass die Firmware (fw)-Dateien nicht erforderlich sind und entfernt wurden. Dies ist normal, da nur Windows-Einheitentreiber mithilfe dieses Verfahrens aktualisiert werden.



Achtung:

- Entpacken Sie die UXSP nicht vor dem Importieren.
- Die Windows UXSPs enthalten Einheitentreiber und Firmwareaktualisierungen. Die Firmwareaktualisierungen in den Windows UXSPs werden gelöscht, wenn die UXSPs in das Repository importiert werden und eine Warnmeldung angezeigt wird. Es werden nur die Einheitentreiber importiert.

Schritt 3. **BS-Einheitentreiber übernehmen**

XClarity Administrator aktualisiert Einheitentreiber nicht automatisch auf verwalteten Servern. Zum Aktualisieren von Einheitentreibern müssen Sie die Einheitentreiber auf ausgewählten Servern manuell übernehmen.

Achtung: Lesen Sie vor der Aktualisierung von Einheitentreibern auf verwalteten Servern die folgenden Hinweise und stellen Sie sicher, dass Sie die anwendbaren erforderlichen Aktionen ausgeführt haben.

- Nicht unterstützte Einheiten können nicht für Aktualisierungen ausgewählt werden.
- Lesen Sie die Hinweise zur Aktualisierung von Einheitentreibern, bevor Sie versuchen, die Einheitentreiber auf verwalteten Servern zu aktualisieren (siehe Hinweise zum Aktualisieren von BS-Einheitentreibern).
- Stellen Sie sicher, dass das Repository die UXSPs und Einheitentreiber enthält, die Sie implementieren möchten (siehe Windows-Einheitentreiber herunterladen).

  Anmerkung: Bei der Erstinstallation von XClarity Administrator sind Katalog und Repository leer.
- XClarity Administrator kann die Windows-Remoteverwaltung (WinRM) über HTTPS oder HTTP verwenden, um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen (HTTPS ist der Standard). Um HTTP zu verwenden, klicken Sie auf **Alle Aktionen → Globale Einstellungen** auf der Seite „Windows-Treiberaktualisierung: Übernehmen“ und deaktivieren Sie **HTTPS für Windows-Treiberaktualisierungen verwenden**.

  Achtung: Bei Verwendung von HTTP werden Windows-Anmeldeinformationen *ohne* Verschlüsselung über das Netzwerk gesendet und können über häufig verfügbare Tools für die Behebung von Netzwerkproblemen angezeigt werden.

  Wichtig:

  – Stellen Sie sicher, dass die Windows-Remoteverwaltung (WinRM) auf dem Zielserver so konfiguriert ist, dass die gleiche Einstellung (HTTPS bzw. HTTP) verwendet wird, die in XClarity Administrator definiert ist (siehe Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren).

  – Stellen Sie sicher, dass WinRM auf dem Zielserver mit der Standardauthentifizierung konfiguriert ist.

  – Vergewissern Sie sich bei Verwendung von HTTPS, dass WinRM auf dem Zielserver mit **allowUnencrypted=false** konfiguriert ist.
- Stellen Sie sicher, dass PowerShell auf dem Zielserver unterstützt wird.
- Stellen Sie sicher, dass der Zielserver eingeschaltet ist, bevor Sie mit der Aktualisierung von Einheitentreibern beginnen. Wenn der Server nicht eingeschaltet ist, wählen Sie den Zielserver aus und klicken Sie auf **Alle Aktionen → Stromversorgungsaktionen → Einschalten**.
- Stellen Sie sicher, dass XClarity Administrator alle erforderlichen Informationen für den Zugriff auf das Hostbetriebssystem hat (siehe Zugriff auf Betriebssysteme auf verwalteten Servern verwalten).
- Wenn Sie beim Aktualisieren von BS-Einheitentreibern einen Domänenaccount verwenden möchten, stellen Sie sicher, dass Sie die erforderliche Konfigurationsdatei erstellt haben (siehe Domänenaccount für BS-Einheitentreiberaktualisierungen konfigurieren).
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Sie können keine Einheitentreiber auf einem verwalteten Server aktualisieren, der von einem laufenden Job blockiert wird. Wenn auf dem Zielserver ein anderer Aktualisierungsjob ausgeführt wird, wird dieser Aktualisierungsjob in eine Warteschlange gestellt, bis der aktuelle Aktualisierungsjob

abgeschlossen ist. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.

Weitere Informationen zur Aktualisierung von Einheitentreibern finden Sie unter Windows-Einheitentreiber übernehmen.

Hinweise zum Aktualisieren von BS-Einheitentreibern

Bevor Sie mit der Aktualisierung von BS-Einheitentreibern für verwaltete Einheiten mit Lenovo XClarity Administrator beginnen, lesen Sie die folgenden wichtigen Hinweise.

Anmerkung: Sie müssen die Berechtigungen **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** oder **lxc-hw-admin** haben, um Einheitentreiber verwalten und implementieren und Stromversorgungsaktionen auf verwalteten Servern von den Windows-Treiberaktualisierungen-Seiten durchführen zu können.

Hinweise zum Netzwerkbetrieb

- Die benötigten Ports und Internetadressen müssen verfügbar sind, bevor Sie mit dem Download von UpdateXpress System Packs (UXSPs) beginnen können. Weitere Informationen finden Sie unter Portverfügbarkeit und Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.
- XClarity Administrator benötigt Zugriff auf das Verwaltungs- und Datennetzwerk, um auf das Betriebssystem zugreifen zu können.
- XClarity Administrator muss mit dem Zielserver (sowohl Baseboard Management Controller als auch Datennetzwerk des Servers) über die Netzwerkschnittstelle (Eth0 oder Eth1) kommunizieren können, die bei Konfiguration des XClarity Administrator-Netzwerkzugriffs ausgewählt wurde, und die Schnittstelle muss mit einer IPv4-Adresse oder einer automatischen IPv6-ULA-Adresse konfiguriert sein.

  Informationen zur Angabe einer Schnittstelle, die für die Betriebssystemimplementierung verwendet wird, finden Sie unter Netzwerkzugriff konfigurieren.

  Weitere Informationen zu Betriebssystem-Implementierungsnetzwerken und -schnittstellen finden Sie unter Hinweise zum Netzwerkbetrieb in der Onlinedokumentation von XClarity Administrator.
- IP-Adressen für das Hostbetriebssystem müssen eindeutig sein.
- XClarity Administrator kann die Windows-Remoteverwaltung (WinRM) über HTTPS oder HTTP verwenden, um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen (HTTPS ist der Standard). Um HTTP zu verwenden, klicken Sie auf **Alle Aktionen → Globale Einstellungen** auf der Seite „Windows-Treiberaktualisierung: Übernehmen“ und deaktivieren Sie **HTTPS für Windows-Treiberaktualisierungen verwenden**.

  Achtung: Bei Verwendung von HTTP werden Windows-Anmeldeinformationen *ohne* Verschlüsselung über das Netzwerk gesendet und können über häufig verfügbare Tools für die Behebung von Netzwerkproblemen angezeigt werden.

Hinweise zu verwalteten Einheiten

- Windows-Einheitentreiber werden nicht für ThinkAgile, ThinkSystem SR635 und ThinkSystem SR655 Server unterstützt.
- Es werden nur ThinkSystem-, Lenovo System x- und Lenovo Flex System-Server unterstützt.
- XClarity Administrator überprüft die Beziehung zwischen den Management-Controller und dem Betriebssystem nicht. Der Baseboard Management Controller dient zum Ein- oder Ausschalten des Servers.
- Vergewissern Sie sich, dass die LAN-über-USB-Schnittstelle aktiviert ist. LAN-über-USB wird verwendet, wenn BS-Einheitentreiber aktualisiert werden.

Hinweise zum Betriebssystem und zu Einheitentreibern

- Sie können Einheitentreiber für die folgenden Betriebssysteme aktualisieren.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  Anmerkung: XClarity Administrator wird nur mit Windows-Versionen getestet, die zum Release-Datum der XClarity Administrator-Version von Microsoft unterstützt werden.
- Die Windows-Remoteverwaltung (WinRM) muss auf dem Zielserver für HTTPS konfiguriert sein (siehe Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren).
- PowerShell muss auf dem Zielserver unterstützt werden.
- Sie müssen Informationen bereitstellen, die für den Zugriff auf das Hostbetriebssystem auf dem Zielserver erforderlich sind, einschließlich BS-IP-Adresse und Anmeldeinformationen (siehe Zugriff auf Betriebssysteme auf verwalteten Servern verwalten). Sie müssen Anmeldeinformationen für einen Benutzeraccount angeben, der über Administratorrechte verfügt.
- XClarity Administrator aktualisiert nur Einheitentreiber, die nicht konform sind. Einheitentreiber sind nicht konform, wenn die Version auf dem Server älter als die Version im ausgewählten UXSP ist. Einheitentreiber mit gleicher oder neuerer Version als die in der ausgewählten UXSP werden übersprungen.
- Die Konformität von Einheitentreibern ist nur korrekt, wenn Hardware vorhanden ist. Ist keine Hardware vorhanden, werden trotzdem Einheitentreiber auf den Server angewendet. Wenn die fehlende Hardware zum Server hinzugefügt wurde, lädt Windows die neueste Version.
- System x-Server unterstützen einige vordefinierten Einheitentreiber nicht, die im Lieferumfang von XClarity Administrator enthalten sind. Um Einheitentreiber für diese Server zu implementieren, erstellen Sie ein angepasstes Profil, das nur die erforderlichen Einheitentreiber enthält.

BS-Einheitentreiber-Repository verwalten

Das *BS-Einheitentreiber-Repository* enthält den Katalog und heruntergeladene Windows-Einheitentreiber.

Zu dieser Aufgabe

Der *Katalog* enthält Informationen über alle Windows UpdateXpress System Packs (UXSPs) und Einheitentreiber-Aktualisierungen, die für alle Lenovo Server, die Windows unterstützen, verfügbar sind. Der Katalog organisiert die Einheitentreiber-Aktualisierungen nach Einheitentyp. Wenn Sie den Katalog aktualisieren, ruft XClarity Administrator Informationen zu den neuesten verfügbaren UXSPs von der Lenovo Website zu Support für Rechenzentrum ab (einschließlich der Metadaten-XML-Datei und der Readme-TXT-Dateien) und speichert die Informationen im Repository. Die Nutzdatendatei (.exe) wird nicht heruntergeladen. Weitere Informationen zum Aktualisieren des Katalogs finden Sie unter BS-Einheitentreiber-Katalog aktualisieren.

Windows UpdateXpress System Packs (UXSPs) enthalten Windows-Einheitentreiber für unterstützte Windows-Versionen und für Lenovo Server, die Windows unterstützen. Sie können Windows UXSPs aus dem Repository herunterladen oder importieren. Windows UXSPs enthalten Windows-Einheitentreiber für unterstützte Windows-Versionen und für Lenovo Server, die Windows unterstützen. UXSPs müssen im Repository verfügbar sein, bevor Sie Windows-Einheitentreiber auf verwalteten Servern aktualisieren können. Weitere Informationen zum Herunterladen von Einheitentreibern finden Sie unter Windows-Einheitentreiber herunterladen .

XClarity Administrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und UXSPs herunterzuladen. Sofern nicht mit dem Internet verbunden, können Sie UXSPs manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Administrator-Host über einen Webbrowser

herunterladen. Dieser UXSPs-Download liegt im ZIP-Format vor und enthält alle erforderlichen Einheitentreiberdateien für den UXSP, einschließlich Nutzdatendatei (.exe), Metadatendatei (.xml) und Änderungsprotokolldatei (.chg) sowie Readme-Dateien (.txt).

Nachdem ein UXSP in das Repository heruntergeladen wurde, werden Informationen zu jedem Einheitentreiber im Paket zur Seite „Windows-Treiberaktualisierungen: Repository“ hinzugefügt. Dies umfasst Veröffentlichungsdatum, Größe und Schweregrad. Der Schweregrad zeigt die Auswirkungen und die Dringlichkeit für die Übernahme der Aktualisierung an. So können Sie ermitteln, wie Ihre Umgebung möglicherweise betroffen ist.

- **Erste Version**. Dies ist die erste Version des Einheitentreibers.
- **Kritisch**. Der Einheitentreiber enthält dringende Fixes für Probleme mit Datenverlusten, der Sicherheit oder der Stabilität.
- **Empfohlen**. Der Einheitentreiber enthält wichtige Fixes für vermutlich auftretende Problem.
- **Nicht kritisch**. Der Einheitentreiber enthält untergeordnete Fixes, Leistungsverbesserungen und Textänderungen.

Anmerkungen:

- Der Schweregrad wird im Verhältnis zur zuvor veröffentlichten Version des Einheitentreibers bewertet. Beispiel: Ist der installierte Einheitentreiber v1.01, die Aktualisierung v1.02 ist „Kritisch“ und die Aktualisierung v1.03 ist „Empfohlen“, so bedeutet dies, dass die Aktualisierung von 1.02 auf 1.03 empfohlen ist und die Aktualisierung von v1.01 auf v1.03 kritisch ist – denn diese ist kumulativ (v1.03 umfasst die kritischen Fixes aus v1.02).
- In speziellen Fällen kann eine Aktualisierung nur für einen bestimmten Maschinentyp empfohlen oder kritisch sein. Weitere Informationen finden Sie in den Versionshinweisen.

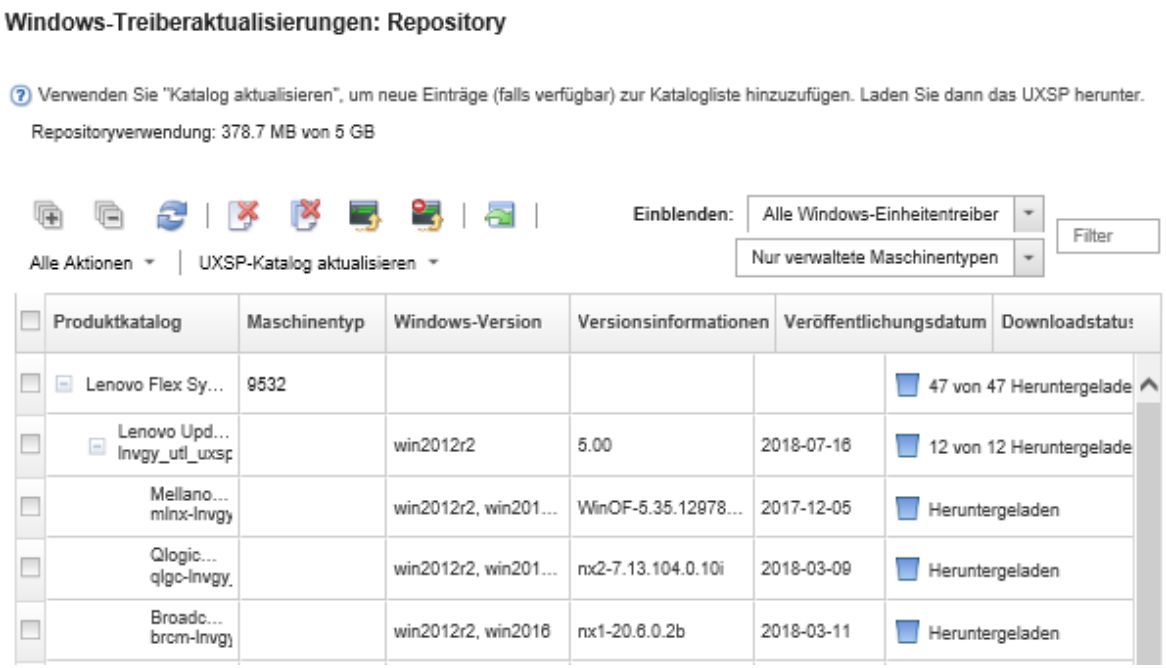
Vorgehensweise

So zeigen Sie im Repository verfügbare UXSPs und Einheitentreiber an:

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Windows-Treiberaktualisierungen: Repository**. Die Seite Windows-Treiberaktualisierungen: Repository wird mit einer Liste verfügbarer UXSPs angezeigt (nach Einheitentyp zusammengefasst).

Schritt 2. Erweitern Sie einen Servertyp und erweitern Sie dann die für diesen Servertyp verfügbaren UXSPs, um die Einheitentreiber aufzulisten, die für diesen Servertyp verfügbar sind.

Sie können die Tabellenspalten sortieren und auf das Symbol **Alle einblenden** ( ) und **Alle ausblenden** ( ) klicken, um die Suche nach bestimmten Einheitentreibern zu erleichtern. Darüber hinaus können Sie die Liste der angezeigten Servertypen und Einheitentreibern filtern, indem Sie eine Option im Menü **Anzeigen** auswählen, um nur die Einheitentreiber eines bestimmten Zeitraums, Einheitentreiber für alle Servertypen oder nur für verwaltete Servertypen anzuzeigen, oder indem Sie Text im Feld **Filter** eingeben.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Rufen Sie die neuesten Informationen zu den verfügbaren UXSPs ab, indem Sie auf **Katalog aktualisieren** klicken.

  Das Abrufen der Informationen kann einige Minuten dauern. Siehe BS-Einheitentreiber-Katalog aktualisieren für weitere Informationen.
- Laden Sie UXSPs und Einheitentreiber mit XClarity Administrator herunter, indem Sie den Katalog aktualisieren und anschließend auf das Symbol **Herunterladen** ( ) klicken. Wenn die UXSPs und Einheitentreiber heruntergeladen und zum Repository hinzugefügt sind, ändert sich der Status zu „Heruntergeladen“.

  Weitere Informationen zum Herunterladen von UXSPs und Einheitentreibern finden Sie unter Windows-Einheitentreiber herunterladen .
- Importieren Sie UXSPs, die Sie manuell aus dem Internet auf eine Arbeitsstation heruntergeladen haben oder Einheitentreiber, die Sie von XClarity Administrator exportiert haben (siehe Windows-Einheitentreiber herunterladen).
- Sie können ausgewählte laufende Downloads stoppen, indem Sie auf das Symbol **Download abbrechen** ( ) klicken.
- Löschen Sie ausgewählte UXSPs oder einzelne Einheitentreiber aus dem Repository, indem Sie auf das Symbol **Löschen** ( ) klicken.

BS-Einheitentreiber-Katalog aktualisieren

Der BS-Einheitentreiber-Katalog enthält Informationen zu allen Windows UpdateXpress System Packs (UXSPs) und Einheitentreibern, die für alle Lenovo Server verfügbar sind, die Windows-Einheitentreiberaktualisierungen unterstützen.

Vorbereitende Schritte

Stellen Sie sicher, dass Lenovo XClarity Administrator mit dem Internet verbunden ist.

Zu dieser Aufgabe

Wenn Sie den Katalog aktualisieren, ruft XClarity Administrator Informationen zu den neuesten verfügbaren UXSPs von der Lenovo Website zu Support für Rechenzentrum ab (einschließlich der Metadaten-XML-Datei und der Readme-TXT-Dateien) und speichert die Informationen im Repository. Die Nutzdatendatei (.exe) wird nicht heruntergeladen. Sie müssen die gewünschten UXSP und BS-Einheitentreiber-Nutzdaten herunterladen, bevor Sie Einheitentreiber auf verwalteten Servern aktualisieren. Weitere Informationen zum Herunterladen von Einheitentreibern finden Sie unter Windows-Einheitentreiber herunterladen .

Anmerkung: Die Aktualisierung des Katalogs kann mehrere Minuten in Anspruch nehmen.

Vorgehensweise

Gehen Sie wie folgt vor, um den Katalog zu aktualisieren.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → Windows-Treiberaktualisierungen: Repository**, um die Seite Windows-Treiberaktualisierungen: Repository anzuzeigen.

Schritt 2. Klicken Sie auf **Katalog aktualisieren** und anschließend auf eine der folgenden Optionen, um Informationen zu den neuesten verfügbaren UXSPs zu erhalten.

- **Ausgewählte aktualisieren – Nur aktuelle Version**. Ruft Informationen zu aktuellen UXSP-Versionen ab, die für die ausgewählten Server verfügbar sind.
- **Alle aktualisieren – Nur aktuelle Version**. Ruft Informationen zu aktuellen UXSP-Versionen ab, die für alle unterstützten Server verfügbar sind.
- **Ausgewählte aktualisieren**. Ruft Informationen zu allen UXSP-Versionen ab, die für die ausgewählten Server verfügbar sind.
- **Alle aktualisieren**. Ruft Informationen zu allen UXSP-Versionen ab, die für alle unterstützten Server verfügbar sind.

Schritt 3. Klicken Sie auf **Katalog aktualisieren**, um sofort zu aktualisieren, oder klicken Sie auf **Zeitplan**, um geplant zu einem späteren Zeitpunkt zu aktualisieren.

Windows-Einheitentreiber herunterladen

Windows UpdateXpress System Packs (UXSPs) enthalten Windows-Einheitentreiber für unterstützte Windows-Versionen und für Lenovo Server, die Windows unterstützen. Sie können Windows UXSPs aus dem Repository herunterladen oder importieren. Windows UXSPs enthalten Windows-Einheitentreiber für unterstützte Windows-Versionen und für Lenovo Server, die Windows unterstützen. UXSPs müssen im Repository verfügbar sein, bevor Sie Windows-Einheitentreiber auf verwalteten Servern aktualisieren können.

Vorbereitende Schritte

Stellen Sie vor dem Herunterladen von UpdateXpress System Packs (UXSPs) sicher, dass alle benötigten Ports und Internetadressen verfügbar sind. Weitere Informationen finden Sie unter Portverfügbarkeit und Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Stellen Sie für den Download von UXSPs mit XClarity Administrator sicher, dass XClarity Administrator mit dem Internet verbunden ist.

Für Internet Explorer sowie Microsoft Edge-Webbrowser besteht ein Upload-Limit von 4 GB. Wenn die Datei, die Sie importieren, größer als 4 GB ist, können Sie einen anderen Webbrowser verwenden (z. B. Chrome oder Firefox).

Zu dieser Aufgabe

XClarity Administrator muss mit dem Internet verbunden sein, um den Katalog zu aktualisieren und UXSPs herunterzuladen. Wenn XClarity Administrator nicht mit dem Internet verbunden ist, können Sie die Dateien manuell auf eine Arbeitsstation mit Netzwerkzugriff auf den XClarity Administrator-Host über einen Webbrowser herunterladen und die Aktualisierungen dann in das Firmwareupdate-Repository importieren.

Über die Spalte **Downloadstatus** auf der Seite „Windows-Treiberaktualisierungen: Repository“ können Sie ermitteln, ob UXSPs im Repository gespeichert sind. Die Spalte enthält einen der folgenden Werte:

- **Heruntergeladen**. Alle Einheitentreiber im UXSP oder der einzelne Einheitentreiber werden in das Repository heruntergeladen.
- *x* **von** *y* **heruntergeladen**. Es werden nur einige Einheitentreiber aus dem UXSP in das Repository heruntergeladen. Die Zahlen in Klammern geben die Anzahl der verfügbaren Einheitentreiber und die Anzahl der heruntergeladenen Einheitentreiber an.
- **Nicht heruntergeladen**. Das UXSP oder der einzelne Einheitentreiber sind auf der Lenovo Unterstützungswebsite verfügbar, wurde aber nicht in das Repository heruntergeladen.

Auf der Seite „Windows-Treiberaktualisierungen: Repository“ wird eine Nachricht angezeigt, wenn der für UXSPs und Einheitentreiber verfügbare Speicherplatz zu mehr als 50 % voll ist. Wenn das Repository zu mehr als 85 % voll ist, wird eine weitere Nachricht auf der Seite angezeigt. Sie können den belegten Speicherplatz im Repository reduzieren, indem Sie nicht genutzte Dateien entfernen. Wählen Sie dazu die Zieldateien aus und klicken Sie auf das Symbol **Löschen** ( ). Weitere Informationen finden Sie unter Plattenspeicher verwalten.

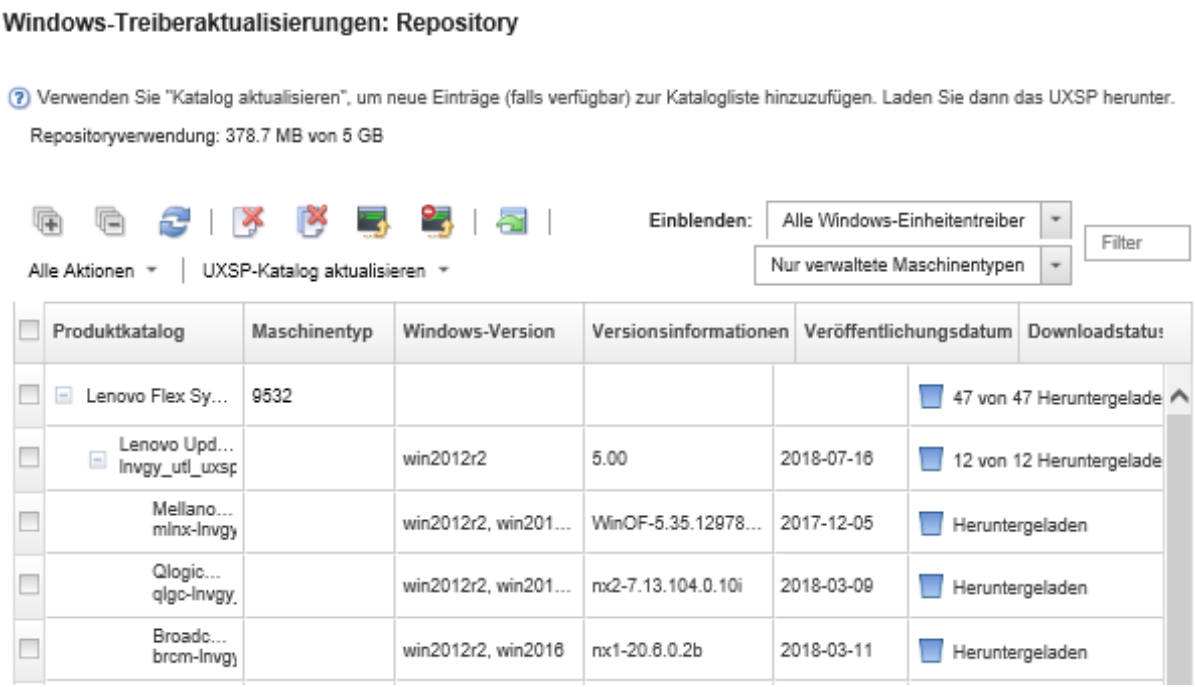
Achtung: Die Windows UXSPs enthalten Einheitentreiber und Firmwareaktualisierungen. Die Firmwareaktualisierungen in den Windows UXSPs werden gelöscht, wenn die UXSPs in das Repository importiert werden und eine Warnmeldung angezeigt wird. Es werden nur die Einheitentreiber importiert.

Vorgehensweise

Um UXSPs und bestimmte Einheitentreiber herunterzuladen, befolgen Sie eines der folgenden Verfahren.

- Wenn XClarity Administrator mit dem Internet verbunden ist:
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → Windows-Treiberaktualisierungen: Repository**, um die Seite Windows-Treiberaktualisierungen: Repository anzuzeigen.
  2. Klicken Sie auf **Katalog aktualisieren** und anschließend auf eine der folgenden Optionen, um Informationen zu den neuesten verfügbaren UXSPs zu erhalten.
     - **Ausgewählte aktualisieren – Nur aktuelle Version**. Ruft Informationen zu aktuellen UXSP-Versionen ab, die für die ausgewählten Server verfügbar sind.
     - **Alle aktualisieren – Nur aktuelle Version**. Ruft Informationen zu aktuellen UXSP-Versionen ab, die für alle unterstützten Server verfügbar sind.
     - **Ausgewählte aktualisieren**. Ruft Informationen zu allen UXSP-Versionen ab, die für die ausgewählten Server verfügbar sind.
     - **Alle aktualisieren**. Ruft Informationen zu allen UXSP-Versionen ab, die für alle unterstützten Server verfügbar sind.

     Anmerkung: Die Aktualisierung des Katalogs kann mehrere Minuten in Anspruch nehmen.
  3. Erweitern Sie den Servertyp, um die Liste der verfügbaren UXSPs anzuzeigen. Erweitern Sie die UXSP, um eine Liste der verfügbaren Einheitentreiber anzuzeigen.



4. Wählen Sie ein oder mehrere Ziel-UXSPs und Einheitentreiber für den Download aus.
5. Klicken Sie auf das Symbol **Ausgewählte herunterladen** ( ).
6. Klicken Sie auf **Herunterladen**, um den Download sofort zu starten, oder klicken Sie auf **Zeitplan**, um den Download geplant zu einem späteren Zeitpunkt auszuführen.

   Das Herunterladen der UXSPs kann einige Minuten dauern. Wenn die UXSPs und Einheitentreiber heruntergeladen und im Repository gespeichert wurden, wird die Zeile im Katalog hervorgehoben und die Spalte **Downloadstatus** ändert sich zu „Heruntergeladen“.

   Sie können den Status des Downloadprozesses im Jobprotokoll überwachen. Klicken Sie im XClarity Administrator-Menü auf **Überwachung → Jobs**. Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

- Wenn XClarity Administrator *nicht* mit dem Internet verbunden ist:
  1. Laden Sie die UXSPs auf eine Arbeitsstation herunter, die über eine Netzwerkverbindung zum XClarity Administrator-Host von Lenovo Website zu Support für Rechenzentrum verfügt.
  2. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → Windows-Treiberaktualisierungen: Repository**, um die Seite Windows-Treiberaktualisierungen: Repository anzuzeigen.
  3. Klicken Sie auf das Symbol **Importieren** ( ).
  4. Klicken Sie auf **Dateien auswählen** und wählen Sie die Position der UXSP auf der Arbeitsstation aus.
  5. Wählen Sie die ZIP-Datei von UXSP aus (entpacken Sie diese nicht vor dem Import) und klicken Sie auf **Öffnen**.

     Die UXSP-ZIP-Datei enthält die Metadatendatei (.xml), die Nutzlastdatei (.exe), die Änderungshistoriendatei (.chg) und die Readme-Datei (.txt).
  6. Klicken Sie auf **Importieren**.

     Sie können den Status des Importprozesses im Jobprotokoll überwachen. Klicken Sie im XClarity Administrator-Menü auf **Überwachung → Jobs**. Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

Nach dieser Aufgabe

Auf dieser Seite können Sie die folgenden Aktionen für ausgewählte UXSPs ausführen.

- Sie können einen laufenden Download abbrechen, indem Sie auf das Symbol **Download abbrechen** () klicken.
- Löschen Sie alle UXSP zugeordneten Dateien, indem Sie auf das Symbol **Löschen** () klicken.

Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren

Lenovo XClarity Administrator verwendet die Windows-Remoteverwaltung (WinRM) über HTTPS oder HTTP, um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen. WinRM muss ordnungsgemäß auf den Zielservern konfiguriert sein, bevor BS-Einheitentreiber aktualisiert werden können.

Vorbereitende Schritte

Die erforderlichen Ports müssen verfügbar sein. Weitere Informationen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

Weitere Informationen zum Konfigurieren von Windows Server vor der Aktualisierung des BS-Einheitentreibers finden Sie unter Whitepaper zur Vorbereitung von XClarity Administrator für BS-Einheitentreiberaktualisierungen.

Vorgehensweise

Um Windows Server so zu konfigurieren, dass die Aktualisierung von BS-Einheitentreibern unterstützt wird, gehen Sie wie folgt vor.

- **Für HTTPS**
  1. Signieren und installieren Sie ein Serverzertifikat auf jedem der Windows-Zielsysteme.

     Wichtig: Das Zertifikat muss die folgenden Informationen enthalten.

     – Betreff: Stellen Sie sicher, dass die Domänenkomponente festgelegt ist (z. B. DC=labs, DC=com, DC=company).

     – Alternativer Name: Stellen Sie sicher, dass der DNS-Name und die Host-IP-Adresse konfiguriert sind (z. B. DNS-Name=node1325C554A6F.labs.company.com und IP-Adresse=10.245.43.149).
  2. Konfigurieren Sie die Remoteverwaltungsbefehle und -daten über eine HTTPS-Verbindung, indem Sie einen der folgenden Befehle über eine Administrator-Eingabeaufforderung ausführen, und bestätigen Sie anschließend die vorgeschlagenen Konfigurationsänderungen.

     –
     ```
     winrm quickconfig -transport:https
     ```

     –
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     Informationen zur manuellen Einrichtung eines WinRM-HTTPS-Listeners gemäß WinRM-Dokumentation finden Sie unter WinRM für HTTPS-Website konfigurieren.
  3. Aktivieren Sie die Standardauthentifizierung für lokale Windows-Benutzer durch Ausführen des folgenden Befehls über eine Administrator-Eingabeaufforderung.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  4. Um eine mögliche Zeitlimitüberschreitung und das Senden von WinRM-Anforderungsfehlern bei der Konformitätsprüfung und Durchführung von Treiberaktualisierungen zu vermeiden, erhöhen Sie den

Standardwert für die Zeitlimitüberschreitung von WinRM-Antworten, indem Sie den folgenden Befehl über eine Administrator-Eingabeaufforderung ausführen. Es wird ein Wert von 280.000 empfohlen. Weitere Informationen finden Sie unter Installation und Konfiguration für Windows- Remoteverwaltung-Website.

```
winrm set winrm/config @{MaxTimeoutms="280000"}
```

5. Öffnen Sie den Port in der Firewall, den Sie für den WinRM HTTPS-Listener konfiguriert haben. Der Standard-HTTPS-Port ist 5986. Zum Beispiel

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
protocol=TCP localport=5986
```

6. Wenn Sie HTTPS-Listener verwenden, gehen Sie wie folgt vor, um das Zertifikat zum XClarity Administrator-Truststore hinzuzufügen. Indem Sie das Zertifikat zum Truststore hinzufügen, kann XClarity Administrator die WinRM HTTPS-Listener als vertrauenswürdig einstufen, mit denen es eine Verbindung hergestellt wird. Wiederholen Sie die folgenden Schritte für zusätzliche Zertifizierungspfade, die für die Windows-Remoteverwaltung als vertrauenswürdig eingestuft werden müssen.
   a. Ermitteln und sammeln Sie das Stammzertifikat der Zertifizierungsstelle, das Sie zum Signieren der Serverzertifikate für das Windows-Zielsystem verwendet haben. Wenn Sie keinen Zugriff auf das CA-Stammzertifikat haben, sammeln Sie das Serverzertifikat selbst oder ein anderes Zertifikat im Zertifizierungspfad.
   b. Wählen Sie in der Menüleiste von XClarity Administrator die Optionen **Verwaltung → Sicherheit** aus, um die Seite Sicherheit aufzurufen.
   c. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Vertrauenswürdige Zertifikate**.
   d. Klicken Sie auf das Symbol **Erstellen** ( ), um das Dialogfeld Zertifikat hinzufügen anzuzeigen.
   e. Suchen Sie nach der Zertifikatsdatei, die Sie in Schritt 1 erfasst haben, oder kopieren Sie die Inhalte des Zertifikatsdatei und fügen Sie sie im Textfeld ein.
   f. Klicken Sie auf **Erstellen**.
7. Wenn der WinRM-Listener auf Ihren Windows-Zielsystemen ausgeführt wird, kann XClarity Administrator eine Verbindung mit diesen Systemen herstellen und Aktualisierungen der Einheitentreiber durchführen.

- **Für HTTP**
  1. Konfigurieren Sie die Remoteverwaltungsbefehle und -daten über eine HTTP-Verbindung, indem Sie den folgenden Befehl über eine Administrator-Eingabeaufforderung ausführen, und bestätigen Sie die vorgeschlagenen Konfigurationsänderungen.

```
winrm quickconfig
```

  2. Aktivieren Sie die Standardauthentifizierung für lokale Windows-Benutzer durch Ausführen des folgenden Befehls über eine Administrator-Eingabeaufforderung.

```
winrm set winrm/config/service/Auth @{Basic="true"}
```

  3. Weisen Sie genügend Hauptspeicher für die Aktualisierungsbefehle auf diesem System zu, indem sie den folgenden Befehl über eine Administrator-Eingabeaufforderung ausführen.

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

  4. Lassen Sie unverschlüsselte Daten zu, indem Sie den folgenden Befehl über eine Administrator-Eingabeaufforderung ausführen.

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

  5. Öffnen Sie den Port in der Firewall, den Sie für den WinRM-HTTP-Listener konfiguriert haben. Der Standard-HTTPS-Port ist 5985. Zum Beispiel

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
protocol=TCP localport=5985
```

Wenn der WinRM-Listener auf Ihren Windows-Zielsystemen ausgeführt wird, kann XClarity Administrator eine Verbindung mit diesen Systemen herstellen und Aktualisierungen der Einheitentreiber durchführen.

Domänenaccount für BS-Einheitentreiberaktualisierungen konfigurieren

Mithilfe von Domänenaccounts können Sie die Berechtigungen einfach mit einem Domänencontroller verwalten. Für die Verwendung eines Domänenaccounts beim Aktualisieren von BS-Einheitentreibern müssen Sie einen Domänenaccount konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass sich die verwalteten Windows-Server in einem Domänennetzwerk befinden, bevor Sie Domänenaccounts konfigurieren.

Wenn Sie den Windows-Benutzeraccount in Lenovo XClarity Administrator hinzufügen, verwenden Sie das Format `USER@DOMAIN`. Das Format `DOMAIN/USER` wird nicht unterstützt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Domänenaccount zu konfigurieren.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Windows-Treiberaktualisierungen: Übernehmen**. Die Seite Windows-Treiberaktualisierungen: Übernehmen wird angezeigt.

Schritt 2. Klicken Sie auf **Alle Aktionen → Domänenaccount verwalten**. Die Seite „Domänenaccounts“ wird angezeigt.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ), um einen Bereich für den Domänenaccount hinzuzufügen. Das Dialogfeld Bereich erstellen wird angezeigt.

Schritt 4. Geben Sie einen Namen und einen oder mehrere Schlüsselverteilungszentrum-Hostnamen für den Bereich an. Verwenden Sie das Symbol **Hinzufügen** ( ), um einen weiteren Hostnamen hinzuzufügen, und verwenden Sie das Symbol **Entfernen** ( ), um einen Hostnamen zu entfernen.

Schritt 5. Klicken Sie auf **OK**, um den Bereich zu speichern.

Schritt 6. Auf der Seite „Domänenaccounts“ können Sie auch den Bereich auswählen, der standardmäßig verwendet werden soll.

Schritt 7. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Nach dieser Aufgabe

Über die Seite „Domänenaccount konfigurieren“ können Sie die folgenden Aktionen ausführen.

- Ändern Sie einen ausgewählten Bereich, indem Sie auf das Symbol **Bearbeiten** ( ) klicken.
- Löschen Sie einen ausgewählten Bereich über das Symbol **Löschen** ( ).

Globale Aktualisierungseinstellungen für Windows-Einheitentreiber konfigurieren

Globale Einstellungen dienen als Standardeinstellungen, wenn Aktualisierungen für Windows-Einheitentreiber übernommen werden.

Zu dieser Aufgabe

Über die Seite „Globale Einstellungen“ können Sie die folgenden Einstellungen konfigurieren:

- HTTPS für Windows-Treiberaktualisierungen verwenden
- Einheitentreiber für installierte Hardware anzeigen

Vorgehensweise

So konfigurieren Sie die globalen Einstellungen, die für alle Server verwendet werden:

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Windows-Treiberaktualisierungen: Übernehmen**. Die Seite Windows-Treiberaktualisierungen: Übernehmen wird angezeigt.

Schritt 2. Klicken Sie auf **Alle Aktionen → Globale Einstellungen**, um das Dialogfeld Globale Einstellungen: Windows-Treiberaktualisierungen anwenden anzuzeigen.

Schritt 3. Wählen Sie optional die folgenden Optionen.

- Wählen Sie **HTTPS für Windows-Treiberaktualisierungen verwenden** aus, um die Windows-Remoteverwaltung (WinRM) über HTTPS zu verwenden und um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen (HTTPS ist der Standard).

  Wählen Sie diese Einstellung ab, um HTTP zu verwenden.

  Achtung: Bei Verwendung von HTTP werden Windows-Anmeldeinformationen *ohne* Verschlüsselung über das Netzwerk gesendet und können über häufig verfügbare Tools für die Behebung von Netzwerkproblemen angezeigt werden.
- Wählen Sie **Einheitentreiber für installierte Hardware anzeigen** aus, um nur Einheitentreiber für verwaltete Hardware aufzulisten.

  Wählen Sie diese Einstellung ab, um alle Einheitentreiber in den importierten UpdateXpress System Packs (UXSPs) aufzulisten.

  Wichtig: Nachdem Sie diese Option festgelegt haben, müssen Sie eine Konformitätsprüfung durchführen. Klicken Sie dazu auf das Symbol **Konformitätsprüfung** ( ) auf der Seite Windows-Treiberaktualisierungen: Übernehmen.

Schritt 4. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Windows-Einheitentreiber übernehmen

Sie können Einheitentreiber auf verwalteten Servern mit Windows übernehmen.

Vorbereitende Schritte

- Lenovo XClarity Administrator verwendet die Windows-Remoteverwaltung (WinRM) über HTTPS oder HTTP, um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen. WinRM muss ordnungsgemäß auf den Zielservern konfiguriert sein, bevor BS-Einheitentreiber aktualisiert werden können (siehe Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren)
- Nicht unterstützte Einheiten können nicht für Aktualisierungen ausgewählt werden.

- Lesen Sie die Hinweise zur Aktualisierung von Einheitentreibern, bevor Sie versuchen, die Einheitentreiber auf verwalteten Servern zu aktualisieren (siehe Hinweise zum Aktualisieren von BS-Einheitentreibern).
- Stellen Sie sicher, dass das Repository die UXSPs und Einheitentreiber enthält, die Sie implementieren möchten (siehe Windows-Einheitentreiber herunterladen).

  Anmerkung: Bei der Erstinstallation von XClarity Administrator sind Katalog und Repository leer.
- XClarity Administrator kann die Windows-Remoteverwaltung (WinRM) über HTTPS oder HTTP verwenden, um Befehle zur Aktualisierung von Einheitentreibern auf Windows-Zielsystemen auszuführen (HTTPS ist der Standard). Um HTTP zu verwenden, klicken Sie auf **Alle Aktionen → Globale Einstellungen** auf der Seite „Windows-Treiberaktualisierung: Übernehmen“ und deaktivieren Sie **HTTPS für Windows-Treiberaktualisierungen verwenden**.

  Achtung: Bei Verwendung von HTTP werden Windows-Anmeldeinformationen *ohne* Verschlüsselung über das Netzwerk gesendet und können über häufig verfügbare Tools für die Behebung von Netzwerkproblemen angezeigt werden.

  Wichtig:

  – Stellen Sie sicher, dass die Windows-Remoteverwaltung (WinRM) auf dem Zielserver so konfiguriert ist, dass die gleiche Einstellung (HTTPS bzw. HTTP) verwendet wird, die in XClarity Administrator definiert ist (siehe Windows Server für BS-Einheitentreiberaktualisierungen konfigurieren).
  – Stellen Sie sicher, dass WinRM auf dem Zielserver mit der Standardauthentifizierung konfiguriert ist.
  – Vergewissern Sie sich bei Verwendung von HTTPS, dass WinRM auf dem Zielserver mit **allowUnencrypted=false** konfiguriert ist.
- Stellen Sie sicher, dass PowerShell auf dem Zielserver unterstützt wird.
- Stellen Sie sicher, dass der Zielserver eingeschaltet ist, bevor Sie mit der Aktualisierung von Einheitentreibern beginnen. Wenn der Server nicht eingeschaltet ist, wählen Sie den Zielserver aus und klicken Sie auf **Alle Aktionen → Stromversorgungsaktionen → Einschalten**.
- Stellen Sie sicher, dass XClarity Administrator alle erforderlichen Informationen für den Zugriff auf das Hostbetriebssystem hat (siehe Zugriff auf Betriebssysteme auf verwalteten Servern verwalten).
- Wenn Sie beim Aktualisieren von BS-Einheitentreibern einen Domänenaccount verwenden möchten, stellen Sie sicher, dass Sie die erforderliche Konfigurationsdatei erstellt haben (siehe Domänenaccount für BS-Einheitentreiberaktualisierungen konfigurieren).
- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Sie können keine Einheitentreiber auf einem verwalteten Server aktualisieren, der von einem laufenden Job blockiert wird. Wenn auf dem Zielserver ein anderer Aktualisierungsjob ausgeführt wird, wird dieser Aktualisierungsjob in eine Warteschlange gestellt, bis der aktuelle Aktualisierungsjob abgeschlossen ist. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.

Zu dieser Aufgabe

XClarity Administrator aktualisiert nur Einheitentreiber, die nicht konform sind. Einheitentreiber sind nicht konform, wenn die Version auf dem Server älter als die Version im ausgewählten UXSP ist. Einheitentreiber mit gleicher oder neuerer Version als die in der ausgewählten UXSP werden übersprungen.

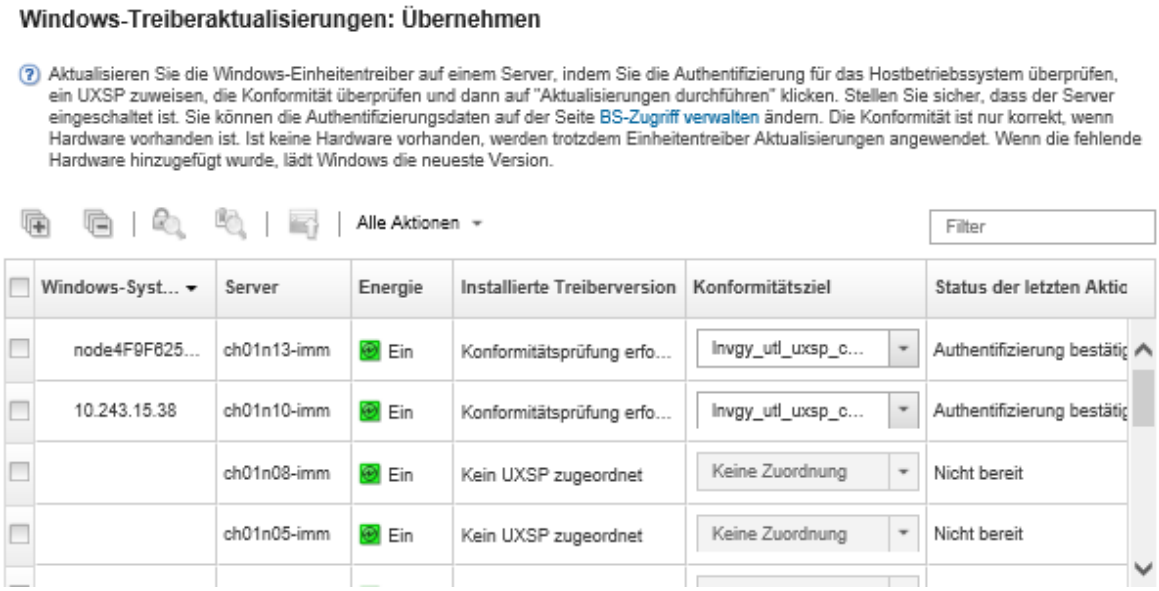
Vorgehensweise

So übernehmen Sie Windows-Einheitentreiber auf verwalteten Servern:

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → Windows-Treiberaktualisierungen: Übernehmen**, um die Seite Windows-Treiberaktualisierungen: Übernehmen anzuzeigen.

Wichtig:

- Um die Einheitentreiber auf dem Zielserver ermitteln und die Kompatibilität bestimmen zu können, müssen Sie den Zielserver auswählen und die Konformitätsprüfung durchführen. Nachdem die Konformitätsprüfung zum ersten Mal ausgeführt wurde, können Sie die Zeile erweitern, um eine Liste der Einheitentreiber auf dem Zielserver anzuzeigen.
- Die Spalte **Windows-System** enthält den Hostnamen oder die IP-Adresse des Hostbetriebssystems.
- Die Spalte **Server** gibt Namen und IP-Adresse des verwalteten Servers an.



Schritt 2. Wählen Sie einen oder mehrere Zielserver und Einheitentreiber aus.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Darüber hinaus können Sie die Liste der angezeigten Server filtern, indem Sie Text im Feld **Filter** (z. B. einen Namen oder eine IP-Adresse) eingeben.

Tipp:

- Sie können alle Einheitentreiber für ein bestimmtes Betriebssystem aktualisieren oder ein Betriebssystem erweitern und nur bestimmte Einheiten aktualisieren.
- Die Spalte **Aktualisierungsstatus** zeigt den Authentifizierungsstatus für jeden Server und den Aktualisierungsstatus für jede Einheitentreiber an.
- Die Spalte **BS-Anmeldeinformationen** enthält die gespeicherten Anmeldeinformationen, die zur Authentifizierung des Betriebssystems verwendet werden (z. B. „901 – company\USER1“).

  Wenn für das Hostbetriebssystem auf dem Zielserver keine Anmeldeinformationen für das Betriebssystem definiert sind, wird das Dialogfeld BS-Anmeldeinformationen bearbeiten angezeigt. Geben Sie für einen einzelnen Zielserver den Benutzernamen und das Kennwort an, die für diesen Vorgang verwendet werden sollen. Wählen Sie für mehrere Zielserver die gespeicherten Anmeldeinformationen aus, die für jeden Server verwendet werden sollen. Klicken Sie dann auf **Speichern**.

  Anmerkung: Die Anmeldeinformationen für das Betriebssystem, die Sie im Dialogfeld BS-Anmeldeinformationen bearbeiten ausgewählt haben, werden nicht für das Hostbetriebssystem gespeichert. Informationen zum Speichern von Betriebssystem-Anmeldeinformationen finden Sie unter Zugriff auf Betriebssysteme auf verwalteten Servern verwalten.

Schritt 3. Klicken Sie auf das Symbol **Authentifizierung prüfen** (), um eine Authentifizierungs- und erforderliche Prüfungen durchzuführen.

XClarity Administrator verbindet sich mithilfe der gespeicherten Anmeldeinformationen aus der Spalte **BS-Anmeldeinformationen** mit dem Hostbetriebssystem, bestimmt die BS-Version, stellt sicher, dass WinRM aktiviert ist, führt zusätzliche erforderliche Prüfungen durch trennt dann die Verbindung mit dem Hostbetriebssystem.

Weitere Informationen zum Ändern der gespeicherten Anmeldeinformationen für das Hostbetriebssystem finden Sie unter Zugriff auf Betriebssysteme auf verwalteten Servern verwalten.

Schritt 4. Wählen Sie für jeden Zielserver das Ziel-UXSP aus, das Sie zur Aktualisierung der Einheitentreiber aus der Spalte **Konformitätsziel** verwenden möchten.

Schritt 5. Wählen Sie die Zielserver erneut aus und klicken Sie auf das Symbol **Konformitätsprüfung** (), um die Konformität der einzelnen Einheitentreiber zu überprüfen.

Die Konformitätsprüfung aktualisiert den Konformitätsstatus in der Spalte **Installierte Treiberversion**. Diese Spalte zeigt den allgemeinen Konformitätsstatus für den Server und die installierte Version und den Konformitätsstatus für jeden Einheitentreiber entsprechend dem zugeordneten UXSP an.

-  **Konform**. Der installierte Einheitentreiber weist dieselbe oder eine neuere Version als die im zugeordneten UXSP auf.
-  **Nicht konform**. Der installierte Einheitentreiber ist älter als die Version im zugeordneten UXSP auf. Klicken Sie auf den Link, um weitere Informationen zur Non-Konformität zu erhalten.

Anmerkung: Die Konformität von Einheitentreibern ist nur korrekt, wenn Hardware vorhanden ist. Ist keine Hardware vorhanden, werden trotzdem Einheitentreiber auf den Server angewendet. Wenn die fehlende Hardware zum Server hinzugefügt wurde, lädt Windows die neueste Version.

Schritt 6. Klicken Sie auf das Symbol **Aktualisierungen durchführen** ().

Schritt 7. Wählen Sie eine der folgenden Aktualisierungsregeln aus.

- **Alle Aktualisierungen bei einem Fehler anhalten.** Wenn beim Aktualisieren eines Einheitentreibers auf einer Zieleinheit ein Fehler auftritt, wird der Aktualisierungsprozess für alle Zieleinheiten im aktuellen Einheitentreiber-Aktualisierungsjob gestoppt. In diesem Fall wird keine der Einheitentreiberaktualisierungen im UXSP für die Zieleinheit übernommen. Der aktuell auf den Zieleinheiten installierte Einheitentreiber bleibt in Kraft.
- **Bei einem Fehler fortfahren**. Wenn beim Aktualisieren eines Einheitentreibers auf der Zieleinheit ein Fehler auftritt, aktualisiert der Aktualisierungsprozess den Einheitentreiber der entsprechenden Einheit nicht. Der Aktualisierungsprozess wird jedoch zur Aktualisierung aller anderen Einheitentreiber in der Einheit und aller anderen Zieleinheiten im aktuellen Einheitentreiber-Aktualisierungsjob fortgesetzt.
- **Bei einem Fehler zum nächsten System wechseln**. Wenn beim Aktualisieren eines Einheitentreibers in der Einheit ein Fehler auftritt, stoppt der Aktualisierungsprozess alle Versuche, die Einheitentreiber für die entsprechende Einheit zu aktualisieren. Die aktuell auf der Einheit installierten Einheitentreiber bleiben also bestehen. Der Aktualisierungsprozess fährt mit der Aktualisierung aller anderen Einheiten im aktuellen Einheitentreiber-Aktualisierungsjob fort.

Schritt 8. Klicken Sie auf **Aktualisierungen durchführen**, um sofort zu aktualisieren, oder klicken Sie auf **Zeitplan**, um diese Aktualisierung geplant zu einem späteren Zeitpunkt auszuführen.

Nach dieser Aufgabe

Wenn der Wechsel zum Wartungsmodus bei einem Zielserver beim Übernehmen einer Aktualisierung fehlschlägt, versuchen Sie, die Aktualisierung erneut zu übernehmen.

Wenn Aktualisierungen nicht erfolgreich abgeschlossen werden, finden Sie unter Hinweise zum Aktualisieren von BS-Einheitentreibern Informationen zur Fehlerbehebung und Korrekturmaßnahmen.

Auf der Seite Windows-Treiberaktualisierung: Übernehmen können Sie die folgenden Aktionen ausführen.

- Sie können den Status der Einheitentreiberaktualisierung direkt über die Seite „Übernehmen“ in der Spalte **Aktualisierungsstatus** anzeigen.
- Sie können den Status der Einheitentreiberaktualisierung im Jobprotokoll überwachen. Klicken Sie im XClarity Administrator-Menü auf **Überwachung → Jobs**.

  Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

  Wenn der Aktualisierungsjob abgeschlossen ist, können Sie auf der Seite „Windows-Treiberaktualisierungen: Übernehmen“ überprüfen, dass die Einheiten konform sind. Die aktuelle, auf der jeweiligen Einheit aktive Treiberversion wird in der Spalte **Installierte Treiberversion** angezeigt.

Kapitel 15. Betriebssysteme auf Bare-Metal-Servern installieren

Sie können Lenovo XClarity Administrator verwenden, um das BS-Images-Repository zu verwalten und Betriebssystem-Images auf bis 28 Bare-Metal-Servern gleichzeitig zu implementieren.

Weitere Informationen:

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

Vorbereitende Schritte

Sie können XClarity Administrator nach Ablauf der 90 Tage weiterhin kostenlos verwenden, um Hardware zu verwalten und zu überwachen. Sie müssen jedoch Lizenzen für den vollständigen Funktionsumfang für jeden verwalteten Server erwerben, der erweiterte Lenovo XClarity Administrator-Funktionen unterstützt, um die Funktion „BS-Implementierung“ verwenden zu können. Lenovo XClarity Pro umfasst die Berechtigung für Service und Support sowie die Lizenz für den vollständigen Funktionsumfang. Weitere Informationen zum Kauf von Lenovo XClarity Pro erhalten Sie von Ihrem Lenovo-Ansprechpartner oder autorisierten Business Partner. Weitere Informationen finden Sie unter Lizenz für den vollständigen Funktionsumfang installieren in der Onlinedokumentation zu XClarity Administrator.

Zu dieser Aufgabe

XClarity Administrator bietet eine einfache Methode, um Betriebssystem-Images auf *Bare-Metal*-Servern zu implementieren, auf denen normalerweise kein Betriebssystem installiert ist.

Achtung: Wenn Sie ein Betriebssystem auf einem Server implementieren, auf dem bereits ein Betriebssystem installiert ist, führt XClarity Administrator 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-Adaptern, die auf dem Server installiert sind, wirken sich auf die Zeit aus, die XClarity Administrator für das Ausführen des Bestands auf dem Server benötigt. 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.
- Netzwerkdatenverkehr. XClarity Administrator lädt das Betriebssystem-Image über das Datennetzwerk oder das Betriebssystem-Implementierungsnetzwerk herunter.
- Die Hardwarekonfiguration auf dem Host, auf dem die virtuelle Lenovo XClarity Administrator-Einheit installiert ist. Die Arbeitsspeichergröße, die Prozessoren und der Festplattenspeicher können Einfluss auf die Zeiten zum Herunterladen haben.

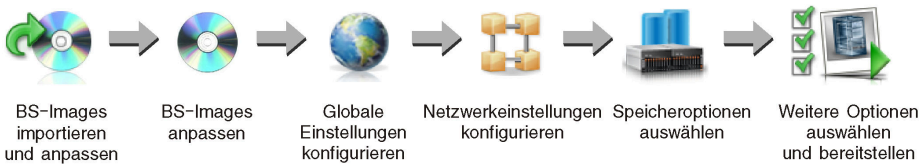
Wichtig: Um ein Betriebssystem-Image von XClarity Administrator zu implementieren, muss mindestens eine der XClarity Administrator-Schnittstellen (Eth0 oder Eth1) eine IP-Netzwerkverbindung zu der Servernetzwerkschnittstelle haben, die für den Zugriff auf das Hostbetriebssystem verwendet wird. Für die Betriebssystembereitstellung wird die auf der Seite Netzwerkzugriff definierte Schnittstelle genutzt. Weitere Informationen zu den Netzwerkeinstellungen finden Sie unter Netzwerkzugriff konfigurieren.

Bevor Sie eine Bare-Metal-Implementierung des Betriebssystems auf einem Server ausführen, bereiten Sie den Server vor. Aktualisieren Sie die Firmware auf die neueste Version und verwenden Sie Konfigurationsmuster, um den Server zu konfigurieren. Weitere Informationen finden Sie unter Firmware auf verwalteten Einheiten aktualisieren und Server mithilfe von Konfigurationsmustern konfigurieren.

Achtung: Es wird empfohlen, XClarity Administrator *nicht* für eine Bare-Metal-Implementierung des Betriebssystems auf Converged- und ThinkAgile-Einheiten zu verwenden.

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 BS-Image auf einem Server implementieren können, müssen Sie das Betriebssystem in das Repository importieren. Wenn Sie ein BS-Image importieren, führt XClarity Administrator Folgendes aus:

- 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.

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 für bestimmte Konfigurationen implementiert werden können.

Sie können auch unterstützte *angepasste Betriebssysteme* importieren. Dieses angepasste Image enthält ein vordefiniertes Platzhalterprofil, das nicht implementiert werden kann. Sie müssen ein angepasstes Profil importieren, das implementiert werden kann, oder basierend auf den Platzhalterprofil Ihr eigenes angepasstes Profil erstellen. Nachdem das angepasste Profil hinzugefügt wurde, wird das Profilplatzhalter automatisch entfernt.

Für Microsoft Windows Server 2016 und 2019 können Sie ein angepasstes Betriebssystem-Image für jede Version importieren. Das importierte Basis-Image enthält vordefinierte Profile, die die Installationskonfigurationen für dieses Image beschreiben. Sie können im angepassten BS-Image keine benutzerdefinierten Profile erstellen.

Eine Liste der unterstützten Basis- und angepassten Betriebssysteme finden Sie unter Unterstützte BetriebssystemeUnterstützte Betriebssysteme in der Onlinedokumentation von Lenovo XClarity Administrator.

Schritt 2. **(Optional) BS-Image anpassen.**

Sie können ein BS-Image anpassen, indem Sie Einheitentreiber, Boot-Dateien (nur für Windows), Konfigurationseinstellungen, Unattend-Dateien, Nach-Installationsskripts und Software hinzufügen. Wenn Sie ein Basis-BS-Image anpassen, erstellt XClarity Administrator ein angepasstes BS-Image-Profil, das die angepassten Dateien und Installationsoptionen enthält.

Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Schritt 3. **Globale Einstellungen konfigurieren.**

Globale Einstellungen sind Konfigurationsoptionen, die für die Betriebssystembereitstellung als Standard dienen. Sie können die folgenden globalen Einstellungen konfigurieren.

- Das Kennwort für den Administratorbenutzeraccount, der für die Bereitstellung der Betriebssysteme verwendet wird.
- Die Methode für die Zuweisung von IP-Adressen zu den Servern.
- Zur Aktivierung der installierten Betriebssysteme verwendete Lizenzschlüssel.
- Im Rahmen der Windows-Betriebssystembereitstellung können Sie optional einer Active Directory-Domäne beitreten.

Schritt 4. **Netzwerkeinstellungen konfigurieren.**

Sie können die Netzwerkeinstellungen für jeden Server angeben, auf dem Betriebssysteme implementiert werden sollen.

Wenn Sie DHCP zum dynamischen Zuweisen von IP-Adressen verwenden, müssen Sie die MAC-Adresse konfigurieren.

Wenn Sie statische IP-Adressen verwenden, müssen Sie die folgenden Netzwerkeinstellungen für einen Server konfigurieren, bevor Sie ein Betriebssystem auf diesem Server bereitstellen können. Nachdem diese Einstellungen konfiguriert sind, ändert sich der Bereitstellungsstatus zu „Bereit“. (Beachten Sie, dass einige Felder nicht für statische IPv6-Adressen verfügbar sind.)

- Hostname

  Der Hostname muss mit den folgenden Richtlinien übereinstimmen:
  - Die Hostnamen der einzelnen verwalteten Server müssen eindeutig sein.
  - Der Hostname darf Zeichenfolgen (Beschriftungen) enthalten, die durch einen Punkt (.) getrennt sind.
  - Eine Beschriftung kann ASCII-Zeichen, Ziffern und Bindestriche (-) enthalten. Die Zeichenfolge darf aber nicht mit einem Bindestrich beginnen oder enden und nicht nur Ziffern enthalten.
  - Die erste Beschriftung kann 2 bis 15 Zeichen lang sein. Nachfolgende Beschriftungen können 2 bis 63 Zeichen lang sein.
  - Die Gesamtlänge des Hostnamens darf 255 Zeichen nicht überschreiten.
- Die MAC-Adresse des Anschlusses auf dem Host, über den das Betriebssystem installiert wird.

  Die MAC-Adresse ist standardmäßig auf AUTO festgelegt. Diese Einstellung 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 XClarity Administrator-Host automatisch neu gestartet, um die erkannte MAC-Adresse für die Bereitstellung zu verwenden..

  Sie finden den Status des Ports für die MAC-Adresse, der für die BS-Implementierung verwendet wird, im Dropdown-Menü **MAC-Adresse** im Dialogfenster Netzwerkeinstellungen.

Wenn mehrere Ports aktiviert sind oder alle Ports ausgefallen sind, wird standardmäßig AUTO verwendet.

Anmerkungen:

- Virtuelle Netzwerkanschlüsse werden nicht unterstützt. Verwenden Sie keinen physischen Netzwerkanschluss, um mehrere virtuelle Netzwerkanschlüsse zu simulieren.
- Wenn die Netzwerkeinstellung des Servers auf „AUTO“ festgelegt ist, kann XClarity Administrator die Netzwerkanschlüsse in den Steckplätzen 1 – 16 automatisch erkennen. Mindestens ein Anschluss an den Steckplätzen 1 – 16 muss eine Verbindung zu XClarity Administrator haben.
- Wenn Sie für die MAC-Adresse einen Netzwerkanschluss in Steckplatz 17 oder höher verwenden möchten, können Sie das Programm „AUTO“ nicht verwenden. Stattdessen müssen Sie die Netzwerkeinstellung des Servers auf die MAC-Adresse des bestimmten Ports festlegen, den Sie verwenden möchten.
- Bei ThinkServer-Servern werden nicht alle MAC-Adressen des Hosts angezeigt. In den meisten Fällen werden MAC-Adressen für AnyFabric-Ethernet-Adapter im Dialogfeld Netzwerkeinstellungen ändern aufgelistet. MAC-Adressen für andere Ethernet-Adapter (z. B. Lan-On-Motherboard) werden nicht angezeigt. Wenn die MAC-Adresse für einen Adapter nicht verfügbar ist, verwenden Sie für die Nicht-VLAN-Bereitstellung die AUTO-Methode.

- IP-Adresse und Subnetzmaske
- IP-Gateway
- Bis zu zwei DNS-Server (Domain Name System)
- MTU-Geschwindigkeit
- VLAN-ID, wenn der VLAN-IP-Modus aktiviert ist

Wenn Sie VLAN verwenden, können Sie dem konfigurierten Hostnetzwerkadapter eine VLAN-ID zuordnen.

Schritt 5. **Speicheroptionen auswählen**

Sie können für jede Implementierung die gewünschte Speicherposition auswählen, an der das Betriebssystem implementiert werden soll. Je nach Betriebssystem können Sie für die Implementierung ein lokales Festplattenlaufwerk, einen integrierten Hypervisor-Schlüssel oder ein SAN festlegen.

Schritt 6. **Wählen Sie zusätzliche Optionen und angepasste Konfigurationseinstellungen aus und implementieren Sie das BS-Image.**

Sie können zusätzliche Implementierungsoptionen, z. B. den Lizenzschlüssel für die BS-Implementierung, und angepasste Konfigurationseinstellungen konfigurieren. Wenn Sie Microsoft Windows installieren, können Sie außerdem die Active Directory-Domäne für den Beitritt konfigurieren.

Anmerkungen:

- Wenn Sie angepasste Konfigurationseinstellungen für ein bestimmtes angepasstes BS-Profil definiert haben, müssen Sie Werte für die erforderlichen angepassten Konfigurationseinstellungen definieren, bevor Sie das Profil auf einem Server implementieren können.
- Beim Implementieren eines angepassten BS-Profils mit angepassten Einstellungen müssen alle Zielserver dasselbe angepasste BS-Profil verwenden und die Werte für die angepassten Einstellungen gelten für alle Zielserver.

Wählen Sie dann die Zielserver für die Implementierung und die BS-Images, die implementiert werden sollen, aus. Berücksichtigen Sie dabei, dass der Server den Implementierungsstatus „Bereitstellung“ aufweisen muss, damit ein Betriebssystem implementiert werden kann.

Sie können Betriebssystem-Images auf bis zu 28 Servern gleichzeitig implementieren.

Lesen Sie Hinweise zur Betriebssystembereitstellung, bevor Sie versuchen, ein Betriebssystem-Image zu implementieren.

Hinweise zur Betriebssystembereitstellung

Lesen Sie die folgenden Hinweise, bevor Sie versuchen, ein Betriebssystem-Image bereitzustellen.

Lenovo XClarity Administrator Hinweise

- Stellen Sie sicher, dass derzeit keine Jobs auf dem Zielserver ausgeführt werden. Klicken Sie auf **Überwachung → Jobs**, um eine Liste mit aktiven Jobs anzuzeigen.
- Stellen Sie sicher, dass auf dem Zielserver 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 Die Details eines verwalteten Servers anzeigen).
- Stellen Sie sicher, dass im Dialogfenster Globale Einstellungen: Betriebssysteme implementieren ein Kennwort für das Administratoraccount angegeben ist, das für die Implementierung des Betriebssystems verwendet werden soll. Weitere Informationen zum Festlegen des Kennworts finden Sie unter Globale BS-Implementierungseinstellungen konfigurieren.
- Stellen Sie sicher, dass die globalen Standardeinstellungen für diese Betriebssystembereitstellung richtig sind (siehe Globale BS-Implementierungseinstellungen konfigurieren).

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 XClarity Administrator-Repository werden auf bestimmten Hardwareplattformen möglicherweise nicht unterstützt. Nur BS-Image-Profile, die von ausgewählten Servern unterstützt werden, sind auf der Seite „BS-Images bereitstellen“ aufgeführt. Sie können in Lenovo OS Interoperability Guide-Website bestimmen, ob ein Betriebssystem mit einem bestimmten Server kompatibel ist.
- Für Windows müssen Sie eine Boot-Datei in das BS-Images-Repository importieren, bevor Sie ein Windows-Profil implementieren können. Lenovo fasst die vordefinierte Boot-Datei WinPE_64.wim mit verschiedenen Einheitentreibern in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Da die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Dateien** importieren.
- Für SLES 15 und 15 SP1 müssen Sie sowohl das Installationsprogramm-Image als auch das zugehörige Paket-Image von den Support-Center-Website für Server-BS importieren. Für SLES 15 SP2 oder höher müssen Sie nur das Image "Komplette Installationsmedien" importieren, da die Unified Installer- und Packages-DVDs von SUSE Linux Enterprise Server 15 und 15 SP1 veraltet sind.

- Bei ThinkSystem-Servern enthält XClarity Administrator Out-of-Box-Einheitentreiber zur Installation des Betriebssystems und grundlegender Netzwerk- und Speicherkonfigurationen für das finale Betriebssystem. Stellen Sie bei anderen Servern sicher, dass das zu implementierende Betriebssystem-Image über die entsprechenden Einheitentreiber für Ihre Ethernet-, Fibre Channel- und Speicheradapter-Hardware verfügt. Wenn der Einheitentreiber für E/A-Adapter nicht im Betriebssystem enthalten ist, wird dieser Adapter bei der Betriebssystembereitstellung nicht unterstützt. Installieren Sie immer ein aktuelles Betriebssystem, um sicherzustellen, dass die neuesten erforderlichen Inbox-Einheitentreiber für E/A-Adapter und Boot-Dateien vorhanden sind. Sie können auch Out-of-Box-Einheitentreiber und Boot-Dateien auch zu Betriebssystemen hinzufügen, die in XClarity Administrator importiert wurden (siehe BS-Image-Profile anpassen in der Onlinedokumentation von XClarity Administrator).

  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.
- Für die Bereitstellung von SLES 12 SP2 für ThinkSystem Server muss ein kISO-Profil verwendet werden. Um die kISO-Profile zu beziehen, müssen Sie das entsprechende SLES kISO-Image importieren, nachdem Sie das SLES-Basisbetriebssystem importiert haben. Sie können das SLES-kISO-Image von Linux-Support – Downloads-Website herunterladen.

  Anmerkungen:

  – Das SLES kISO-Image wird zur maximalen Anzahl an importierten BS-Images hinzugezählt.

    Eine Liste der unterstützten Basis- und angepassten Betriebssysteme finden Sie unter Unterstützte BetriebssystemeUnterstützte Betriebssysteme in der Onlinedokumentation von Lenovo XClarity Administrator.

  – Wenn Sie alle kISO-Profile löschen, müssen Sie das SLES-Basisbetriebssystem löschen und anschließend erneut das Basisbetriebssystem und das kISO-Image importieren, um SLES 12 SP2 auf einem ThinkSystem Server zu implementieren.

  – Wenn Sie ein angepasstes BS-Profil basierend auf einem kISO-Profil erstellen, sind die vordefinierten Einheitentreiber im Basisbetriebssystem nicht enthalten. Stattdessen werden die Einheitentreiber, die im kISO enthalten sind, verwendet. Sie können auch Einheitentreiber zum angepassten BS-Profil hinzufügen (siehe Angepasstes BS-Image-Profil erstellen).

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 XClarity Administrator mit dem Zielserver (sowohl Baseboard Management Controller als auch Datennetzwerk der Server) über die Netzwerkschnittstelle (Eth0 oder Eth1) kommunizieren kann, die bei Konfiguration der XClarity Administrator-Netzwerkeinstellungen ausgewählt wurde.

  Informationen zur Angabe einer Schnittstelle, die für die Betriebssystemimplementierung verwendet wird, finden Sie unter Netzwerkzugriff konfigurieren.

  Weitere Informationen zu Betriebssystem-Implementierungsnetzwerken und -schnittstellen finden Sie unter Hinweise zum Netzwerkbetrieb in der Onlinedokumentation von XClarity Administrator.
- Stellen Sie sicher, dass die IP-Adressen für das Hostbetriebssystem eindeutig sind. XClarity Administrator sucht nach doppelten IP-Adressen, die Sie beim Implementierungsprozess für die Netzwerkadresse angeben.
- Wenn die Netzwerkverbindung langsam oder instabil ist, kann die Implementierung von Betriebssystemen unvorhersehbare Ergebnisse zur Folge haben.

- Die XClarity Administrator Netzwerkschnittstelle, die für die Verwaltung verwendet wird, muss über dieselbe IP-Adressmethode, die Sie im Dialogfeld „Globale Einstellungen: Betriebssysteme implementieren“ ausgewählt haben, mit dem Baseboard Management Controller verbunden sein. Wenn XClarity Administrator beispielsweise die Konfiguration so eingerichtet ist, dass sie eth0 für die Verwaltung verwendet, und Sie bei der Konfiguration des implementierten Betriebssystems statisch zugewiesene statische IPv6-Adressen verwenden, muss eth0 mit einer IPv6-Adresse konfiguriert werden, die über eine Verbindung zum Baseboard Management Controller verfügt.
- Wenn Sie keine IPv6-Adressen in den globalen Einstellungen für die BS-Implementierung verwenden möchten, muss die IPv6-Adresse für XClarity Administrator zum Baseboard Management Controller und dem Datennetzwerk der Server weiterleitbar sein.
- Der IPv6-Modus wird nicht für ThinkServer unterstützt (siehe IPv6-Konfigurationseinschränkungen in der Onlinedokumentation von XClarity Administrator).
- Wenn Sie DHCP zum dynamischen Zuweisen von IP-Adressen verwenden, müssen Sie die MAC-Adresse konfigurieren.
- Wenn Sie statische IP-Adressen verwenden, müssen Sie die folgenden Netzwerkeinstellungen für einen Server konfigurieren, bevor Sie ein Betriebssystem auf diesem Server bereitstellen können. Nachdem diese Einstellungen konfiguriert sind, ändert sich der Bereitstellungsstatus zu „Bereit“. (Beachten Sie, dass einige Felder nicht für statische IPv6-Adressen verfügbar sind.)

  – Hostname

    Der Hostname muss mit den folgenden Richtlinien übereinstimmen:
    – Die Hostnamen der einzelnen verwalteten Server müssen eindeutig sein.
    – Der Hostname darf Zeichenfolgen (Beschriftungen) enthalten, die durch einen Punkt (.) getrennt sind.
    – Eine Beschriftung kann ASCII-Zeichen, Ziffern und Bindestriche (-) enthalten. Die Zeichenfolge darf aber nicht mit einem Bindestrich beginnen oder enden und nicht nur Ziffern enthalten.
    – Die erste Beschriftung kann 2 bis 15 Zeichen lang sein. Nachfolgende Beschriftungen können 2 bis 63 Zeichen lang sein.
    – Die Gesamtlänge des Hostnamens darf 255 Zeichen nicht überschreiten.

  – Die MAC-Adresse des Anschlusses auf dem Host, über den das Betriebssystem installiert wird.

    Die MAC-Adresse ist standardmäßig auf AUTO festgelegt. Diese Einstellung 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 XClarity Administrator-Host automatisch neu gestartet, um die erkannte MAC-Adresse für die Bereitstellung zu verwenden..

    Sie finden den Status des Ports für die MAC-Adresse, der für die BS-Implementierung verwendet wird, im Dropdown-Menü **MAC-Adresse** im Dialogfenster Netzwerkeinstellungen. Wenn mehrere Ports aktiviert sind oder alle Ports ausgefallen sind, wird standardmäßig AUTO verwendet.

    Anmerkungen:

    – Virtuelle Netzwerkanschlüsse werden nicht unterstützt. Verwenden Sie keinen physischen Netzwerkanschluss, um mehrere virtuelle Netzwerkanschlüsse zu simulieren.
    – Wenn die Netzwerkeinstellung des Servers auf „AUTO“ festgelegt ist, kann XClarity Administrator die Netzwerkanschlüsse in den Steckplätzen 1 – 16 automatisch erkennen. Mindestens ein Anschluss an den Steckplätzen 1 – 16 muss eine Verbindung zu XClarity Administrator haben.
    – Wenn Sie für die MAC-Adresse einen Netzwerkanschluss in Steckplatz 17 oder höher verwenden möchten, können Sie das Programm „AUTO“ nicht verwenden. Stattdessen müssen Sie die Netzwerkeinstellung des Servers auf die MAC-Adresse des bestimmten Ports festlegen, den Sie verwenden möchten.
    – Bei ThinkServer-Servern werden nicht alle MAC-Adressen des Hosts angezeigt. In den meisten Fällen werden MAC-Adressen für AnyFabric-Ethernet-Adapter im Dialogfeld Netzwerkeinstellungen

ändern aufgelistet. MAC-Adressen für andere Ethernet-Adapter (z. B. Lan-On-Motherboard) werden nicht angezeigt. Wenn die MAC-Adresse für einen Adapter nicht verfügbar ist, verwenden Sie für die Nicht-VLAN-Bereitstellung die AUTO-Methode.

  - IP-Adresse und Subnetzmaske
  - IP-Gateway
  - Bis zu zwei DNS-Server (Domain Name System)
  - MTU-Geschwindigkeit
  - VLAN-ID, wenn der VLAN-IP-Modus aktiviert ist
- Wenn Sie VLAN verwenden, können Sie dem konfigurierten Hostnetzwerkadapter eine VLAN-ID zuordnen.

Weitere Informationen zu Betriebssystem-Bereitstellungsnetzwerken und -schnittstellen finden Sie unter Netzwerkeinstellungen für verwaltete Server konfigurieren und Netzwerkeinstellungen für verwaltete Server konfigurieren und Hinweise zum Netzwerkbetrieb in der XClarity Administrator-Onlinedokumentation.

Hinweise zu Speicher- und Bootoptionen

- Vergewissern Sie sich vor dem Implementieren eines Betriebssystems, dass als UEFI-Bootoption auf dem Zielserver „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. Weitere Informationen finden Sie unter BS-Installationsprogramm kann das Laufwerk für die Installation von XClarity Administrator nicht finden in der XClarity Administrator Onlinedokumentation.

    Diese Ausnahme gilt nicht für M.2-Laufwerke.
  - Wenn eine verwaltete Einheit sowohl nicht für Hardware-RAID konfigurierte lokale Laufwerke (SATA, SAS oder SSD) als auch M.2-Laufwerke besitzt, müssen Sie für die Verwendung von M.2-Laufwerken die lokalen Laufwerke deaktivieren, oder Sie müssen die M.2-Laufwerke deaktivieren, wenn Sie lokale Laufwerke verwenden möchten. Sie können interne Speichercontrollereinheiten und Legacy- sowie UEFI-ROM-Speicheroptionen mithilfe der Konfigurationsmuster deaktivieren, indem Sie „Lokale Festplatte deaktivieren“ auf der Registerkarte „Lokaler Speicher“ des Assistenten auswählen, oder ein Konfigurationsmuster aus einem vorhandenen Server erstellen und anschließend die M.2-Einheiten im erweiterten UEFI-Muster deaktivieren.
  - 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.
- Bei der Bereitstellung von RHEL wird nicht unterstützt, dass mehrere Ports mit derselben LUN auf dem Zielspeicher verbunden sind.
- 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.

- Wenn Sie Microsoft Windows auf einem Server implementieren, dürfen auf den angeschlossenen Laufwerken keine Systempartitionen vorhanden sein (siehe BS-Implementierung schlägt wegen vorhandener Systempartitionen auf angeschlossenem Plattenlaufwerk fehl in der XClarity Administrator Onlinedokumentation).
- 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. Weitere Informationen finden Sie unter Booten des BS-Installationsprogramms auf einem ThinkServer-Server nicht möglich – XClarity Administrator in der Onlinedokumentation von XClarity Administrator.
  - 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 Speicherposition für verwaltete Server auswählen.

Hinweise zu verwalteten Einheiten

- Weitere Informationen zu Einschränkungen bei Betriebssystemimplementierungen für bestimmte Einheiten finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Öffnen Sie die Registerkarte **Kompatibilität** und klicken Sie dann auf den Link für die entsprechenden Einheitentypen.
- Stellen Sie sicher, dass keine angehängten Medien (z. B. ISOs) auf dem Zielserver vorhanden sind. Sorgen Sie außerdem dafür, dass keine aktiven fernen Mediensitzungen auf dem Management-Controller geöffnet sind.
- Stellen Sie sicher, dass der Zeitstempel im BIOS auf das aktuelle Datum und die Uhrzeit eingestellt ist.
- Stellen Sie bei Servern mit XCC2, aktiviertem Systemschutz und der festgelegten Aktion **BS-Start verhindern** sicher, dass der Systemschutz auf der Einheit konform ist. Wenn der Systemschutz nicht konform ist, werden die Einheiten daran gehindert, den Bootvorgang abzuschließen, wodurch die BS-Implementierung fehlschlägt. Damit Sie diese Einheit bereitstellen können, reagieren Sie manuell auf die Systemschutz-Bootaufforderung, damit die Einheiten normal booten können.
- Stellen Sie bei ThinkSystem- und System x-Servern 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 bei Flex System-Servern sicher, dass das Gehäuse eingeschaltet ist.
- Stellen Sie sicher, dass auf konvergenten, NeXtScale- und System x-Servern 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 Den Status eines verwalteten Servers anzeigen). Weitere Informationen zu den auf Ihren Servern installierten FoD-Schlüsseln finden Sie unter Features on Demand-Schlüssel anzeigen.
- Für ThinkSystem-Server und ThinkAgile-Einheiten ist die Funktion XClarity Controller Enterprise für die Betriebssystemimplementierung erforderlich. Weitere Informationen finden Sie unter Features on Demand-Schlüssel anzeigen
- Für Converged- und ThinkAgile-Einheiten wird empfohlen, XClarity Administrator *nicht* für eine Bare-Metal-Implementierung des Betriebssystems zu verwenden.

Unterstützte Betriebssysteme

Lenovo XClarity Administrator unterstützt die Implementierung verschiedener Betriebssysteme. In das BS-Images-Repository von XClarity Administrator können nur unterstützte Versionen der Betriebssysteme geladen werden.

Wichtig:

- Weitere Informationen zu Einschränkungen bei Betriebssystemimplementierungen für bestimmte Einheiten finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Öffnen Sie die Registerkarte **Kompatibilität** und klicken Sie dann auf den Link für die entsprechenden Einheitentypen.
- Die Funktion zur Verschlüsselungsverwaltung von XClarity Administrator 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 Administrator bereitgestellt werden können.
- Betriebssystem-Images im XClarity Administrator-Repository werden auf bestimmten Hardwareplattformen möglicherweise nicht unterstützt. Nur BS-Image-Profile, die von ausgewählten Servern unterstützt werden, sind auf der Seite „BS-Images bereitstellen“ aufgeführt. 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 Administrator bereitgestellt werden können.

Betriebssystem	Versionen	Hinweise
CentOS Linux	7.2 and later 8.0 8.1 8.2	**Anmerkungen:** • Alle vorhandenen und zukünftigen Nebenversionen werden unterstützt, es sei denn, wenn nicht anders vermerkt. • DHCP, statische IPv4- und statische IPv6-Adressen werden unterstützt. • VLAN-Tagging wird nicht unterstützt. • Out-of-Box-Treiber werden nicht unterstützt. • Die Anpassung des BS-Profils wird nicht unterstützt. • CentOS8.3 wird nicht unterstützt.
Microsoft® Windows® Azure Stack HCI	20H2 21H2	Die Anpassung des BS-Profils wird nicht unterstützt.
Microsoft Windows Client	10 21H2 10 22H2 11 22H2	

Betriebssystem	Versionen	Hinweise
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	Einzelhandels- und Volumenlizenzversionen werden unterstützt. **Anmerkung:** XClarity Administrator wird nur mit Windows-Versionen getestet, die zum Release-Datum der XClarity Administrator-Version von Microsoft unterstützt werden. Die folgenden Versionen werden *nicht unterstützt*: • Windows Reseller Option Kit (ROK) • Windows Server Semi-Annual Channel (SAC) v1709, v1803 und v1809 • Windows Server2019 Essentials • Windows Server 2016 Nanoserver • Windows Server 2012 Evaluierungsversion • Windows Server-Images auf verwalteten Servern mit integrierten Hypervisor-Schlüsseln Windows Server2012 R2 auf Servern mit Intel CLX-Prozessoren Sie müssen den integrierten Hypervisor-Schlüssel physisch von den Zielservern entfernen, bevor Sie ein Windows-Image implementieren. Dazu zählt Hyper-V über eines der Virtualisierungsprofile. – Datacenter – Rechenzentrumskern – Rechenzentrumsvirtualisierung (Hyper-V) – Rechenzentrums-Virtualisierungskern (Hyper-V mit Kern) – Standard – Standardkern – Standardvirtualisierung (Hyper-V) – Standardvirtualisierungskern (Hyper-V mit Kern)
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x 9.x	Enthält KVM **Anmerkungen:** • 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 RHELv7.4 oder höher empfohlen. • Zum Bereitstellen von RHEL7.2 muss die globale IP-Zuordnung für die Verwendung von IPv4-Adressen konfiguriert sein. Weitere Informationen zu globalen Einstellungen finden Sie unter Globale BS-Implementierungseinstellungen konfigurieren. • Bei IPv6-Netzwerken mit geringer Bandbreite wurden fehlgeschlagene BS-Implementierungen festgestellt, die auf Zeitlimitüberschreitungen beim BS-Installationsprogramm zurückgehen. • VLAN-Tagging wird nicht unterstützt.
Rocky Linux	8.x 9.x	**Anmerkungen:** • Alle vorhandenen und zukünftigen Nebenversionen werden unterstützt, es sei denn, wenn nicht anders vermerkt. • DHCP, statische IPv4- und statische IPv6-Adressen werden unterstützt. • VLAN-Tagging wird nicht unterstützt. • Out-of-Box-Treiber werden nicht unterstützt.

Betriebssystem	Versionen	Hinweise
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Einschließlich KVM- und Xen-Hypervisoren **Anmerkungen:** • 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. • Bei IPv6-Netzwerken mit geringer Bandbreite wurden fehlgeschlagene BS-Implementierungen festgestellt, die auf Zeitlimitüberschreitungen beim BS-Installationsprogramm zurückgehen. • Für die Bereitstellung von SLES 12 SP2 auf einem ThinkSystem Server muss ein kISO-Profil verwendet werden. Um die kISO-Profile abzurufen, müssen Sie das entsprechende SLES kISO-Image importieren. Siehe Hinweise zur Betriebssystembereitstellung für weitere Informationen. • Für SLES 15 und 15 SP1 müssen Sie sowohl das Installationsprogramm-Image als auch das zugehörige Paket-Image von den Support-Center-Website für Server-BS importieren. Für SLES 15 SP2 oder höher müssen Sie nur das Image "Komplette Installationsmedien" importieren, da die Unified Installer- und Packages-DVDs von SUSE Linux Enterprise Server 15 und 15 SP1 veraltet sind. • VLAN-Tagging wird nicht unterstützt.
Ubuntu-Server	20.04.x 22.04.x	**Anmerkungen:** • Das Image kann auf der ausgewählten Speicheroption (lokales Festplattenlaufwerk, M.2-Laufwerk oder FC-SAN-Datenträger) installiert werden. • Alle vorhandenen und zukünftigen Nebenversionen werden unterstützt, es sei denn, wenn nicht anders vermerkt. • Es wird nur DHCP unterstützt. Statische IPv4- und statische IPv6-Adressen *werden nicht* unterstützt. • VLAN-Tagging *wird nicht* unterstützt. • Out-of-Box-Treiber *werden nicht* unterstützt. • Die Anpassung des BS-Profils *wird nicht* unterstützt.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.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 Verwaltungstools von Lenovo unterstützen außerdem eine vereinfachte ESXi-Verwaltung mit ausgewählten Systemx-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:** • Alle vorhandenen und zukünftigen Aktualisierungspakete für 6.0, 6.5, 6.7, 7.0 und 8.0 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). Sie können Out-of-Box-Einheitentreiber hinzufügen, indem Sie eigene angepasste OS0image-Profile erstellen (siehe BS-Image-Profile anpassen).

Betriebssystem	Versionen	Hinweise
		• Für einige Versionen der angepassten Lenovo VMware ESXi-Images sind möglicherweise separate Images für System x, ThinkSystem 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. • Die folgenden Versionen werden für ThinkServer-Einheiten unterstützt: ESXi 6.0u3, 6.5 und höher. • Während der Installation von ESXi5.5 (alle Aktualisierungen) oder 6.0 auf einem Server in einem Flex System Gehäuse antwortet der Server möglicherweise nicht mehr oder wird kurz nach der folgenden Meldung neu gestartet: `Loading image.pld` • ESXi 5.5 erfordert, dass im Speicher abgebildeter E/A-Platz (MMIO; memory-mapped I/O) innerhalb der ursprünglichen 4GB des Systems konfiguriert wird. Je nach verwendeter Konfiguration versuchen bestimmte Systeme, mehr Hauptspeicher als 4GB zu verwenden, was Fehler verursachen kann. Informationen zum Beheben des Problems finden Sie unter VMware-Bereitstellung verursacht Blockierung des Systems oder Neustart in der Onlinedokumentation von XClarity Administrator. • Wenn Sie ESXi mit einem statischen IPv6-Modus implementieren, wird der auf der Seite „Netzwerkeinstellungen“ in XClarity Administrator definierte Hostname nicht in der implementierten ESXi-Instanz konfiguriert. Stattdessen wird der Standardhostname `localhost` verwendet. Sie müssen den Hostnamen manuell im implementierten ESXi festlegen, um ihn an den in XClarity Administrator definierten Hostnamen anzupassen. • Wenn Sie ESXi auf einem verwalteten Server implementieren, verschiebt das Betriebssystem das Laufwerk, auf dem das Betriebssystem installiert ist, nicht explizit an den Anfang der Bootreihenfolge. Wenn eine Booteinheit mit einem bootfähigen Betriebssystem oder PXE-Server vor der ESXi-Booteinheit angegeben ist, startet ESXi nicht. Für die Implementierung von ESXi aktualisiert XClarity Administrator die Bootreihenfolge für die meisten Server, um sicherzustellen, dass die ESXi-Booteinheit oben auf der Liste steht. ThinkServer-Server bieten jedoch keine Möglichkeit, damit XClarity Administrator die Bootreihenfolge dahingehend aktualisieren kann. Sie müssen die PXE-Boot-Unterstützung deaktivieren oder bootfähige Einheiten (außer dem Laufwerk mit der Installation) entfernen, bevor sie das Betriebssystem implementieren können. Weitere Informationen finden Sie unter Betriebssystem startet nicht, nachdem ESXi auf dem ThinkServer-Server implementiert wurde in der Onlinedokumentation von XClarity Administrator. **Tipp**: Sie können ein für die Virtualisierung bestimmtes, vordefiniertes, erweitertes UEFI-Muster verwenden, statt **MM Config** über das Setup Utility für jeden Server zu definieren. Mit diesem Muster wird die MM Config-Option auf 3GB festgelegt und die PCI-64-Bit-Ressourcenzuordnung deaktiviert. Weitere Informationen zu diesen Mustern finden Sie unter Erweiterte UEFI-Einstellungen definieren.

Betriebssystem-Image-Profile

Wenn Sie ein BS-Image in das BS-Images-Repository importieren, erstellt Lenovo XClarity Administrator mindestens ein Profil für dieses Image und speichert es im BS-Images-Repository. Jedes vordefinierte *Profil* enthält das BS-Image und die Installationsoptionen für dieses Image.

Attribute für BS-Image-Profil

Attribute für OS-Image-Profil bieten zusätzliche Informationen zu einem BS-Image-Profil. Es können die folgenden Attribute angezeigt werden.

- **kISO**. Sie müssen zur Bereitstellung von SLES 12 SP2 für einen ThinkSystem Server ein kISO-Profil verwenden. Sie können das SLES-kISO-Image von Linux-Support – Downloads-Website herunterladen.

Vordefinierte BS-Image-Profile

Der folgenden Tabelle sind die Profile aufgeführt, die von XClarity Administrator vordefinierten sind, wenn Sie ein Betriebssystem-Image importieren. Diese Tabelle enthält außerdem die Pakete, die in den einzelnen Profilen enthalten sind.

Sie können ein angepasstes BS-Image-Profil für ein Basisbetriebssystem erstellen. Weitere Informationen finden Sie unter BS-Image-Profile anpassen.

Betriebssystem	Profil	Pakete im Profil	

CentOS Linux	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`	

	Virtualisie-rung	`%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`
			`libicu`
			`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`

Betriebssystem	Profil	Pakete im Profil
Microsoft® Windows® Azure Stack HCI	Azure	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="Containers" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />
Microsoft Windows Client	Enterprise	
	Enterprise N	
	Workstations Pro	
	Workstati-ons_Pro N	
Microsoft Windows Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />
Microsoft Windows Server **Anmerkung:** Enthält Hyper-V über das *Virtualisierungsprofil.*	Datacenter	GUI
	Rechenzent-rumsvirtuali-sierung	GUI Hyper-V role
	Rechenzent-rums-Virtualisie-rungskern	Hyper-V role
	Rechenzent-rumskern	
	Standard	GUI
	Standardvir-tualisierung	GUI Hyper-V role
	Standardvir-tualisierungs-kern	Hyper-V role
	Standardkern	
Angepasster Microsoft Windows Server	Rechenzent-rum_ angepasst	

Betriebssystem	Profil	Pakete im Profil	
	Standard_ angepasst		
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	
	Virtualisie-rung	%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 libicu 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
Rocky Linux	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	

Betriebssystem	Profil	Pakete im Profil	
	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 libicu 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) 15	Basis und Basis	<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>	
	Minimal und Minimal	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	
	Virtualisierung – KVM und Virtualisierung – KVM	<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>	

Betriebssystem	Profil	Pakete im Profil
	Virtualisierung – Xen und Virtualisierung – Xen	<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>
Ubuntu	Minimal	OpenSSH-Server
	Virtualisierung	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
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 Ports aufgeführt, die offen sein müssen (nicht blockiert).

Kommunikation	RHEL-, Centos- und Rocky-Virtualisierungsprofil[1]	RHEL-, Centos- sowie Rocky Basis- und Minimalprofile[1]	SLES-Virtualisierungs-, Basis- und Minimalprofile[2]	Ubuntu-Virtualisierungs- und Minimalprofile[3]	VMware ESXi-Virtualisierungsprofil[4]	Windows-Profile
Ausgehend (Ports auf externen Systemen geöffnet)	• Kommunikation mit RHEL KVM-Netzwerkgeräten – TCP und UDP an Ports **53** und **67** • Kommunikation mit SNMP-Agenten – UDP an Port **161** • Kommunikation mit SLP-Serviceagent, SLP-Verzeichnisagent – TCP und UDP an Port **427** • CIM-XML über HTTP-Kommunikation – TCP on Port **15988** und **15989** • Kommunikation für virtuelle KVM-Server – TCP an Ports **49152 - 49215**					• SMB-Kommunikation – TCP an Port **445**
Eingehend (Ports auf der XClarity Administrator Einheit	• SSH – TCP an Port **22** • RHEL KVM-Netzwerkgeräte – TCP und UDP an Ports **53** und **67** • SNMP-Agenten –	• SSH – TCP an Port **22** • BS-Implementierung – TCP und UDP an Ports **445, 3900** und **8443**	• BS-Implementierung – TCP und UDP an Ports **445, 3900** und **8443**	• BS-Implementierung – TCP und UDP an Ports **445, 3900** und **8443**	• BS-Implementierung – TCP und UDP an Ports **445, 3900** und **8443**	• BS-Implementierung – TCP und UDP an Ports **445, 3900** und **8443**

Kommunikation	RHEL-, Centos- und Rocky-Virtualisierungsprofil[1]	RHEL-, Centos- sowie Rocky Basis- und Minimalprofile[1]	SLES-Virtualisierungs-, Basis- und Minimalprofile[2]	Ubuntu-Virtualisierungs- und Minimalprofile[3]	VMware ESXi-Virtualisierungsprofil[4]	Windows-Profile
geöffnet)	UDP an Port **162** • BS-Implementierung – TCP und UDP an Ports **445, 3900** und **8443** • SLP-Serviceagent, SLP-Verzeichnisagent – TCP und UDP an Port **427** • Virtueller KVM-Server – TCP an Ports **49152 - 49215**					

1. Standardmäßig blockieren die Red Hat Enterprise Linux (RHEL)-Profile alle bis auf die in der folgenden Tabelle aufgeführten Ports.
2. 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.
3. Bei Ubuntu Linux Server werden einige offene Ports dynamisch auf Grundlage von Betriebssystemversion und Profilen zugewiesen. Eine vollständige Liste aller offenen Ports finden Sie in der Dokumentation für Ubuntu Server.
4. Eine vollständige Liste aller offenen Ports für VMware vSphere Hypervisor (ESXi) mit Lenovo-Anpassung finden Sie in der VMware-Dokumentation für ESXi auf der VMware Knowledge Base-Website.

Remote-Dateiserver konfigurieren

Sie können Betriebssystem-Images, Einheitentreiber und Boot-Dateien vom lokalen System oder einem Remote-Dateiserver in das BS-Images-Repository importieren. Um die Dateien von einem Remote-Dateiserver zu importieren, müssen Sie zunächst ein Profil erstellen, das zum Authentifizieren der Verbindung mit dem Remote-Dateiserver verwendet wird.

Zu dieser Aufgabe

Folgende Verschlüsselungsalgorithmen werden unterstützt:
- RSA – 2048 Bit
- RSA – 4096 Bit
- ECDSA – 521 Bit (secp521r1-Kurve)

Die folgenden Protokolle werden unterstützt:
- HTTP ohne Authentifizierung.

- HTTP mit Standardauthentifizierung.
- HTTPS (Zertifikatsüberprüfung) mit Standardauthentifizierung.
- HTTPS (Zertifikatsüberprüfung) ohne Authentifizierung.
- FTP mit Kennwortauthentifizierung.
- SFTP (Clientüberprüfung) mit Kennwortauthentifizierung.
- SFTP (Clientüberprüfung) mit Public-Key-Authentifizierung.

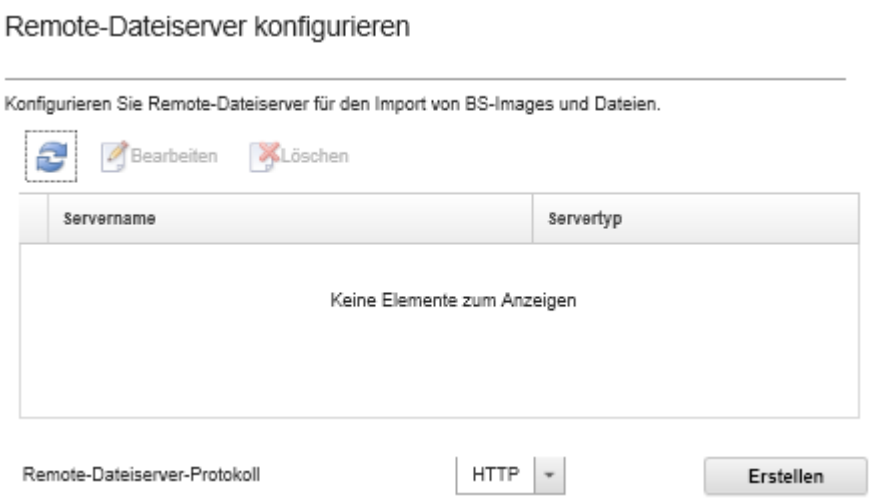
Bei der SFTP-basierten Public-Key-Authentifizierung und HTTPS-Zertifikatsüberprüfung überprüft Lenovo XClarity Administrator das Zertifikat des Remote-Dateiservers. Wenn das Serverzertifikat nicht im Truststore vorhanden ist, werden Sie aufgefordert, das Serverzertifikat zu akzeptieren und im Truststore hinzuzufügen. Informationen zur Fehlerbehebung bei Überprüfungsproblemen finden Sie unter Serverzertifizierungsüberprüfung fehlgeschlagen in der Onlinedokumentation von XClarity Administrator.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Remote-Dateiserver zu konfigurieren.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf das Symbol für **Dateiserver konfigurieren** ( ), um das Dialogfenster Remote-Dateiserver konfigurieren anzuzeigen.



Schritt 3. Wählen Sie das Protokoll für den Remote-Dateiserver aus der Liste **Remote-Dateiserver-Protokoll** aus.

Schritt 4. Klicken Sie auf **Erstellen**. Das Dialogfenster „Remote-Dateiserver konfigurieren“ wird angezeigt.

Anmerkung: Die Anzeige in diesem Dialogfenster hängt vom ausgewählten Protokoll ab.

Schritt 5. Geben Sie den Servernamen, die Adresse und den Port ein.

Schritt 6. Bei HTTP, HTTPS, FTP und SFTP mit Standardauthentifizierung geben Sie einen Benutzernamen und ein Kennwort ein, wenn die Authentifizierung für den Zugriff auf den Server erforderlich ist.

Schritt 7. Bei SFTP mit Standardauthentifizierung klicken Sie auf **Serverzertifikat überprüfen**, um die Signatur für den öffentlichen Schlüssel abzurufen.

Anmerkung: Möglicherweise wird ein Dialogfeld angezeigt, in dem Sie darauf hingewiesen werden, dass der Betriebssystemimplementierungsprozess dem öffentlichen Schlüssel des SFTP-Dateiservers nicht vertraut. Klicken Sie auf **OK**, um den öffentlichen SFTP-Schlüssel im vertrauenswürdigen Schlüsselspeicher des Betriebssystems zu speichern und ihm zu vertrauen.

Im Erfolgsfall wird die Signatur des öffentlichen Schlüssels im Feld **Public-Key-Signatur des SFTP-Servers** angezeigt.

Schritt 8. Bei SFTP mit Public-Key-Authentifizierung:

a. Geben Sie einen Verschlüsselungstext und das Kennwort ein und wählen Sie den Schlüsseltyp aus, falls die Authentifizierung für den Zugriff auf den Server erforderlich ist.

b. Klicken Sie auf **Verwaltungsserver-Schlüssel generieren**, um die Signatur für den öffentlichen Schlüssel abzurufen.

c. Kopieren Sie den generierten Schlüssel in die Datei authorized_keys auf Ihrem SFTP-Remote-Dateiserver.

d. Wählen Sie das Kontrollkästchen **Der Verwaltungsschlüssel wurde auf den Server kopiert** in XClarity Administrator aus.

e. Klicken Sie auf **Serverzertifikat überprüfen**, um die Signatur des öffentlichen Schlüssels zu prüfen.

Anmerkung: Möglicherweise wird ein Dialogfeld angezeigt, in dem Sie darauf hingewiesen werden, dass der Betriebssystemimplementierungsprozess dem öffentlichen Schlüssel des SFTP-Dateiservers nicht vertraut. Klicken Sie auf **OK**, um den öffentlichen SFTP-Schlüssel im vertrauenswürdigen Schlüsselspeicher des Betriebssystems zu speichern und ihm zu vertrauen. Im Erfolgsfall wird die Signatur des öffentlichen Schlüssels im Feld **Public-Key-Signatur des SFTP-Servers** angezeigt.

f. Klicken Sie auf **Speichern**.

Schritt 9. Klicken Sie auf **Server speichern**.

Nach dieser Aufgabe

Im Dialogfenster Remote-Dateiserver konfigurieren können Sie die folgenden Aktionen ausführen:

- Aktualisieren Sie die Liste der Remote-Dateiserver, indem Sie auf das Symbol für **Aktualisieren** ( ) klicken.
- Zum Ändern des ausgewählten Remote-Dateiservers klicken Sie auf das Symbol für **Bearbeiten** ( ).
- Um einen ausgewählten Remote-Dateiserver zu entfernen, klicken Sie auf das Symbol für **Löschen** ( ).

Betriebssystem-Images importieren

Bevor Sie ein lizenziertes Betriebssystem auf verwalteten Server implementieren können, müssen Sie zunächst das Image in das XClarity Administrator BS-Images-Repository importieren.

Zu dieser Aufgabe

Informationen zu Betriebssystem-Images, die Sie importieren und implementieren können, finden Sie unter Unterstützte Betriebssysteme.

Eine Liste der unterstützten Basis- und angepassten Betriebssysteme finden Sie unter Unterstützte BetriebssystemeUnterstützte Betriebssysteme in der Onlinedokumentation von Lenovo XClarity Administrator.

Sie können jeweils nur ein Image importieren. Warten Sie, bis das Image im BS-Images-Repository angezeigt wird, bevor Sie versuchen, ein weiteres Image zu importieren. Das Importieren des Betriebssystems kann eine Weile dauern.

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 Administrator:

- 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 Datei, die Sie importieren, größer als 4 GB ist, können Sie einen anderen Webbrowser verwenden (z. B. Chrome oder Firefox) oder die Datei auf einen Remote-Dateiserver kopieren und mithilfe der Option **Remote-Import** importieren.

Vorgehensweise

Gehen Sie wie folgt vor, um das Betriebssystem-Image in das BS-Images-Repository zu implementieren.

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 auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite BS-Images bereitstellen: BS-Images verwalten anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Image importieren** (), um das Dialogfeld BS-Image importieren anzuzeigen.

Schritt 4. Klicken Sie auf die Registerkarte **Lokal**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote**, um Dateien von einem Remote-Dateiserver hochzuladen.

Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** (). Siehe Remote-Dateiserver konfigurieren für weitere Informationen.

Schritt 5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.

Schritt 6. Geben Sie den Pfad und den ISO-Image-Dateinamen ein oder klicken Sie auf **Durchsuchen**, um das ISO-Image zu finden, das Sie importieren möchten.

Wenn Sie sich für den *lokalen Dateiserver* entschieden haben, müssen Sie den absoluten Pfad zur ISO-Image-Datei angeben. Wenn Sie einen *Remote-Dateiserver* verwenden, müssen Sie den absoluten Pfad (z. B. `/home/user/isos.osimage.iso`) oder den relativen Pfad (z. B. `/isos.osimage.iso`) zur ISO-Image-Datei angeben (abhängig von der Konfiguration des Remote-Dateiservers). Wenn die Datei nicht gefunden wird, überprüfen Sie, ob der Pfad zur Datei korrekt ist, und versuchen Sie es erneut.

Schritt 7. **Optional:** Geben Sie eine Beschreibung für das BS-Image ein.

Schritt 8. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass das in XClarity Administrator importierte ISO-Image nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende 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.

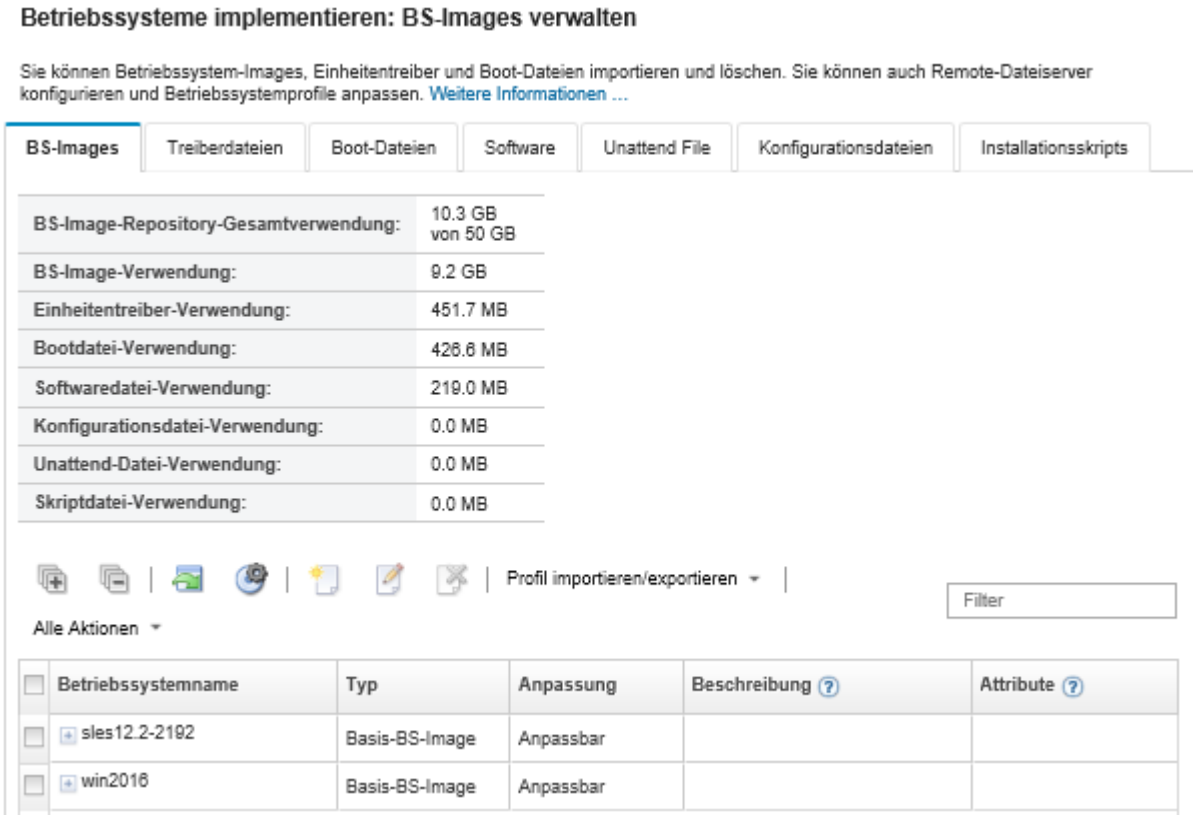
Es werden drei Prüfsummentypen unterstützt:
- **MD5**
- **SHA1**
- **SHA256**

Schritt 9. Klicken Sie auf **Importieren**.

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. Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das das Betriebssystem-Image hochgeladen wird, vor dem Abschluss des Hochladevorgangs schließen, schlägt der Import fehl.

Ergebnisse

XClarity Administrator lädt das BS-Image hoch und erstellt ein Image-Profil im BS-Images-Repository.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** ( ) klicken.
- Fügen Sie ein BS-Image ein, indem Sie auf das Symbol **Angepasstes Profil erstellen** ( ) klicken.

- Ändern Sie ein BS-Image, indem Sie auf das Symbol **Bearbeiten** () klicken.
- Importieren Sie ein angepasstes BS-Image-Profil und wenden Sie es auf ein Basis-BS-Image an, indem Sie auf **Profil importieren/exportieren → Angepasstes Profil-Image importieren** klicken (siehe Angepasstes BS-Image-Profil importieren).
- Löschen Sie ein ausgewähltes BS-Image oder angepasstes BS-Image-Profil durch Klicken auf das Symbol **Löschen** ().
- Klicken Sie auf **Profil importieren/exportieren → Angepasstes Profil-Image exportieren**, um ein ausgewähltes angepasstes BS-Image-Profil zu exportieren.

Anmerkung: Beim Importieren von Windows Server-Images müssen Sie auch die zugeordnete Paketdatei importieren. Lenovo fasst die vordefinierte Boot-Datei WinPE_64.wim mit verschiedenen Einheitentreibern in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Da die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Dateien** importieren..Weitere Informationen finden Sie in den Abschnitten Boot-Dateien importieren und Einheitentreiber importieren.

BS-Image-Profile anpassen

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 auch beim Basisbetriebssystem-Image angepasste Profile erstellen, die für bestimmte Konfigurationen implementiert werden können. Das angepasste Profil enthält die angepassten Dateien und Installationsoptionen.

Anmerkung: Sie können kein angepasstes BS-Image-Profil für ein angepasstes Microsoft Windows Server-Image erstellen.

Mehrere Beispielszenarien für das Anpassen und Implementieren von BS-Images, einschließlich Windows und SLES, sind nur auf Englisch verfügbar. Weitere Informationen finden Sie unter End-to-End-Szenarien für das Einrichten neuer Einheiten.

Sie können die folgenden Dateitypen zu einem angepassten BS-Image-Profil hinzufügen.

- **Boot-Dateien**

  Eine Boot-Datei fungiert als Bootstrap-Installationsumgebung. Für Windows ist dies eine Windows-Vorinstallationsdatei (WinPE). Zum Implementieren von Windows ist eine WinPE-Boot-Datei erforderlich.

  Lenovo XClarity Administrator unterstützt vordefinierte und angepasste Boot-Dateien.

  – **Vordefinierte Boot-Dateien**. Lenovo stellt eine WinPE_64.wim Boot-Datei zur Verfügung, die zum Implementieren vordefinierter BS-Image-Profiles verwendet werden kann.

    Lenovo fasst die vordefinierte Boot-Datei WinPE_64.wim mit verschiedenen Einheitentreibern in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Da die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Dateien** importieren.

    Anmerkungen:

    – Eine vordefinierte Boot-Datei ist nicht mit XClarity Administrator geladen. Sie müssen eine Boot-Datei in das BS-Images-Repository importieren, bevor Sie ein Windows-Profil implementieren können.

  - Sie können keine vordefinierten Boot-Dateien löschen, die bei der Installation von XClarity Administrator geladen wurden, aber Sie können vordefinierte Boot-Dateien löschen, die aus einem Lenovo Paket importiert wurden.
  - Für XClarity Administrator müssen die importierten Paketdateien von Lenovo signiert sein. Beim Importieren einer Paketdatei muss auch eine ASC-Signaturdatei importiert werden.
- **Angepasste Boot-Dateien**. Sie können eine WinPE-Boot-Datei zum Anpassen von Bootoptionen für die Implementierung von Windows erstellen. Sie können dann die Boot-Datei dem angepassten Windows-Profile hinzufügen.

  XClarity Administrator stellt Skripts für die Erstellung von Boot-Dateien im richtigen Format zur Verfügung. Weitere Informationen zum Erstellen von angepassten Boot-Dateien finden Sie unter Boot-(WinPE)-Datei erstellen und Website mit einer Einführung in Windows PE (WinPE).

  Die folgenden Dateitypen werden für das Importieren von angepassten Boot-Dateien unterstützt.

Betriebssystem	Unterstützte Boot-Dateitypen	Unterstützte Paketdateitypen
CentOS Linux	Nicht unterstützt	Nicht unterstützt
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	Nicht unterstützt
Microsoft Windows Hyper-V Server	Eine ZIP-Datei, die eine WinPE-Datei enthält, wird mithilfe des **genimage.cmd**-Skripts erstellt	Eine ZIP-Datei, die Einheitentreiber und Boot-Dateien enthält
Microsoft Windows Server	Eine ZIP-Datei, die eine WinPE-Datei enthält, wird mithilfe des **genimage.cmd**-Skripts erstellt	Eine ZIP-Datei, die Einheitentreiber und Boot-Dateien enthält
Red Hat® Enterprise Linux (RHEL) Server	Nicht unterstützt	Nicht unterstützt
Rocky Linux	Nicht unterstützt	Nicht unterstützt
SUSE® Linux Enterprise Server (SLES)	Nicht unterstützt	Nicht unterstützt
Ubuntu	Nicht unterstützt	Nicht unterstützt
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Nicht unterstützt	Nicht unterstützt

- **Einheitentreiber**

  Sie müssen sicherstellen, dass das Betriebssystem-Image, das Sie implementieren möchten, über die entsprechenden Einheitentreiber für Ihre Ethernet-, Fibre Channel- und Speicheradapter-Hardware verfügt. Wenn der Einheitentreiber für E/A-Adapter nicht im Betriebssystems-Image oder -Profil enthalten ist, wird dieser Adapter bei der BS-Implementierung nicht unterstützt. Sie können angepasste BS-Image-Profile erstellen, die die Out-of-Box-Einheitentreiber enthalten, die Sie benötigen.

  Lenovo XClarity Administrator unterstützt In-Box-Einheitentreiber sowie vordefinierte und angepasste Out-of-Box-Einheitentreiber.

  - **In-Box-Einheitentreiber**. XClarity Administrator verwaltet keine Inbox-Einheitentreiber. Installieren Sie immer ein aktuelles Betriebssystem, um sicherzustellen, dass die neuesten erforderlichen In-Box-Einheitentreiber vorhanden sind.

    Anmerkung: Sie können einem angepassten Windows-Profil Inbox-Einheitentreiber hinzufügen, indem Sie eine angepasste WinPE-Boot-Datei erstellen und die Einheitentreiberdateien in das Hostsystem im Verzeichnis `C:\drivers` kopieren. Wenn Sie ein angepasstes BS-Image-Profil erstellen, das die angepasste Boot-Datei verwendet, sind die Einheitentreiber im Verzeichnis C:\drivers bei WinPE und

dem finalen BS enthalten. Sie werden wie Inbox-Treiber behandelt. Aus diesem Grund müssen Sie diese Inbox-Einheitentreiber nicht in XClarity Administrator importieren, wenn Sie Einheitentreiber angeben, die bei der Erstellung des angepassten BS-Image-Profils verwendet werden sollen.

- **Vordefinierte Einheitentreiber**. Bei ThinkSystem-Servern enthält XClarity Administrator eine Gruppe von Out-of-Box-Einheitentreibern für Linux zur Installation des Betriebssystems und grundlegende Netzwerk- und Speicherkonfigurationen für das finale Betriebssystem. Sie können diese vordefinierten Einheitentreiber den angepassten BS-Image-Profilen hinzufügen und dann die Profile auf verwalteten Servern implementieren.

  Lenovo fasst auch vordefinierte Einheitentreiber in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Die Paketdateien sind derzeit nur für Windows verfügbar. Wenn die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Image** importieren.

  Anmerkungen:

  - Die vordefinierten BS-Image-Profile enthalten standardmäßig die vordefinierten Einheitentreiber.
  - Sie können keine vordefinierten Einheitentreiber löschen, die bei der Installation von XClarity Administrator geladen wurden, aber Sie können vordefinierte Einheitentreiber löschen, die aus einem Lenovo Paket importiert wurden.
  - Für XClarity Administrator müssen die importierten Paketdateien von Lenovo signiert sein. Beim Importieren einer Paketdatei muss auch eine ASC-Signaturdatei importiert werden.
- **Angepasste Einheitentreiber**. Sie können Out-of-Box-Einheitentreiber in das BS-Images-Repository importieren und dann diese Einheitentreiber einem angepassten BS-Image-Profil hinzufügen.

  Sie erhalten Einheitentreiber von Lenovo YUM Repository-Webseite, vom Anbieter (z. B. Red Hat), oder über einen angepassten Einheitentreiber, den Sie selbst erstellen. Für einige Windows-Einheitentreiber kann ein angepasster Einheitentreiber durch Extrahieren des Einheitentreibers aus der ausführbaren Installationsdatei in Ihr lokales System und durch Erstellen einer ZIP-Archivdatei generiert werden.

  Die folgenden Dateitypen werden für das Importieren von angepassten Einheitentreibern unterstützt.

Betriebssystem	Unterstützte Dateitypen für Einheitentreiber
CentOS Linux	Nicht unterstützt
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt
Microsoft Windows Hyper-V Server	Eine ZIP-Datei, die unformatierte Einheitentreiberdateien enthält, die in der Regel als INF-, CAT- und DLL-Dateien gruppiert sind.
Microsoft Windows Server	Eine ZIP-Datei, die unformatierte Einheitentreiberdateien enthält, die in der Regel als INF-, CAT- und DLL-Dateien gruppiert sind.
Red Hat® Enterprise Linux (RHEL) Server	Datenträger zur Treiberaktualisierung (Driver Update Disk, DUD) in einem RPM- oder ISO-Image-Format **Anmerkung:** Wenn Sie eine DUD-RPM auf das angepasste Profil anwenden, wird die RPM nur auf dem letzten Betriebssystem installiert. Sie wird nicht in der Installationsumgebung (initrd) installiert. Um einen angepassten Einheitentreiber in initrd zu installieren, importieren Sie eine DUD-ISO und wenden Sie die ISO auf das angepasste Profil an.
Rocky Linux	Nicht unterstützt

Betriebssystem	Unterstützte Dateitypen für Einheitentreiber
SUSE® Linux Enterprise Server (SLES)	Treiberaktualisierungsplatte (DUD) in einem RPM- oder ISO-Image-Format **Anmerkung:** Wenn Sie eine DUD-RPM auf das angepasste Profil anwenden, wird die RPM nur auf dem letzten Betriebssystem installiert. Sie wird nicht in der Installationsumgebung (initrd) installiert. Um einen angepassten Einheitentreiber in initrd zu installieren, importieren Sie eine DUD-ISO und wenden Sie die ISO auf das angepasste Profil an.
Ubuntu	Nicht unterstützt
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Einheitentreiber im VIB-Image-Format

Anmerkung: Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

- **Angepasste Konfigurationseinstellungen**

  Konfigurationseinstellungen beschreiben Daten, die während der BS-Implementierung dynamisch gesammelt werden müssen. Lenovo XClarity Administrator verwendet eine Gruppe vordefinierter Konfigurationseinstellungen, einschließlich globaler, Netzwerk- und Speicherpositionseinstellungen. Sie können diese vordefinierten Konfigurationseinstellungen verwenden und angepasste Einstellungen hinzufügen, die nicht über XClarity Administrator verfügbar sind.

  Die angepassten Konfigurationseinstellungen werden im Format eines JSON-Schemas definiert. Das Schema muss der JSON-Spezifikation entsprechen.

  Beim Importieren von angepassten Konfigurationseinstellungen in XClarity Administrator überprüft XClarity Administrator das JSON-Schema. Wenn die Überprüfung erfolgreich ist, erstellt XClarity Administrator angepasste Makros für jede Einstellung.

  Sie können die angepassten Makros in der Unattend-Datei und im Nach-Installationsskript verwenden.

  In Unattend-Dateien

  Sie können die angepasste Konfigurationsdatei einer Unattend-Datei zuordnen und diese angepassten Makros (und vordefinierten Makros) in diese Unattend-Datei aufnehmen.

  Sie können einem angepassten Profil eine oder mehrere angepasste Konfigurationseinstellungsdateien hinzufügen. Wenn Sie das BS-Profil auf einer Gruppe von Zielservern implementieren, können Sie auswählen, welche Konfigurationseinstellungsdatei verwendet wird. XClarity Administrator rendert die Registerkarte **Angepasste Einstellungen** im Dialogfenster „BS-Image implementieren“ basierend auf dem JSON-Schema in der Konfigurationseinstellungsdatei und ermöglicht Ihnen die Angabe von Werten für jede Einstellung (JSON-Objekt), die in der Datei definiert ist.

  Anmerkung: Die BS-Implementierung wird nicht fortgesetzt, wenn keine Eingabe für alle erforderlichen angepassten Konfigurationseinstellungen angegeben ist.

  In Nach-Installationsskripts

  Nachdem die Daten während der BS-Implementierung gesammelt wurden, erstellt XClarity Administrator eine Instanz der Konfigurationseinstellungsdatei (die die angepassten Einstellungen in der ausgewählten Datei und eine Teilmenge der vordefinierten Einstellungen enthält) auf dem Hostsystem, das vom Nach-Installationsskript verwendet werden kann.

  Anmerkungen:

- Die Konfigurationseinstellungsdatei ist in Bezug auf ein angepasstes BS-Image-Profil eindeutig.
- Sie können keine Konfigurationseinstellungen für vordefinierte BS-Image-Profile ändern.
- Konfigurationseinstellungen werden nur für die folgenden Betriebssysteme unterstützt:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization 6.0u3 und spätere Aktualisierungen sowie 6.5 und höher

Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

- **Angepasste Unattend-Dateien**

  Sie können BS-Image-Profile so anpassen, dass Unattend-Dateien zur automatisierten Implementierung des Betriebssystems verwendet werden.

  Die folgenden Dateitypen werden für angepasste Unattend-Dateien unterstützt.

Betriebssystem	**Unterstützte Dateitypen**	**Weitere Informationen**
CentOS Linux	Nicht unterstützt	
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	
Microsoft Windows Hyper-V Server	Nicht unterstützt	
Microsoft Windows Server	Unattend (.xml)	Weitere Informationen zu Unattend-Dateien finden Sie unter Website zur Referenz für das unbeaufsichtigte Windows-Setup.
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Weitere Informationen zu Unattend-Dateien finden Sie unter Red Hat: Website zum Automatisieren der Installation mit Kickstart. Beachten Sie beim Hinzufügen von %pre-, %post- und %firstboot-Abschnitten in der Datei die folgenden Aspekte. – Sie können mehrere %pre-, %post- und %firstboot-Abschnitte zur Unattend-Datei hinzufügen. Achten Sie dabei aber auf die Reihenfolge der Abschnitte. – Wenn das empfohlene **#predefined.unattendSettings.preinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator einen %pre-Abschnitt vor allen anderen %pre-Abschnitten in der Datei hinzu. – Wenn das empfohlene **#predefined.unattendSettings.postinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator %post- und einen %firstboot-Abschnitte vor allen anderen %post- und %firstboot-Abschnitten in der Datei hinzu.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
Rocky Linux	Kickstart (.cfg)	Weitere Informationen zu Unattend-Dateien finden Sie unter Red Hat: Website zum Automatisieren der Installation mit Kickstart. Beachten Sie beim Hinzufügen von %pre-, %post- und %firstboot-Abschnitten in der Datei die folgenden Aspekte. – Sie können mehrere %pre-, %post- und %firstboot-Abschnitte zur Unattend-Datei hinzufügen. Achten Sie dabei aber auf die Reihenfolge der Abschnitte. – Wenn das empfohlene **#predefined.unattendSettings.preinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator einen %pre-Abschnitt vor allen anderen %pre-Abschnitten in der Datei hinzu. – Wenn das empfohlene **#predefined.unattendSettings.postinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator %post- und einen %firstboot-Abschnitte vor allen anderen %post- und %firstboot-Abschnitten in der Datei hinzu.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Weitere Informationen zu Unattend-Dateien finden Sie unter SUSE: AutoYaST-Website.
Ubuntu	Nicht unterstützt	
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Kickstart (.cfg)	Nur für ESXi 6.0u3 und spätere Aktualisierungen und 6.5 und höher unterstützt. Weitere Informationen zu Unattend-Dateien finden Sie unter VMware: Hosts mithilfe einer Script-Website installieren oder aktualisieren. Beachten Sie beim Hinzufügen von %pre-, %post- und %firstboot-Abschnitten in der Datei die folgenden Aspekte. – Sie können mehrere %pre-, %post- und %firstboot-Abschnitte zur Unattend-Datei hinzufügen. Achten Sie dabei aber auf die Reihenfolge der Abschnitte. – Wenn das empfohlene **#predefined.unattendSettings.preinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator einen %pre-Abschnitt vor allen anderen %pre-Abschnitten in der Datei hinzu. – Wenn das empfohlene **#predefined.unattendSettings.postinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator %post- und einen %firstboot-Abschnitte vor allen anderen %post- und %firstboot-Abschnitten in der Datei hinzu.

Achtung:

– Sie können vordefinierte und angepasste Makros (Konfigurationseinstellungen) mit dem eindeutigen Namen des Objekts in die Unattend-Datei einfügen. Vordefinierte Werte sind basierend auf den XClarity Administrator-Instanzen dynamisch. Angepasste Makros sind basierend auf Benutzereingaben dynamisch, die während der BS-Implementierung festgelegt werden.

  Anmerkungen:

  – Umschließen Sie den Makronamen mit einem Rautensymbol (#).

  - Trennen Sie bei verschachtelten Objekten jeden Objektnamen mit einem Punkt (z. B. **#server_settings.server0.locale#**).
  - Bei angepassten Makros darf der oberste Objektname nicht enthalten sein. Stellen Sie dem Makronamen bei vordefinierten Makros das Präfix „predefined“ voran.
  - Wenn ein Objekt von einer Vorlage erstellt wird, wird an den Namen eine eindeutige Nummer angehängt, beginnend mit 0 (z. B. **server0** und **server1**).
  - Sie können den Namen für jedes Makro im Dialogfeld „BS-Images implementieren“ auf den Registerkarten „Angepasste Einstellungen“ anzeigen, indem Sie mit der Maustaste über das Hilfe-Symbol (?) neben jeder angepassten Einstellung bewegen.
  - Eine Liste der vordefinierten Makros finden Sie unter Vordefinierte Makros. Informationen zu angepassten Konfigurationseinstellungen und Makros finden Sie unter Angepasste Makros.
- XClarity Administrator bietet die folgenden vordefinierten Makros, die zur Statusübertragung vom BS-Installationsprogramm sowie für andere wichtige Installationsschritte verwendet werden. Es wird empfohlen, diese Makros in die Unattend-Datei zu integrieren (siehe Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

- **Angepasste Installationsskripts**

  Sie können BS-Image-Profile so anpassen, dass nach Abschluss der BS-Implementierung ein Installationsskript ausgeführt wird.

  Derzeit werden nur Nach-Installationsskripts unterstützt.

  In der folgenden Tabelle sind die Dateitypen für die Installationsskripts aufgeführt, die Lenovo XClarity Administrator für jedes Betriebssystem unterstützt. Beachten Sie, dass bestimmte Betriebssystemversionen nicht alle Dateitypen unterstützen, die von XClarity Administrator unterstützt werden (z. B. einige RHEL-Versionen enthalten möglicherweise kein Perl im minimalen Profil, sodass Perl-Skripts nicht ausgeführt werden). Sie müssen sicherstellen, dass Sie den richtigen Dateityp für die Betriebssystemversionen verwenden, die Sie implementieren möchten.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
CentOS Linux	Nicht unterstützt	
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	
Microsoft Windows Hyper-V Server	Nicht unterstützt	
Microsoft® Windows® Server	Befehlsdatei (.cmd), PowerShell (.ps1)	Der Standardpfad für angepasste Daten und Dateien ist `C:\lxca`. Weitere Informationen zu Installationsskripts finden Sie unter Website zum Hinzufügen eines angepassten Skripts zu Windows Setup.
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm oder .pl), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter RHEL: Website zu Nach-Installationsskripts.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
Rocky Linux	Bash (.sh), Perl (.pm oder .pl), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter RHEL: Website zu Nach-Installationsskripts.
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm oder .pl), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter SUSE: Website zu benutzerdefinierten Skripts.
Ubuntu	Nicht unterstützt	
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Bash (.sh), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter VMware: Website zur Installation und Aktualisierung von Skripts.

- **Angepasste Software**

  Sie können BS-Image-Profile so anpassen, dass nach Abschluss der BS-Implementierung und Nach-Installationsskripts angepasste Software-Nutzdaten installiert werden.

  Die folgenden Dateitypen werden für angepasste Software unterstützt.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
CentOS Linux	Nicht unterstützt	
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	
Microsoft Windows Hyper-V Server	Nicht unterstützt	
Microsoft Windows® Server	Eine .zip-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
Rocky Linux	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
Ubuntu	Nicht unterstützt	
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.

Angepasstes BS-Image-Profil importieren

Sie können ein angepasstes BS-Image-Profil importieren und es zu einem vorhandenen kompatiblen Basisbetriebssystem-Image hinzufügen.

Zu dieser Aufgabe

Bevor Sie ein angepasstes Profil importieren können, muss das Basis-BS-Image importiert werden.

Ein angepasstes BS-Image-Profil kann nur zu einem Basis-BS-Image desselben Typs hinzugefügt werden. Wenn das exportierte Profil beispielsweise für ein Windows 2016-Image bestimmt ist, kann das Profil nur in ein vorhandenes Windows 2016-Image importiert und dort hinzugefügt werden, das im BS-Images-Repository vorhanden ist.

Das BS-Images-Repository kann eine unbegrenzte Anzahl von angepassten Profilen speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Vorgehensweise

Gehen Sie wie folgt vor, um ein angepasstes BS-Image-Profil zu importieren.

Schritt 1. Klicken Sie auf der Menüleiste von Lenovo XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Wählen Sie auf der Registerkarte **BS-Images** das Basisbetriebssystem-Image aus, das dem angepassten BS-Image-Profil hinzugefügt werden soll.

Schritt 3. Klicken Sie auf **Profil importieren/exportieren → Angepasstes Profil-Image importieren**. Das Dialogfenster Angepasstes BS-Image-Profil importieren wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** (). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .

Schritt 5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.

Schritt 6. Geben Sie den Profilnamen ein oder klicken Sie auf **Durchsuchen**, um das Profil zu finden, das Sie importieren möchten.

Schritt 7. **Optional:** Wählen Sie bei lokalen Importen einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

Es werden drei Prüfsummentypen unterstützt:
- **MD5**
- **SHA1**
- **SHA256**

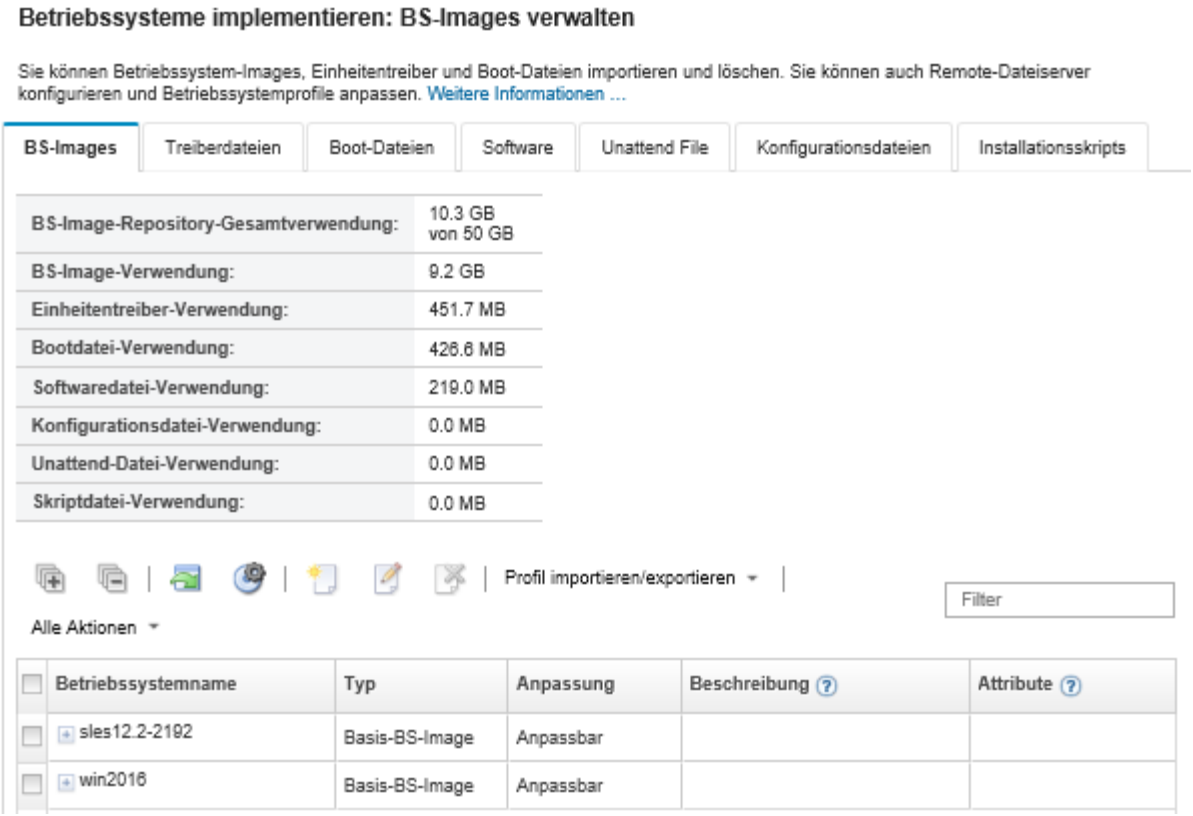
Schritt 8. Klicken Sie auf **Importieren**.

Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Das angepasste BS-Image-Profil wird unter dem Basisbetriebssystem auf der Seite „BS-Images verwalten“ aufgeführt.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie ein angepasstes BS-Image-Profil (siehe Angepasstes BS-Image-Profil erstellen).
- Klicken Sie auf **Profil importieren/exportieren → Angepasstes Profil-Image exportieren**, um ein ausgewähltes angepasstes BS-Image-Profil zu exportieren.

  Wichtig: Sie können angepasste BS-Image-Profile in einen Remote-Dateiserver exportieren, der für die Verwendung von FTP- oder SFTP-Protokollen eingerichtet ist. Sie können nicht in einen Remote-Dateiserver exportieren, der für die Verwendung von HTTP oder HTTPS eingerichtet ist.
- Zum Ändern des ausgewählten angepassten BS-Image-Profils klicken Sie auf das Symbol für **Bearbeiten** ( ).
- Um ein ausgewähltes angepasstes BS-Image-Profil zu entfernen, klicken Sie auf das Symbol für **Löschen** ( ).

Boot-Dateien importieren

Sie können Boot-Dateien in das BS-Images-Repository importieren. Diese Dateien können dann zum Anpassen und Implementieren von Windows-Images verwendet werden.

Zu dieser Aufgabe

Eine Boot-Datei fungiert als Bootstrap-Installationsumgebung. Für Windows ist dies eine Windows-Vorinstallationsdatei (WinPE). Zum Implementieren von Windows ist eine WinPE-Boot-Datei erforderlich.

Lenovo XClarity Administrator unterstützt vordefinierte und angepasste Boot-Dateien.

- **Vordefinierte Boot-Dateien**. Lenovo stellt eine WinPE_64.wim Boot-Datei zur Verfügung, die zum Implementieren vordefinierter BS-Image-Profiles verwendet werden kann.

  Lenovo fasst die vordefinierte Boot-Datei WinPE_64.wim mit verschiedenen Einheitentreibern in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Da die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Dateien** importieren.

  Anmerkungen:

  – Eine vordefinierte Boot-Datei ist nicht mit XClarity Administrator geladen. Sie müssen eine Boot-Datei in das BS-Images-Repository importieren, bevor Sie ein Windows-Profil implementieren können.

  – Sie können keine vordefinierten Boot-Dateien löschen, die bei der Installation von XClarity Administrator geladen wurden, aber Sie können vordefinierte Boot-Dateien löschen, die aus einem Lenovo Paket importiert wurden.

  – Für XClarity Administrator müssen die importierten Paketdateien von Lenovo signiert sein. Beim Importieren einer Paketdatei muss auch eine ASC-Signaturdatei importiert werden.

- **Angepasste Boot-Dateien**. Sie können eine WinPE-Boot-Datei zum Anpassen von Bootoptionen für die Implementierung von Windows erstellen. Sie können dann die Boot-Datei dem angepassten Windows-Profile hinzufügen.

  XClarity Administrator stellt Skripts für die Erstellung von Boot-Dateien im richtigen Format zur Verfügung. Weitere Informationen zum Erstellen von angepassten Boot-Dateien finden Sie unter Boot-(WinPE)-Datei erstellen und Website mit einer Einführung in Windows PE (WinPE).

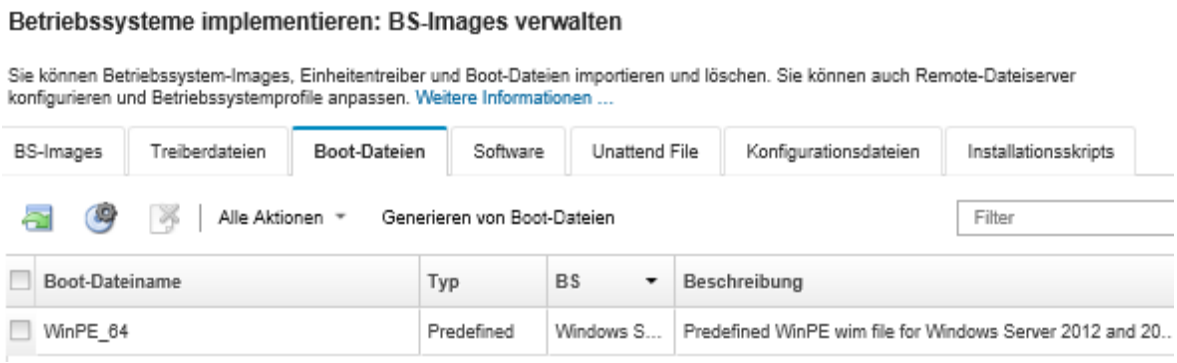
  Die folgenden Dateitypen werden für das Importieren von angepassten Boot-Dateien unterstützt.

Betriebssystem	Unterstützte Boot-Dateitypen	Unterstützte Paketdateitypen
CentOS Linux	Nicht unterstützt	Nicht unterstützt
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	Nicht unterstützt
Microsoft Windows Hyper-V Server	Eine ZIP-Datei, die eine WinPE-Datei enthält, wird mithilfe des **genimage.cmd**-Skripts erstellt	Eine ZIP-Datei, die Einheitentreiber und Boot-Dateien enthält
Microsoft Windows Server	Eine ZIP-Datei, die eine WinPE-Datei enthält, wird mithilfe des **genimage.cmd**-Skripts erstellt	Eine ZIP-Datei, die Einheitentreiber und Boot-Dateien enthält
Red Hat® Enterprise Linux (RHEL) Server	Nicht unterstützt	Nicht unterstützt
Rocky Linux	Nicht unterstützt	Nicht unterstützt
SUSE® Linux Enterprise Server (SLES)	Nicht unterstützt	Nicht unterstützt
Ubuntu	Nicht unterstützt	Nicht unterstützt
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Nicht unterstützt	Nicht unterstützt

Anmerkung: Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Vorgehensweise

- Gehen Sie wie folgt vor, um eine Windows Paketdatei, die Boot-Dateien enthält, in das BS-Images-Repository zu importieren.
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Boot-Dateien**.



  3. Klicken Sie auf **Downloads → Windows Paketdateien**, um auf die Lenovo Unterstützungswebseite zu gehen und laden Sie die entsprechende Paketdatei und die zugeordnete Signaturdatei für das BS-Image auf das lokale System herunter.
  4. Klicken Sie auf das Symbol für **Paketdatei importieren** ( ). Das Dialogfenster Paketdatei importieren wird angezeigt.
  5. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

     Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** ( ). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .
  6. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.
  7. Wählen Sie den Betriebssystemtyp und die Version:
  8. Geben Sie den Dateinamen der Paketdatei und die zugeordnete Signaturdatei ein oder klicken Sie auf **Durchsuchen**, um nach den Dateien zu suchen, die Sie importieren möchten.
  9. **Optional**: Geben Sie eine Beschreibung für die Paketdatei ein.
  10. Klicken Sie auf **Importieren**.

      Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

      Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.
- Gehen Sie wie folgt vor, um eine einzelne Boot-Datei in das BS-Images-Repository zu importieren.
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

2. Klicken Sie auf die Registerkarte **Boot-Dateien**.
3. Klicken Sie auf das Symbol für **Datei importieren** (). Das Dialogfenster Datei importieren wird angezeigt.
4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

   Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** (). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .
5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.
6. Wählen Sie den Betriebssystemtyp und die Version:
7. Geben Sie den Dateinamen ein oder klicken Sie auf **Durchsuchen**, um nach der Boot-Datei zu suchen, die Sie importieren möchten.
8. **Optional:** Geben Sie eine Beschreibung für die Boot-Datei ein.
9. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

   Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

   Es werden drei Prüfsummentypen unterstützt:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Klicken Sie auf **Importieren**.

    Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

    Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Die Boot-Datei ist auf der Seite BS-Images verwalten auf der Registerkarte **Boot-Dateien** aufgeführt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** () klicken.
- Um eine ausgewählte Boot-Datei zu entfernen, klicken Sie auf das Symbol für **Löschen** ().
- Fügen Sie einem angepassten BS-Image-Profil eine Boot-Datei hinzu (siehe Angepasstes BS-Image-Profil erstellen).

Boot-(WinPE)-Datei erstellen

Sie können Boot-Dateien erstellen, die zum Anpassen von Windows-Images verwendet werden können.

Vorbereitende Schritte

- Stellen Sie sicher, dass das Betriebssystem, das Sie bereitstellen möchten, auf dem Host installiert ist. Z. B. Wenn Sie die Bereitstellung von Windows 2016 unter Verwendung der WinPE-Dateien planen, installieren Sie Windows 2016 auf dem Host.
- Stellen Sie sicher, dass das Microsoft ADK, das mit dem installierten Betriebssystem kompatibel ist, ebenfalls auf dem Host installiert ist. Beispielsweise ist für Windows 2012R2 das ADK Version 8.1 Update erforderlich.
- Fordern Sie die Einheitentreiber im INF-Format an, die Sie zu der Boot-Datei hinzufügen möchten.

  Sie erhalten Einheitentreiber von Lenovo YUM Repository-Webseite, vom Anbieter (z. B. Red Hat), oder über einen angepassten Einheitentreiber, den Sie selbst erstellen. Für einige Windows-Einheitentreiber kann ein angepasster Einheitentreiber durch Extrahieren des Einheitentreibers aus der ausführbaren Installationsdatei in Ihr lokales System und durch Erstellen einer ZIP-Archivdatei generiert werden.

  Lenovo fasst auch vordefinierte Einheitentreiber in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Die Paketdateien sind derzeit nur für Windows verfügbar. Wenn die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Image** importieren.
- Laden Sie die Dateien `genimage.cmd` und `startnet.cmd` auf den Host in ein temporäres Verzeichnis herunter, wie `C:\customwim`.

  Der Befehl `genimage.cmd` wird zum Generieren der WinPE Boot-Dateien einschließlich der WIM-Datei verwendet. Der Befehl `startnet.cmd` wird von XClarity Administrator verwendet, um den Windows-Installer zu booten.
- Entscheiden Sie, wie Sie Einheitentreiber in die Boot-Datei einfügen möchten. Sie haben dafür eine der folgenden Möglichkeiten:
  - Fügen Sie Inbox-Einheitentreiber zu einem benutzerdefinierten Windows-Profil hinzu, indem Sie die Einheitentreiberdateien in das Hostsystem im Verzeichnis C:\drivers kopieren. Diese werden bei den Boot-Dateien enthalten sein, wenn später genimage.cmd ausgeführt wird.

    Anmerkung: Wenn Sie ein angepasstes BS-Image-Profil erstellen, das die angepasste Boot-Datei verwendet, sind die Einheitentreiber im Verzeichnis C:\drivers bei WinPE und dem finalen BS enthalten. Sie werden wie Inbox-Treiber behandelt. Aus diesem Grund müssen Sie diese Inbox-Einheitentreiber nicht in XClarity Administrator importieren, wenn Sie Einheitentreiber angeben, die bei der Erstellung des angepassten BS-Image-Profils verwendet werden sollen.
  - Fügen Sie Out-of-Box-Boot-Einheitentreiber direkt zur Boot-Datei hinzu.

    Anmerkung: Wenn Sie diese Methode verwenden, werden die Einheitentreiber nur für die Boot-Datei und dementsprechend für die WinPE-Installationsumgebung übernommen. Die Einheitentreiber werden nicht für das final installierte Betriebssystem übernommen. Sie müssen die Einheitentreiber manuell in das BS-Images-Einheitentreiber-Repository importieren und für die Verwendung als Teil der BS-Image-Profilanpassung auswählen.
- Weitere Informationen zu Boot-Dateien finden Sie im Abschnitt Website mit einer Einführung in Windows PE (WinPE).

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Boot-Datei zu erstellen:

Schritt 1. Verwenden Sie eine Benutzer-ID mit Administratorrechten und führen Sie den Windows ADK-Befehl „Deployment and Imaging Tools Environment“ aus. Eine Befehlssitzung wird angezeigt.

Schritt 2. Wechseln Sie in der Befehlssitzung zum Verzeichnis, in das die Dateien `genimage.cmd` und `starnet.cmd` heruntergeladen wurden (zum Beispiel `C:\customwim`).

Schritt 3. Stellen Sie sicher, dass sich keine zuvor angehängten Images auf dem Host befinden, indem Sie den folgenden Befehl ausführen:
```
dism /get-mountedwiminfo
```

Wenn es angehängte Images gibt, löschen Sie diese, indem Sie den folgenden Befehl ausführen:

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

Schritt 4. Wenn Sie Inbox-Einheitentreiber zu einem benutzerdefinierten Windows-Profil hinzufügen, kopieren Sie die unaufbereiteten Einheitentreiberdateien im INF-Format in das Hostsystem im Verzeichnis `C:\drivers`.

Schritt 5. Führen Sie den folgenden Befehl aus, um die Boot-Datei im WIM-Format zu generieren, und warten Sie dann einige Minuten, bis der Befehl ausgeführt wurde.
```
genimage.cmd amd64 <ADK_Version>
```

Dabei ist *<ADK_Version>* einer der folgenden Werte.

- **8.1**. Für Windows 2012 R2
- **10**. Für Windows 2016

Dieser Befehl erstellt die Boot-Datei: `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Schritt 6. Hängen Sie die Boot-Datei an, indem Sie den folgenden Befehl ausführen:
```
DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
```

Schritt 7. Wenn Sie Out-of-Box-Einheitentreiber direkt zur Boot-Datei hinzufügen, gehen Sie wie folgt vor:

1. Erstellen Sie die folgenden Verzeichnisstruktur, in der *<os_release>* `2012`, `2012R2` oder `2016` ist.
   ```
   drivers\<os_release>\
   ```
2. Kopieren Sie die Einheitentreiber im INF-Format in ein Verzeichnis in diesem Pfad, beispielsweise:
   ```
   drivers\<os_release>\<driver1>\<driver1_files>
   ```
3. Kopieren Sie das `drivers`-Verzeichnis in das Verzeichnis zum Anhängen, beispielsweise:
   ```
   C:\WinPE_64\mount\drivers
   ```

Schritt 8. Führen Sie zusätzliche Anpassungen an der Boot-Datei durch, wie das Hinzufügen von Ordnern, Dateien, Startskripts, Sprachpaketen und Apps. Weitere Informationen zum Anpassen von Boot-Dateien finden Sie im Abschnitt WinPE: Website zum Anhängen und Anpassen.

Schritt 9. Hängen Sie das Image ab, indem Sie den folgenden Befehl ausführen:
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

Schritt 10. Komprimieren Sie den Inhalt des Verzeichnisses `C:\WinPE_64\media` in eine ZIP-Datei namens `WinPE_64.zip`.

Schritt 11. Importieren Sie die ZIP-Datei in XClarity Administrator (siehe Boot-Dateien importieren).

Einheitentreiber importieren

Sie können einzelne Einheitentreiber und Paketdateien in das BS-Images-Repository importieren. Diese Dateien können dann zum Anpassen von Linux- und Windows-Images verwendet werden.

Zu dieser Aufgabe

Sie müssen sicherstellen, dass das Betriebssystem-Image, das Sie implementieren möchten, über die entsprechenden Einheitentreiber für Ihre Ethernet-, Fibre Channel- und Speicheradapter-Hardware verfügt. Wenn der Einheitentreiber für E/A-Adapter nicht im Betriebssystems-Image oder -Profil enthalten ist, wird dieser Adapter bei der BS-Implementierung nicht unterstützt. Sie können angepasste BS-Image-Profile erstellen, die die Out-of-Box-Einheitentreiber enthalten, die Sie benötigen.

Lenovo XClarity Administrator unterstützt In-Box-Einheitentreiber sowie vordefinierte und angepasste Out-of-Box-Einheitentreiber.

- **In-Box-Einheitentreiber**. XClarity Administrator verwaltet keine Inbox-Einheitentreiber. Installieren Sie immer ein aktuelles Betriebssystem, um sicherzustellen, dass die neuesten erforderlichen In-Box-Einheitentreiber vorhanden sind.

  Anmerkung: Sie können einem angepassten Windows-Profil Inbox-Einheitentreiber hinzufügen, indem Sie eine angepasste WinPE-Boot-Datei erstellen und die Einheitentreiberdateien in das Hostsystem im Verzeichnis `C:\drivers` kopieren. Wenn Sie ein angepasstes BS-Image-Profil erstellen, das die angepasste Boot-Datei verwendet, sind die Einheitentreiber im Verzeichnis C:\drivers bei WinPE und dem finalen BS enthalten. Sie werden wie Inbox-Treiber behandelt. Aus diesem Grund müssen Sie diese Inbox-Einheitentreiber nicht in XClarity Administrator importieren, wenn Sie Einheitentreiber angeben, die bei der Erstellung des angepassten BS-Image-Profils verwendet werden sollen.
- **Vordefinierte Einheitentreiber**. Bei ThinkSystem-Servern enthält XClarity Administrator eine Gruppe von Out-of-Box-Einheitentreibern für Linux zur Installation des Betriebssystems und grundlegende Netzwerk- und Speicherkonfigurationen für das finale Betriebssystem. Sie können diese vordefinierten Einheitentreiber den angepassten BS-Image-Profilen hinzufügen und dann die Profile auf verwalteten Servern implementieren.

  Lenovo fasst auch vordefinierte Einheitentreiber in einem Paket zusammen, das von Lenovo Windows-Einheitentreiber und WinPE-Images-Repository Website heruntergeladen und anschließend in das BS-Images-Repository importiert werden kann. Die Paketdateien sind derzeit nur für Windows verfügbar. Wenn die Paketdatei Einheitentreiber und Boot-Dateien enthält, können Sie die Paketdatei von der Registerkarte **Einheitentreiber** oder **Boot-Image** importieren.

  Anmerkungen:

  - Die vordefinierten BS-Image-Profile enthalten standardmäßig die vordefinierten Einheitentreiber.
  - Sie können keine vordefinierten Einheitentreiber löschen, die bei der Installation von XClarity Administrator geladen wurden, aber Sie können vordefinierte Einheitentreiber löschen, die aus einem Lenovo Paket importiert wurden.
  - Für XClarity Administrator müssen die importierten Paketdateien von Lenovo signiert sein. Beim Importieren einer Paketdatei muss auch eine ASC-Signaturdatei importiert werden.
- **Angepasste Einheitentreiber**. Sie können Out-of-Box-Einheitentreiber in das BS-Images-Repository importieren und dann diese Einheitentreiber einem angepassten BS-Image-Profil hinzufügen.

  Sie erhalten Einheitentreiber von Lenovo YUM Repository-Webseite, vom Anbieter (z. B. Red Hat), oder über einen angepassten Einheitentreiber, den Sie selbst erstellen. Für einige Windows-Einheitentreiber kann ein angepasster Einheitentreiber durch Extrahieren des Einheitentreibers aus der ausführbaren Installationsdatei in Ihr lokales System und durch Erstellen einer ZIP-Archivdatei generiert werden.

  Die folgenden Dateitypen werden für das Importieren von angepassten Einheitentreibern unterstützt.

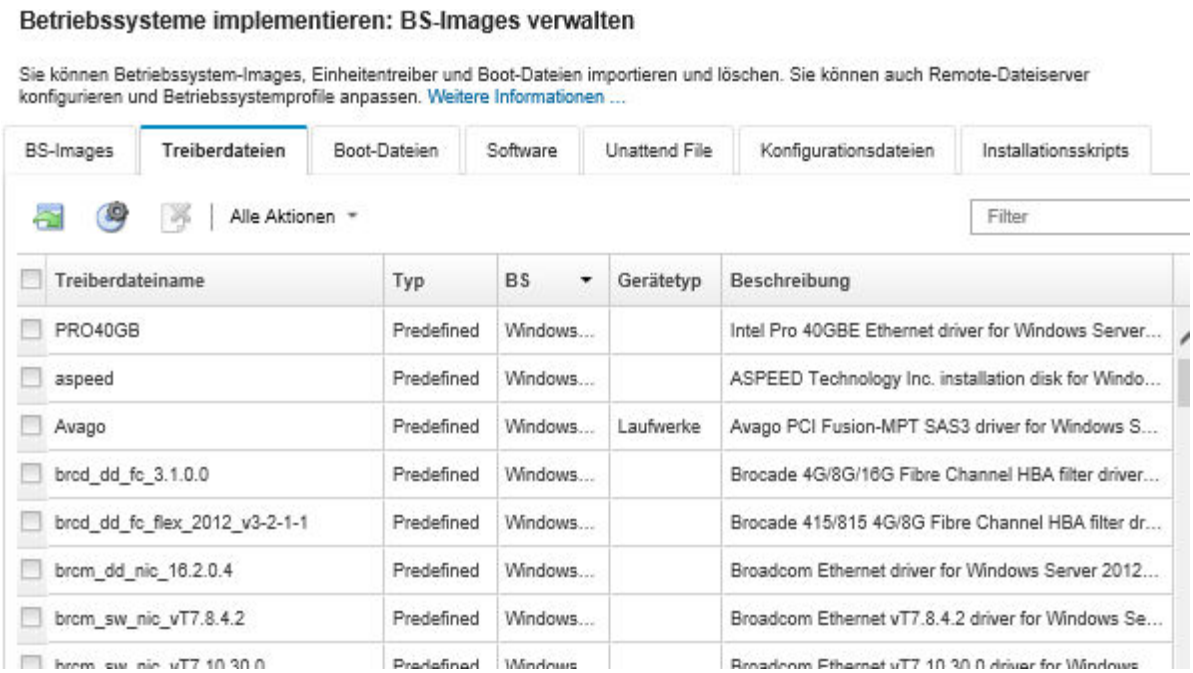
Betriebssystem	Unterstützte Dateitypen für Einheitentreiber
CentOS Linux	Nicht unterstützt
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt

Betriebssystem	Unterstützte Dateitypen für Einheitentreiber
Microsoft Windows Hyper-V Server	Eine ZIP-Datei, die unformatierte Einheitentreiberdateien enthält, die in der Regel als INF-, CAT- und DLL-Dateien gruppiert sind.
Microsoft Windows Server	Eine ZIP-Datei, die unformatierte Einheitentreiberdateien enthält, die in der Regel als INF-, CAT- und DLL-Dateien gruppiert sind.
Red Hat® Enterprise Linux (RHEL) Server	Datenträger zur Treiberaktualisierung (Driver Update Disk, DUD) in einem RPM- oder ISO-Image-Format **Anmerkung:** Wenn Sie eine DUD-RPM auf das angepasste Profil anwenden, wird die RPM nur auf dem letzten Betriebssystem installiert. Sie wird nicht in der Installationsumgebung (initrd) installiert. Um einen angepassten Einheitentreiber in initrd zu installieren, importieren Sie eine DUD-ISO und wenden Sie die ISO auf das angepasste Profil an.
Rocky Linux	Nicht unterstützt
SUSE® Linux Enterprise Server (SLES)	Treiberaktualisierungsplatte (DUD) in einem RPM- oder ISO-Image-Format **Anmerkung:** Wenn Sie eine DUD-RPM auf das angepasste Profil anwenden, wird die RPM nur auf dem letzten Betriebssystem installiert. Sie wird nicht in der Installationsumgebung (initrd) installiert. Um einen angepassten Einheitentreiber in initrd zu installieren, importieren Sie eine DUD-ISO und wenden Sie die ISO auf das angepasste Profil an.
Ubuntu	Nicht unterstützt
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Einheitentreiber im VIB-Image-Format

Anmerkung: Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Vorgehensweise

- Gehen Sie wie folgt vor, um eine Windows Paketdatei, die Einheitentreiber enthält, in das BS-Images-Repository zu importieren.
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Treiberdatei**.



3. Klicken Sie auf **Downloads → Windows Paketdateien**, um auf die Lenovo Unterstützungswebseite zu gehen und laden Sie die entsprechende Paketdatei und die zugeordnete Signaturdatei für das BS-Image auf das lokale System herunter.
4. Klicken Sie auf das Symbol für **Paketdatei importieren** ( ). Das Dialogfenster Paketdatei importieren wird angezeigt.
5. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

   Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** ( ). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .
6. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.
7. Wählen Sie den Betriebssystemtyp und die Version:
8. Geben Sie den Dateinamen der Paketdatei und die zugeordnete Signaturdatei ein oder klicken Sie auf **Durchsuchen**, um nach den Dateien zu suchen, die Sie importieren möchten.
9. **Optional**: Geben Sie eine Beschreibung für die Paketdatei ein.
10. Klicken Sie auf **Importieren**.

    Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

    Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

- Gehen Sie wie folgt vor, um einen einzelnen Einheitentreiber in das BS-Images-Repository zu importieren.
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Treiberdateien**.

3. Klicken Sie auf das Symbol für **Datei importieren** (). Das Dialogfenster Datei importieren wird angezeigt.
4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

   Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** (). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .
5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.
6. Wählen Sie den Betriebssystemtyp und die Version:
7. Geben Sie den Dateinamen ein oder klicken Sie auf **Durchsuchen**, um den Einheitentreiber zu finden, den Sie importieren möchten.
8. **Optional**: Geben Sie eine Beschreibung für den Einheitentreiber ein.
9. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

   Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

   Es werden drei Prüfsummentypen unterstützt:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Klicken Sie auf **Importieren**.

    Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

    Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Das Einheitentreiber-Image ist auf der Seite BS-Images verwalten auf der Registerkarte **Treiberdateien** aufgeführt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** () klicken.
- Klicken Sie auf das Symbol für **Löschen** (), um einen ausgewählten Einheitentreiber zu entfernen.
- Fügen Sie einem angepassten BS-Image-Profil einen Einheitentreiber hinzu (siehe Angepasstes BS-Image-Profil erstellen).

Angepasste Konfigurationseinstellungen importieren

Konfigurationseinstellungen beschreiben Daten, die während der BS-Implementierung dynamisch gesammelt werden müssen. Lenovo XClarity Administrator verwendet eine Gruppe vordefinierter Konfigurationseinstellungen, einschließlich globaler, Netzwerk- und Speicherpositionseinstellungen. Sie können diese vordefinierten Konfigurationseinstellungen verwenden und angepasste Einstellungen hinzufügen, die nicht über XClarity Administrator verfügbar sind.

Zu dieser Aufgabe

Die angepassten Konfigurationseinstellungen werden im Format eines JSON-Schemas definiert. Das Schema muss der JSON-Spezifikation entsprechen.

Beim Importieren von angepassten Konfigurationseinstellungen in XClarity Administrator überprüft XClarity Administrator das JSON-Schema. Wenn die Überprüfung erfolgreich ist, erstellt XClarity Administrator angepasste Makros für jede Einstellung.

Sie können die angepassten Makros in der Unattend-Datei und im Nach-Installationsskript verwenden.

In Unattend-Dateien

Sie können die angepasste Konfigurationsdatei einer Unattend-Datei zuordnen und diese angepassten Makros (und vordefinierten Makros) in diese Unattend-Datei aufnehmen.

Sie können einem angepassten Profil eine oder mehrere angepasste Konfigurationseinstellungsdateien hinzufügen. Wenn Sie das BS-Profil auf einer Gruppe von Zielservern implementieren, können Sie auswählen, welche Konfigurationseinstellungsdatei verwendet wird. XClarity Administrator rendert die Registerkarte **Angepasste Einstellungen** im Dialogfenster „BS-Image implementieren“ basierend auf dem JSON-Schema in der Konfigurationseinstellungsdatei und ermöglicht Ihnen die Angabe von Werten für jede Einstellung (JSON-Objekt), die in der Datei definiert ist.

Anmerkung: Die BS-Implementierung wird nicht fortgesetzt, wenn keine Eingabe für alle erforderlichen angepassten Konfigurationseinstellungen angegeben ist.

In Nach-Installationsskripts

Nachdem die Daten während der BS-Implementierung gesammelt wurden, erstellt XClarity Administrator eine Instanz der Konfigurationseinstellungsdatei (die die angepassten Einstellungen in der ausgewählten Datei und eine Teilmenge der vordefinierten Einstellungen enthält) auf dem Hostsystem, das vom Nach-Installationsskript verwendet werden kann.

Anmerkungen:

- Die Konfigurationseinstellungsdatei ist in Bezug auf ein angepasstes BS-Image-Profil eindeutig.
- Sie können keine Konfigurationseinstellungen für vordefinierte BS-Image-Profile ändern.
- Konfigurationseinstellungen werden nur für die folgenden Betriebssysteme unterstützt:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization 6.0u3 und spätere Aktualisierungen sowie 6.5 und höher

Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Vorgehensweise

Gehen Sie wie folgt vor, um Konfigurationseinstellungsdateien in das BS-Images-Repository zu importieren.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Konfigurationseinstellungen**.

Schritt 3. Klicken Sie auf das Symbol für **Datei importieren** ( ). Das Dialogfenster „Konfigurationseinstellungen importieren“ wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** ( ). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .

Schritt 5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.

Schritt 6. Wählen Sie den Betriebssystemtyp aus.

Schritt 7. Geben Sie den Dateinamen der Konfigurationseinstellungsdatei ein oder klicken Sie auf **Durchsuchen**, um die Datei zu finden, die Sie importieren möchten.

Schritt 8. **Optional**: Geben Sie eine Beschreibung für die Konfigurationseinstellungen ein.

Tipp: Verwenden Sie das Feld **Beschreibung**, um zwischen angepassten Dateien mit demselben Namen zu unterscheiden.

Schritt 9. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

Es werden drei Prüfsummentypen unterstützt:
- **MD5**
- **SHA1**

- **SHA256**

Schritt 10. Klicken Sie auf **Importieren**. Wenn Sie die Datei importieren, wird das JSON-Format überprüft. Wenn Fehler gefunden werden, wird ein Dialogfenster mit der Fehlernachricht und Position angezeigt.

Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

Achtung: Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Die Konfigurationseinstellungsdateien werden in der Registerkarte **Konfigurationseinstellungen** auf der Seite „BS-Images verwalten“ aufgeführt.

Über diese Seite können Sie außerdem die folgenden Aktionen ausführen.

- Erstellen Sie eine Konfigurationseinstellungsdatei, indem Sie auf das Symbol **Erstellen** klicken ( ) und dann Dateiname, Beschreibung, Betriebssystemtyp, Konfigurationseinstellungen und Werte angeben. Klicken Sie auf **Überprüfen**, um das Schema vor dem Speichern der Datei zu prüfen.

  Der Editor bestimmt die Position aller Fehler, die in der Datei gefunden werden. Beachten Sie, dass einige Nachrichten nur auf Englisch angezeigt werden.
- Zum Anzeigen und Ändern einer Konfigurationseinstellungsdatei klicken Sie auf das Symbol **Bearbeiten** ( ).

  Sie können keine Konfigurationseinstellungsdatei bearbeiten, die einer Unattend-Datei zugeordnet ist.

  Der Editor bestimmt die Position aller Fehler, die in der Datei gefunden werden. Beachten Sie, dass einige Nachrichten nur auf Englisch angezeigt werden.
- Zum Kopieren einer Konfigurationseinstellungsdatei klicken Sie auf das Symbol **Kopieren** ( ).

  Wenn Sie eine Konfigurationseinstellungsdatei kopieren, die einer Unattend-Datei zugeordnet ist, wird auch die zugeordnete Unattend-Datei kopiert und die Zuordnung zwischen den beiden Dateien wird automatisch erstellt.
- Um ausgewählte Konfigurationseinstellungsdateien zu entfernen, klicken Sie auf das Symbol **Löschen** ( ).
- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** ( ) klicken.

Weitere Informationen zum Hinzufügen von Konfigurationseinstellungen zu einem angepassten BS-Image-Profil finden Sie unter Angepasstes BS-Image-Profil erstellen.

Angepasste Makros

Makros geben Ihnen die Möglichkeit, einer Unattend-Datei oder einem Nach-Installationsskript Variablendaten (Konfigurationseinstellungen) hinzuzufügen. Lenovo XClarity Administrator ermöglicht es Ihnen, Ihre eigenen angepassten Einstellungen durch Erstellen einer angepassten Konfigurationseinstellungsdatei mithilfe des JSON-Formats zu definieren.

Der Wert für jede angepasste Konfigurationseinstellung hängt von der Benutzereingabe während der Betriebssystem-Implementierung ab.

Beim Importieren von angepassten Konfigurationseinstellungen in XClarity Administrator überprüft XClarity Administrator das JSON-Schema. Wenn die Überprüfung erfolgreich ist, erstellt XClarity Administrator angepasste Makros für jede Einstellung.

Zum Einfügen von angepassten Makros in eine Unattend-Datei oder ein Nach-Installationsskript verwenden Sie den eindeutigen Namen des Objekts, trennen Sie verschachtelte Objekte mit einem Punkt und umschließen Sie den Makronamen mit einem Rautensymbol (#), z.B. **#server_settings.server0.locale#**.

Anmerkungen:

- Beachten Sie, dass der oberste Objektname nicht enthalten sein darf.
- Wenn ein Objekt von einer Vorlage erstellt wird, wird an den Namen eine eindeutige Nummer angehängt, beginnend mit 0 (z.B. server0 und server1).
- Sie können den Namen für jedes Makro im Dialogfeld „BS-Images implementieren“ auf den Registerkarten „Angepasste Einstellungen“ anzeigen, indem Sie mit der Maustaste über das Symbol **Hilfe** () neben jeder angepassten Einstellung bewegen.

Konfigurationseinstellungen

Sie können angepasste Konfigurationseinstellungen definieren, auf die Folgendes zutrifft:

- Sie gelten für alle Zielserver oder nur für einen bestimmten Zielserver.
- Sie haben statische (nicht konfigurierbare) Werte oder dynamische (konfigurierbare) Werte, die eingegeben werden, wenn Sie das BS-Image-Profil implementieren.
- Sie verfügen über eine variable Anzahl an Elementen basierend auf einer Vorlage. Sie können beispielsweise eine Konfigurationseinstellung definieren, die es Ihnen ermöglicht, während der Implementierung 0 bis 3 NTP-Server anzugeben.

Allgemeine Einstellungen

Während der BS-Implementierung werden die UI-Elemente in der Registerkarte **Allgemeine Einstellungen** im Dialogfenster „BS-Image implementieren“ basierend auf den Objekten gerendert, die im Objekt **content** vertreten sind. Die Objekte beschreiben die Einstellungen und Werte, die alle Zielserver für die BS-Implementierung erfordern.

Um Einstellungen darzustellen, die auf allen Servern vertreten sind, muss die JSON-Datei ein übergeordnetes Objekt mit einem verschachtelten Objekt enthalten, das das Name/Wert-Paar `"common":true` enthält.

Im folgenden Beispiel wird derselbe konfigurierbare (dynamische) NTP-Server für alle Server verwendet.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
```

```
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
         }],
         "type": "array"
      },
      ...,
   }
```

Im folgenden Beispiel wird dasselbe nicht konfigurierbare (statische) Protokollverzeichnis für Nach-Installationsskripte verwendet.

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Serverspezifische Einstellungen

Während der BS-Implementierung werden die UI-Elemente in der Registerkarte **Serverspezifische Einstellungen** im Dialogfenster „BS-Image implementieren“ basierend auf den Objekten gerendert, die in den **content**-Objekten der Vorlage vertreten sind. Die Objekte beschreiben die Einstellungen und Werte, die ein bestimmter Zielserver für die BS-Implementierung erfordert.

Nachdem die serverspezifischen Werte in der Benutzeroberfläche erfasst wurden, wird in der JSON-Datei ein Objekt **content** für jeden Zielserver erstellt, das auf dem Objekt **template** basiert. Jedes **content**-Objekt enthält ein eindeutiges **name**- und **targetServer**-Feld und alle Werte, die für diesen Server eingegeben wurden.

Um die serverspezifischen Einstellungen darzustellen, muss die JSON-Datei ein übergeordnetes Objekt mit dem folgenden Inhalt enthalten:

- Das Name/Wert-Paar `"category":"dynamic"`.
- Ein verschachteltes Objekt, das das Name/Wert-Paar `"common":false` enthält. Nur ein `"common": false`-Objekt wird im Inhalt des übergeordneten Objekts unterstützt.
- Ein Vorlagenobjekt mit einem integrierten Inhaltsobjekt. Dieses Vorlagenarray kann nur ein Objekt enthalten.

Wenn Sie z.B. ein eindeutiges BS-Gebietsschema für jeden Zielserver definieren möchten:

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
```

```
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
      }],
      "type": "assoc_array"
   },
   ...,
}
```

JSON-Spezifikation

In der folgenden Tabelle werden die Felder beschrieben, die in der JSON-Spezifikation zulässig sind.

Parameter	Erforderlich/ Optional	Typ	Beschreibung
autoCreateInstance	Optional	Boolesch	Gibt an, ob eine Instanz des Vorlagenobjekts bei der Bereitstellung automatisch in einer JSON-Datei erstellt wird. Es kann einen der folgenden Werte aufweisen. • **true**: Eine Instanz des Vorlagenobjekts wird bei der Bereitstellung automatisch in einer JSON-Datei erstellt. • **false**: Eine Instanz des Vorlagenobjekts wird bei der Bereitstellung *nicht* automatisch in einer JSON-Datei erstellt. (Standardwert) **Anmerkung:** Dieses Feld kann nur im Vorlagenobjekt platziert werden.
category	Erforderlich	Zeichenkette	Gibt an, wie der Wert jeder Einstellung bestückt ist. Dies kann einer der folgenden Werte sein: • **dynamic**: Der Wert wird bei der Ausführungszeit durch den Benutzer eingegeben. Während der BS-Implementierung werden Sie von Lenovo XClarity Administrator zur Eingabe dieses Werts aufgefordert. • **predefined**: Der Wert wird von Lenovo XClarity Administrator vordefiniert. • **static**: Der Wert wird im Schema festgelegt und bei der Ausführungszeit nicht geändert. Verschachtelte Objekte übernehmen den Wert dieses Felds von ihrem übergeordneten Objekt. Wenn **category** im übergeordneten Objekt auf `static` festgelegt ist, muss es auch in allen verschachtelten Objekten auf `static` festgelegt werden. Wenn **category** im übergeordneten Objekt auf `dynamic` festgelegt ist, kann es in verschachtelten Objekten entweder `static` oder `dynamic` sein.

Parameter	Erforderlich/ Optional	Typ	Beschreibung
choices	Optional	Array mit Werten, die mit der Eigenschaft **type** übereinstimmen	Array der statischen Werte (z.B. Zeichenfolgen oder Ganzzahlen) für die Konfigurationseinstellung, aus der der Benutzer während der BS-Implementierung wählen kann (z.B. `["enabled","disabled"]`).
common	Optional	Boolesch	Gibt an, ob dieses Konfigurationsschema für alle Zielserver gilt. • **true**: Das Objekt gilt für alle Zielserver. • **false**: (default) Das Objekt gilt für einen bestimmten Zielserver. Verschachtelte Objekte übernehmen den Wert dieses Felds von ihrem übergeordneten Objekt. Wenn **common** im übergeordneten Objekt auf `true` festgelegt ist, muss es auch in allen verschachtelten Objekten auf `true` festgelegt werden. Wenn **common** im übergeordneten Objekt auf `false` festgelegt ist, muss es in allen verschachtelten Objekten auf `false` festgelegt werden.
content	Optional	Objektarray	Muster, das verschachtelte Objekte im Schema darstellt. Nachdem die vom Benutzer eingegebenen Daten während der BS-Implementierung erfasst wurden, stellt dieses Feld die finalen Werte für eine angegebene Vorlage in der Instanz der Konfigurationseinstellungsdatei dar, die für die Implementierung erstellt wird.
default	Optional	Abhängig von **type**	Der Standardwert.
description	Optional	Zeichenkette	Beschreibung des Objekts.
label	Optional	Zeichenkette	Bezeichnung für die Einstellung in der Benutzerschnittstelle, die während der BS-Implementierung angezeigt wird.
max	Optional	Ganzzahl	Maximaler Wert, wenn **type** auf eine Ganzzahl festgelegt ist. Der Standardwert ist unbegrenzt.
maxElements	Optional	Ganzzahl	Maximale Anzahl der Eingaben im Array für dieses Objekt.
min	Optional	Ganzzahl	Minimaler Wert, wenn **type** auf eine Ganzzahl festgelegt ist. Der Standardwert lautet 0.
minElements	Optional	Ganzzahl	Minimale Anzahl der Eingaben im Array für dieses Objekt.

Parameter	Erforderlich/ Optional	Typ	Beschreibung
name	Erforderlich	Zeichenkette	Eindeutiger Name des Objekts. Dieser Name kann nur die folgenden Zeichen enthalten: alphanumerische Zeichen (a-z, A-Z und 0-9), Unterstrich (_) und Bindestrich (-). Sie können in der Unattend-Datei auf **name** als angepasstes Makro verweisen. Beim Verweis auf ein verschachteltes **name**-Objekt müssen Sie jedes Objekt mit einem Punkt trennen (z.B. `mydeploy.node.locale`).
optional	Erforderlich	Boolesch	Gibt an, ob das Objekt optional ist. Es kann einen der folgenden Werte aufweisen. • **true**: Das Feld ist optional. • **false**: Das Feld ist erforderlich.
regex	Optional	Zeichenkette	Regulärer Ausdruck für die Überprüfung des Werts (z.B. `"[\\w\\.]{1,64}$"`).
script	Optional	Zeichenfolgenarray	Liste der durch ein Komma voneinander getrennten Skripts, die von den Daten in diesem Objekt abhängig sind (z.B. `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`). **Anmerkung:** Die Skripts müssen für das BS-Image-Profil als Installationsskript oder angepasste Software verfügbar sein.
targetServer	Optional	Zeichenkette	UUID des Servers, der das Ziel für die BS-Implementierung ist. Wenn „common“ den Wert „true“ hat, kann dieses Feld null oder leer sein, und der Zielserver wird während der BS-Implementierung festgelegt.

Parameter	Erfor-derlich/ Optional	Typ	Beschreibung

template	Optional	Objektar-ray	Muster, das wiederverwendbare Objekte darstellt. Während der BS-Implementierung kann diese Vorlage mehrere Instanzen des Objekts darstellen. Die Felder **minElements** und **maxElements** können zum Begrenzen der Anzahl der Instanzen verwendet werden.
			
			Im folgenden Beispiel wird eine Vorlage für die Darstellung eines Arrays von 1 bis 3 NTP-Servern verwendet.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"template": [{`
			`"autoCreateInstance": true,`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string"`
			`}],`
			`"type": "array"`
			`},`
			
			Nachdem die vom Benutzer eingegebenen Werte während der BS-Implementierung erfasst wurden, wird eine Instanz der Konfigurationseinstellungsdatei mit bestimmten Inhalten für jede Einheit erstellt, auf der das BS implementiert werden soll.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"content": [{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver0",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string",`
			`"value": "192.0.2.1"`
			`}],`

Parameter	Erfor-derlich/ Optional	Typ	Beschreibung

			<pre>"template": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Anmerkungen:**
			• Eine Vorlage ist auf der obersten Ebene der serverspezifischen Objekte *erforderlich* (common = false).
			• Wenn bei **category** `static` festgelegt ist, wird das Feld „template“ ignoriert.

type	Erforder-lich	Zeichen-kette	Datentyp für das Objekt. Es kann einen der folgenden Werte aufweisen. • **array** • **assoc_array** • **boolean** • **integer** • **password** • **string** • **user_data**
value	Optional	Zeichen-kette	Ein einzelner statischer Wert für die Konfigurationseinstellung. **Anmerkungen:** • Wenn **default** festgelegt ist, kann dieses Feld leer oder null sein. Andernfalls müssen Sie einen Wert eingeben, der **type** entspricht. • Wenn für **type** `password` festgelegt ist, geben Sie eine unverschlüsselte Zeichenfolge an. • Wenn für **type** `assoc_array` oder `array` festgelegt ist, müssen Sie außerdem ein leeres **content**-Feld festlegen. • Wenn bei **type** `user_data` festgelegt ist, geben Sie einen gültigen **value** im JSON-Format ein. • Wenn **regex** festgelegt ist, wird dieser Wert mit dem angegebenen regulären Ausdruck überprüft.

Im folgenden Beispiel definieren die Konfigurationseinstellungen Ländereinstellungen für SLES-Implementierungen, die zu einem angepassten Profil hinzugefügt werden können.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
```

```
    "optional": false,
    "template": [{
        "autoCreateInstance": true,
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logging.",
    "name": "logpath",
```

```
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Im folgenden Beispiel wird die Instanz der Konfigurationseinstellungsdatei gezeigt, die auf dem Hostsystem erstellt wird, nachdem die vom Benutzer eingegebenen Werte während der Implementierung definiert werden.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
```

```
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server1",
        "optional": false,
        "type": "assoc_array",
        "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
```

```
        "common": true,
        "description": "NTP Servers",
        "label": "NTP Servers",
        "maxElements": 3,
        "minElements": 0,
        "name": "common-ntpservers",
        "optional": true,
        "content": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Vordefinierte Makros

Makros geben Ihnen die Möglichkeit, einer Unattend-Datei oder einem Nach-Installationsskript Variablendaten (Konfigurationseinstellungen) hinzuzufügen. Lenovo XClarity Administrator bietet eine Reihe von vordefinierten Konfigurationseinstellungen, die Sie verwenden können.

Zum Einfügen von angepassten Makros in eine Unattend-Datei oder ein Nach-Installationsskript stellen Sie dem Makronamen bei vordefinierten Makros das Präfix „predefined“ voran, trennen Sie verschachtelte Objekte mit einem Punkt und umschließen Sie den Makronamen mit einem Rautensymbol (#), z. B. **#predefined.globalSettings.ipAssignment#**.

Der Wert für jedes vordefinierte Makro variiert je nach XClarity Administrator-Instanz. Mit Feld **BS-Images implementieren → Globale Einstellungen → IP-Zuordnung** können Sie beispielsweise den IP-Modus festlegen. Nachdem die vom Benutzer eingegebenen Werte während der BS-Implementierung erfasst wurden, wird der Wert in den vordefinierten Konfigurationseinstellungen über das vordefinierte Makro **#predefined.globalSettings.ipAssignment#** und in der Instanz der Konfigurationseinstellungs-JSON-Datei unter dem Objektnamen „ipAssignment“ dargestellt.

In der folgenden Tabelle werden die vordefinierten Makros (Konfigurationseinstellungen) aufgeführt, die XClarity Administrator verfügbar sind.

Makroname	Typ	Beschreibung
vordefiniert	Objekt	Informationen zu allen vordefinierten BS-Implementierungseinstellungen
globalSettings	Objekt	Informationen zu globalen BS-Implementierungseinstellungen.
credentials	Objekt-tarray	Informationen zu Benutzeranmeldeinformationen
name	Zeichen-kette	
type	Zeichen-kette	Betriebssystemtyp. Es kann einen der folgenden Werte aufweisen. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	Zeichen-kette	Host-Netzwerkeinstellungsoption für die Betriebssystemimplementierung. Es kann einen der folgenden Werte aufweisen. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	Zeichen-kette	Gibt an, ob der VLAN-Modus verwendet wird. Es kann einen der folgenden Werte aufweisen. • **true**: Der VLAN-Modus wird verwendet. • **false**: Der VLAN-Modus wird nicht verwendet.
hostPlatforms	Objekt	Bereitstellungseinstellungen der Host-Plattformen
licenseKey	Zeichen-kette	Lizenzschlüssel zur Verwendung für Microsoft Windows oder VMware ESXi. Wenn Sie keinen Lizenzschlüssel haben, können Sie in diesem Feld „null“ eintragen.
networkSettings	Bereich	Informationen zu Netzwerkeinstellungen
dns1	Zeichen-kette	Bevorzugter DNS-Server für den Hostserver zur Verwendung nach Implementierung des Betriebssystems
dns2	Zeichen-kette	Alternativer DNS-Server für den Hostserver zur Verwendung nach Implementierung des Betriebssystems

Makroname	Typ	Beschreibung
gateway	Zeichen-kette	Gateway für den Hostserver zur Verwendung nach Implementierung des Betriebssystems. Es wird verwendet, wenn die Netzwerkeinstellungen in den globalen BS-Implementierungseinstellungen auf „static“ festgelegt sind. **Tipp:** Verwenden Sie GET /osdeployment/globalSettings zur Bestimmung des IP-Modus.
hostname	Zeichen-kette	Hostname für den Hostserver. Wenn kein Hostname angegeben ist, wird ein Standard-Hostname zugewiesen.
ipAddress	Zeichen-kette	IP-Adresse für den Hostserver zur Verwendung nach Implementierung des Betriebssystems. Sie wird verwendet, wenn die Netzwerkeinstellungen in den globalen BS-Implementierungseinstellungen auf „static“ festgelegt sind.
mtu	Lang	Größte zu übertragende Einheit (Maximum Transmission Unit – MTU) für den Host zur Verwendung nach Implementierung des Betriebssystems.
prefixLength	Zeichen-kette	Präfixlänge für die Host-IP-Adresse zur Verwendung nach Implementierung des Betriebssystems. Sie wird verwendet, wenn die Netzwerkeinstellungen in den globalen BS-Implementierungseinstellungen auf „static IPv6“ festgelegt sind.
selectedMAC	Zeichen-kette	MAC-Adresse des Hostservers, an die die IP-Adresse gebunden werden soll. Die MAC-Adresse ist standardmäßig auf AUTO festgelegt. Diese Einstellung 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 XClarity Administrator-Host automatisch neu gestartet, um die erkannte MAC-Adresse für die Bereitstellung zu verwenden. und selectedMAC werden für die neu erkannte MAC-Adresse festgelegt. Der VLAN-Modus wird nur für Server unterstützt, die MAC-Adressen in ihrem Bestand haben. Wenn für einen Server nur die MAC-Adresse AUTO verfügbar ist, können keine VLANs zur Bereitstellung von Betriebssystemen auf dem Server verwendet werden. **Tipp:** Verwenden Sie den Antwortparameter **macaddress** in GET /hostPlatforms, um die MAC-Adresse abzurufen.
subnetCIDRNumber	Ganzzahl	Die Subnetzmaske des Hostservers, die nach der Implementierung des Betriebssystems verwendet werden soll, im CIDR-Format (Classless Inter-Domain Routing). Es wird verwendet, wenn die Netzwerkeinstellungen in den globalen BS-Implementierungseinstellungen auf „static“ festgelegt sind. Der CIDR-Nummer wird in der Regel ein Schrägstrich „/“ vorangestellt und sie folgt der IP-Adresse. Beispiel: Eine IP-Adresse 131.10.55.70 mit Subnetzmaske 255.0.0.0 (die aus 8 Netzwerk-Bits besteht) wird als 131.10.55.70 /8 dargestellt. Weitere Informationen finden Sie unter Tutorial-Website für CIDR-Notation. **Tipp:** Verwenden Sie GET /osdeployment/globalSettings zur Bestimmung des IP-Modus.

Makroname	Typ	Beschreibung
subnetMask	Zeichenkette	Subnetzmaske für den Hostserver zur Verwendung nach Implementierung des Betriebssystems in Dezimalschreibweise mit Punkten (z. B. 255.0.0.0). Es wird verwendet, wenn die Netzwerkeinstellungen in den globalen BS-Implementierungseinstellungen auf „static“ festgelegt sind. **Tipp:** Verwenden Sie GET /osdeployment/globalSettings zur Bestimmung des IP-Modus.
vlanId	Zeichenkette	VLAN-ID für Betriebssystem-VLAN-Tagging. Dieser Parameter ist nur gültig, wenn der VLAN-Modus aktiviert ist. Um zu ermitteln, ob der VLAN-Modus aktiviert ist, verwenden Sie GET /osdeployment/globalSettings in der Onlinedokumentation von XClarity Administrator. **Wichtig:** Geben Sie nur dann eine VLAN-ID an, wenn ein VLAN-Tag für die Funktion im Netzwerk erforderlich ist. Die Verwendung von VLAN-Tags kann sich auf das Netzwerkrouting zwischen dem Hostbetriebssystem und XClarity Administrator auswirken.
selectedImage	Zeichenkette	Profil-ID des zu implementierenden Betriebssystem-Images. **Tipp:** Verwenden Sie den Antwortparameter **availableImages** in GET /hostPlatforms, um die Profil-IDs des Betriebssystem-Images abzurufen.
storageSettings	Bereich	Bevorzugte Speicherposition, an der Betriebssystem-Images implementiert werden sollen
targetDevice	Zeichenkette	Zieleinheit. Es kann einen der folgenden Werte aufweisen. • **localdisk**. Lokales Festplattenlaufwerk. Es wird das erste aufgelistete lokale Festplattenlaufwerk im verwalteten Server verwendet. • **M.2drive**. M.2-Laufwerk Das erste aufgelistete M.2-Laufwerk im verwalteten Server wird verwendet. • **usbdisk**. Integrierter USB-Hypervisor. Diese Position ist nur anwendbar, wenn ein VMware ESXi-Image auf verwalteten Servern implementiert wird. Wenn auf dem verwalteten Server zwei Hypervisor-Schlüssel installiert sind, wählt das VMware-Installationsprogramm den zuerst aufgelisteten Schlüssel für die Implementierung aus. • **lunpluswwn=***LUN@WWN*. FC SAN-Speicher (z. B. `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN-Speicher (z. B. `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Die Angabe des *IQN* ist optional, wenn nur ein iSCSI-Ziel konfiguriert ist. Wenn der *IQN* nicht angegeben ist, wird das erste erkannte iSCSI-Ziel für OSDN ausgewählt. Falls angegeben, wird eine exakte Übereinstimmung erzielt. **Anmerkung:** Bei ThinkServer-Servern ist dieser Wert immer „localdisk“.
unattendFileId	Zeichenkette	ID der Unattend-Datei, die mit dieser Implementierung verwendet werden soll
uuid	Zeichenkette	UUID des Hostservers, auf dem das Betriebssystem implementiert werden soll
imageSettings	Objekt	Informationen zu den einzelnen BS-Images und Image-Profilen
name	Zeichenkette	Name des Betriebssystem-Images
Profil	Zeichenkette	Name des Image-Profils

Makroname	Typ	Beschreibung
otherSettings	Objekt	Zusätzliche Einstellungen, die sich auf die aktuell laufenden BS-Implementierungsjobs beziehen
deployDataAndSoftwareLocation	Zeichenkette	Pfad zu den extrahierten Software-Nutzdaten, angepassten Dateien und Implementierungsdaten (z. B. Zertifikate und Protokolle)

installRepoUrl	Zeichenkette	(nur SLES 15 und höher) URL für das importierte Paket-Image
		Sie können dieses vordefinierte Makro in der angepassten Unattend-Datei für die „media_url“ im Add-On-Abschnitt verwenden, z. B.
		`<add-on>`
		`<add_on_products config:type="list">`
		`<listentry>`
		`<media_url>`**#predefined.otherSettings.installRepoUrl#**
		`</media_url>`
		`<product>sle-module-basesystem</product>`
		`<product_dir>/Module-Basesystem</product_dir>`
		`</listentry>`
		`</add_on_products>`
		`</add-on>`

lxcaIp	Zeichenkette	IP-Adresse der XClarity Administrator-Instanz.
lxcaRelease	Zeichenkette	XClarity Administrator-Version (z. B. 2.0.0)
jobId	Zeichenkette	ID des aktuell ausgeführten BS-Implementierungsjobs
ntpServer	Zeichenkette	NTP-Server, der XClarity Administrator zugeordnet ist
statusSettings	Objekt	Statuseinstellungen der BS-Implementierung.
urlStatus	Zeichenkette	HTTPS-URL (einschließlich Port), die XClarity Administrator für Statusmeldungen verwendet
certLocation	Zeichenkette	Ordner mit den Zertifikaten, die erforderlich sind, um vom Host-BS beim ersten Booten auf den Webservice **urlStatus** zugreifen zu können
sdkLocation	Zeichenkette	Position der von XClarity Administrator bereitgestellten Hilfeskripts und Schnittstellen für den Zugriff auf den XClarity Administrator
timezone	Zeichenkette	Zeitzone, die für XClarity Administrator festgelegt ist (z. B. Amerika/New_York)
unattendSettings	Objekt	Einstellungen zur Bestückung der Unattend-Datei. Diese Werte sind für die Version von XClarity Administrator eindeutig.
networkConfig	Zeichenkette	(nur ESXi und RHEL) Vordefinierter Inhalt von XClarity Administrator zur Verwendung bei der Unattend-Installationszeit. Dadurch werden die Netzwerkeinstellungen für das Betriebssystem konfiguriert.

Makroname	Typ	Beschreibung
preinstallConfig	Zeichen-kette	Vordefinierter Inhalt von XClarity Administrator zur Verwendung bei der Vor-Installation-Unattend-Zeit. Dies umfasst auch den Vor-Installationsstatus. • Für ESXi und RHEL wird der Vor-Installations-Skript-Hook %pre verwendet. • Für SLES wird der Vor-Installations-Skript-Hook <scripts> verwendet. **Achtung:** Es wird empfohlen, dieses Makro in der angepassten Unattend-Datei zu integrieren. Sie können das Makro in der Unattend-Datei an einer beliebigen Stelle nach Zeile 1 (nach dem <xml>-Tag) positionieren.
postinstallConfig	Zeichen-kette	Vordefinierter Inhalt von XClarity Administrator zu Verwendung, nachdem der Server konfiguriert und zum ersten Mal gebootet wird. Dies umfasst auch den Nach-Installationsstatus. • Für ESXi und RHEL wird der Nach-Installations-Skript-Hook %post verwendet. • Für SLES wird der Nach-Installations-Skript-Hook <scripts> verwendet. • Für Windows wird der Abschnitt „specialize settings“ verwendet. **Achtung:** Es wird empfohlen, dieses Makro in der angepassten Unattend-Datei zu integrieren. Sie können das Makro in der Unattend-Datei an einer beliebigen Stelle nach Zeile 1 (nach dem <xml>-Tag) positionieren.
reportWorkloadNotComplete	Zeichen-kette	Wenn dieses Makro vorhanden ist, meldet das Makro „postinstallConfig“ nicht den Status „BS-Installation abgeschlossen (17)“. Das angepasste Profil muss als abgeschlossen gemeldet werden.
storageConfig	Zeichen-kette	(nur ESXi und RHEL) Vordefinierter Inhalt von XClarity Administrator zur Verwendung bei der Unattend-Installationszeit. Dadurch werden die Speichereinstellungen für das Betriebssystem konfiguriert.

Angepasste Unattend-Dateien importieren

Sie können angepasste Unattend-Dateien in das BS-Images-Repository importieren. Diese Dateien können dann zum Anpassen von Linux- und Windows-BS-Image-Profilen verwendet werden.

Zu dieser Aufgabe

Die folgenden Dateitypen werden für angepasste Unattend-Dateien unterstützt.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
CentOS Linux	Nicht unterstützt	
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	
Microsoft Windows Hyper-V Server	Nicht unterstützt	
Microsoft Windows Server	Unattend (.xml)	Weitere Informationen zu Unattend-Dateien finden Sie unter Website zur Referenz für das unbeaufsichtigte Windows-Setup.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Weitere Informationen zu Unattend-Dateien finden Sie unter Red Hat: Website zum Automatisieren der Installation mit Kickstart. Beachten Sie beim Hinzufügen von %pre-, %post- und % firstboot-Abschnitten in der Datei die folgenden Aspekte. • Sie können mehrere %pre-, %post- und %firstboot-Abschnitte zur Unattend-Datei hinzufügen. Achten Sie dabei aber auf die Reihenfolge der Abschnitte. • Wenn das empfohlene **#predefined.unattendSettings.preinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator einen %pre-Abschnitt vor allen anderen %pre-Abschnitten in der Datei hinzu. • Wenn das empfohlene **#predefined.unattendSettings.postinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator %post- und einen %firstboot-Abschnitte vor allen anderen %post- und % firstboot-Abschnitten in der Datei hinzu.
Rocky Linux	Kickstart (.cfg)	Weitere Informationen zu Unattend-Dateien finden Sie unter Red Hat: Website zum Automatisieren der Installation mit Kickstart. Beachten Sie beim Hinzufügen von %pre-, %post- und % firstboot-Abschnitten in der Datei die folgenden Aspekte. • Sie können mehrere %pre-, %post- und %firstboot-Abschnitte zur Unattend-Datei hinzufügen. Achten Sie dabei aber auf die Reihenfolge der Abschnitte. • Wenn das empfohlene **#predefined.unattendSettings.preinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator einen %pre-Abschnitt vor allen anderen %pre-Abschnitten in der Datei hinzu. • Wenn das empfohlene **#predefined.unattendSettings.postinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator %post- und einen %firstboot-Abschnitte vor allen anderen %post- und % firstboot-Abschnitten in der Datei hinzu.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Weitere Informationen zu Unattend-Dateien finden Sie unter SUSE: AutoYaST-Website.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
Ubuntu	Nicht unterstützt	
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Kickstart (.cfg)	Nur für ESXi 6.0u3 und spätere Aktualisierungen und 6.5 und höher unterstützt. Weitere Informationen zu Unattend-Dateien finden Sie unter VMware: Hosts mithilfe einer Script-Website installieren oder aktualisieren. Beachten Sie beim Hinzufügen von %pre-, %post- und %firstboot-Abschnitten in der Datei die folgenden Aspekte. • Sie können mehrere %pre-, %post- und %firstboot-Abschnitte zur Unattend-Datei hinzufügen. Achten Sie dabei aber auf die Reihenfolge der Abschnitte. • Wenn das empfohlene **#predefined.unattendSettings.preinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator einen %pre-Abschnitt vor allen anderen %pre-Abschnitten in der Datei hinzu. • Wenn das empfohlene **#predefined.unattendSettings.postinstallConfig#**-Makro in der Unattend-Datei vorhanden ist, fügt XClarity Administrator %post- und einen %firstboot-Abschnitte vor allen anderen %post- und %firstboot-Abschnitten in der Datei hinzu.

Achtung:

- Sie können vordefinierte und angepasste Makros (Konfigurationseinstellungen) mit dem eindeutigen Namen des Objekts in die Unattend-Datei einfügen. Vordefinierte Werte sind basierend auf den XClarity Administrator-Instanzen dynamisch. Angepasste Makros sind basierend auf Benutzereingaben dynamisch, die während der BS-Implementierung festgelegt werden.

  Anmerkungen:

  - Umschließen Sie den Makronamen mit einem Rautensymbol (#).
  - Trennen Sie bei verschachtelten Objekten jeden Objektnamen mit einem Punkt (z. B. **#server_settings.server0.locale#**).
  - Bei angepassten Makros darf der oberste Objektname nicht enthalten sein. Stellen Sie dem Makronamen bei vordefinierten Makros das Präfix „predefined“ voran.
  - Wenn ein Objekt von einer Vorlage erstellt wird, wird an den Namen eine eindeutige Nummer angehängt, beginnend mit 0 (z. B. **server0** und **server1**).
  - Sie können den Namen für jedes Makro im Dialogfeld „BS-Images implementieren“ auf den Registerkarten „Angepasste Einstellungen“ anzeigen, indem Sie mit der Maustaste über das Hilfe-Symbol () neben jeder angepassten Einstellung bewegen.
  - Eine Liste der vordefinierten Makros finden Sie unter Vordefinierte Makros. Informationen zu angepassten Konfigurationseinstellungen und Makros finden Sie unter Angepasste Makros.
- XClarity Administrator bietet die folgenden vordefinierten Makros, die zur Statusübertragung vom BS-Installationsprogramm sowie für andere wichtige Installationsschritte verwendet werden. Es wird empfohlen, diese Makros in die Unattend-Datei zu integrieren (siehe Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Vorgehensweise

Gehen Sie wie folgt vor, um Unattend-Dateien in das BS-Images-Repository zu importieren.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Unattend-Dateien**.

Schritt 3. Klicken Sie auf das Symbol für **Datei importieren** ( ). Das Dialogfenster „Datei importieren“ wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** ( ). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .

Schritt 5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.

Schritt 6. Wählen Sie den Betriebssystemtyp aus.

Schritt 7. Geben Sie den Dateinamen der Unattend-Datei ein oder klicken Sie auf **Durchsuchen**, um die Datei zu finden, die Sie importieren möchten.

Schritt 8. **Optional**: Geben Sie eine Beschreibung für die Unattend-Datei ein.

Tipp: Verwenden Sie das Feld **Beschreibung**, um zwischen angepassten Dateien mit demselben Namen zu unterscheiden.

Schritt 9. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

Es werden drei Prüfsummentypen unterstützt:
- **MD5**
- **SHA1**
- **SHA256**

Schritt 10. Klicken Sie auf **Importieren**.

Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Das Unattend-Datei-Image ist auf der Seite BS-Images verwalten in der Registerkarte **Unattend-Dateien** aufgeführt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Sie können eine Unattend-Datei erstellen, indem Sie auf das Symbol **Erstellen** klicken ().

  Der Editor bestimmt die Position aller Fehler, die in der Datei gefunden werden. Beachten Sie, dass einige Nachrichten nur auf Englisch angezeigt werden.
- Ordnen Sie eine Unattend-Datei einer Konfigurationseinstellungsdatei zu (siehe Unattend-Datei einer Konfigurationseinstellungsdatei zuordnen).
- Zum Anzeigen und Ändern einer Unattend-Datei klicken Sie auf das Symbol **Bearbeiten** ().

  Der Editor bestimmt die Position aller Fehler, die in der Datei gefunden werden. Beachten Sie, dass einige Nachrichten nur auf Englisch angezeigt werden.
- Kopieren Sie eine Unattend-Datei, indem Sie auf das Symbol **Kopieren** klicken ().

  Wenn Sie eine Unattend-Datei kopieren, die einer Konfigurationseinstellungsdatei zugeordnet ist, wird auch die zugeordnete Konfigurationseinstellungsdatei kopiert und die Zuordnung zwischen den beiden Dateien wird automatisch erstellt.
- Um ausgewählte Unattend-Dateien zu entfernen, klicken Sie auf das Symbol **Löschen** ().
- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** () klicken.

Weitere Informationen zum Hinzufügen einer Unattend-Datei zu einem angepassten BS-Image-Profil finden Sie unter Angepasstes BS-Image-Profil erstellen.

Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei

Sie können einer Unattend-Datei vordefinierte und angepasste Makros hinzufügen.

Zu dieser Aufgabe

Makros bieten Ihnen die Möglichkeit, dynamische Daten (Konfigurationseinstellungen) zu einer Unattend-Datei hinzuzufügen. Die Datenwerte stellen Sie bei der Implementierung des BS-Image-Profils zur Verfügung.

Lenovo XClarity Administrator stellt *vordefinierte* Makros bereit, die Sie zu einer Unattend-Datei hinzufügen können, ohne eine angepasste Konfigurationseinstellungsdatei zuzuordnen. Eine Liste der vordefinierten Makros finden Sie unter Vordefinierte Makros.

Es wird empfohlen, dies folgenden vordefinierten Makros in die angepasste Unattend-Datei zu integrieren.

- **#predefined.unattendSettings.preinstallConfig#** und **#predefined.unattendSettings postinstallConfig#**. Diese vordefinierten Makros werden zur Statusübertragung vom BS-Installationsprogramm sowie für andere wichtige Installationsschritte verwendet.

  In den folgenden BS-Implementierungsbeispielszenarien finden Sie weitere Informationen dazu, wie Sie die Installationskonfigurationsmakros integrieren.
  - RHEL und eine Hello World PHP-Anwendung mit einer angepassten Unattend-Datei implementieren
  - SLES 12 SP3 mit einem konfigurierbaren Gebietsschema und NTP-Servern implementieren
  - VMware ESXi v6.7 mit Lenovo Customization über eine statische IP-Adresse auf einer lokalen Festplatte implementieren
  - Windows 2016 mit angepassten Funktionen implementieren
- **#predefined.unattendSettings.networkConfig#**: (nur für ESXi und RHEL) Ermöglicht XClarity Administrator, das Netzwerk zu konfigurieren. Dieses Makro verwendet die Netzwerkeinstellungen, die auf der Seite „BS-Images bereitstellen“ angegeben sind. Wenn Sie dieses Makro nicht in die Unattend-Datei integrieren oder wenn die Netzwerkeinstellungen nicht in XClarity Administrator definiert sind, müssen Sie die IP-Schnittstelle als Teil der Unattend-Datei konfigurieren, sodass der Host über eine Netzwerkroute zurück zu XClarity Administrator verfügt.

  In den folgenden BS-Implementierungsbeispielszenarien finden Sie weitere Informationen dazu, wie Sie das Netzwerkkonfigurationsmakro integrieren.
  - RHEL und eine Hello World PHP-Anwendung mit einer angepassten Unattend-Datei implementieren
  - VMware ESXi v6.7 mit Lenovo Customization über eine statische IP-Adresse auf einer lokalen Festplatte implementieren
- **#predefined.unattendSettings.storageConfig#**. (nur für ESXi und RHEL) Ermöglicht XClarity Administrator, Speicher auf dem Host zu konfigurieren. Dieses Makro verwendet die Speichereinstellungen, die auf der Seite „BS-Images bereitstellen“ angegeben sind. Wenn Sie dieses Makro nicht in die Unattend-Datei integrieren oder wenn die Speichereinstellungen nicht in XClarity Administrator definiert sind, müssen Sie die Speicherkonfiguration in der Unattend-Datei angeben.

  In den folgenden BS-Implementierungsbeispielszenarien finden Sie weitere Informationen dazu, wie Sie das Speicherkonfigurationsmakro integrieren.
  - RHEL und eine Hello World PHP-Anwendung mit einer angepassten Unattend-Datei implementieren
  - VMware ESXi v6.7 mit Lenovo Customization über eine statische IP-Adresse auf einer lokalen Festplatte implementieren

Sie können *angepasste* Makros erstellen, indem Sie eine Konfigurationseinstellungsdatei erstellen und die Unattend-Datei dann mit einer angepassten Konfigurationseinstellungsdatei verknüpfen. Wenn Sie die Datei mit den angepassten Konfigurationseinstellungen importieren, erstellt XClarity Administrator für jede Konfigurationseinstellung in der Datei ein Makro.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Makros zu einer Unattend-Datei hinzuzufügen.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Unattend-Dateien**.

Schritt 3. Wählen Sie die Unattend-Datei aus, die Sie bearbeiten möchten.

Schritt 4. Klicken Sie auf das **Bearbeiten**-Symbol (), um das Dialogfeld Unattend-Datei bearbeiten anzuzeigen.

Schritt 5. Fügen Sie die empfohlenen vordefinierten Makros hinzu, z. B.:

1. Positionieren Sie den Cursor in der Unattend-Datei irgendwo nach Zeile 1 (nach dem <xml>-Tag).
2. Erweitern Sie die Liste **predefine → unattendSettings** in der Liste der verfügbaren Makros.
3. Klicken Sie auf die Makros **preinstallConfig** und **postinstallConfig**, um die erforderlichen vordefinierten Makros zur Unattend-Datei hinzuzufügen.

   Der folgende Code wird der Datei hinzugefügt:

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Schritt 6. Fügen Sie weitere vordefinierte oder angepasste Makros hinzu, indem Sie den Cursor an der richtigen Stelle in der Unattend-Datei platzieren und dann auf das Makro aus der Liste klicken.

Schritt 7. Klicken Sie auf **Speichern**.

Unattend-Datei einer Konfigurationseinstellungsdatei zuordnen

Sie können einer Unattend-Datei Konfigurationseinstellungen zuordnen und anschließend die zugeordneten angepassten Makros zur Unattend-Datei hinzufügen.

Zu dieser Aufgabe

Sie können vordefinierte Makros zu einer Unattend-Datei hinzufügen, ohne eine angepasste Konfigurationseinstellungsdatei zuzuordnen.

Sie können keine Konfigurationseinstellungsdateien bearbeiten, die Unattend-Dateien zugeordnet sind. Sie können allerdings eine zugeordnete Datei kopieren und dann die Kopie bearbeiten.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Unattend-Datei mit einer Konfigurationseinstellungsdatei zu verknüpfen.

Schritt 1. Klicken Sie auf der Menüleiste von Lenovo XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Unattend-Dateien**.

Schritt 3. Wählen Sie die angepasste Unattend-Datei aus.

Schritt 4. Klicken Sie auf das Symbol **Konfigurationsdatei zuordnen** (), um das Dialogfeld „Unattend-Datei zuordnen“ anzuzeigen.

Schritt 5. Wählen Sie eine Konfigurationseinstellungsdatei aus, die der Unattend-Datei zugeordnet werden soll.

Schritt 6. Sie können vordefinierte und angepasste Makros zur Unattend-Datei hinzufügen. Platzieren Sie dazu den Cursor im Editor an der Position, an der Sie das Makro hinzufügen möchten, und wählen Sie das Makro aus der verfügbaren Liste aus (siehe Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei).

Sie können Makros mithilfe des eindeutigen Namens des Objekts zur Unattend-Datei hinzufügen. Bei Objekten mit verschachtelten Namen müssen Sie jedes Objekt mit einem Punkt trennen (z. B. `server_specific_settings.server.locale`). Beachten Sie, dass der oberste Namen nicht enthalten sein darf.

Schritt 7. Klicken Sie auf **Zuordnen**, um die Dateien zu verbinden.

Angepasste Installationsskripts importieren

Sie können Installationsskripts in das BS-Images-Repository importieren. Diese Dateien können dann zum Anpassen von Linux- und Windows-Images verwendet werden.

Zu dieser Aufgabe

Derzeit werden nur Nach-Installationsskripts unterstützt.

In der folgenden Tabelle sind die Dateitypen für die Installationsskripts aufgeführt, die Lenovo XClarity Administrator für jedes Betriebssystem unterstützt. Beachten Sie, dass bestimmte Betriebssystemversionen nicht alle Dateitypen unterstützen, die von XClarity Administrator unterstützt werden (z. B. einige RHEL-Versionen enthalten möglicherweise kein Perl im minimalen Profil, sodass Perl-Skripts nicht ausgeführt werden). Sie müssen sicherstellen, dass Sie den richtigen Dateityp für die Betriebssystemversionen verwenden, die Sie implementieren möchten.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
CentOS Linux	Nicht unterstützt	
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	
Microsoft Windows Hyper-V Server	Nicht unterstützt	
Microsoft® Windows® Server	Befehlsdatei (.cmd), PowerShell (.ps1)	Der Standardpfad für angepasste Daten und Dateien ist `C:\lxca`. Weitere Informationen zu Installationsskripts finden Sie unter Website zum Hinzufügen eines angepassten Skripts zu Windows Setup.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm oder .pl), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter RHEL: Website zu Nach-Installationsskripts.
Rocky Linux	Bash (.sh), Perl (.pm oder .pl), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter RHEL: Website zu Nach-Installationsskripts.
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm oder .pl), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter SUSE: Website zu benutzerdefinierten Skripts.
Ubuntu	Nicht unterstützt	
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Bash (.sh), Python (.py)	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`. Weitere Informationen zu Installationsskripts finden Sie unter VMware: Website zur Installation und Aktualisierung von Skripts.

Anmerkung: Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Nachdem die Daten während der BS-Implementierung gesammelt wurden, erstellt XClarity Administrator eine Instanz der Konfigurationseinstellungsdatei (die die angepassten Einstellungen in der ausgewählten Datei und eine Teilmenge der vordefinierten Einstellungen enthält) auf dem Hostsystem, das vom Nach-Installationsskript verwendet werden kann.

Sie können vordefinierte und angepasste Makros (Konfigurationseinstellungen) mit dem eindeutigen Namen des Objekts in das Nach-Installationsskript einfügen. Vordefinierte Werte sind basierend auf den XClarity Administrator-Instanzen dynamisch. Angepasste Makros sind basierend auf Benutzereingaben dynamisch, die während der BS-Implementierung festgelegt werden.

Anmerkungen:

- Umschließen Sie den Makronamen mit einem Rautensymbol (#).
- Trennen Sie bei verschachtelten Objekten jeden Objektnamen mit einem Punkt (z. B. **#server_settings. server0.locale#**).
- Bei angepassten Makros darf der oberste Objektname nicht enthalten sein. Stellen Sie dem Makronamen bei vordefinierten Makros das Präfix „predefined“ voran.
- Wenn ein Objekt von einer Vorlage erstellt wird, wird an den Namen eine eindeutige Nummer angehängt, beginnend mit 0 (z. B. **server0** und **server1**).
- Sie können den Namen für jedes Makro im Dialogfeld „BS-Images implementieren“ auf den Registerkarten „Angepasste Einstellungen“ anzeigen, indem Sie mit der Maustaste über das Hilfe-Symbol () neben jeder angepassten Einstellung bewegen.

- Eine Liste der vordefinierten Makros finden Sie unter Vordefinierte Makros. Informationen zu angepassten Konfigurationseinstellungen und Makros finden Sie unter Angepasste Makros.

Die empfohlenen vordefinierten Makros in der Unattend-Datei melden den Implementierungsstatus des finalen BS sowie den Status während des Herunterladens und Ausführens von Nach-Installationsskripts. Sie können das Nach-Installationsskript ändern, um je nach dem Zielbetriebssystem angepasste Statusmeldungen einzuschließen. Siehe Angepasste Statusmeldungen zu Installationsskripts hinzufügen für weitere Informationen.

Vorgehensweise

Gehen Sie wie folgt vor, um Installationsskripts in das BS-Images-Repository zu importieren.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Installationsskripts**.

Schritt 3. Klicken Sie auf das Symbol für **Datei importieren** ( ). Das Dialogfenster „Installationsskript importieren“ wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** ( ). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .

Schritt 5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.

Schritt 6. Wählen Sie den Betriebssystemtyp aus.

Schritt 7. Geben Sie den Dateinamen des Installationsskripts ein oder klicken Sie auf **Durchsuchen**, um die Datei zu finden, die Sie importieren möchten.

Schritt 8. **Optional**: Geben Sie eine Beschreibung für das Installationsskript ein.

Tipp: Verwenden Sie das Feld **Beschreibung**, um zwischen angepassten Dateien mit demselben Namen zu unterscheiden.

Schritt 9. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren

Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

Es werden drei Prüfsummentypen unterstützt:
- **MD5**
- **SHA1**
- **SHA256**

Schritt 10. Klicken Sie auf **Importieren**.

Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Die Installationsskripts sind auf der Seite BS-Images verwalten in der Registerkarte **Installationsskripts** aufgeführt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** ( ) klicken.
- Um ausgewählte Installationsskripts zu entfernen, klicken Sie auf das Symbol **Löschen** ( ).

Weitere Informationen zum Hinzufügen eines Installationsskripts zu einem angepassten BS-Image-Profil finden Sie unter Angepasstes BS-Image-Profil erstellen.

Angepasste Statusmeldungen zu Installationsskripts hinzufügen

Die empfohlenen vordefinierten Makros in der Unattend-Datei melden den Implementierungsstatus des finalen BS sowie den Status während des Herunterladens und Ausführens von Nach-Installationsskripts. Sie können zusätzliche Statusmeldungen zu Nacht-Installationsskripts hinzufügen.

Linux

Für Linux können Sie den folgenden `curl`-Befehl für die Statusmeldung hinzufügen.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Dabei kann <*status_ID*> einer der folgenden Werte sein.
- **44**. Workload-Implementierung war erfolgreich
- **45**. Workload-Implementierung wird mit Warnung ausgeführt
- **46**. Workload-Implementierung ist fehlgeschlagen
- **47**. Workload-Implementierungsnachricht
- **48**. Fehler bei angepasstem Nach-Installationsskript

Beachten Sie, dass der `curl`-Befehl vordefinierte Makros für die HTTPS-URL verwendet, die Lenovo XClarity Administrator für Statusmeldungen (**predefined.otherSettings.statusSettings.urlStatus**) und für den Ordner verwendet, der die Zertifikate enthält, die erforderlich sind, um vom Host-BS beim ersten Booten auf

den Webdienst urlStatus (**predefined.otherSettings.statusSettings.certLocation**) zugreifen zu können. Im folgenden Beispiel wird gemeldet, dass im Nach-Installationsskript ein Fehler aufgetreten ist.

Im folgenden Beispiel wird gemeldet, dass im Nach-Installationsskript ein Fehler aufgetreten ist.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

Bei Windows können Sie das `LXCA.psm1`-Skript importieren und anschließend die folgenden Befehle zur Statusmeldung ausführen.

- **initializeRestClient**

  Initialisiert den REST-Client. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen. Dieser Befehl ist vor dem Ausführen der Meldungsbefehle erforderlich.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  Stellt sicher, dass sich XClarity Administrator mit dem Hostserver verbinden kann. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen. Dieser Befehl ist optional, wird aber beim Installationsskript vor dem Ausführen der Meldungsbefehle empfohlen.

  ```
  testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

  Gibt eine Meldung über den erfolgreichen Abschluss aus, die im Jobprotokoll von XClarity Administrator gespeichert wird. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen.

  Tipp: Wenn das Makro **#predefined.unattendSettings.reportWorkloadNotComplete#** in einer angepassten Unatted-Datei oder einem Nach-Installationsskript enthalten ist, fügen Sie den Befehl **reportWorkloadDeploymentSucceeded** zum Nach-Installationsskript hinzu, um einen erfolgreichen Abschluss zu melden. Andernfalls meldet XClarity Administrator automatisch einen Abgeschlossen-Status, nachdem alle Nach-Installationsskripts ausgeführt wurden.

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  Gibt eine Warnmeldung aus, die im Jobprotokoll von XClarity Administrator gespeichert wird. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Gibt eine Fehlermeldung aus, die im Jobprotokoll von XClarity Administrator gespeichert wird. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  Gibt eine Fehlermeldung für das Nach-Installationsskript aus, die im Jobprotokoll von XClarity Administrator gespeichert wird. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Gibt eine allgemeine Meldung aus, die im Jobprotokoll von XClarity Administrator gespeichert wird, ohne den Status der Implementierung zu beeinflussen. Verwenden Sie die folgende Syntax, um diesen Befehl auszuführen.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Dabei ist <*message_text*> die Nachricht, die an XClarity Administrator für jede Statusbedingung zurückgegeben werden soll.

Beachten Sie, dass diese Befehle vordefinierte Makros für die IP-Adresse der XClarity Administrator-Instanz (**#predefined.otherSettings.lxcaIp#**) und für die UUID des Hostservers verwenden, auf dem das Betriebssystem implementiert werden soll (**# predefined.hostPlatforms.uuid#**).

Im folgenden Beispiel wird ein PowerShell-Installationsskript gezeigt, das Java installiert und bei Fehlschlagen der Installation einen Fehler meldet

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Angepasste Software importieren

Sie können Software in das BS-Images-Repository importieren. Diese Dateien können dann zum Anpassen von Linux- und Windows-Images verwendet werden.

Zu dieser Aufgabe

Die angepassten Softwaredateien werden installiert, nachdem die Betriebssystemimplementierung und die Nach-Installationsskripts abgeschlossen sind.

Die folgenden Dateitypen werden für angepasste Software unterstützt.

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
CentOS Linux	Nicht unterstützt	
Microsoft® Windows® Azure Stack HCI	Nicht unterstützt	

Betriebssystem	Unterstützte Dateitypen	Weitere Informationen
Microsoft Windows Hyper-V Server	Nicht unterstützt	
Microsoft Windows® Server	Eine .zip-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
Rocky Linux	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
Ubuntu	Nicht unterstützt	
VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization	Eine .tar.gz-Datei mit den Software-Nutzdaten.	Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.

Anmerkung: Das BS-Images-Repository kann eine unbegrenzte Anzahl von vordefinierten und angepassten Dateien speichern, wenn ausreichend Speicherplatz für die Dateien verfügbar ist.

Vorgehensweise

Gehen Sie wie folgt vor, um Software in das BS-Images-Repository zu importieren.

Schritt 1. Klicken Sie auf der Menüleiste von Lenovo XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Software**.

Schritt 3. Klicken Sie auf das Symbol für **Datei importieren** ( ). Das Dialogfenster „Installationsskript importieren“ wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Lokaler Import**, um Dateien vom lokalen System hochzuladen, oder klicken Sie auf die Registerkarte **Remote-Import**, um Dateien von einem Remote-Dateiserver hochzuladen.

Anmerkung: Um eine Datei von einem Remote-Dateiserver hochzuladen, müssen Sie zuerst ein Remote-Dateiserverprofil erstellen. Klicken Sie dazu auf das Symbol für **Dateiserver konfigurieren** ( ). Weitere Informationen finden Sie unter Remote-Dateiserver konfigurieren .

Schritt 5. Wenn Sie einen Remote-Dateiserver verwenden, wählen Sie den gewünschten Server aus der Liste **Remote-Dateiserver** aus.

Schritt 6. Wählen Sie den Betriebssystemtyp aus.

Schritt 7. Geben Sie den Dateinamen der Softwaredatei ein oder klicken Sie auf **Durchsuchen**, um die Datei zu finden, die Sie importieren möchten.

Schritt 8. **Optional**: Geben Sie eine Beschreibung für die Softwaredatei ein.

Tipp: Verwenden Sie das Feld **Beschreibung**, um zwischen angepassten Dateien mit demselben Namen zu unterscheiden.

Schritt 9. **Optional:** Wählen Sie einen Prüfsummentyp aus, um zu überprüfen, dass die hochgeladene Datei nicht fehlerhaft ist. Kopieren Sie dann den Prüfsummenwert und fügen Sie ihn in das entsprechende Textfeld ein.

Beim Auswählen eines Prüfsummentyps müssen Sie einen Prüfsummenwert angeben, damit die hochgeladene Datei auf Integrität und Sicherheit geprüft wird. Der Wert muss aus einer sicheren Quelle einer vertrauenswürdigen Organisation stammen. Wenn die hochgeladene Datei mit dem Prüfsummenwert übereinstimmt, können Sie ohne Sicherheitsbedenken mit der Bereitstellung fortfahren. Andernfalls müssen Sie die Datei erneut hochladen oder den Prüfsummenwert überprüfen.

Es werden drei Prüfsummentypen unterstützt:
- **MD5**
- **SHA1**
- **SHA256**

Schritt 10. Klicken Sie auf **Importieren**.

Tipp: Die Datei wird über eine sichere Netzwerkverbindung hochgeladen. Daher beeinflussen die Zuverlässigkeit und Leistung des Netzwerks, wie lange das Importieren der Datei dauert.

Wenn Sie die Webbrowser-Registerkarte oder das Fenster, über das die Datei hochgeladen wird, vor dem Abschluss des lokalen Hochladevorgangs schließen, schlägt der Import fehl.

Nach dieser Aufgabe

Die Installationsskripts sind auf der Seite BS-Images verwalten in der Registerkarte **Software** aufgeführt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie ein Remote-Dateiserverprofil, indem Sie auf das Symbol **Dateiserver konfigurieren** () klicken.
- Um ausgewählte Softwaredateien zu entfernen, klicken Sie auf das Symbol **Löschen** ().

Weitere Informationen zum Hinzufügen einer Softwaredatei zu einem angepassten BS-Image-Profil finden Sie unter Angepasstes BS-Image-Profil erstellen.

Angepasstes BS-Image-Profil erstellen

Sie können angepasste Einheitentreiber, Boot-Dateien (nur Windows), Konfigurationseinstellungen, Unattend-Dateien, Installationsskripts und Software zu einem vordefinierten BS-Image-Profil hinzufügen, das im BS-Images-Repository vorhanden ist. Wenn Sie einem BS-Image Dateien hinzufügen, erstellt Lenovo XClarity Administrator ein angepasstes Profil für dieses BS-Image. Das angepasste Profil enthält die angepassten Dateien und Installationsoptionen.

Vorbereitende Schritte

Die angepassten Dateien, die Sie hinzufügen möchten, müssen im BS-Image-Repository vorhanden sein (siehe Boot-Dateien importieren, Einheitentreiber importieren, Angepasste Konfigurationseinstellungen

importieren, Angepasste Unattend-Dateien importieren, Angepasste Installationsskripts importieren und Angepasste Software importieren).

Vorgehensweise

Gehen Sie wie folgt vor, um ein BS-Image anzupassen:

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **BS-Images**.

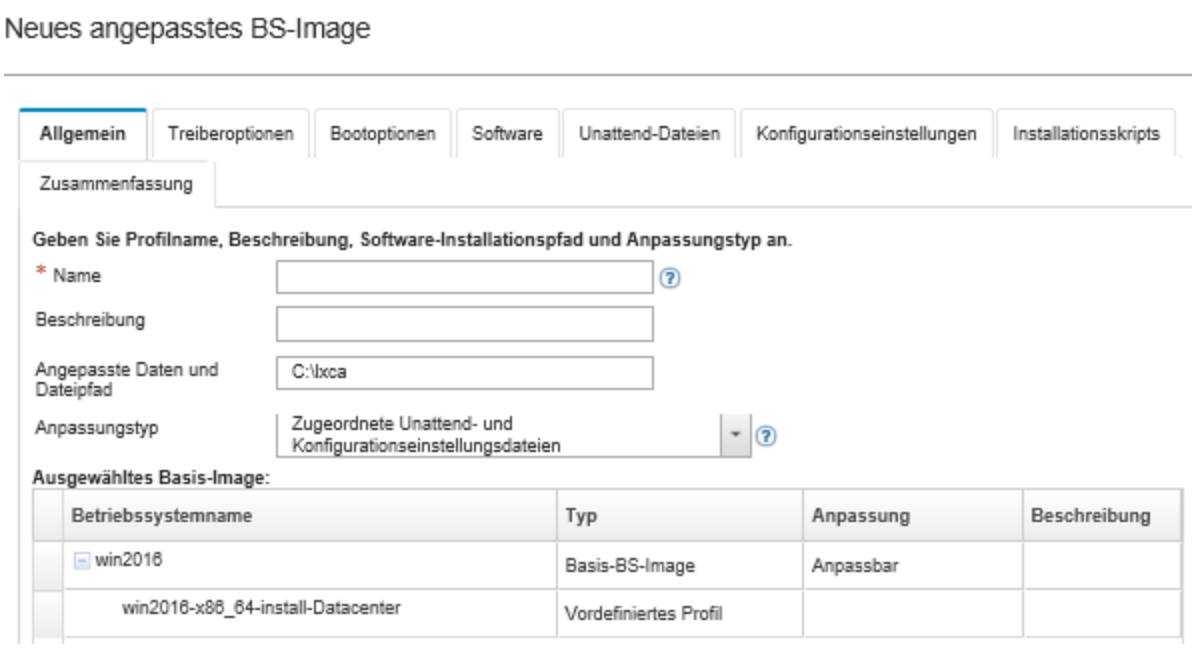
Schritt 3. Wählen Sie das vordefinierte BS-Image-Profil aus, das angepasst werden soll.

In der Spalte **Anpassung** wird angegeben, welche Betriebssystem-Images angepasst werden können. Klicken Sie auf das Symbol für **Hilfe** ( ), um weitere Informationen zum Anpassen eines bestimmten Betriebssystem-Image anzuzeigen.

- **Anpassbar**. Das Betriebssystem-Image kann angepasst werden, wurde jedoch noch nicht angepasst.
- **Nicht anpassbar**. Dieses Betriebssystem-Image kann nicht angepasst werden.

Anmerkung: Sie können weitere Basis-BS-Images (im ISO-Format) von einem lokalen oder einem fernen System importieren, indem Sie auf das Symbol für **Datei importieren** ( ) klicken.

Schritt 4. Klicken Sie auf das Symbol für **Angepasstes Profil erstellen** ( ). Das Dialogfenster „Neues angepasstes BS-Image“ wird angezeigt.



Schritt 5. Geben Sie auf der Registerkarte **Allgemein** einen Namen, eine Beschreibung, einen Pfad für die angepassten Dateien und Implementierungsdaten auf dem Implementierungshost und einen Anpassungstyp für das neue angepasste BS-Image-Profil ein.

Der Anpassungstyp kann einer der folgenden Werte sein:

- **Nur Unattend-Dateien**
- **Nur Konfigurationsdateien**
- **Nicht zugeordnete Unattend- und Konfigurationsdateien**
- **Zugeordnete Unattend- und Konfigurationsdateien**

- **Keine Angabe**

Schritt 6. Klicken Sie auf **Weiter**.

Schritt 7. Wählen Sie in der Registerkarte **Einheitentreiber** den Einheitentreiber aus, der dem Linux-BS-Image-Profil hinzugefügt werden soll.

Eine Liste der unterstützten Formate finden Sie unter Einheitentreiber importieren.

Die ausgewählte Datei wird nach Abschluss des Konfigurationsassistenten angewendet.

Anmerkung: Sie können weitere Einheitentreiber von einem lokalen oder einem fernen System importieren, indem Sie auf das Symbol für **Datei importieren** () klicken.

Schritt 8. Klicken Sie auf **Weiter**.

Schritt 9. (Nur Windows) Wählen Sie in der Registerkarte **Bootoptionen** die Boot-Dateien aus, die dem Windows-BS-Image-Profil hinzugefügt werden sollen.

Eine Liste der unterstützten Formate finden Sie unter Boot-Dateien importieren.

Die ausgewählte Datei wird nach Abschluss des Konfigurationsassistenten angewendet.

Schritt 10. Klicken Sie auf **Weiter**.

Schritt 11. Wählen Sie in der Registerkarte **Konfigurationseinstellungen** (falls zutreffend) eine oder mehrere angepasste Konfigurationsdateien aus, die dem BS-Image-Profil hinzugefügt werden sollen. Sie können maximal eine Datei auswählen.

Schritt 12. Klicken Sie auf **Weiter**.

Schritt 13. In der Registerkarte **Unattend-Dateien**:

a. Wählen Sie die Unattend-Datei aus, die Sie zum BS-Image-Profil hinzufügen möchten.

   Eine Liste der unterstützten Formate finden Sie unter Angepasste Unattend-Dateien importieren.

   Die ausgewählte Datei wird nach Abschluss des Konfigurationsassistenten angewendet.

b. Wählen Sie in der Spalte **Zugeordnete Konfigurationsdatei** eine Konfigurationsdatei aus, die der Unattend-Datei zugeordnet werden soll.

c. Optional können Sie angepasste Makros auswählen, die in der ausgewählten Konfigurationsdatei verfügbar sind, oder angepasste Makros im XML-Format hinzufügen.

Schritt 14. Klicken Sie auf **Weiter**.

Schritt 15. Wählen Sie in der Registerkarte **Installationsskripts** (falls zutreffend) die Installationsskripts aus, die dem Windows-BS-Image-Profil hinzugefügt werden sollen. Sie können maximal ein Nach-Installationsskript auswählen.

Eine Liste der unterstützten Formate finden Sie unter Angepasste Installationsskripts importieren.

Die ausgewählte Datei wird nach Abschluss des Konfigurationsassistenten angewendet.

Anmerkung: Sie können weitere Installationsskripts von einem lokalen oder einem fernen System importieren, indem Sie auf das Symbol **Datei importieren** () klicken.

Schritt 16. Klicken Sie auf **Weiter**.

Schritt 17. Wählen Sie in der Registerkarte **Software** die Software aus, die dem Linux-BS-Image-Profil hinzugefügt werden soll.

Eine Liste der unterstützten Formate finden Sie unter Angepasste Software importieren.

Die ausgewählte Datei wird nach Abschluss des Konfigurationsassistenten angewendet.

Anmerkung: Sie können weitere Software von einem lokalen oder einem fernen System importieren, indem Sie auf das Symbol **Datei importieren** () klicken.

Schritt 18. Klicken Sie auf **Weiter**.

Schritt 19. Überprüfen Sie die Einstellungen auf der Registerkarte **Zusammenfassung** und klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Nach dieser Aufgabe

Das angepasste BS-Image-Profil wird unter dem Basisbetriebssystem auf der Registerkarte **BS-Images** auf der Seite „BS-Images verwalten“ aufgeführt.

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Klicken Sie auf **Profil importieren/exportieren → Angepasstes Profil-Image exportieren**, um ein angepasstes BS-Image-Profil zu importieren und auf ein Basis-BS-Image anzuwenden (siehe Angepasstes BS-Image-Profil importieren).
- Klicken Sie auf **Profil importieren/exportieren → Angepasstes Profil-Image exportieren**, um ein ausgewähltes angepasstes BS-Image-Profil zu exportieren.
- Zum Ändern des ausgewählten angepassten BS-Image-Profils klicken Sie auf das Symbol für **Bearbeiten** ().
- Um ein ausgewähltes angepasstes BS-Image-Profil zu entfernen, klicken Sie auf das Symbol für **Löschen** ().

Globale BS-Implementierungseinstellungen konfigurieren

Globale Einstellungen dienen beim Bereitstellen von Betriebssystemen als Standardeinstellungen.

Zu dieser Aufgabe

Über die Seite „Globale Einstellungen“ können Sie die folgenden Einstellungen konfigurieren:

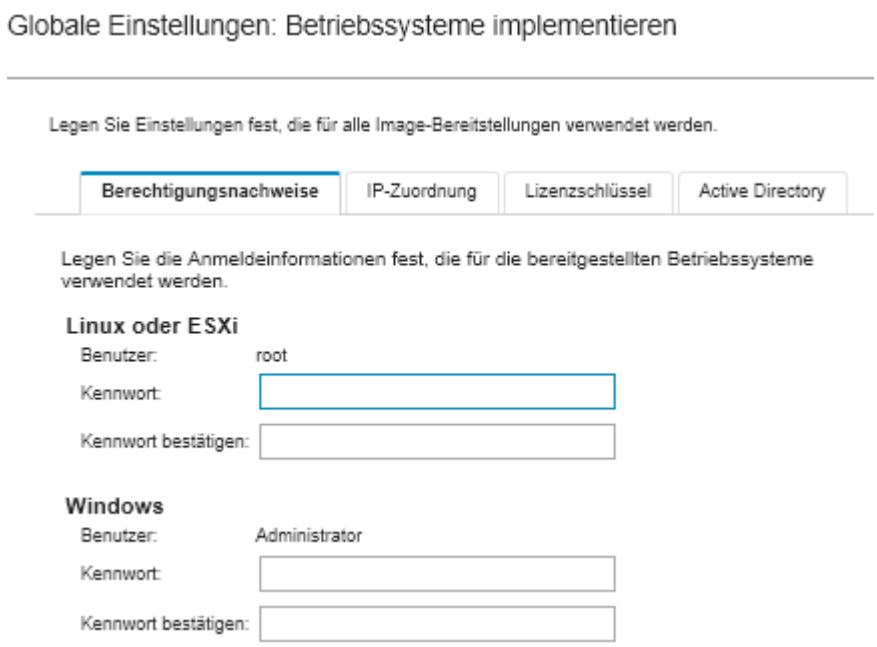
- Das Kennwort für den Administratorbenutzeraccount, der für die Bereitstellung der Betriebssysteme verwendet wird.
- Die Methode für die Zuweisung von IP-Adressen zu den Servern.
- Zur Aktivierung der installierten Betriebssysteme verwendete Lizenzschlüssel.
- Im Rahmen der Windows-Betriebssystembereitstellung können Sie optional einer Active Directory-Domäne beitreten.

Vorgehensweise

So konfigurieren Sie die globalen Einstellungen, die für alle Server verwendet werden:

Schritt 1. Klicken Sie auf der Menüleiste von Lenovo XClarity Administrator auf **Bereitstellung → BS-Images bereitstellen**, um die Seite BS-Images bereitstellen anzuzeigen.

Schritt 2. Klicken Sie auf das Symbol **Globale Einstellungen** (), um das Dialogfeld Globale Einstellungen: Betriebssysteme implementieren anzuzeigen.



Schritt 3. Geben Sie auf der Registerkarte **Anmeldeinformationen** das Kennwort ein, das für die Anmeldung des Administratoraccounts am Betriebssystem verwendet werden soll.

Schritt 4. Wählen Sie auf der Seite **IP-Zuweisung** die folgenden Optionen aus.

a. **Optional:** Wählen Sie **VLANs verwenden** aus, um VLAN-Einstellungen im Netzwerkeinstellungsdialogfeld konfigurieren zu können (siehe Netzwerkeinstellungen für verwaltete Server konfigurieren).

Anmerkungen: Anmerkungen:

- Bei Linux-Betriebssystemimplementierungen wird VLAN-Tagging nicht unterstützt.
- Bei Betriebssystemimplementierungen auf ThinkServer Einheiten wird VLAN-Tagging nicht unterstützt.
- Der VLAN-Modus wird nur für Server unterstützt, die MAC-Adressen in ihrem Bestand haben. Wenn für einen Server nur die MAC-Adresse AUTO verfügbar ist, können keine VLANs zur Bereitstellung von Betriebssystemen auf dem Server verwendet werden.

b. Wählen Sie die Methode für die Zuweisung von IP-Adressen bei der Konfiguration des bereitgestellten Betriebssystems aus:

Anmerkung: Die XClarity Administrator Netzwerkschnittstelle, die für die Verwaltung verwendet wird, muss über dieselbe IP-Adressmethode, die Sie im Dialogfeld „Globale Einstellungen: Betriebssysteme implementieren“ ausgewählt haben, mit dem Baseboard Management Controller verbunden sein. Wenn XClarity Administrator beispielsweise die Konfiguration so eingerichtet ist, dass sie eth0 für die Verwaltung verwendet, und Sie bei der Konfiguration des implementierten Betriebssystems statisch zugewiesene statische IPv6-Adressen verwenden, muss eth0 mit einer IPv6-Adresse konfiguriert werden, die über eine Verbindung zum Baseboard Management Controller verfügt.

- **Statische IPv4-Adresse manuell zuweisen**. Wenn Sie eine statische IPv4-Adresse zuweisen, sorgen Sie dafür, dass die statische IPv4-Adresse, die Gateway-Adresse und die Subnetzmaske vor der Bereitstellung des Betriebssystems konfiguriert werden (siehe Netzwerkeinstellungen für verwaltete Server konfigurieren).
- **Verwenden von DHCP (Dynamic Host Configuration Protocol) zur Zuweisung der Adressen** Wenn Sie bereits in Ihrem Netzwerk über eine DHCPv4-Infrastruktur verfügen, können Sie diese Infrastruktur zum Zuweisen von IP-Adressen verwenden.

Anmerkung: DHCP IPv6 wird für die Betriebssystembereitstellung nicht unterstützt.

- **Statische IPv6-Adresse manuell zuweisen**. Wenn Sie eine statische IPv6-Adressen zuweisen, sorgen Sie dafür, dass die statische IPv6-Adresse, die Gateway-Adresse und die Subnetzmaske vor der Bereitstellung des Betriebssystems konfiguriert werden (siehe Netzwerkeinstellungen für verwaltete Server konfigurieren).

Schritt 5. **Optional:** Legen Sie auf der Registerkarte **Lizenzschlüssel** Volumenlizenzschlüssel fest, die zur Aktivierung der installierte Windows-Betriebssysteme verwendet werden.

Wenn Sie auf dieser Registerkarte globale Volumenlizenzschlüssel festlegen, können Sie die Lizenzschlüssel für jedes Windows-Betriebssystembereitstellungsprofil auf der Seite BS-Images bereitstellen auswählen.

Tipp: XClarity Administrator unterstützt globale Volumenlizenzschlüssel für Windows-Installationen und individuelle Einzelhandelslizenzschlüssel für Windows und VMware ESXi. Sie können einzelne Einzelhandelslizenzschlüssel im Rahmen der Bereitstellung angeben (siehe Ein Betriebssystem-Image implementieren).

Schritt 6. **Optional:** Konfigurieren Sie auf der Registerkarte **Active Directory** die Active Directory-Einstellungen für die Windows-Betriebssystembereitstellungen. Weitere Informationen zur Integration mit Active Directory finden Sie unter In Windows Active Directory integrieren.

Schritt 7. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Netzwerkeinstellungen für verwaltete Server konfigurieren

Netzwerkeinstellungen sind Konfigurationsoptionen, die für jeden Server eindeutig sind. Sie müssen die Netzwerkeinstellungen für einen verwalteten Server konfigurieren, bevor Sie ein Betriebssystem auf diesem Server bereitstellen können.

Zu dieser Aufgabe

Wenn Sie DHCP zum dynamischen Zuweisen von IP-Adressen verwenden, müssen Sie die MAC-Adresse konfigurieren.

Wenn Sie statische IP-Adressen verwenden, müssen Sie die folgenden Netzwerkeinstellungen für einen Server konfigurieren, bevor Sie ein Betriebssystem auf diesem Server bereitstellen können. Nachdem diese Einstellungen konfiguriert sind, ändert sich der Bereitstellungsstatus zu „Bereit“. (Beachten Sie, dass einige Felder nicht für statische IPv6-Adressen verfügbar sind.)

- Hostname

  Der Hostname muss mit den folgenden Richtlinien übereinstimmen:
  - Die Hostnamen der einzelnen verwalteten Server müssen eindeutig sein.
  - Der Hostname darf Zeichenfolgen (Beschriftungen) enthalten, die durch einen Punkt (.) getrennt sind.
  - Eine Beschriftung kann ASCII-Zeichen, Ziffern und Bindestriche (-) enthalten. Die Zeichenfolge darf aber nicht mit einem Bindestrich beginnen oder enden und nicht nur Ziffern enthalten.
  - Die erste Beschriftung kann 2 bis 15 Zeichen lang sein. Nachfolgende Beschriftungen können 2 bis 63 Zeichen lang sein.
  - Die Gesamtlänge des Hostnamens darf 255 Zeichen nicht überschreiten.
- Die MAC-Adresse des Anschlusses auf dem Host, über den das Betriebssystem installiert wird.

  Die MAC-Adresse ist standardmäßig auf AUTO festgelegt. Diese Einstellung 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 XClarity Administrator-Host automatisch neu gestartet, um die erkannte MAC-Adresse für die Bereitstellung zu verwenden..

Sie finden den Status des Ports für die MAC-Adresse, der für die BS-Implementierung verwendet wird, im Dropdown-Menü **MAC-Adresse** im Dialogfenster Netzwerkeinstellungen. Wenn mehrere Ports aktiviert sind oder alle Ports ausgefallen sind, wird standardmäßig AUTO verwendet.

Anmerkungen:

- Virtuelle Netzwerkanschlüsse werden nicht unterstützt. Verwenden Sie keinen physischen Netzwerkanschluss, um mehrere virtuelle Netzwerkanschlüsse zu simulieren.
- Wenn die Netzwerkeinstellung des Servers auf „AUTO“ festgelegt ist, kann XClarity Administrator die Netzwerkanschlüsse in den Steckplätzen 1 – 16 automatisch erkennen. Mindestens ein Anschluss an den Steckplätzen 1 – 16 muss eine Verbindung zu XClarity Administrator haben.
- Wenn Sie für die MAC-Adresse einen Netzwerkanschluss in Steckplatz 17 oder höher verwenden möchten, können Sie das Programm „AUTO“ nicht verwenden. Stattdessen müssen Sie die Netzwerkeinstellung des Servers auf die MAC-Adresse des bestimmten Ports festlegen, den Sie verwenden möchten.
- Bei ThinkServer-Servern werden nicht alle MAC-Adressen des Hosts angezeigt. In den meisten Fällen werden MAC-Adressen für AnyFabric-Ethernet-Adapter im Dialogfeld Netzwerkeinstellungen ändern aufgelistet. MAC-Adressen für andere Ethernet-Adapter (z. B. Lan-On-Motherboard) werden nicht angezeigt. Wenn die MAC-Adresse für einen Adapter nicht verfügbar ist, verwenden Sie für die Nicht-VLAN-Bereitstellung die AUTO-Methode.

- IP-Adresse und Subnetzmaske
- IP-Gateway
- Bis zu zwei DNS-Server (Domain Name System)
- MTU-Geschwindigkeit
- VLAN-ID, wenn der VLAN-IP-Modus aktiviert ist

Wenn Sie VLAN verwenden, können Sie dem konfigurierten Hostnetzwerkadapter eine VLAN-ID zuordnen.

Vorgehensweise

So konfigurieren Sie Netzwerkeinstellungen für einen oder mehrere Server.

Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.

Schritt 2. Wählen Sie mindestens einen zu konfigurierenden Server aus. Sie können bis zu 28 Server auf einmal konfigurieren.

Schritt 3. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen**, um die Seite Netzwerkeinstellungen ändern anzuzeigen.

Schritt 4. Füllen Sie für jeden Server die Felder in der Tabelle aus.

Tipp: Alternativ zum Ausfüllen jeder Zeile können Sie bei einigen Feldern alle Zeilen in der Tabelle aktualisieren:

a. Klicken Sie auf **Alle Zeilen ändern → Hostname**, um die Hostnamen für alle Server über ein vordefiniertes oder angepasstes Benennungsschema festzulegen.

b. Klicken Sie auf **Alle Zeilen ändern → IP-Adresse**, um einen IP-Adressbereich, die Subnetzmaske und das Gateway zuzuweisen. Die IP-Adressen werden, beginnend mit der ersten angezeigten IP-Adresse und endend mit der letzten angezeigten IP-Adresse, für jeden Server zugewiesen. Die Subnetzmaske und die IP-Adresse des Gateways werden für jeden Server übernommen.

c. Klicken Sie auf **Alle Zeilen ändern → Domain Name System (DNS)**, um die vom Betriebssystem verwendeten DNS-Server festzulegen. Wenn das Netzwerk automatisch DNS-Server definiert oder Sie keine DNS-Server definieren möchten, wählen Sie **Keine**.

d. Klicken Sie auf **Alle Zeilen ändern → Maximum Transmission Unit (MTU)**, um die MTU für die konfigurierten Ethernet-Adapter der bereitgestellten Betriebssysteme festzulegen.

e. Klicken Sie auf **Alle Zeilen ändern → VLAN-ID**, um eine bestimmte VLAN-ID für das Betriebssystem-VLAN-Tagging festzulegen.

   Sie können einen Wert zwischen 1 und 4095 angeben. Der Standardwert ist 1; der VLAN-Modus wird also nicht verwendet.

   Diese Option ist nur verfügbar, wenn im Dialogfeld Globale Einstellungen „VLAN verwenden“ aktiviert ist (siehe Globale BS-Implementierungseinstellungen konfigurieren).

   Wichtig:

   - Geben Sie nur dann eine VLAN-ID an, wenn ein VLAN-Tag für die Funktion im Netzwerk erforderlich ist. **VLAN verwenden** kann sich auf das Netzwerkrouting zwischen dem Hostbetriebssystem und XClarity Administrator auswirken.
   - Gehäuse- oder Top-of-Rack-Switches müssen unabhängig voneinander konfiguriert werden, um Pakete mit VLAN-Tagging verarbeiten zu können. Stellen Sie sicher, dass XClarity Administrator und das Datennetzwerk für die korrekte Verarbeitung dieser Pakete konfiguriert sind.
   - Der VLAN-Modus wird nur für Server unterstützt, die MAC-Adressen in ihrem Bestand haben. Wenn für einen Server nur die MAC-Adresse AUTO verfügbar ist, können keine VLANs zur Bereitstellung von Betriebssystemen auf dem Server verwendet werden.
   - VLAN-Tagging wird für die Bereitstellung von Linux-Betriebssystemen nicht unterstützt. Wenn Sie jedoch auf einigen Servern mit VLAN und gleichzeitig auf anderen Servern ohne VLAN eine Bereitstellung durchführen möchten, können Sie sie im VLAN-Modus erzwingen, indem Sie die VLAN-ID auf 1 setzen.

Schritt 5. Klicken Sie auf **OK**, um die Einstellungen zu speichern. Die Einstellungen werden gespeichert. Sie sind nur im lokalen Speicher-Cache des Webbrowsers persistent.

Ergebnisse

Jeder konfigurierte Server wird nun auf der Seite Betriebssystem implementieren: BS-Images implementieren mit dem Bereitstellungsstatus **Bereit** angezeigt.

Speicherposition für verwaltete Server auswählen

Wählen Sie für einen oder mehrere Server die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

Vorbereitende Schritte

Lesen Sie sich die Überlegungen zu Speicher- und Boot-Optionen durch, bevor Sie eine Speicherposition auswählen (siehe Hinweise zur Betriebssystembereitstellung).

Sie können ein Betriebssystem auf den folgenden Arten von Speicher implementieren:

- **Lokales Festplattenlaufwerk**

  Nur mit einem RAID-Controller oder einem SAS/SATA-HBA verbundene Datenträger werden unterstützt.

Lenovo XClarity Administrator installiert das Betriebssystem-Image auf der zuerst aufgelisteten lokalen RAID-Festplatte auf dem verwalteten Server.

Wenn die RAID-Konfiguration auf dem Server nicht ordnungsgemäß konfiguriert wurde oder inaktiv ist, kann Lenovo XClarity Administrator die lokale Festplatte möglicherweise nicht erkennen. Um das Problem zu beheben, aktivieren Sie die RAID-Konfiguration mithilfe von Konfigurationsmustern (siehe Lokalen Speicher definieren) oder über die RAID-Verwaltungssoftware auf dem Server.

Anmerkungen:

- Falls auch ein M.2-Laufwerk vorhanden ist, muss das lokale Festplattenlaufwerke für die Hardware-RAID konfiguriert werden.
- Wenn ein SATA-Adapter aktiviert ist, darf der SATA-Modus *nicht* auf „IDE“ festgelegt sein.
- Auf ThinkServer-Servern können Betriebssysteme nur auf der lokalen Festplatte implementiert werden. SAN-Speicher und integrierte Hypervisoren werden nicht unterstützt.
- Bei ThinkServer-Servern ist die Konfiguration nur über die RAID-Verwaltungssoftware auf dem Server verfügbar.

Ein Beispielszenario für das Implementieren von VMware ESXi 5.5 auf einem lokal installierten Plattenlaufwerk finden Sie unter ESXi auf einem lokalen Festplattenlaufwerk implementieren.

- **(Nur ESXi) Integrierter Hypervisor (USB oder SD-Medienadapter)**

  Diese Position ist nur anwendbar, wenn ein VMware ESXi-Image auf verwalteten Servern implementiert wird.

  Beim integrierten Hypervisor kann es sich um eine der folgenden Einheiten handeln:

  - IBM Lizenz-USB-Stick (PN 41Y8298) oder Lenovo Lizenz-USB-Stick, der an einen bestimmten Anschluss an einem der folgenden Server angehängt ist:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - Auf den folgenden Servern installierter SD-Medienadapter:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    Außerdem muss das Laufwerk wie folgt konfiguriert werden:
    - Die entsprechenden Laufwerke auf dem Medienadapter müssen definiert werden.
    - Der Modus des SD-Medienadapters muss auf **Betrieb** festgelegt werden.
    - Als Eigentümer muss „System“ oder „Nur System“ festgelegt werden.
    - Es muss Schreib-/Lesezugriff festgelegt werden.
    - Dem Laufwerk muss die LUN-Nummer 0 zugeordnet werden.

    Wichtig: Wenn der SD-Medienadapter nicht ordnungsgemäß konfiguriert ist, kann Lenovo XClarity Administrator die Betriebssystembereitstellung auf dem SD-Medienadapter nicht erfolgreich abschließen.

    Sie können den Modus des SD-Medienadapters in **Konfiguration** ändern und den Medienadapter über die Befehlszeilenschnittstelle des Management-Controllers mithilfe des Befehls `sdraid` konfigurieren. Weitere Informationen zum Festlegen des Modus für den SD-Medienadapter und zum Konfigurieren

des Adapters über die Befehlszeilenschnittstelle finden Sie unter Onlinedokumentation für Integrated Management Module II.

Wenn auf dem verwalteten Server zwei Hypervisor-Schlüssel installiert sind, wählt das VMware-Installationsprogramm den zuerst aufgelisteten Schlüssel für die Implementierung aus.

Anmerkung: Der Versuch, Microsoft Windows auf einem verwalteten Server zu implementieren, auf dem ein Hypervisor-Schlüssel installiert ist, kann zu Problemen führen, selbst wenn Sie nicht den integrierten Hypervisor-Schlüssel auswählen. Im Fall von Windows-Implementierungsfehlern entfernen Sie den integrierten Hypervisor-Schlüssel vom verwalteten Server. Versuchen Sie dann, Microsoft Windows erneut auf diesem Server zu implementieren.

- **M.2-Laufwerk**

  Lenovo XClarity Administrator installiert das Betriebssystem-Image auf dem ersten M.2-Laufwerk, das auf dem verwalteten Server konfiguriert ist.

  Der M.2-Speicher wird nur auf ThinkSystem-Servern unterstützt.

  Achtung: Wenn eine verwaltete Einheit sowohl nicht für Hardware-RAID konfigurierte lokale Laufwerke (SATA, SAS oder SSD) als auch M.2-Laufwerke besitzt, müssen Sie für die Verwendung von M.2-Laufwerken die lokalen Laufwerke deaktivieren, oder Sie müssen die M.2-Laufwerke deaktivieren, wenn Sie lokale Laufwerke verwenden möchten. Sie können interne Speichercontrollereinheiten und Legacy- sowie UEFI-ROM-Speicheroptionen mithilfe der Konfigurationsmuster deaktivieren, indem Sie „Lokale Festplatte deaktivieren“ auf der Registerkarte „Lokaler Speicher“ des Assistenten auswählen, oder ein Konfigurationsmuster aus einem vorhandenen Server erstellen und anschließend die M.2-Einheiten im erweiterten UEFI-Muster deaktivieren.

- **SAN-Speicher**

  Lenovo XClarity Administrator installiert das Betriebssystem-Image auf dem SAN-Bootziel, das auf dem verwalteten Server konfiguriert ist.

  Die folgenden Protokolle werden unterstützt.
  - Fibre Channel
  - Fibre Channel over Ethernet
  - SAN iSCSI (nur mit Emulex VFA5.2 2x10 GbE SFP+ Adapter und FCoE/iSCSI SW oder Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter und FCoE/iSCSI SW Adaptern)

  Auf verwalteten Rack-Servern können Sie nur Windows oder RHEL im SAN-Speicher implementieren. Stellen Sie sicher, dass das SAN-Bootziel auf den verwalteten Servern konfiguriert ist. Sie können auch das FC SAN-Bootziel über ein Servermuster konfigurieren (siehe Bootoptionen definieren).

  Implementierung von VMware ESXi:

  - Lokale Festplatten müssen deaktiviert oder vom Server entfernt werden. Sie können die lokalen Festplatten über Servermuster deaktivieren (siehe Lokalen Speicher definieren).
  - Wenn mehrere SAN-Datenträger verfügbar sind, wird nur der erste Datenträger für die Implementierung verwendet.

  Stellen Sie sicher, dass der Betriebssystem-Datenträger, auf dem Sie die Installation ausführen, der einzige Datenträger ist, der dem Betriebssystem angezeigt wird.

  Ein Beispielszenario für das Implementieren von VMware ESXi 5.5 auf SAN-Datenträgern, die mit Servern verbunden sind, finden Sie unter ESXi auf SAN-Speicher implementieren.

Anmerkung: 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. Weitere Informationen finden Sie unter BS-Installationsprogramm kann das Laufwerk für die Installation von XClarity Administrator nicht finden in der XClarity Administrator Onlinedokumentation.

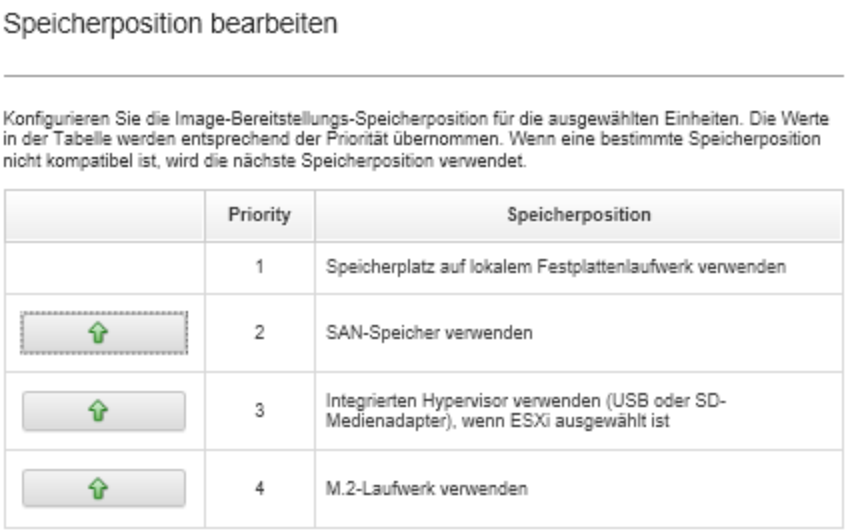
Vorgehensweise

Gehen Sie wie folgt vor, um eine Speicherposition für mindestens einen verwalteten Server auszuwählen.

Schritt 1. Klicken Sie auf der Menüleiste von Lenovo XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite „BS-Images implementieren“ anzuzeigen.

Schritt 2. Wählen Sie die Server aus, für die Sie die Speichereinstellungen ändern möchten.

Schritt 3. Klicken Sie auf **Ausgewählte ändern → Speicherposition**, um die Prioritätenfolge der Speicherpositionen für alle ausgewählten Server zu ändern. Wenn die erste Speicherposition nicht kompatibel ist, wird versucht, die nächste Speicherposition zu verwenden.



Sie können die Priorität für die folgenden Speicherpositionen festlegen:
- **Speicherplatz auf lokalem Festplattenlaufwerk verwenden**
- **Integrierten Hypervisor (USB oder SD-Medienadapter) verwenden, wenn ESXi ausgewählt ist**
- **M.2-Laufwerk verwenden**
- **SAN-Speicher verwenden**

Schritt 4. Wählen Sie für jeden Server in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll. Sie können unter den folgenden Werten auswählen (die den Werten im vorherigen Schritt entsprechen).
- **Lokale Festplatte**
- **Embedded Hypervisor**
- **M.2-Laufwerk**
- **SAN-Speicher**

Wenn Sie **SAN-Speicher**, wird ein Dialogfenster angezeigt, in dem Sie den SAN-Datenträger konfigurieren können. Stellen Sie sicher, dass der Ziel-SAN-Datenträger während der Bereitstellung erreichbar ist.

Wenn die ausgewählte Speicherposition nicht mit dem Server kompatibel ist, versucht Lenovo XClarity Administrator, das Betriebssystem in der Speicherposition zu implementieren, die laut der im vorherigen Schritt definierten Rangfolge als Nächste angegeben ist.

Ein Betriebssystem-Image implementieren

Sie können Lenovo XClarity Administrator verwenden, um ein Betriebssystem-Image auf bis 28 Servern gleichzeitig 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).

Stellen Sie auf der Registerkarte **BS-Images** sicher, dass der **Bereitstellungsstatus** des Betriebssystems, das Sie implementieren möchten, auf „Bereit“ festgelegt ist. Um das Windows-Betriebssystem zu implementieren, ist eine WinPE-Boot-Datei erforderlich. Wenn eine entsprechende WinPE-Datei nicht verfügbar ist, ist **Bereitstellungsstatus** auf „Nicht bereit“ festgelegt, und das Betriebssystem kann nicht implementiert werden. Sie müssen eine WinPE-Datei manuell herunterladen und importieren (siehe Boot-Dateien importieren).

Auf der Registerkarte **BS-Images verwalten** können Sie die Liste der BS-Images verwalten, indem Sie auf **Alle anzeigen → Bereitstellungsstatus** klicken. Sie können die Liste so filtern, dass nur Server mit dem Status „Bereitstellung“, „Nicht bereit“ und „Warnung“ angezeigt werden. Beachten Sie, dass wenn der Implementierungsstatus für ein Betriebssystem-Image „Nicht bereit“ ist, das Betriebssystem nicht in der Liste der zur Bereitstellung geeigneten Betriebssystemen enthalten ist.

Das Gebietsschema Englisch wird standardmäßig unterstützt. Um eine sprachspezifische Ländereinstellung anzugeben, müssen Sie eine angepasste Konfigurationsdatei und eine Unattend-Datei verwenden. Weitere Informationen finden Sie unter SLES 12 SP3 mit einem konfigurierbaren Gebietsschema und NTP-Servern implementieren und Windows 2016 für Japanisch implementieren.

Eine Betriebssystembereitstellung auf zugeordnetem Speicher ohne RAID wird nicht unterstützt.

Achtung: Wenn auf dem Server bereits ein Betriebssystem installiert ist, wird das aktuelle Betriebssystem durch die Implementierung eines BS-Image-Profils überschrieben.

Stellen Sie bei Servern mit XCC2, aktiviertem Systemschutz und der festgelegten Aktion **BS-Start verhindern** sicher, dass der Systemschutz auf der Einheit konform ist. Wenn der Systemschutz nicht konform ist, werden die Einheiten daran gehindert, den Bootvorgang abzuschließen, wodurch die BS-Implementierung fehlschlägt. Damit Sie diese Einheit bereitstellen können, reagieren Sie manuell auf die Systemschutz-Bootaufforderung, damit die Einheiten normal booten können.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Betriebssystem-Image auf einem oder mehreren verwalteten Servern zu implementieren.

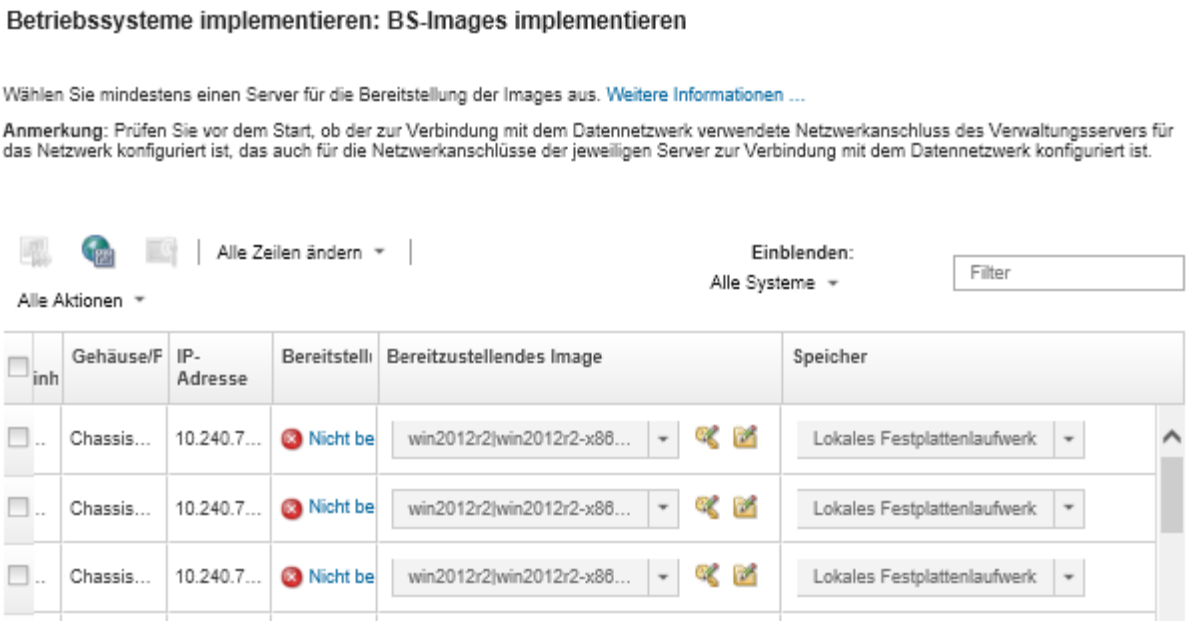
Schritt 1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.

Tipp: Bei skalierbaren Komplexen wird das Betriebssystem auf der primären Partition implementiert. Daher enthält die Serverliste nur die primäre Partition.

Schritt 2. Wählen Sie mindestens einen Server aus, auf dem das Betriebssystem implementiert werden soll. Sie können ein Betriebssystem auf bis zu 28 Servern gleichzeitig implementieren.

Sie können die Tabellenspalten sortieren, um die Suche nach bestimmten Servern zu erleichtern. Darüber hinaus können Sie die Liste der angezeigten Einheiten filtern, indem Sie im Menü **Anzeigen** auswählen, dass nur Einheiten in einem bestimmten Gehäuse, Rack oder Gruppe angezeigt werden, oder indem Sie Text (z. B. einen Namen oder eine IP-Adresse) im Feld **Filter** eingeben.

Tipp: Sie können mehrere Rechenknoten von verschiedenen Gehäusen auswählen, wenn Sie dasselbe Betriebssystem auf allen Rechenknoten implementieren möchten.



Schritt 3. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen**, um die Netzwerkeinstellungen zu konfigurieren.

Siehe Netzwerkeinstellungen für verwaltete Server konfigurieren für weitere Informationen.

Schritt 4. Wählen Sie für jeden Server das zu implementierende BS-Image-Profil aus der Dropdown-Liste in der Spalte **Zu implementierendes Image** aus.

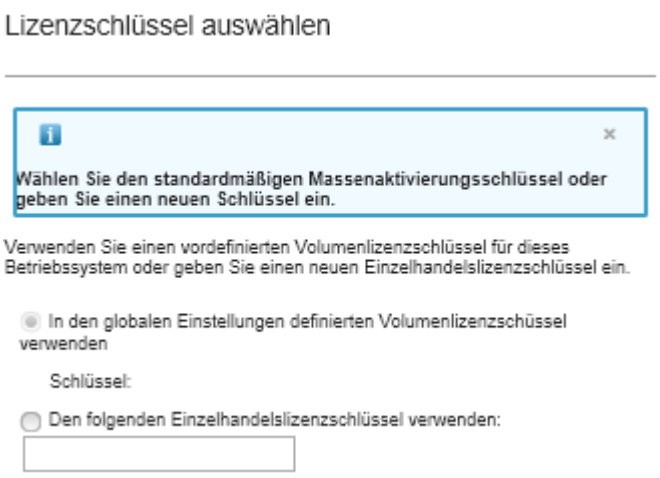
Stellen Sie sicher, dass Sie ein BS-Image-Profil auswählen, das mit dem ausgewählten Server kompatibel ist. Sie können die Kompatibilität über die Profilattribute bestimmen, die in der Spalte **Attribute** auf der Seite BS-Images verwalten aufgeführt sind. Informationen zu Profilattributen finden Sie unter Betriebssystem-Image-Profile.

Schritt 5. Klicken Sie für jeden Server auf das Symbol **Lizenzschlüssel** ( ) und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.

XClarity Administrator unterstützt standardmäßige Datenträger-Lizenzschlüssel für Windows-Installationen und individuelle Einzelhandelslizenzschlüssel für Windows und VMware ESXi.

Um den globalen Datenträger-Lizenzschlüssel zu verwenden, den Sie im Dialogfenster „Globale Einstellungen“ angegeben haben, wählen Sie **In den globalen Einstellungen definierten Volumenlizenzschüssel verwenden** aus. Weitere Informationen zu globalen Datenträger-Lizenzschlüsseln finden Sie unter Globale BS-Implementierungseinstellungen konfigurieren.

Um einen individuellen Einzelhandelslizenzschlüssel zu verwenden, wählen Sie **Den folgenden Einzelhandelslizenzschlüssel verwenden** aus und geben Sie den Schlüssel in das folgende Feld ein.



Schritt 6. **Optional:** Wenn Sie für einen Server ein Windows-Betriebssystem ausgewählt haben, können Sie das Windows-Betriebssystem im Rahmen der Betriebssystembereitstellung mit einer Active Directory-Domäne verknüpfen. Klicken Sie dazu auf das **Ordner**-Symbol ( ), das neben dem Betriebssystem-Image angezeigt wird, und wählen Sie dann den Active Directory-Namen aus.

Um die standardmäßige Active Directory-Domäne zu verwenden, die Sie im Dialogfenster „Globale Einstellungen“ angegeben haben, wählen Sie **Das in den globalen Einstellungen definierte Active Directory verwenden** aus. Weitere Informationen zum Verknüpfen einer Active Directory-Domäne finden Sie unter In Windows Active Directory integrieren.

Um eine bestimmte Active Directory-Domäne zu verwenden, wählen Sie **Folgendes Active Directory verwenden** aus und geben Sie dann die gewünschte Active Directory-Domäne an.

Schritt 7. Wählen Sie für jeden Server in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.
- **Lokale Festplatte**
- **Embedded Hypervisor**
- **M.2-Laufwerk**
- **SAN-Speicher**

Wenn die ausgewählte Speicherposition nicht mit dem Server kompatibel ist, versucht XClarity Administrator, das Betriebssystem in der Speicherposition zu implementieren, die in der Rangfolge als Nächste angegeben ist.

Anmerkung: Für ThinkServer-Server ist nur die Option **Lokale Festplatte** verfügbar.

Weitere Informationen zum Konfigurieren der Speicherposition finden Sie unter Speicherposition für verwaltete Server auswählen.

Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom verwalteten Server.

Schritt 8. Überprüfen Sie, ob als Implementierungsstatus für alle ausgewählten Server „Bereitstellung“ angegeben ist.

Wichtig: Für alle ausgewählten Server muss der Implementierungsstatus „Bereitstellung“ festgelegt sein. Wenn der Status eines Servers „Nicht bereit“ lautet, können Sie auf diesem Server kein Betriebssystem-Image implementieren. Klicken Sie auf den Link **Nicht bereit**, um Informationen zur Fehlerbehebung abzurufen. Wenn die Netzwerkeinstellungen nicht gültig sind,

klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen**, um die Netzwerkeinstellungen zu konfigurieren.

Schritt 9. Klicken Sie auf das Symbol für **Images implementieren** (), um die Betriebssystembereitstellung einzuleiten.

Wenn angepasste Konfigurationseinstellungen zum BS-Image-Profil hinzugefügt wurden, wird die Registerkarte **Angepasste Einstellungen** im Dialogfenster BS-Image implementieren angezeigt. Geben Sie angepassten Einstellungen, allgemeine Servereinstellungen und bestimmte Servereinstellungen an und klicken Sie dann auf **Weiter**, um mit der BS-Implementierung fortzufahren. Beachten Sie, dass die BS-Implementierung nicht fortgesetzt wird, wenn keine Eingabe für alle erforderlichen angepassten Konfigurationseinstellungen angegeben ist.

Nach dieser Aufgabe

Sie können den Status des Implementierungsprozesses im Jobprotokoll überwachen. Klicken Sie im XClarity Administrator-Menü auf **Überwachung → Jobs**. Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

Über den Baseboard Management Controller können Sie eine Fernsteuerungssitzung für den Server einrichten, um den Fortschritt der Installation zu beobachten. Weitere Informationen zur Fernsteuerung finden Sie unter Verwenden der Fernsteuerung zur Verwaltung von Converged-, Flex System-, NeXtScale- und System x-Servern.

Implementierungsinformationen werden für das Betriebssystem gespeichert. Sie können die Implementierungsinformationen anzeigen, indem Sie auf **Bereitstellung → BS-Zugriff verwalten** klicken und dann mit der Maus auf den Servernamen zeigen.

In Windows Active Directory integrieren

Wenn Sie ein Windows-Image mit Lenovo XClarity Administrator implementieren, können Sie eine Active Directory-Domäne im Rahmen der Betriebssystembereitstellung verknüpfen.

Vorbereitende Schritte

Zum Verknüpfen einer Active Directory-Domäne im Rahmen einer Windows-Image-Implementierung müssen Sie den Verwaltungsserver und den Windows-Server, auf dem der betroffene Active Directory-Domänen-Controller ausgeführt wird, konfigurieren. Um diese Konfiguration durchführen zu können, benötigen Sie folgenden Zugriff:

- Ein Administratoraccount mit der Berechtigung, die Active Directory-Serverdomäne zu authentifizieren und zu verknüpfen. Dieser Account muss ähnliche Berechtigungen haben wie die Standard-Domänenadministratorengruppe und Sie können einen Account in dieser Gruppe für diese Konfiguration verwenden.
- Zugriff auf ein Domain Name System (DNS), das in dem Active Directory-Server aufgelöst wird, auf dem der Domänen-Controller ausgeführt wird. Dieses DNS muss in der Option **Netzwerkeinstellungen → DNS** für den Server angegeben werden, auf dem Sie das Betriebssystem implementieren.
- Der Active Directory-Serveradministrator muss den erforderlichen Computernamen auf dem Domänenserver erstellen, bevor Sie das Betriebssystem implementieren. Durch den Verknüpfungsversuch wird kein Computername erstellt. Wenn kein Name angegeben ist, schlägt die Verknüpfung fehl.
- Der Administrator des Active Directory-Servers muss den Hostnamen des Servers, auf dem das Image implementiert wird, als Computernamen unter der Zielorganisationseinheit angeben, indem er auf das Feld **Netzwerkeinstellungen → Hostname** klickt.

Der angegebene Hostname (Computername) muss eindeutig sein. Die Verknüpfung schlägt fehl, wenn ein Name angegeben wird, der bereits von einer anderen Windows-Installation verwendet wird.

Sie können die Active Directory-Domäne über eine der folgenden Methoden verknüpfen:

- **Eine Active Directory-Domäne verwenden**

  Sie können eine bestimmte Active Directory-Domäne aus einer Liste vordefinierter Domänen verwenden. Gehen Sie wie folgt vor, um eine Active Directory-Domäne in XClarity Administrator zu definieren. Wenn Sie beabsichtigen, mehrere Domänen zu verwenden, wiederholen Sie diese Schritte für jeden Domänennamen.

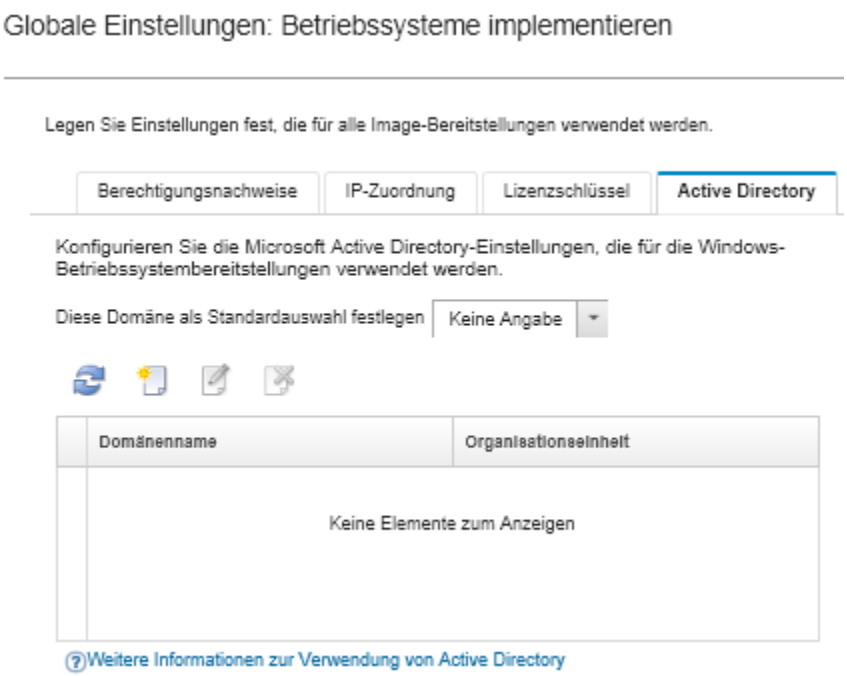
  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite „BS-Images implementieren“ anzuzeigen.
  2. Klicken Sie auf das Symbol **Globale Einstellungen** (), um das Dialogfeld Globale Einstellungen: Betriebssysteme implementieren anzuzeigen.
  3. Klicken Sie auf die Registerkarte **Active Directory**.
  4. Klicken Sie auf das Symbol **Erstellen** (), um das Dialogfeld Neue Active Directory-Domäne hinzufügen anzuzeigen.
  5. Geben Sie den Domänennamen und die Organisationseinheit an.

     Die Betriebssystembereitstellung unterstützt das Verknüpfen einer Domäne und das Erstellen von verschachtelten Organisationseinheiten innerhalb einer Domäne. Wenn Sie Organisationseinheiten angeben, ist es nicht erforderlich, die Organisationseinheit als Teil der Verknüpfung explizit anzugeben. Active Directory kann die richtige Organisationseinheit mithilfe des Domänen- und Computernamens ableiten.
  6. Klicken Sie auf **OK**.

- **Standard-Active Directory-Domäne verwenden**

  Sie können die Standard-Active Directory-Domäne verwenden, die in den globalen Einstellungen definiert ist. Gehen Sie wie folgt vor, um die Standard-Active Directory-Domäne in XClarity Administrator festzulegen.

  1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite „BS-Images implementieren“ anzuzeigen.
  2. Klicken Sie auf das Symbol **Globale Einstellungen** (), um das Dialogfeld Globale Einstellungen: Betriebssysteme implementieren anzuzeigen.
  3. Klicken Sie auf die Registerkarte **Active Directory**.



4. Wählen Sie im Dropdown-Menü **Diese Domäne als Standardauswahl festlegen** die Active Directory-Domäne aus, die standardmäßig für jede Windows-Implementierung verwendet werden soll.
5. Klicken Sie auf **OK**.

- **Metadaten-BLOB-Daten verwenden**

  Sie können Active Directory-Computerkonto-Metadaten (im Base-64-codierten BLOB-Format) verwenden, um die Active Directory-Domäne für Server zu verknüpfen. Gehen Sie wie folgt vor, um Metadaten-BLOB-Daten zu generieren:

  1. Melden Sie sich über ein Administratorkonto beim Computer an. Der Computer muss Teil der Active Directory-Domäne sein, die Sie verknüpfen.
  2. Klicken Sie auf **Start → Programme → Zubehör**. Klicken Sie mit der rechten Maustaste auf **Eingabeaufforderung** und dann auf **Als Administrator ausführen**.
  3. Wechseln Sie zum C:\windows\system32-Verzeichnis.
  4. Führen Sie den Befehl `djoin` mit dem folgenden Format aus, um offline einen Domänenbeitritt auszuführen:
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     Dabei gilt Folgendes:

     – *<AD_domain_name>* ist der Name der Active Directory-Domäne.
     – *<hostname>* ist der Hostname des Servers, auf dem das Image implementiert wird, als Computernamen unter der Zielorganisationseinheit angeben, indem auf das Feld **Netzwerkeinstellungen → Hostname** geklickt wird.

     Dieser Befehl erstellt eine Datei mit der Bezeichnung `blob`, die Metadaten-BLOB-Daten enthält. Der Inhalt dieser Datei wird vom Betriebssystem-Implementierungsprozess verwendet, um die Active Directory-Verknüpfungsdetails anzugeben, halten Sie diese Daten also bereit.

     Die Metadaten-BLOB-Daten sind sensible Daten.

Nähere Informationen zum Implementieren eines Betriebssystem-Images finden Sie unter Ein Betriebssystem-Image implementieren.

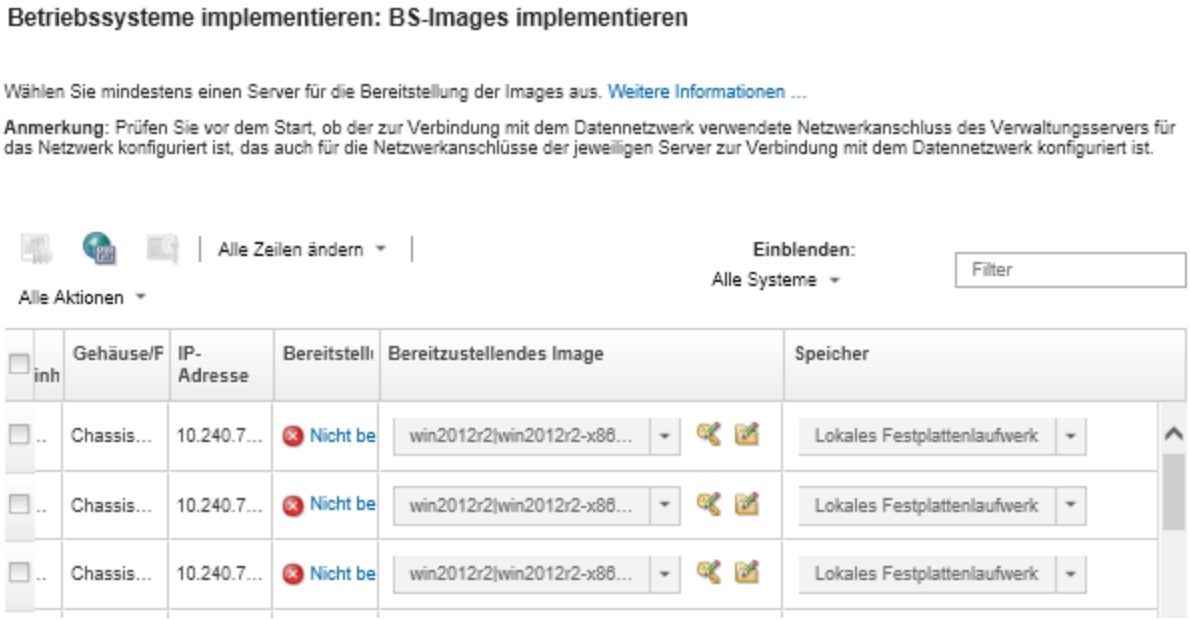
Vorgehensweise

Gehen Sie wie folgt vor, um eine Active Directory-Domäne zu verknüpfen:

Schritt 1. Importieren Sie das Windows-Betriebssystem-Image in das BS-Images-Repository (siehe Betriebssystem-Images importieren).

Schritt 2. Wählen Sie mindestens einen Server aus, auf dem das Betriebssystem implementiert werden soll. Sie können ein Betriebssystem auf bis zu 28 Servern gleichzeitig implementieren.

Tipp: Sie können mehrere Rechenknoten von verschiedenen Gehäusen auswählen, wenn Sie dasselbe Betriebssystem auf allen Rechenknoten implementieren möchten.



Schritt 3. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen**, um die Netzwerkeinstellungen zu konfigurieren.

a. Klicken Sie auf **Alle Zeilen ändern → Domain Name System (DNS)** und geben Sie mindestens ein DNS an, das in die Active Directory-Domäne aufgelöst wird.

b. Geben Sie für jeden Server einen Hostnamen an, der mit einem vorhandenen Computernamen in der Domäne und Organisationseinheit, die Sie verknüpfen, übereinstimmt.

Weitere Informationen zum Festlegen der Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für verwaltete Server konfigurieren.

Schritt 4. Wählen Sie für jeden Server in der Spalte **Zu implementierendes Image** das gewünschte Windows-Betriebssystem-Image aus. Ein Ordner- und Lizenzschlüsselsymbol wird neben dem Image-Namen angezeigt.

Schritt 5. Klicken Sie für jeden Server auf das **Lizenzschlüssel**-Symbol ( ) und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll:

Schritt 6. Klicken Sie für jeden Server auf das **Ordner**-Symbol ( ) und geben Sie den Active Directory-Domäne an. Sie können einen der folgenden Werte auswählen:

- **Das in den globalen Einstellungen definierte Active Directory verwenden**, um die Standard-Domäne zu verwenden.
- **Folgendes Active Directory verwenden**, um eine bestimmte Domäne auszuwählen.
- **Metadaten-BLOB-Daten verwenden**, um den Inhalt der BLOB-Datei anzugeben.

Die Metadaten-BLOB-Daten enthalten sensible Informationen und werden nicht im Feld angezeigt. Diese Informationen sind nur verfügbar, bis der Implementierungsvorgang abgeschlossen ist. Sie sind nicht permanent.

Schritt 7. Wählen Sie für jeden Server in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.
- **Lokale Festplatte**
- **Embedded Hypervisor**
- **M.2-Laufwerk**
- **SAN-Speicher**

Wenn die ausgewählte Speicherposition nicht mit dem Server kompatibel ist, versucht XClarity Administrator, das Betriebssystem in der Speicherposition zu implementieren, die in der Rangfolge als Nächste angegeben ist.

Weitere Informationen zum Konfigurieren der Speicherposition finden Sie unter Speicherposition für verwaltete Server auswählen.

Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom verwalteten Server.

Schritt 8. Überprüfen Sie, ob als Implementierungsstatus für alle ausgewählten Server „Bereitstellung“ angegeben ist.

Wenn der Status eines Servers „Nicht bereit“ lautet, können Sie auf diesem Server kein Betriebssystem-Image implementieren. Klicken Sie auf den Link **Nicht bereit**, um Informationen zur Fehlerbehebung abzurufen. Wenn die Netzwerkeinstellungen nicht gültig sind, klicken Sie auf **Ausgewählte geändert → Netzwerkeinstellungen**, um die Netzwerkeinstellungen zu konfigurieren.

Schritt 9. Klicken Sie auf das Symbol für **Images implementieren** (), um die Betriebssystembereitstellung einzuleiten.

Geben Sie im Dialogfeld Bestätigung implementieren die Anmeldeinformationen ein, die für die Authentifizierung des Active Directory-Servers und Verknüpfung der Domäne erforderlich sind. Aus Sicherheitsgründen werden diese Anmeldeinformationen nicht in XClarity Administrator gespeichert. Sie müssen die Anmeldeinformationen für jede Windows-Implementierung angeben, die der Domäne angeschlossen wird.

Sie können den Status des Implementierungsprozesses im Jobprotokoll überwachen. Klicken Sie im XClarity Administrator-Menü auf **Überwachung → Jobs**. Weitere Informationen zum Jobprotokoll finden Sie unter Jobs überwachen.

Ergebnisse

Wenn die Betriebssystembereitstellung abgeschlossen ist, öffnen Sie einen Webbrowser und melden Sie sich bei der IP-Adresse an, die Sie auf der Seite Netzwerkeinstellungen ändern angegeben haben. Melden Sie sich an, um mit dem Konfigurationsprozess fortzufahren.

BS-Implementierungsszenarien

Verwenden Sie diese Szenarien zum Anpassen und Implementieren von Betriebssystemen auf verwalteten Servern.

RHEL mit angepassten Einheitentreibern implementieren

In diesem Szenario werden das Red Hat Enterprise Linux-(RHEL)-Betriebssystem und zusätzliche Einheitentreiber installiert, die nicht beim Basisbetriebssystem verfügbar sind. Es wird ein angepasstes Profil verwendet, das die zusätzlichen Einheitentreiber enthält. Das angepasste Profil kann dann auf der Seite „BS-Images implementieren“ ausgewählt werden.

Vorbereitende Schritte

Beim Implementieren eines Betriebssystems mit Lenovo XClarity Administrator muss das Betriebssystem über die entsprechenden Einheitentreiber für Ihre Ethernet-, Fibre Channel- und Speicheradapter-Hardware verfügen. Wenn ein Einheitentreiber nicht im Betriebssystem enthalten ist, wird dieser Adapter bei der BS-Implementierung nicht unterstützt. Bei XClarity Administrator v1.2.0 und höher können Sie ein Betriebssystem durch das Hinzufügen von Einheitentreibern anpassen.

Sie erhalten Einheitentreiber von Lenovo YUM Repository-Webseite, vom Anbieter (z. B. Red Hat), oder über einen angepassten Einheitentreiber, den Sie selbst erstellen. Für einige Windows-Einheitentreiber kann ein angepasster Einheitentreiber durch Extrahieren des Einheitentreibers aus der ausführbaren Installationsdatei in Ihr lokales System und durch Erstellen einer ZIP-Archivdatei generiert werden.

Anmerkung: RHEL-Einheitentreiber müssen im RPM- oder ISO-Image-Format sein.

Vorgehensweise

Gehen Sie wie folgt vor, um RHEL mit angepassten Einheitentreibern zu implementieren.

Schritt 1. Laden Sie das RHEL-Basisbetriebssystem von der Red Hat-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ( ).
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um nach dem zu importierenden RHEL-Image zu suchen und es auszuwählen (z. B. `RHEL-<ver>–<date>-Server-x86_64-dvd1.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Laden Sie die angepassten Einheitentreiber auf das lokale System herunter und importieren Sie die Dateien in das BS-Images-Repository. Weitere Informationen finden Sie unter Einheitentreiber importieren.

1. Klicken Sie auf die Registerkarte **Einheitentreiber**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `RHEL` für das Betriebssystem aus.
5. Wählen Sie die Version des Betriebssystems aus.
6. Wählen Sie den Einheitentyp aus.
7. Klicken Sie auf **Durchsuchen**, um nach dem zu importierenden Einheitentreiber zu suchen und ihn auszuwählen (zum Beispiel `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 3. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepassten Einheitentreiber enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Virtualization`).
3. Klicken Sie auf das **Erstellen**-Symbol (), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. `Angepasste RHEL mit Einheitentreibern`).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Keine** als Anpassungstyp aus.
   d. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Registerkarte **Treiberoptionen** die angepassten Einheitentreiber aus, die im Profil enthalten sein sollen, und klicken Sie auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Klicken Sie auf der Registerkarte **Software** auf **Weiter**.
7. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 4. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. <*Basis_BS*>|<*Zeitstempel*>`_Angepasste RHEL mit Einheitentreibern`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** () und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.
   e. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystemimplementierung ausgewählt wurde) vom verwalteten Server.
   f. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.
3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
5. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

RHEL und eine Hello World PHP-Anwendung mit einer angepassten Unattend-Datei implementieren

In diesem Szenario wird das Betriebssystem RHEL zusammen mit angepasster Software (Apache HTTP, PHP und einer Hello World PHP-Anwendung) installiert. Es wird ein angepasstes BS-Image-Profil verwendet, das die angepasste Unattend-Datei und ein Nach-Installationsskript enthält, welches das Betriebssystem beim internen Lenovo RHEL Abonnementservice registriert, sodass die YUM Repositorys verwendet werden können. Außerdem installiert es die Apache- und PHP-Pakete, konfiguriert die Firewall, um Apache-Verbindungen zuzulassen, erstellt eine Hello World PHP-Anwendung und kopiert diese in das Apache-Webserver-Verzeichnis und konfiguriert die Apache-Konfigurationsdateien zur Unterstützung von PHP.

Vorbereitende Schritte

Sie haben für die Implementierung von RHEL mit angepasster Software verschiedene Möglichkeiten. Bei diesem Beispiel wird eine angepasste Attend-Datei verwendet, die Sie das angepasste BS-Image-Profil integrieren. Sie können auch ein Nach-Installationsskript verwenden, das angepasste Software installiert, die Sie in das Repository importieren und in das angepasste BS-Image-Profil integrieren. Informationen zum Installieren von Software mit einem Nach-Installationsskript finden Sie unter RHEL und eine Hello World PHP-Anwendung mit angepasster Software und einem Nach-Installationsskript implementieren.

In diesem Szenario wird die folgenden Beispieldatei verwendet.

- RHEL_installSoftware_customUnattend.cfg Diese angepasste Unattend-Datei verwendet Werte in vordefinierten und angepassten Makros und installiert und konfiguriert die angepasste Software.

Vorgehensweise

Zum Implementieren von RHEL mit angepasster Software über eine angepasste Unattend-Datei führen Sie die folgenden Schritte aus.

Schritt 1. Laden Sie das RHEL-Basisbetriebssystem von der Red Hat-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ( ).
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um nach dem zu importierenden RHEL-Image zu suchen und es auszuwählen (z. B. `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Ändern Sie die RHEL-Unattend-Datei (Kickstart), um das Betriebssystem bei Ihrem RHEL-Satelliten-Abonnementservice zu registrieren, die HTTP (Apache)- und PHP-Pakete zu installieren und eine einfache Hello World PHP-Anwendung zu erstellen, die erforderlichen vordefinierten Makros und ggf. andere vordefinierte Makros hinzuzufügen, z. B. IP-Adresse, Gateway, DNS und Hostnamen-Einstellungen, und dann die angepasste Datei in das BS-Images-Repository zu importieren. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren

Fügen Sie Befehle hinzu, um den Host beim RHEL-Satelliten zu registrieren, z. B.:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Wichtig: Geben Sie in der Unattend-Beispieldatei die IP-Adresse Ihres Satellitenservers und Ihrer Organisation basierend auf der Konfiguration unseres Abonnementservice an.

Fügen Befehle hinzu, um den Host zu aktualisieren und die Apache- und PHP-Pakete zu installieren und zu konfigurieren, z. B.:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Anmerkung: Die Unattend-Beispieldatei ändert die Standardpakete, die mit der Kickstart-Datei installiert werden. Sie gibt die Apache- und PHO-Pakete im Abschnitt „%packages“ an.

Nur für ESXi und RHEL: XClarity Administrator bietet das Makro **#predefined.unattendSettings.networkConfig#** an, das alle Netzwerkeinstellungen hinzufügt, die auf der Benutzeroberfläche für die Unattend-Datei definiert sind, sowie das Makro **#predefined.unattendSettings.storageConfig#**, das alle Speichereinstellungen hinzufügt, die auf der Benutzeroberfläche für die Unattend-Datei definiert sind. Die Unattend-Beispieldatei enthält bereits diese Makros.

XClarity Administrator bietet außerdem einige allgemeine Komfortmakros, z. B. OOB-Treiberinjektion, Statusmeldungen, Nach-Installationsskripts und angepasste Software. Zur Verwendung dieser vordefinierten Makros müssen Sie jedoch die folgenden Makros in der angepassten Unattend-Datei angeben. Die Beispieldatei enthält bereits die benötigten Makros.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

Die Beispieldatei enthält bereits die erforderlichen Makros und zusätzliche vordefinierte Makros für die dynamische Angabe der Netzwerkeinstellungen beim Zielserver und Zeitzone. Weitere Informationen zum Hinzufügen von Makros zu Unattend.Dateien finden Sie unter Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei.

Sie können auch Befehle zum Senden von angepassten Nachrichten an das Jobprotokoll in XClarity Administrator hinzufügen. Siehe Angepasste Statusmeldungen zu Installationsskripts hinzufügen für weitere Informationen.

Gehen Sie wie folgt vor, um das angepasste Installationsskript zu importieren. Siehe Angepasste Installationsskripts importieren für weitere Informationen.

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `RHEL` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Softwaredatei zu suchen und auszuwählen (z. B. `RHEL_installSoftware_customUnattend.cfg`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 3. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepasste Software und das Nach-Installationsskript enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Basic`).
3. Klicken Sie auf das **Erstellen**-Symbol ( ), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein, z. B. `Angepasste RHEL mit Software über angepasste Unattend`.
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie für den Anpassungstyp **Nur Unattend-Dateien** aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Klicken Sie auf der Registerkarte **Software** auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Unattend-Dateien** die angepasste Unattend-Datei aus (z. B. `RHEL_installSoftware_customUnattend.cfg`) und klicken Sie auf **Weiter**.
8. Klicken Sie auf der Registerkarte **Installationsskripts** auf **Weiter**.
9. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
10. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 4. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp:

      - VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
      - Die Netzwerkeinstellungen, die Sie im Dialogfeld „Netzwerkeinstellungen“ angeben, werden bei der Ausführung mithilfe der Makros **#predefined.hostPlatforms.networkSettings.<*setting*>#** zur Unattend-Datei hinzugefügt.

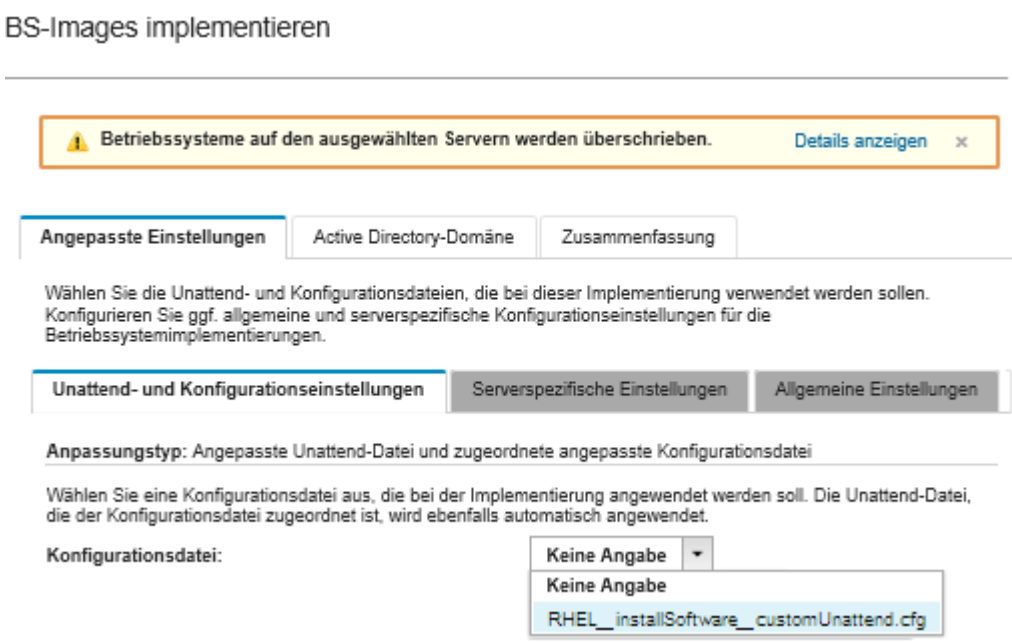
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. <*Basis_BS*>|<*Zeitstempel*>_`Angepasste RHEL mit Software über angepasste Unattend`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.

   d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** () und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.
   e. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystemimplementierung ausgewählt wurde) vom verwalteten Server.

   f. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.
3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Klicken Sie auf der Registerkarte „Angepasste Einstellungen“ auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Unattend-Datei aus (z. B. `RHEL_installSoftware_customUnattend.cfg`).



5. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
6. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

RHEL und eine Hello World PHP-Anwendung mit angepasster Software und einem Nach-Installationsskript implementieren

In diesem Szenario wird das Betriebssystem RHEL zusammen mit angepasster Software (Apache HTTP, PHP und einer Hello World PHP-Anwendung) installiert. Es wird ein angepasstes BS-Image-Profil verwendet, das die angepasste Software und ein Nach-Installationsskript enthält, welches das Betriebssystem beim internen Lenovo RHEL Abonnementservice registriert, sodass die YUM Repositorys verwendet werden können. Außerdem installiert es die Apache- und PHP-Pakete, konfiguriert die Firewall, um Apache-Verbindungen zuzulassen, erstellt eine Hello World PHP-Anwendung und kopiert diese in das Apache-Webserver-Verzeichnis und konfiguriert die Apache-Konfigurationsdateien zur Unterstützung von PHP. Die angepassten Softwarepakete werden während der Implementierung zum Host exportiert und für die Verwendung durch das angepasste Nach-Installationsskript verfügbar gemacht.

Vorbereitende Schritte

Sie haben für die Implementierung von RHEL und einer Hello World PHP-Anwendung verschiedene Möglichkeiten. Bei diesem Beispiel wird ein Nach-Installationsskript verwendet, das angepasste Software installiert, die Sie in das Repository importieren und in das angepasste BS-Image-Profil integrieren. Sie können auch eine angepasste Attend-Datei verwenden, die Sie das angepasste BS-Image-Profil integrieren. Informationen zur Installation von Software mit einer angepassten Attend-Datei finden Sie unter RHEL und eine Hello World PHP-Anwendung mit einer angepassten Unattend-Datei implementieren.

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- httpd.conf. Dies ist die Installationsdatei für Apache HTTP.
- hello_world.php Dies ist die Hello World PHP-Anwendung.
- RHEL_installSoftware_customScript.sh Dieses Nach-Installationsskript installiert und konfiguriert die angepasste Software.

Anmerkungen:

- RHEL-Installationsskripts können einem der folgenden Formate vorliegen: Bash (.sh), Perl (.pm oder .pl), Python (.py)
- Softwaredateien und Installationsskripts werden über den angepassten Daten- und Dateipfad installiert, den Sie während der Bereitstellung angeben. Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.

Vorgehensweise

Zum Implementieren von RHEL mit angepasster Software über ein Nach-Installationsskript führen Sie die folgenden Schritte aus.

Schritt 1. Laden Sie das RHEL-Basisbetriebssystem von der Red Hat-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um nach dem zu importierenden RHEL-Image zu suchen und es auszuwählen (z. B. `RHEL-<ver>–<date>-Server-x86_64-dvd1.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Laden Sie die angepasste Software auf das lokale System herunter und importieren Sie die Dateien in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Software importieren.

Tipp: Um die angepasste Software in XClarity Administrator zu importieren, müssen die Dateien in einer TAR.GZ-Datei enthalten sein. Komprimieren Sie für dieses Beispiel die Softwarebeispieldateien `httpd.conf` und `index.php` in einer TAR.GZ-Datei namens `RHEL_installSoftware_customsw.tar.gz`, bevor Sie fortfahren.

1. Klicken Sie auf die Registerkarte **Software**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `RHEL` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Softwaredatei zu suchen und auszuwählen (z. B. `RHEL_installSoftware_customsw.tar.gz`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 3. Erstellen Sie ein angepasstes Nach-Installationsskript und importieren Sie die Datei in das BS-images-Repository.

Fügen Sie Befehle hinzu, um den Host beim RHEL-Satelliten zu registrieren, z. B.:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Fügen einen Befehl hinzu, um den Host zu aktualisieren und die Apache- und PHP-Pakete zu installieren und zu konfigurieren, z. B.:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd
```

```
systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Fügen Sie Befehle hinzu, um unsere PHP-Anwendung zum Web-Serversatellite hinzuzufügen, z. B.:
`cp` **`#predefined.otherSettings.deployDataAndSoftwareLocation#`**`/lxca/index.php /var/www/html/index.php`

Fügen Sie Befehle hinzu, um Apache HTTP zu konfigurieren, z. B.:
```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Beachten Sie, dass diese Befehle vordefinierte Makros für den Pfad zu den extrahierten Daten und Softwaredateien verwenden (**predefined.otherSettings.deployDataAndSoftwareLocation**).

Sie können auch Befehle zum Senden von angepassten Nachrichten an das Jobprotokoll in XClarity Administrator hinzufügen. Siehe Angepasste Statusmeldungen zu Installationsskripts hinzufügen für weitere Informationen.

Gehen Sie wie folgt vor, um das angepasste Installationsskript zu importieren. Weitere Informationen finden Sie unter Angepasste Installationsskripts importieren.

1. Klicken Sie auf die Registerkarte **Installationsskripts**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `RHEL` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das zu importierende Nach-Installationsskript aus (z. B. `RHEL_installSoftware_customScript.sh`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 4. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepasste Software und das Nach-Installationsskript enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Basic`).
3. Klicken Sie auf das **Erstellen**-Symbol ( ), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. `Angepasstes RHEL mit Software über Nach-Installationsskript`).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Keine** als Anpassungstyp aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Wählen Sie auf der Registerkarte **Software** die Installationsdateien der Software aus (z. B. `httpd.conf` und `index.php`) und klicken Sie auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Installationsskripts** die Installationsskripts aus (z. B. `RHEL_installSoftware_customScript.sh`) und klicken Sie auf **Weiter**.

8. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
9. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 5. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. *<Basis_BS>*|*<Zeitstempel>*_`Angepasstes RHEL mit Software über Nach-Installationsskript`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystemimplementierung ausgewählt wurde) vom verwalteten Server.
   e. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.
3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
5. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

Implementieren von SLES 12 SP3 mit angepassten Paketen und Zeitzone

In diesem Szenario werden das Betriebssystem SLES 12 SP3 (in englischer Sprache) und mehrere optionale SLES-Pakete installiert. Außerdem wird die Zeitzone abgefragt. Es wird ein angepasstes BS-Image-Profil verwendet, das eine angepasste Konfigurationsdatei und eine angepasste Unattend-Datei enthält. Dieses angepasste Profil kann auf der Seite „BS-Images implementieren“ ausgewählt werden. Dann können die angepassten SLE-Pakete ausgewählt und die Zeitzone auf der Registerkarte **Angepasste Einstellungen** festgelegt werden. Die ausgewählten Werte werden durch die angepassten Makros in der angepassten Unattend-Datei ersetzt und das SLES-AutoYaST-Installationsprogramm verwendet die Werte in der Unattend-Datei, um das Betriebssystem zu konfigurieren.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- SLES_installPackages_customConfig.json. Diese Konfigurationsdatei fragt die Zeitzone und optional zu installierende SLES-Pakete (Linux, Apache, MySQL, PHP-Softwarepaket, SLES-Mailserverpaket und SLES-Dateiserverpaket) ab.

- SLES_installPackages_customUnattend.xml Diese Unattend-Datei verwendet Werte in vordefinierten Makros und angepassten Makros, die in der Konfigurationsdatei definiert sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um SLES 12 SP3 mithilfe eines angepassten OS-Image-Profils auf Servern bereitzustellen.

Schritt 1. Laden Sie das SLES-Basisbetriebssystem von der SUSE-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um das zu importierende SLES 12 SP3-Image zu suchen und auszuwählen (z. B. `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Erstellen Sie eine angepasste Konfigurationseinstellungsdatei und importieren Sie die Datei in das BS-Images-Repository.

Die Konfigurationseinstellungsdatei ist eine JSON-Datei, die die Daten beschreibt, die während des BS-Implementierungsprozesses dynamisch gesammelt werden müssen. Für dieses Szenario möchten wir die optionalen SLES-Pakete angeben, die installiert werden können (einschließlich SLES Linux, Apache, MySQL, PHP-Softwarepaket, SLES-Mailserverpaket und SLES-Dateiserverpaket), sowie eine Zeitzone, die für jede BS-Implementierung verwendet werden soll. Weitere Informationen zum Erstellen von Konfigurationseinstellungsdateien finden Sie unter Angepasste Makros.

Um die Datei mit den Konfigurationseinstellungen zu importieren, führen Sie diese Schritte aus. Weitere Informationen finden Sie unter Angepasste Konfigurationseinstellungen importieren.

1. Klicken Sie auf die Registerkarte **Konfigurationsdateien**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `SLES` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Konfigurationseinstellungsdatei zu suchen und auszuwählen (z. B. `SLES_installPackages_customConfig.json`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

   Anmerkung: Wenn Sie eine angepasste Konfigurationseinstellungsdatei importieren, generiert XClarity Administrator angepasste Makros für jede Einstellung in der Datei. Sie können diese Makros zur Unattend-Datei hinzufügen. Während der BS-Implementierung werden die Makros durch aktuelle Werte ersetzt.

Schritt 3. Ändern Sie die SLES-Unattend-Datei, um dynamische Werte für die optionalen SLES-Pakete und die Zeitzone anzugeben, und importieren Sie dann die angepasste Datei in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren.

Fügen Sie im Abschnitt **<general>** die Zeitzoneninformationen hinzu, z. B.:

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

Fügen Sie im Abschnitt **<patterns>** drei Pattern-Tags hinzu. Diese Tags werden für die angepassten Makros für die optionalen SLES-Paket-Einstellungen verwendet. Beispiel:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Anmerkungen:

- Diese Tags befinden sich in der Unattend-Beispieldatei.
- Bei der Verwendung einer angepassten Unattend-Datei bietet XClarity Administrator einige der normalen Komfortfunktionen nicht, die Sie haben, wenn Sie eine vordefinierte Unattend-Datei verwenden würden. Zum Beispiel müssen **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** und **<UserAccounts>** für Administrator, **<Interfaces>** für Netzwerk und die **<package>**-Liste für Installationsfunktionen in der angepassten Unattend-Datei angegeben werden, die hochgeladen wird.

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `SLES` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Unattend-Datei zu suchen und auszuwählen (z. B. `SLES_installPackages_customUnattend.xml`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

   Anmerkung: Es wird eine Warnung angezeigt, dass in der Unattend-Datei vordefinierte Makros fehlen. Diese Warnung können Sie vorerst ignorieren. Sie werden die vordefinierten Makros im nächsten Schritt hinzufügen.
7. Klicken Sie in der Warnung auf **Schließen**, um das Dialogfeld Unattend-Datei bearbeiten zu öffnen.

Schritt 4. Verknüpfen Sie die angepasste Unattend-Datei mit der angepassten Konfigurationseinstellungsdatei und fügen Sie der Unattend-Datei die erforderlichen vordefinierten und angepassten Makros (Einstellungen) aus der Konfigurationseinstellungsdatei hinzu. Weitere

Informationen finden Sie unter Unattend-Datei einer Konfigurationseinstellungsdatei zuordnen und Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei.

Tipp: Optional können Sie die angepasste Unattend-Datei der angepassten Datei mit den Konfigurationseinstellungen zuordnen und Makros hinzufügen, wenn Sie die Unattend-Datei importieren.

1. Wählen Sie im Dialogfeld Unattend-Datei bearbeiten die Konfigurationseinstellungsdatei aus, die Sie der Unattend-Datei aus der Dropdown-Liste **Konfigurationsdatei zuordnen** zuordnen möchten (z. B. `SLES_installPackages_customConfig`).
2. Fügen Sie der Unattend-Datei die erforderlichen vordefinierten Makros hinzu.
   a. Wählen Sie **Vordefiniert** aus der Dropdown-Liste **Verfügbare Makros** aus.
   b. Positionieren Sie den Cursor in der Unattend-Datei irgendwo nach Zeile 1 (nach dem **<xml>**-Tag).
   c. Erweitern Sie die Liste **predefined → unattendSettings** in der Liste der verfügbaren vordefinierten Makros.
   d. Klicken Sie auf die Makros **preinstallConfig** und **postinstallConfig**, um die Makros zur Unattend-Datei hinzuzufügen.

   Beispiele:

   ```
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
   <profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
   ```
3. Fügen Sie das angepasste Makro zur Angabe der Zeitzone hinzu.
   a. Wählen Sie **Custom** aus der Dropdown-Liste **Verfügbare Makros** aus.
   b. Platzieren Sie den Cursor hinter dem **<hwclock>**-Tag und klicken Sie auf **timezone**, um das Zeitzonenmakro hinzuzufügen.
   c. Platzieren Sie den Cursor hinter dem **<timezone>**-Tag und klicken Sie auf **timezone**, um das Zeitzonenmakro hinzuzufügen.

   Beispiele:

   ```
   <timezone>
      <hwclock>#timezone#</hwclock>
      <timezone>#timezone#</timezone>
   </timezone>
   ```
4. Fügen Sie das angepasste Makro für die Angabe der optionalen SLES-Pakete hinzu.
   a. Erweitern Sie die Liste **server-settings → node** in der Liste der verfügbaren angepassten Makros.
   b. Positionieren Sie den Cursor in einem der leeren **<pattern>**-Tags und klicken Sie auf **fileserver**.
   c. Positionieren Sie den Cursor in einem der leeren **<pattern>**-Tags und klicken Sie auf **lampserver**.
   d. Positionieren Sie den Cursor in einem der leeren **<pattern>**-Tags und klicken Sie auf **mailserver**.

   Beispiele:

   ```
   <patterns config:type="list">
      <pattern>32bit</pattern>
      <pattern>Basis-Devel</pattern>
      <pattern>Minimal</pattern>
      <pattern>WBEM</pattern>
      <pattern>apparmor</pattern>
   ```

```
    <pattern>base</pattern>
    <pattern>documentation</pattern>
    <pattern>fips</pattern>
    <pattern>gateway_server</pattern>
    <pattern>ofed</pattern>
    <pattern>printing</pattern>
    <pattern>sap_server</pattern>
    <pattern>x11</pattern>
    <pattern>#server-settings.node.fileserver#</pattern>
    <pattern>#server-settings.node.lampserver#</pattern>
    <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Klicken Sie auf **Speichern**, um die Dateien miteinander zu verknüpfen und die Änderungen in der Unattend-Datei zu speichern.

Schritt 5. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepassten Konfigurationseinstellungen und Unattend-Dateien enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Basic`).
3. Klicken Sie auf das **Erstellen**-Symbol ( ), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein, z. B. `Custom SLES mit optionalen Paketen`.
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Zugeordnete Unattend- und Konfigurationseinstellungsdateien** für den Anpassungstyp aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Klicken Sie auf der Registerkarte **Software** auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Unattend-Dateien** die Unattend-Datei aus (z. B. `SLES_installPackages_customUnattend.xml`) und klicken Sie auf **Weiter**.

   Die zugeordnete Konfigurationseinstellungsdatei wird automatisch ausgewählt.
8. Klicken Sie auf der Registerkarte **Installationsskripts** auf **Weiter**.
9. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
10. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 6. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.

c. Wählen Sie das angepasste BS-Image-Profil (z. B. *<Basis_BS>*|*<Zeitstempel>*`_Custom SLES mit optionalen Paketen`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

   Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.

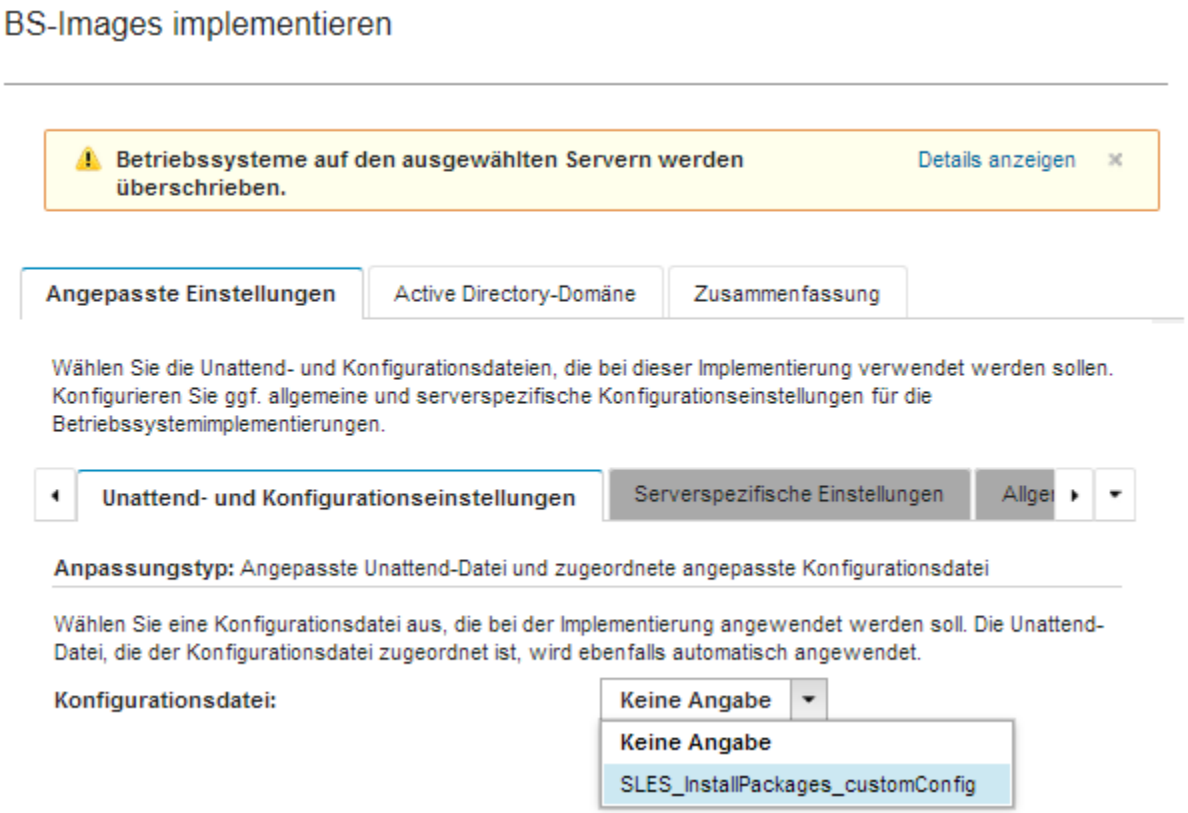
d. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

   Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystemimplementierung ausgewählt wurde) vom verwalteten Server.

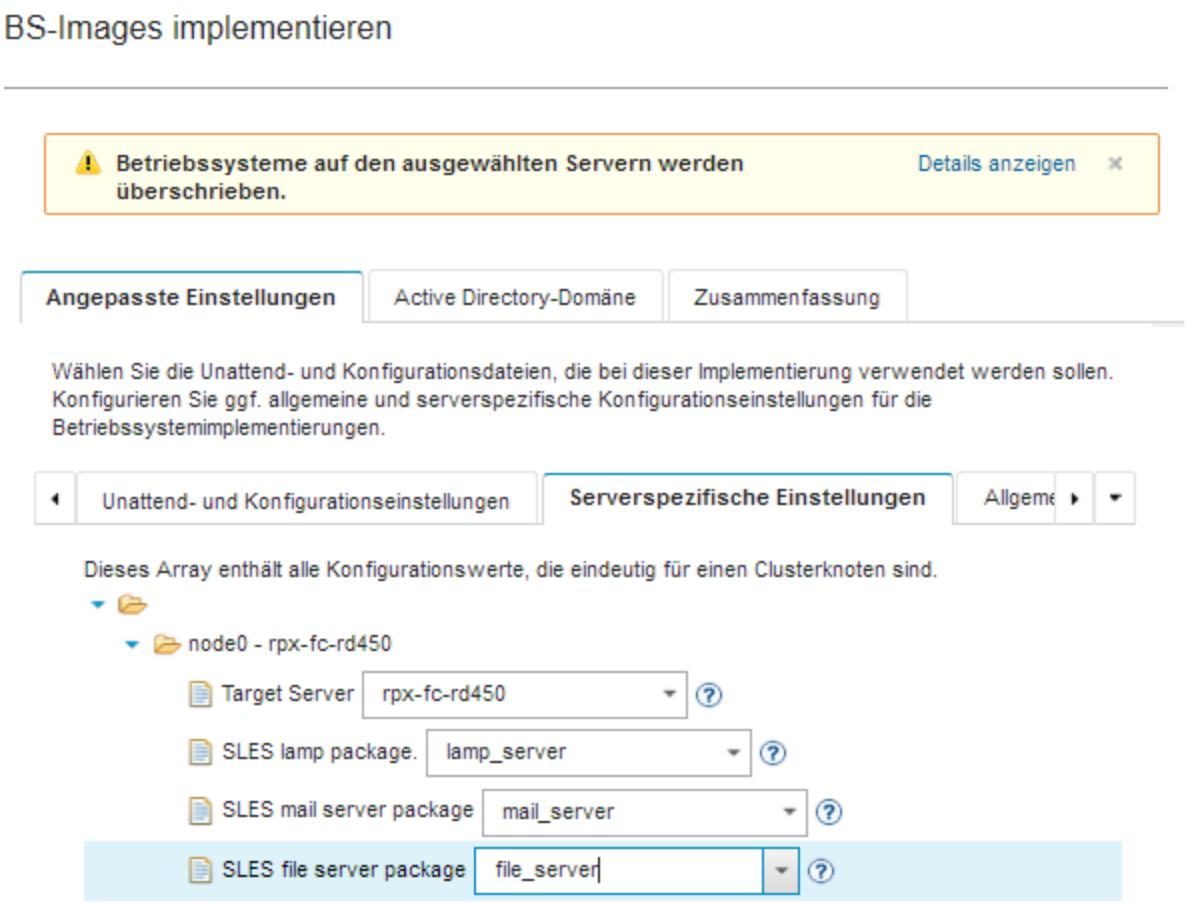
e. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.

3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Klicken Sie auf der Registerkarte **Angepasste Einstellungen** auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Konfigurationseinstellungsdatei aus (z. B. `SLES_installPackages_customConfig`).

   Anmerkung: Die zugeordnete angepasste Unattend-Datei wird automatisch ausgewählt.



5. Wählen Sie auf der Unterregisterkarte **Serverspezifische Einstellungen** den Zielserver und die optionalen SLES-Pakete aus, die Sie implementieren möchten.



6. Wählen Sie auf der Unterregisterkarte **Allgemeine Einstellungen** die Zeitzone aus, die für alle Zielserver eingestellt werden soll.

7. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
8. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

SLES 12 SP3 mit angepasster Software implementieren

In diesem Szenario wird das SLES 12 SP3 Betriebssystem zusammen mit angepasster Software (Java und Eclipse IDE) installiert. Es wird ein angepasstes Profil verwendet, das die angepasste Software und Nach-Installationsskripts zum Installieren und Konfigurieren der angepassten Software enthält. Die angepassten Softwarepakete werden während der Implementierung auf den Host kopiert und für die Verwendung durch das angepasste Nach-Installationsskript verfügbar gemacht.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- jre-8u151-linux-x64.tar.gz. Dies ist die Installationsdatei für Java für Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz Dies ist die Installationsdatei für Eclipse IDE.
- SLES_installSoftware_customScript.sh Dieses Nach-Installationsskript erstellt einen Benutzer zum Starten von Eclipse und installiert Eclipse IDE und Java.

Anmerkungen:

- SLES-Installationsskripten können eines der folgenden Formate aufweisen: Bash (.sh), Perl (.pm oder .pl), Python (.py)
- Softwaredateien und Installationsskripts werden über den angepassten Daten- und Dateipfad installiert, den Sie während der Bereitstellung angeben. Der Standardpfad für angepasste Daten und Dateien ist `/home/lxca`.
- Für SLES 12 SP3 benötigt die Eclipse IDE den GCC-Compiler, der im vordefinierten Basisprofil enthalten ist. In diesem Szenario wird ein angepasstes BS-Image-Profil mit dem vordefinierten Basisprofil erstellt. Wenn Sie ein anderes Profil verwenden möchten, müssen Sie sicherstellen, dass das Profil den GCC Compiler enthält.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um SLES 12 SP3 mit angepasster Software zu implementieren.

Schritt 1. Laden Sie das SLES 12 SP3-Basisbetriebssystem von der SUSE-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um das zu importierende SLES 12 SP3-Image zu suchen und auszuwählen (z. B. `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Laden Sie die angepasste Software auf das lokale System herunter und importieren Sie die Dateien in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Software importieren.

1. Klicken Sie auf die Registerkarte **Software**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.

4. Wählen Sie SLES für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Softwaredatei zu suchen und auszuwählen (z. B. jre-8u151-linux-x64.tar.gz).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.
7. Klicken Sie erneut auf das Symbol **Importieren** ( ).
8. Klicken Sie auf **Lokaler Import**.
9. Wählen Sie SLES für das Betriebssystem aus.
10. Klicken Sie auf **Durchsuchen**, um die zu importierende Softwaredatei zu suchen und auszuwählen (z. B. eclipse-4.6.3-3.1.x86_64.tar.gz).
11. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 3. Erstellen Sie ein angepasstes Nach-Installationsskript und importieren Sie die Datei in das BS-images-Repository.

Fügen Sie dieser Datei Befehle zum Erstellen eines Benutzers hinzu, um Eclipse zu starten, z. B.:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "PasswOrd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Fügen Sie Befehle zum Installieren der Software hinzu, z. B.:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Beachten Sie, dass diese Befehle vordefinierte Makros für die HTTPS-URL verwenden, die XClarity Administrator für Statusmeldungen (**predefined.otherSettings.statusSettings.urlStatus**) für den Ordner mit den Zertifikaten, die beim ersten Start für den Zugriff auf den urlStatus-Webdienst vom Hostbetriebssystem benötigt werden (**predefined.otherSettings.statusSettings.certLocation**) und für den Pfad zu den extrahierten Daten- und Softwaredateien (**predefined.otherSettings.deployDataAndSoftwareLocation**) verwendet.

Sie können auch Befehle zum Senden von angepassten Nachrichten an das Jobprotokoll in XClarity Administrator hinzufügen, wie in der Beispieldatei dargestellt. Siehe Angepasste Statusmeldungen zu Installationsskripts hinzufügen für weitere Informationen.

Gehen Sie wie folgt vor, um das angepasste Installationsskript zu importieren. Weitere Informationen finden Sie unter Angepasste Installationsskripts importieren.

1. Klicken Sie auf die Registerkarte **Installationsskripts**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie SLES für das Betriebssystem aus.

5. Klicken Sie auf **Durchsuchen** und wählen Sie das zu importierende Nach-Installationsskript aus (z. B. `SLES_installSoftware_customScript.sh`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 4. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepasste Software und das Nach-Installationsskript enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Basic`).
3. Klicken Sie auf das **Erstellen**-Symbol ( ), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein, z. B. `Angepasste SLES mit Software`.
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Keine** als Anpassungstyp aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Wählen Sie auf der Registerkarte **Software** die Installationsdateien der Software aus (z. B. `jre-8u151-linux-x64.tar.gz` und `eclipse-4.6.3-3.1.x86_64.tar.gz`) und klicken Sie auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Installationsskripts** die Installationsskripts aus (z. B. `SLES_installSoftware_customScript.sh`) und klicken Sie auf **Weiter**.
8. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
9. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 5. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. *<Basis_BS>*|*<Zeitstempel>*`_Angepasste SLES mit Software`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystemimplementierung ausgewählt wurde) vom verwalteten Server.
   e. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.

3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
5. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

SLES 12 SP3 mit einem konfigurierbaren Gebietsschema und NTP-Servern implementieren

In diesem Szenario wird das SLES 12 SP3 Betriebssystem installiert, mit entweder Englisch, Brasilianisch oder Japanisch aktiviert für die Tastatur- und Betriebssystemeinstellungen. Außerdem wird die IP-Adresse für bis zu drei NTP-Server konfiguriert. Es wird ein benutzerdefiniertes BS-Image-Profil verwendet, das eine Unattend-Datei (mit vordefinierten und benutzerdefinierten Makros) und eine Konfigurationseinstellungsdatei zur Auswahl der Gebietsschemata und NTP-Servereinstellungen enthält. Dieses angepasste Profil kann auf der Seite „BS-Images implementieren“ ausgewählt werden. Dann können die Gebietsschemata und NTP-Server-Einstellungen auf der Registerkarte **Angepasste Einstellungen** ausgewählt werden. Die angegebenen Werte werden durch die angepassten Makros in der angepassten Unattend-Datei ersetzt und das SLES-AutoYaST-Installationsprogramm verwendet die Werte in der Unattend-Datei, um das Betriebssystem zu konfigurieren.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- SLES_locale_customConfig.json. Diese angepasste Konfigurationsdatei fragt die Sprache ab, die für das Betriebssystem-Gebietsschema und die Tastatur für SLES und für den NTP-Server installiert werden soll.
- SLES_locale_customUnattend.xml. Diese angepasste Unattend-Datei verwendet Werte in angepassten Makros, die in der Konfigurationsdatei definiert sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um SLES 12 SP3 mithilfe eines angepassten BS-Image-Profils zu implementieren.

Schritt 1. Laden Sie das SLES-Basisbetriebssystem von der SUSE-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um das zu importierende SLES 12 SP3-Image zu suchen und auszuwählen (z. B. `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist.

Schritt 2. Erstellen Sie eine angepasste Konfigurationseinstellungsdatei und importieren Sie die Datei in das BS-Images-Repository.

Die Konfigurationseinstellungsdatei ist eine JSON-Datei, die die Daten beschreibt, die während des BS-Implementierungsprozesses dynamisch gesammelt werden müssen. Für dieses Szenario möchten wir das Betriebssystem-Gebietsschema (en_US, ja_JP, pt_BR), das Tastatur-Gebietsschema (english-us, Japanese oder portugese-br) und bis zu drei NTP-Server-IP-Adressen

angeben, die für jede BS-Bereitstellung verwendet werden sollen. Weitere Informationen zum Erstellen von Konfigurationseinstellungsdateien finden Sie unter Angepasste Makros.

Um die Datei mit den Konfigurationseinstellungen zu importieren, führen Sie diese Schritte aus. Weitere Informationen finden Sie unter Angepasste Konfigurationseinstellungen importieren.

1. Klicken Sie auf die Registerkarte **Konfigurationsdateien**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `SLES` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Konfigurationseinstellungsdatei zu suchen und auszuwählen (z. B. `SLES_locale_customConfig.json`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

   Anmerkung: Wenn Sie eine angepasste Konfigurationseinstellungsdatei importieren, generiert XClarity Administrator angepasste Makros für jede Einstellung in der Datei. Sie können diese Makros zur Unattend-Datei hinzufügen. Während der BS-Implementierung werden die Makros durch aktuelle Werte ersetzt.

Schritt 3. Ändern Sie die SLES-Unattend-Datei, um dynamische Werte für das Betriebssystem-Gebietsschema, das Tastatur-Gebietsschema und die IP-Adresse der NTP-Server Pakete anzugeben und importieren Sie dann die angepasste Datei in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren.

Fügen Sie direkt nach dem <profile>-Tag die NTP-Server- und Netzwerkinformationen hinzu. Das folgende Beispiel enthält Tags für zwei NTP-Server. Die IP-Adressen werden in einem späteren Schritt als Makros hinzugefügt.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

Fügen Sie im Abschnitt <general> das BS- und Tastatur-Gebietsschema hinzu, wie im folgenden Beispiel dargestellt. Die Ländereinstellungen für Tastatur und Betriebssystem werden in einem späteren Schritt als Makros hinzugefügt.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Anmerkung: Bei der Verwendung einer angepassten Unattend-Datei bietet XClarity Administrator einige der normalen Komfortfunktionen nicht, die Sie haben, wenn Sie eine vordefinierte Unattend-

Datei verwenden würden. Zum Beispiel müssen **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** und **<UserAccounts>** für Administrator, **<Interfaces>** für Netzwerk und die **<package>**-Liste für Installationsfunktionen in der angepassten Unattend-Datei angegeben werden, die hochgeladen wird.

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `SLES` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Unattend-Datei zu suchen und auszuwählen (z. B. `SLES_locale_customUnattend.xml`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 4. Verknüpfen Sie die angepasste Unattend-Datei mit der angepassten Konfigurationseinstellungsdatei und fügen Sie der Unattend-Datei die erforderlichen vordefinierten und angepassten Makros (Einstellungen) aus der Konfigurationseinstellungsdatei hinzu. Weitere Informationen finden Sie unter Unattend-Datei einer Konfigurationseinstellungsdatei zuordnen und Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei.

Tipp: Optional können Sie die angepasste Unattend-Datei der angepassten Datei mit den Konfigurationseinstellungen zuordnen und Makros hinzufügen, wenn Sie die Unattend-Datei importieren.

1. Wählen Sie auf der Registerkarte **Unattend-Dateien** die angepasste Unattend-Datei aus (z. B. `SLES_locale_customUnattend.xml`).
2. Klicken Sie auf das Symbol **Konfigurationsdatei zuordnen** (), um das Dialogfeld „Unattend-Datei zuordnen“ anzuzeigen.
3. Wählen Sie die Konfigurationseinstellungsdatei aus, die Sie mit der Unattend-Datei verknüpfen möchten (z. B. `SLES_locale_customConfig`).
4. Fügen Sie der Unattend-Datei die erforderlichen vordefinierten Makros hinzu.
   a. Wählen Sie **Vordefiniert** aus der Dropdown-Liste **Verfügbare Makros** aus.
   b. Positionieren Sie den Cursor in der Unattend-Datei irgendwo nach Zeile 1 (nach dem **<xml>**-Tag).
   c. Erweitern Sie die Liste **predefined → unattendSettings** in der Liste der verfügbaren vordefinierten Makros.
   d. Klicken Sie auf die Makros **preinstallConfig** und **postinstallConfig**, um die Makros hinzuzufügen.

   Beispiele:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Fügen Sie das angepasste Makro zur Angabe des Betriebssystem-Gebietsschemas hinzu.
   a. Wählen Sie **Custom** aus der Dropdown-Liste **Verfügbare Makros** aus.
   b. Positionieren Sie den Cursor hinter dem **<language>**-Tag.
   c. Erweitern Sie **server-settings → node** in der Liste der verfügbaren angepassten Makros und klicken Sie dann auf **locale**, um das OS-Gebietsschema-Makro hinzuzufügen.

Beispiele:

```
<language>#server-settings.node.locale#</language>
```

6. Fügen Sie das angepasste Makro zur Angabe des Tastatur-Gebietsschemas hinzu.
   a. Positionieren Sie den Cursor hinter dem **<keymap>**-Tag.
   b. Erweitern Sie **server-settings → node** in der Liste der verfügbaren angepassten Makros und klicken Sie dann auf **keyboardLocale**, um das Tastatur-Gebietsschema-Makro hinzuzufügen.

   Beispiele:

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Fügen Sie das angepasste Makro für die Angabe der IP-Adressen der NTP-Server hinzu.

   In diesem Szenario verwendet die angepasste Datei mit den Konfigurationseinstellungen eine Vorlage, um null bis drei NTP-Server anzugeben. Bei Verwendung von Vorlagen in der Datei mit den Konfigurationseinstellungen werden Makros, die der Vorlage zugeordnet sind, im Dialogfeld „Unattend-Datei zuordnen“ nicht angezeigt. Stattdessen müssen Sie die Unattend-Datei manuell bearbeiten und die Makros und die entsprechenden Tags hinzufügen.

   Um beispielsweise drei NTP-Server einzubeziehen, würden Sie der Unattend-Datei die folgenden Tags und Makros hinzufügen. Diese Tags und Makros sind in der Unattend-Beispieldatei für dieses Szenario bereits vorhanden.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address>#server-settings.ntpserver1#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver2#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver3#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
    <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Klicken Sie auf **Zuordnen**, um die Dateien miteinander zu verknüpfen und die Änderungen in der Unattend-Datei zu speichern.

Schritt 5. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepassten Konfigurationseinstellungen und Unattend-Dateien enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Basic`).

3. Klicken Sie auf das **Erstellen**-Symbol ( ), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. `Angepasstes SLES für BS und Tastatur-Gebietsschema und NTP-Server`).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Zugeordnete Unattend- und Konfigurationseinstellungsdateien** für den Anpassungstyp aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Klicken Sie auf der Registerkarte **Software** auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Unattend-Dateien** die Unattend-Datei aus (z. B. `SLES_locale_customUnattend.xml`) und klicken Sie auf **Weiter**.

   Die zugeordnete Konfigurationseinstellungsdatei wird automatisch ausgewählt.
8. Klicken Sie auf der Registerkarte **Installationsskripts** auf **Weiter**.
9. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
10. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 6. Implementieren Sie das angepasste BS-Image-Profil auf dem Zielserver. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

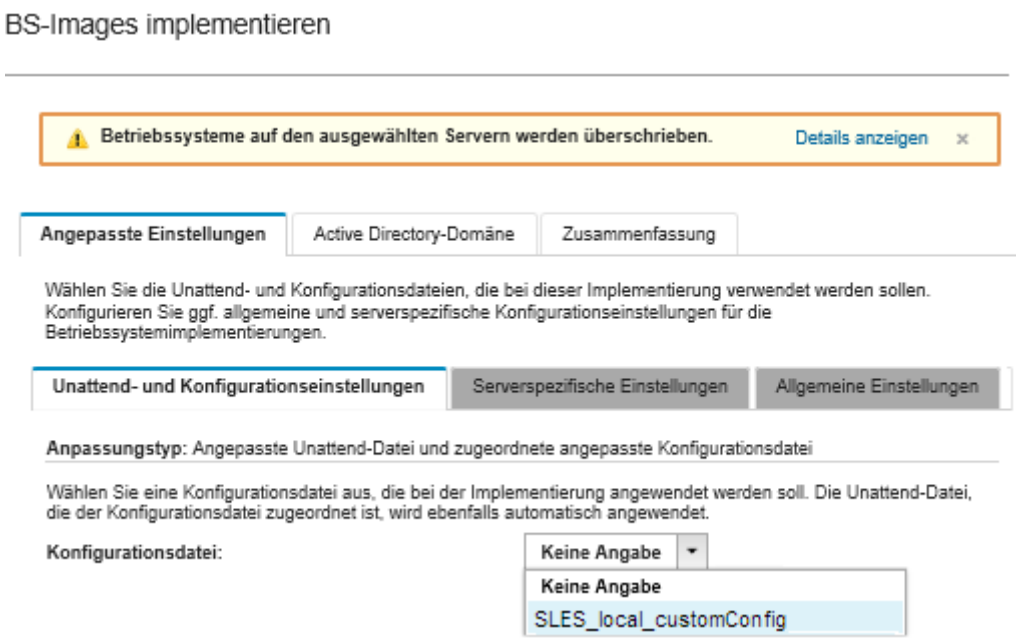
      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. <*Basis_BS*>|<*Zeitstempel*>_`Angepasstes SLES für BS und Tastatur-Gebietsschema und NTP-Server`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom verwalteten Server.
   e. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.
3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** ( ), um die Betriebssystemimplementierung einzuleiten.

4. Klicken Sie auf der Registerkarte **Angepasste Einstellungen** auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Konfigurationseinstellungsdatei aus (z. B. `SLES_locale_customConfig`).

   Anmerkung: Die zugeordnete angepasste Unattend-Datei wird automatisch ausgewählt.



5. Wählen Sie auf der Unterregisterkarte **Serverspezifische Einstellungen** den Zielserver, das BS-Gebietsschema und das Tastatur-Gebietsschema aus.
6. Klicken Sie auf der Unterregisterkarte **Allgemeine Einstellungen** auf **Hinzufügen**, um die IP-Adresse von bis zu drei NTP-Servern anzugeben.
7. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
8. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

VMware ESXi v6.7 mit Lenovo Customization über eine statische IP-Adresse auf einer lokalen Festplatte implementieren

In diesem Szenario wird VMware ESXi v6.7 mit Lenovo Customization über die statische IP-Adresse des Hostservers auf der lokalen Festplatten installiert. Es wird ein angepasstes BS-Image-Profil verwendet, das eine Unattend-Datei mit vordefinierten Makros enthält. Dieses angepasste Profil kann auf der Seite „BS-Images implementieren“ ausgewählt werden. Bekannte Werte werden durch die vordefinierten Makros in der angepassten Unattend-Datei ersetzt und das VMware ESXi Kickstart-Installationsprogramm verwendet die Werte in der Unattend-Datei, um das Betriebssystem zu konfigurieren.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- ESXi_staticIP_customUnattend.cfg. Diese angepasste Unattend-Datei verwendet Werte in vordefinierten Makros.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um VMware ESXi v6.7 mithilfe eines angepassten BS-Image-Profils auf Servern zu implementieren.

Schritt 1. Laden Sie VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization von der VMware-Support – Downloads-Website-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um das zu importierende ESXi-Image zu suchen und auszuwählen (z. B. `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist.

Schritt 2. Bearbeiten Sie die ESXi Unattend-(Kickstart-)Datei, um die erforderlichen vordefinierten Makros und ggf. andere vordefinierte Makros hinzuzufügen, z. B. IP-Adresse, Gateway, DNS- und Hostname-Einstellungen, und importieren Sie die angepasste Datei anschließend in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren.

Nur für ESXi und RHEL bietet XClarity Administrator das Makro **#predefined.unattendSettings.networkConfig#** an, das alle Netzwerkeinstellungen hinzufügt, die auf der Benutzeroberfläche für die Unattend-Datei definiert sind. Da in diesem Beispiel eine Einstellung (**--addvmportgroup**) festgelegt wird, die nicht in der Benutzeroberfläche definiert ist, wird das Makro **#predefinedunattendSettings.storageConfig#** nicht in der Beispiel-Unattend-Datei verwendet. Stattdessen werden Netzwerkeinstellungen einzeln zur Datei hinzugefügt und es werden die Makros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#** verwendet.

XClarity Administrator bietet nur für ESXi und RHEL zudem das Makro **#predefined.unattendSettings.storageConfig#** an, das alle Speichereinstellungen hinzufügt, die auf der Benutzeroberfläche für die Unattend-Datei definiert sind. Da in diesem Beispiel Einstellungen (**--novmfsondisk** und **–ignoressd**) festgelegt werden, die nicht in der Benutzeroberfläche definiert sind, wird das Makro **#predefinedunattendSettings.storageConfig#** nicht in der Beispiel-Unattend-Datei verwendet. Stattdessen werden die Speichereinstellungen einzeln hinzugefügt und **--firstdisk=local** ist fest in der Datei codiert.

Anmerkung: XClarity Administrator bietet einige grundlegende Komfortmakros, z. B. OOB-Treiberinjektion, Statusmeldungen, Nach-Installationsskripts und angepasste Software. Zur Verwendung dieser vordefinierten Makros müssen Sie jedoch die folgenden Makros in der angepassten Unattend-Datei angeben. Die Beispieldatei enthält bereits die benötigten Makros. Beachten Sie, dass die Reihenfolge der vordefinierten Makros aufgrund des enthaltenen % firstboot-Abschnitts wichtig ist. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

Die Beispieldatei enthält bereits die erforderlichen Makros und zusätzliche vordefinierte Makros für die dynamische Eingabe der Netzwerkeinstellungen beim Zielserver. Weitere Informationen zum Hinzufügen von Makros zu Unattend.Dateien finden Sie unter Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei.

Weitere Informationen über die verfügbaren vordefinierten Makros finden Sie unter Vordefinierte Makros.

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `ESXi` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Unattend-Datei zu suchen und auszuwählen (z. B. `ESXi_staticIP_customUnattend.cfg`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 3. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepasste Unattend-Datei enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Virtualization`).
3. Klicken Sie auf das **Erstellen**-Symbol (), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. `ESXi angepasst mit statischer IP`).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie für den Anpassungstyp **Nur Unattend-Dateien** aus.
   d. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Registerkarte **Unattend-Dateien** die Unattend-Datei aus (z. B. `ESXi_staticIP_customUnattend.cfg`) und klicken Sie auf **Weiter**.
6. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
7. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 4. Implementieren Sie das angepasste BS-Image-Profil auf dem Zielserver. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp:

      - VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
      - Die Netzwerkeinstellungen, die Sie im Dialogfeld „Netzwerkeinstellungen“ angeben, werden bei der Ausführung mithilfe der Makros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#** zur Unattend-Datei hinzugefügt.

   c. Wählen Sie das angepasste BS-Image-Profil (z. B. <*Basis_BS*>|<*Zeitstempel*>`_ESXi angepasst mit statischer IP`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

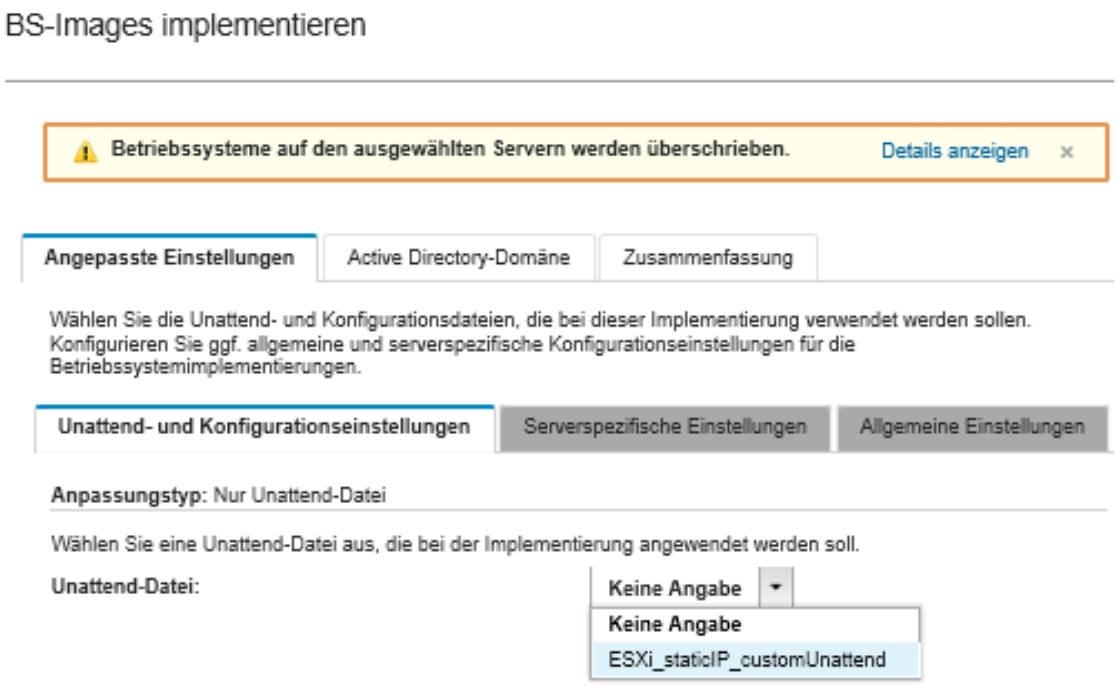
      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.

d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** ( ) und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.

e. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.

Anmerkung: Da **--firstdisk=local** in der Unattend-Datei festgelegt ist, müssen Sie keine bevorzugte Speicherposition in der Spalte **Speicher** angeben. Die Einstellung in der Benutzeroberfläche wird ignoriert.

3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** ( ), um die Betriebssystemimplementierung einzuleiten.
4. Klicken Sie auf der Registerkarte **Angepasste Einstellungen** auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Unattend-Datei aus (z. B. `ESXi_staticIP_customUnattend.cfg`).



5. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
6. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

VMware ESXi v6.7 mit Lenovo Customization mit konfigurierbarem Gebietsschema und Anmeldeinformationen für einen zweiten Benutzer implementieren

In diesem Szenario wird VMware ESXi v6.7 mit Lenovo Customization mit einer konfigurierbaren Sprache für das Tastatur-Gebietsschema und Anmeldeinformationen für einen zweiten ESXi-Benutzer installiert. In diesem Beispiel werden zudem grundlegende Netzwerk- und Speichereinstellungen verwendet, die auf der Benutzeroberfläche definiert sind. Es wird ein angepasstes BS-Image-Profil verwendet, das eine Unattend-Datei (mit vordefinierten und angepassten Makros) und eine Konfigurationseinstellungsdatei zur Auswahl des Kennworts enthält. Dieses angepasste Profil kann auf der Seite „BS-Images implementieren“ ausgewählt werden. Anschließend kann das Kennwort in der Registerkarte **Angepasste Einstellungen** festgelegt werden. Der angegebene Wert wird durch das angepasste Makro in der angepassten Unattend-Datei ersetzt und das ESXi-Installationsprogramm verwendet diese Werte in der Unattend-Datei, um das Betriebssystem zu konfigurieren.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- ESXi_locale_customConfig.json. Diese angepasste Konfigurationsdatei fragt die Sprache für das Tastatur-Gebietsschema und die Anmeldeinformationen für den zweiten ESXi-Benutzer ab.
- ESXi_locale_customUnattend.cfg. Diese angepasste Unattend-Datei verwendet Werte in vordefinierten und angepassten Makros, die in der Konfigurationsdatei definiert sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um VMware ESXi v6.7 mithilfe eines angepassten BS-Image-Profils auf Servern zu implementieren.

Schritt 1. Laden Sie VMware vSphere® Hypervisor (ESXi) mit Lenovo Customization von der VMware-Support – Downloads-Website-Website auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ( ).
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen**, um das zu importierende ESXi-Image zu suchen und auszuwählen (z. B. `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist.

Schritt 2. Erstellen Sie eine angepasste Konfigurationseinstellungsdatei und importieren Sie die Datei in das BS-Images-Repository.

Die Konfigurationseinstellungsdatei ist eine JSON-Datei, die die Daten beschreibt, die während des BS-Implementierungsprozesses dynamisch gesammelt werden müssen. In diesem Szenario möchten wir das Tastatur-Gebietsschema und Benutzer-ID und Kennwort für einen zweiten ESXi-Benutzer für jede BS-Implementierung implementieren. Weitere Informationen zum Erstellen von Konfigurationseinstellungsdateien finden Sie unter Angepasste Makros.

Um die Datei mit den Konfigurationseinstellungen zu importieren, führen Sie diese Schritte aus. Weitere Informationen finden Sie unter Angepasste Konfigurationseinstellungen importieren.

1. Klicken Sie auf die Registerkarte **Konfigurationsdateien**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `ESXi` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Konfigurationseinstellungsdatei zu suchen und auszuwählen (z. B. `ESXi_locale_customConfig.json`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

   Anmerkung: Wenn Sie eine angepasste Konfigurationseinstellungsdatei importieren, generiert XClarity Administrator angepasste Makros für jede Einstellung in der Datei. Sie können diese Makros zur Unattend-Datei hinzufügen. Während der BS-Implementierung werden die Makros durch aktuelle Werte ersetzt.

Schritt 3. Ändern Sie die ESXi-Unattend-(Kickstart-)Datei, um das Betriebssystem- und Tastatur-Gebietsschema und Anmeldeinformationen für den zweiten ESXi-Benutzer anzugeben, und importieren Sie dann die angepasste Datei in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren.

Geben Sie Befehle zum Festlegen des Tastatur-Gebietsschemas an, z. B.:

```
# Set the keyboard locale
keyboard ''
```

Geben Sie Befehle zum Erstellen eines zweiten ESXi-Benutzers an. Im folgenden Beispiel werden *<user_id>* und *<password>* im nächsten Schritt mit angepassten Makros ersetzt.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das **Importieren**-Symbol ( ).
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `ESXi` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Unattend-Datei zu suchen und auszuwählen (z. B. `ESXi_locale_customUnattend.cfg`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 4. Verknüpfen Sie die angepasste Unattend-Datei mit der angepassten Konfigurationseinstellungsdatei und fügen Sie der Unattend-Datei die erforderlichen vordefinierten und angepassten Makros (Einstellungen) aus der Konfigurationseinstellungsdatei hinzu. Weitere Informationen finden Sie unter Unattend-Datei einer Konfigurationseinstellungsdatei zuordnen und Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei.

Tipp:

- Optional können Sie die angepasste Unattend-Datei der angepassten Datei mit den Konfigurationseinstellungen zuordnen und Makros hinzufügen, wenn Sie die Unattend-Datei importieren.
- XClarity Administrator bietet einige grundlegende Komfortmakros, z. B. OOB-Treiberinjektion, Statusmeldungen, Nach-Installationsskripts und angepasste Software. Zur Verwendung dieser vordefinierten Makros müssen Sie jedoch die folgenden Makros in der angepassten Unattend-Datei angeben. Die Beispieldatei enthält bereits die benötigten Makros. Beachten Sie, dass die Reihenfolge der vordefinierten Makros aufgrund des enthaltenen %firstboot-Abschnitts wichtig ist. Weitere Informationen finden Sie unter Angepasste Unattend-Dateien importieren.
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- XClarity Administrator bietet auch Makros, die alle Netzwerk- und Speicherpositionseinstellungen einfügen, die in der Benutzeroberfläche definiert sind. Diese Makros sind hilfreich, wenn für die Bereitstellung nur Standardeinstellungen erforderlich sind. Die Beispieldatei enthält bereits die benötigten Makros.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

Weitere Informationen zum Hinzufügen von Makros zu Unattend.Dateien finden Sie unter Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei. Weitere Informationen über die verfügbaren vordefinierten Makros finden Sie unter Vordefinierte Makros.

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei der angepassten Konfigurationseinstellungsdatei zuzuordnen.

1. Wählen Sie auf der Registerkarte **Unattend-Dateien** die angepasste Unattend-Datei aus (z. B. `ESXi_locale_customUnattend.cfg`).
2. Klicken Sie auf das Symbol **Konfigurationsdatei zuordnen** (), um das Dialogfeld „Unattend-Datei zuordnen“ anzuzeigen.
3. Wählen Sie die Konfigurationseinstellungsdatei aus, die Sie mit der Unattend-Datei verknüpfen möchten (z. B. `ESXi_locale_customConfig`).
4. Wählen Sie **Custom** aus der Dropdown-Liste **Verfügbare Makros** aus.
5. Fügen Sie das angepasste Makro zum Festlegen des Tastatur-Gebietsschemas hinzu, indem Sie den Cursor zwischen den einzelnen Anführungszeichen nach „Tastatur“ platzieren und dann auf **keyboard_locale** klicken.

   Beispiele:

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```

6. Fügen Sie das angepasste Makro zum Festlegen der ID des zweiten Benutzers hinzu, indem Sie den Cursor an jeder Position platzieren, an der Sie die Benutzer-ID einfügen möchten, und dann auf **second_user_id** klicken. Ersetzen Sie jedes Vorkommen von *<user_id>* in der Beispieldatei mit dem angepassten Makro.

   Beispiele:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

7. Fügen Sie das angepasste Makro zum Festlegen des Kennworts des zweiten Benutzers hinzu, indem Sie den Cursor an der Position platzieren, an der Sie das Kennwort einfügen möchten, und dann auf **second_user_password** klicken. Ersetzen Sie *<password>* in der Beispieldatei mit dem angepassten Makro.

   Beispiele:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

8. Klicken Sie auf **Zuordnen**, um die Dateien miteinander zu verknüpfen und die Änderungen in der Unattend-Datei zu speichern.

Schritt 5. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepassten Konfigurationseinstellungen und Unattend-Dateien enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Virtualization`).
3. Klicken Sie auf das **Erstellen**-Symbol (), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. `ESXi angepasst mit angepasstem Gebietsschema und Anmeldeinformationen für zweiten Benutzer`).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Zugeordnete Unattend- und Konfigurationseinstellungsdateien** für den Anpassungstyp aus.

d. Klicken Sie auf **Weiter**.

5. Wählen Sie auf der Registerkarte **Unattend-Dateien** die Unattend-Datei aus (z. B. `ESXi_locale_customUnattend.cfg`) und klicken Sie auf **Weiter**.

   Die zugeordnete Konfigurationseinstellungsdatei wird automatisch ausgewählt.

6. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
7. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 6. Implementieren Sie das angepasste BS-Image-Profil auf dem Zielserver. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp:

      - VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
      - Die Netzwerkeinstellungen, die Sie im Dialogfeld „Netzwerkeinstellungen“ angeben, werden bei der Ausführung mithilfe des Makros **#predefined.hostPlatforms.networkConfig#** zur Unattend-Datei hinzugefügt.

   c. Wählen Sie das angepasste BS-Image-Profil (z. B. <*Basis_BS*>|<*Zeitstempel*>`_ESXi angepasst mit angepasstem Gebietsschema und Anmeldeinformationen für zweiten Benutzer`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.

   d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** () und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.
   e. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

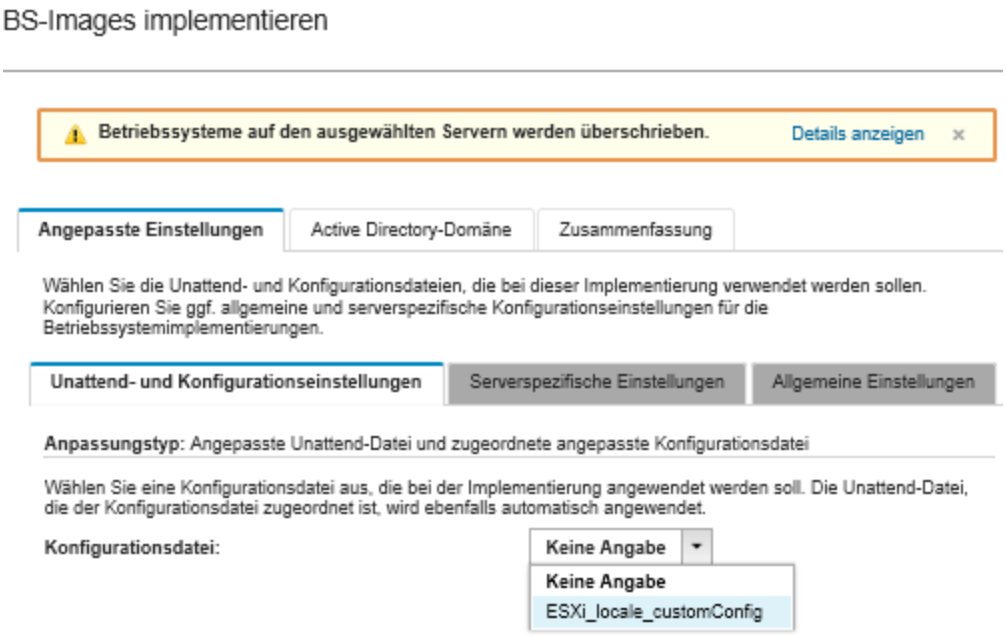
      Anmerkungen:

      - Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom verwalteten Server.
      - Die Speichereinstellungen, die Sie im Dialogfeld „Speichereinstellungen“ angeben, werden bei der Ausführung mithilfe des Makros **#predefined.hostPlatforms.storageConfig#** zur Unattend-Datei hinzugefügt.

   f. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.

3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Klicken Sie auf der Registerkarte **Angepasste Einstellungen** auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Konfigurationseinstellungsdatei aus (z. B. `ESXi_locale_customConfig`).

Anmerkung: Die zugeordnete angepasste Unattend-Datei wird automatisch ausgewählt.



5. Wählen Sie auf der Unterregisterkarte **Serverspezifische Einstellungen** das Tastatur-Gebietsschema und die Anmeldeinformationen für den zweiten ESXi-Benutzer aus.
6. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
7. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

Windows 2016 mit angepassten Funktionen implementieren

In diesem Szenario werden das Betriebssystem Windows 2016 und verschiedene zusätzliche Funktionen installiert. Es wird ein angepasstes Profil verwendet, das eine angepasste Unattend-Datei enthält. Das angepasste Profil kann dann auf der Seite „BS-Images implementieren“ ausgewählt werden.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- Windows_installFeatures_customUnattend.xml. Diese angepassten Unattend-Datei installiert die WindowsMediaPlayer- und BitLocker-Funktionen und verwendet vordefinierte Makros für dynamische Werte.

Vorgehensweise

Gehen Sie wie folgt vor, um Windows 2016 mit angepassten Funktionen zu implementieren.

Schritt 1. Laden Sie das japanische Windows 2016-Betriebssystem auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ( ).
4. Klicken Sie auf **Lokaler Import**.

5. Klicken Sie auf **Durchsuchen** und wählen Sie das BS-Image aus, die Sie importieren möchten (z. B. `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Laden Sie die Paketdatei für Windows 2016 auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Einheitentreiber importieren

Die Paketdatei enthält die neuesten Einheitentreiber und WinPE-Boot-Dateien, die Sie Ihren angepassten BS-Image-Profilen hinzufügen können. In diesem Szenario wird eine angepasste Boot-Datei verwendet, sodass die Boot-Datei im Paket nicht verwendet wird.

1. Klicken Sie auf die Registerkarte **Treiberdateien**.
2. Klicken Sie auf **Downloads → Windows Paketdateien**, um auf die Lenovo Unterstützungswebseite zu gehen und laden Sie die Paketdatei für Windows 2016 auf das lokale System herunter.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das BS-Image aus, das Sie importieren möchten (z. B. `bundle_win2016_20180126130051.zip`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 3. Ändern Sie die Windows Unattend-Datei, um zusätzliche Funktionen zu installieren (z. B. WindowsMediaPlayer und BitLocker), und importieren Sie die angepasste Datei in das BS-Images-Repository.

Fügen Sie im Abschnitt „Wartung“ der Windows-Unattend-Datei die zu installierenden Funktionen hinzu, z. B.

```
<servicing>
   <package action="configure">
      <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
                        processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
                        language=""></assemblyIdentity>
      <selection name="Microsoft-Hyper-V" state="true"></selection>
      <selection name="MultipathIo" state="true"></selection>
      <selection name="FailoverCluster-PowerShell" state="true"></selection>
      <selection name="FailoverCluster-FullServer" state="true"></selection>
      <selection name="FailoverCluster-CmdInterface" state="true"></selection>
      <selection name="FailoverCluster-AutomationServer" state="true"></selection>
      <selection name="FailoverCluster-AdminPak" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
      <selection name="ServerManager-Core-RSAT" state="true"></selection>
      <selection name="WindowsMediaPlayer" state="true"></selection>
      <selection name="BitLocker" state="true"></selection>
   </package>
</servicing>
```

Anmerkungen:

- Diese Tags befinden sich in der Unattend-Beispieldatei.
- Bei der Verwendung einer angepassten Unattend-Datei bietet XClarity Administrator einige der normalen Komfortfunktionen nicht, die Sie haben, wenn Sie eine vordefinierte Unattend-Datei verwenden würden. Zum Beispiel müssen die Ziele `<DiskConfiguration>`, `<ImageInstall>`,

<ProductKey> und <UserAccounts> für den Administrator, <Interfaces> für das Netzwerk und <package>-Liste für die Installationsfunktionen in der angepassten Unattend-Datei angegeben werden, die hochgeladen wird.

Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren. Siehe Angepasste Unattend-Dateien importieren für weitere Informationen.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das Symbol **Importieren** ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie Windows für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die angepasste Unattend-Datei zu suchen und auszuwählen (z. B. Windows_installFeatures_customUnattend.xml).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

XClarity Administrator bietet einige allgemeine Komfortmakros, z. B. OOB-Treiberinjektion, Statusmeldungen, Nach-Installationsskripts und angepasste Software. Zur Verwendung dieser vordefinierten Makros müssen Sie jedoch die folgenden Makros in der angepassten Unattend-Datei angeben.

- #predefined.unattendSettings.preinstallConfig#
- #predefined.unattendSettings.postinstallConfig#

Die Beispieldatei enthält bereits den Code zum Installieren der zusätzlichen Features, der erforderlichen Makros und anderer Makros, die für die dynamische Eingabe benötigt werden. Weitere Informationen zum Hinzufügen von Makros zu Unattend.Dateien finden Sie unter Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei.

Weitere Informationen über die verfügbaren vordefinierten Makros finden Sie unter Vordefinierte Makros.

Schritt 4. Erstellen Sie ein angepasstes BS-Image-Profil, das die Unattend-Datei enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie das Profil zum Anpassen aus (z. B. win2016-x86_64-install-Datacenter_Virtualization).
3. Klicken Sie auf das **Erstellen**-Symbol (), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. Windows angepasst mit Funktionen).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie für den Anpassungstyp **Nur Unattend-Dateien** aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Klicken Sie auf der Registerkarte **Boot-Optionen** auf **Weiter**. Die vordefinierte WinPE Boot-Datei ist standardmäßig ausgewählt.
7. Klicken Sie auf der Registerkarte **Software** auf **Weiter**.
8. Wählen Sie auf der Registerkarte **Unattend-Dateien** die angepasste Unattend-Datei aus (z. B. Windows_installFeatures_customUnattend.xml) und klicken Sie auf **Weiter**.
9. Klicken Sie auf der Registerkarte **Installationsskripts** auf **Weiter**.

10. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
11. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 5. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, Subnetzmaske, Gateway, DNS, MTU und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. *<Basis_BS>*|*<Zeitstempel>*`_Windows angepasst mit Funktionen`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** () und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.
   e. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom verwalteten Server.
   f. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.
3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Klicken Sie auf der Registerkarte **Angepasste Einstellungen** auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Unattend-Datei aus (z. B. `Windows_installFeatures_customUnattend.xml`).
5. (Optional) Geben Sie auf der Registerkarte **Active Directory-Domäne** die Informationen zum Verknüpfen einer Active Directory-Domäne im Rahmen einer Windows-Image-Implementierung an (siehe In Windows Active Directory integrieren
6. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
7. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

Windows 2016 mit angepasster Software implementieren

In diesem Szenario wird das Windows 2016 Betriebssystem zusammen mit angepasster Software (Java und Eclipse IDE) installiert. Es wird ein angepasstes Profil verwendet, das die angepasste Software und Nach-Installationsskripts zum Installieren und Konfigurieren der angepassten Software enthält. Die angepassten Softwarepakete werden während der Implementierung auf den Host kopiert und für die Verwendung durch das angepasste Nach-Installationsskript verfügbar gemacht.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- jre-8u151-windows-x64-with-configfile.zip. Dies ist die Installationsdatei für Java für Eclipse.
- eclipse-java-oxygen-1a-win32-x86_64.zip Dies ist die Installationsdatei für Eclipse IDE.
- Windows_installSoftware_customScript.ps1 Dieses Nach-Installationsskript erstellt einen Benutzer zum Starten von Eclipse und installiert Eclipse IDE und Java.

Anmerkungen:

- Windows-Installationsskripten können eines der folgenden Formate aufweisen: Befehlsdatei (.cmd), PowerShell (.ps1)
- Softwaredateien und Installationsskripts werden über den angepassten Daten- und Dateipfad installiert, den Sie während der Bereitstellung angeben. Der Standardpfad für angepasste Daten und Dateien ist `C:\lxca`.

Vorgehensweise

Gehen Sie wie folgt vor, um Windows 2016 mit angepasster Software zu implementieren.

Schritt 1. Laden Sie das japanische Windows 2016-Betriebssystem auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das BS-Image aus, die Sie importieren möchten (z. B. `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Laden Sie die Paketdatei für Windows 2016 auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Einheitentreiber importieren

Die Paketdatei enthält die neuesten Einheitentreiber und WinPE-Boot-Dateien, die Sie Ihren angepassten BS-Image-Profilen hinzufügen können. In diesem Szenario wird eine angepasste Boot-Datei verwendet, sodass die Boot-Datei im Paket nicht verwendet wird.

1. Klicken Sie auf die Registerkarte **Treiberdateien**.
2. Klicken Sie auf **Downloads → Windows Paketdateien**, um auf die Lenovo Unterstützungswebseite zu gehen und laden Sie die Paketdatei für Windows 2016 auf das lokale System herunter.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das BS-Image aus, das Sie importieren möchten (z. B. `bundle_win2016_20180126130051.zip`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 3. Laden Sie die angepasste Software auf das lokale System herunter und importieren Sie die Dateien in das BS-Images-Repository. Weitere Informationen finden Sie unter Angepasste Software importieren

1. Klicken Sie auf die Registerkarte **Software**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `Windows` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Konfigurationseinstellungsdatei zu suchen und auszuwählen (z. B. `jre-8u151-windows-x64-with-configfile.zip`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.
7. Klicken Sie erneut auf das Symbol **Importieren** ().
8. Klicken Sie auf **Lokaler Import**.
9. Wählen Sie `Windows` für das Betriebssystem aus.
10. Klicken Sie auf **Durchsuchen**, um die zu importierende Konfigurationseinstellungsdatei zu suchen und auszuwählen (z. B. `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 4. Erstellen Sie ein angepasstes Nach-Installationsskript und importieren Sie die Datei in das BS-images-Repository.

Fügen Sie Befehle zum Installieren der Software hinzu, z. B.:

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Beachten Sie, dass diese Befehle das vordefinierte Makro für den Pfad zu den extrahierten Daten und Softwaredateien verwenden (**predefined.otherSettings.deployDataAndSoftwareLocation**).

Sie können auch Befehle zum Senden von angepassten Nachrichten an das Jobprotokoll in XClarity Administrator hinzufügen, wie in der Beispieldatei dargestellt. Siehe Angepasste Statusmeldungen zu Installationsskripts hinzufügen für weitere Informationen.

Gehen Sie wie folgt vor, um das angepasste Installationsskript zu importieren. Weitere Informationen finden Sie unter Angepasste Installationsskripts importieren.

1. Klicken Sie auf die Registerkarte **Installationsskripts**.
2. Klicken Sie auf das **Importieren**-Symbol ().
3. Klicken Sie auf **Lokaler Import**.
4. Wählen Sie `Windows` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die zu importierende Unattend-Datei zu suchen und auszuwählen (z. B. `Windows_installSoftware_customScript.ps1`).

6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 5. Erstellen Sie ein angepasstes BS-Image-Profil, das die angepasste Unattend-Datei enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie ein BS-Profil zum Anpassen aus (z. B. `Datacenter virtualization`).
3. Klicken Sie auf das **Erstellen**-Symbol (), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein (z. B. `Windows angepasst mit Software`).
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie **Keine** als Anpassungstyp aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Klicken Sie auf der Registerkarte **Boot-Optionen** auf **Weiter**. Die vordefinierte WinPE Boot-Datei ist standardmäßig ausgewählt.
7. Wählen Sie auf der Registerkarte **Software** die Installationsdateien der Software aus (z. B. `jre-8u151-windows-x64-with-configfile.zip` und `eclipse-java-oxygen-1a-win32-x86_64.zip`) und klicken Sie auf **Weiter**.
8. Wählen Sie auf der Registerkarte **Installationsskripts** die Installationsskripts aus (z. B. `Windows_installSoftware_customScript.ps1`) und klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
10. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

Schritt 6. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, DNS-, MTU- und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. *<Basis_BS>*|*<Zeitstempel>*`_Windows angepasst mit Software`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** () und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.
   e. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystemimplementierung ausgewählt wurde) vom verwalteten Server.

f. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.

3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
5. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

Windows 2016 für Japanisch implementieren

In diesem Szenario wird das Windows 2016 Betriebssystem auf mehreren Servern mit Japanisch für die Tastatur und die Ländereinstellung des Betriebssystems installiert. Es wird ein angepasstes Profil verwendet, das eine angepasste WinPE-Boot-Datei und Unattend-Datei enthält. Das angepasste Profil kann dann auf der Seite „BS-Images implementieren“ ausgewählt werden.

Vorbereitende Schritte

In diesem Szenario werden die folgenden Beispieldateien verwendet.

- `WinPE_64_ja.zip`. Diese benutzerdefinierte Windows Boot-Datei (WinPE) installiert das japanische Gebietsschema.
- Windows_locale_customUnattend.xml. Diese angepasste Unattend-Datei verwendet die WinPE-Datei, um Japanisch zu installieren.

Anmerkungen: In der angepassten Unattend-Beispieldatei wird von Folgendem ausgegangen:

- Der Server hat nur eine sichtbare Festplatte (Festplatte 0) und noch keine Systempartition.
- Der statische IPv4-Modus wird verwendet und legt eine statische IP-Adresse fest (die in der angepassten Unattend-Datei als vordefiniertes Makro verwendet wird).

Vorgehensweise

Gehen Sie wie folgt vor, um das japanische Windows 2016 auf Zielservern mit einem angepassten BS-Image-Profil zu implementieren.

Schritt 1. Laden Sie das japanische Windows 2016-Betriebssystem auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Betriebssystem-Images importieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images verwalten**, um die Seite Betriebssystem implementieren: BS-Images verwalten anzuzeigen.
2. Klicken Sie auf die Registerkarte **BS-Images**.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das BS-Image aus, die Sie importieren möchten (z. B. `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Klicken Sie auf **Importieren**, um das Image in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 2. Laden Sie die Paketdatei für Windows 2016 auf das lokale System herunter und importieren Sie das Image in das BS-Images-Repository. Weitere Informationen finden Sie unter Einheitentreiber importieren

Die Paketdatei enthält die neuesten Einheitentreiber und WinPE-Boot-Dateien, die Sie Ihren angepassten BS-Image-Profilen hinzufügen können. In diesem Szenario wird eine angepasste Boot-Datei verwendet, sodass die Boot-Datei im Paket nicht verwendet wird.

1. Klicken Sie auf die Registerkarte **Treiberdateien**.
2. Klicken Sie auf **Downloads → Windows Paketdateien**, um auf die Lenovo Unterstützungswebseite zu gehen und laden Sie die Paketdatei für Windows 2016 auf das lokale System herunter.
3. Klicken Sie auf das Symbol **Importieren** ().
4. Klicken Sie auf **Lokaler Import**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das BS-Image aus, das Sie importieren möchten (z. B. `bundle_win2016_20180126130051.zip`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.
7. Warten Sie, bis der Importvorgang abgeschlossen ist. Dies kann eine Weile dauern.

Schritt 3. Erstellen Sie eine angepasste WinPE-Boot-Datei, die das japanische Gebietsschema während der WinPE-Installation verwendet, und importieren Sie die Datei in das BS-images-Repository.

XClarity Administrator verwendet eine vordefinierte Windows PreInstallation-(WinPE-)Boot-Datei zur Installation des Windows-Betriebssystems. Die Ländereinstellung, die mit dieser vordefinierten Boot-Datei verwendet wird, ist Englisch (en-US). Wenn Sie die beim Windows Setup verwendete Ländereinstellung ändern wollen, können Sie eine angepasste WinPE-Boot-Datei mit der gewünschten Ländereinstellung erstellen und diese angepasste Boot-Datei Ihrem angepassten Profil zuweisen.

Weitere Informationen zum Einfügen von Gebietsschemata bei WinPE finden Sie unter Website für Windows WinPE: Pakete hinzufügen.

Wichtig: Die Angabe einer nicht-englischen Ländereinstellung in der WinPE-Boot-Datei ändert nicht die Ländereinstellung des final implementierten BS. Es ändert nur die Ländereinstellung, die während der Installation und Konfiguration von Windows angezeigt wird.

Führen Sie die folgenden Schritte aus, um eine angepasste WinPE-Boot-Datei zu erstellen, die das japanische Gebietsschema enthält. Siehe Boot-(WinPE)-Datei erstellen für weitere Informationen.

1. Verwenden Sie eine Benutzer-ID mit Administratorrechten und führen Sie den Windows ADK-Befehl „Deployment and Imaging Tools Environment“ aus. Eine Befehlssitzung wird angezeigt.
2. Wechseln Sie in der Befehlssitzung zum Verzeichnis, in das die Dateien `genimage.cmd` und `starnet.cmd` heruntergeladen wurden (zum Beispiel `C:\customwim`).
3. Stellen Sie sicher, dass sich keine zuvor angehängten Images auf dem Host befinden, indem Sie den folgenden Befehl ausführen:
   ```
   dism /get-mountedwiminfo
   ```
   Wenn es angehängte Images gibt, löschen Sie diese, indem Sie den folgenden Befehl ausführen:
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```
4. Wenn Sie Inbox-Einheitentreiber zu einem benutzerdefinierten Windows-Profil hinzufügen, kopieren Sie die unaufbereiteten Einheitentreiberdateien im INF-Format in das Hostsystem im Verzeichnis `C:\drivers`.

5. Führen Sie den folgenden Befehl aus, um die Boot-Datei im WIM-Format zu generieren, und warten Sie dann einige Minuten, bis der Befehl ausgeführt wurde.
   `genimage.cmd amd64 <ADK_Version>`

   Dabei ist *<ADK_Version>* einer der folgenden Werte.

   - **8.1**. Für Windows 2012 R2
   - **10**. Für Windows 2016

   Dieser Befehl erstellt eine Boot-Datei namens `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Hängen Sie die Boot-Datei an, indem Sie den folgenden Befehl ausführen:
   `DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`
7. Wenn Sie Out-of-Box-Einheitentreiber direkt zur Boot-Datei hinzufügen, gehen Sie wie folgt vor:
   a. Erstellen Sie die folgenden Verzeichnisstruktur. *<os_release>* ist dabei `2012R2` oder `2016`.
      `drivers\<os_release>\`
   b. Kopieren Sie die Einheitentreiber im INF-Format in ein Verzeichnis in diesem Pfad, beispielsweise:
      `drivers\<os_release>\<driver1>\<driver1_files>`
   c. Kopieren Sie das `drivers`-Verzeichnis in das Verzeichnis zum Anhängen, beispielsweise:
      `C:\WinPE_64\mount\drivers`
8. **Optional:** Führen Sie zusätzliche Anpassungen an der Boot-Datei durch, wie das Hinzufügen von Ordnern, Dateien, Startskripts, Sprachpaketen und Apps. Weitere Informationen zum Anpassen von Boot-Dateien finden Sie im Abschnitt WinPE: Website zum Anhängen und Anpassen.
9. Fügen Sie z. B. japanische Pakete hinzu.
10. Zeigen Sie installierte Pakete an, um sicherzustellen, dass die Japanisch-spezifischen Pakete installiert sind.
```
Dism /Add-Package /Image:"C:\WinPE_64\mount"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```
11. Überprüfen Sie die Internationalen Einstellungen im Image.
    `Dism /Get-Packages /Image:"C:\WinPE_64\mount"`
12. Hängen Sie das Image ab, indem Sie den folgenden Befehl ausführen:
    `DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`
13. Komprimieren Sie den Inhalt des Verzeichnisses `C:\WinPE_64\media` in eine ZIP-Datei namens `WinPE_64_ja.zip`.

14. Importieren Sie die ZIP-Datei in XClarity Administrator (siehe Boot-Dateien importieren).
    a. Klicken Sie auf die Registerkarte **Boot-Dateien**.
    b. Klicken Sie auf das Symbol **Importieren** ().
    c. Klicken Sie auf **Lokaler Import**.
    d. Wählen Sie `Windows` für das Betriebssystem aus.
    e. Klicken Sie auf **Durchsuchen**, um die zu importierende angepasste Boot-Datei zu suchen und auszuwählen (z. B. `WinPE_64_ja.zip`).
    f. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 4. Ändern Sie die Windows Unattend-Datei, um anzugeben, dass Japanisch im BS-Image enthalten ist, und importieren Sie die angepasste Datei in das BS-Images-Repository.

Fügen Sie Japanisch im Schritt „windowsPE“ der Windows-Installation als Betriebssystemsprache und Ländereinstellung hinzu, z. B.:

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Anmerkung: Bei der Verwendung einer angepassten Unattend-Datei bietet XClarity Administrator einige der normalen Komfortfunktionen nicht, die Sie haben, wenn Sie eine vordefinierte Unattend-Datei verwenden würden. Zum Beispiel müssen die Ziele `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` und `<UserAccounts>` für den Administrator, `<Interfaces>` für das Netzwerk und `<package>`-Liste für die Installationsfunktionen in der angepassten Unattend-Datei angegeben werden, die hochgeladen wird.

XClarity Administrator bietet einige grundlegende Komfortmakros, z. B. OOB-Treiberinjektion, Statusmeldungen, Nach-Installationsskripts und angepasste Software. Zur Verwendung dieser vordefinierten Makros müssen Sie jedoch die folgenden Makros in der angepassten Unattend-Datei angeben.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

Die Beispieldatei enthält bereits die benötigten Makros. Weitere Informationen zum Hinzufügen von Makros zu Unattend.Dateien finden Sie unter Injizieren von vordefinierten und angepassten Makros in eine Unattend-Datei. Weitere Informationen über die verfügbaren vordefinierten Makros finden Sie unter Vordefinierte Makros.

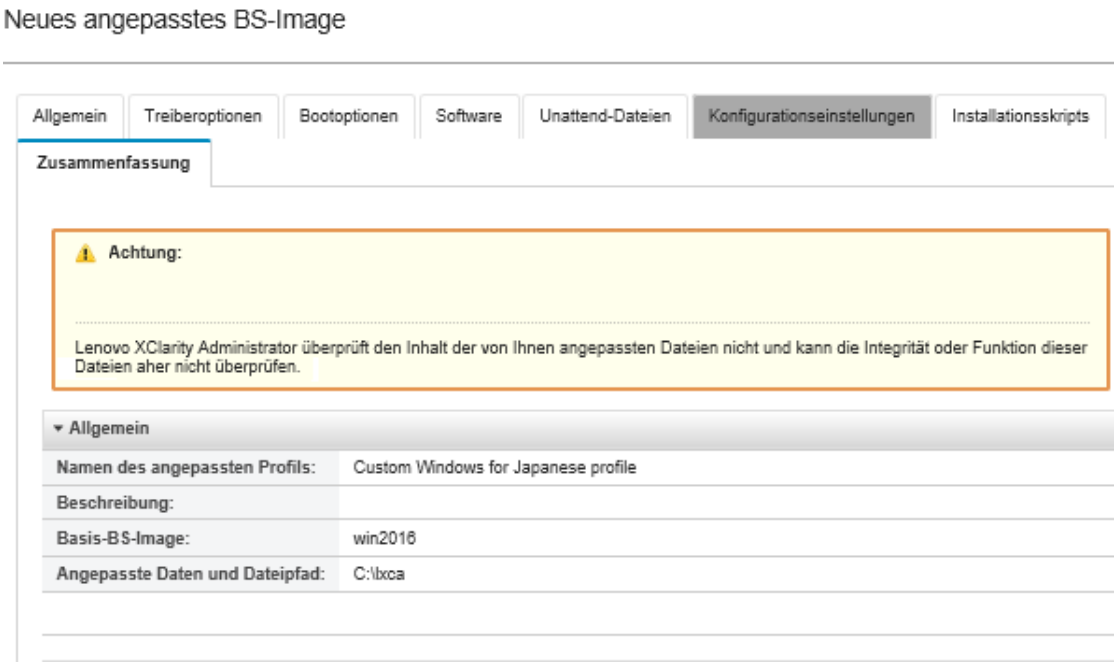
Gehen Sie wie folgt vor, um die angepasste Unattend-Datei zu importieren. Siehe Angepasste Unattend-Dateien importieren für weitere Informationen.

1. Klicken Sie auf die Registerkarte **Unattend-Dateien**.
2. Klicken Sie auf das Symbol **Importieren** ().
3. Klicken Sie auf **Lokaler Import**.

4. Wählen Sie `Windows` für das Betriebssystem aus.
5. Klicken Sie auf **Durchsuchen**, um die angepasste Unattend-Datei zu suchen und auszuwählen (z. B. `Windows_locale_customUnattend.xml`).
6. Klicken Sie auf **Importieren**, um die Datei in das BS-Images-Repository hochzuladen.

Schritt 5. Erstellen Sie ein angepasste BS-Image-Profil, das die angepasste Boot-Datei (WinPE) und Unattend-Datei enthält. Weitere Informationen finden Sie unter Angepasstes BS-Image-Profil erstellen.

1. Klicken Sie auf die Registerkarte **BS-Images**.
2. Wählen Sie das Profil zum Anpassen aus (z. B. `win2016-x86_64-install-Datacenter_Virtualization`).
3. Klicken Sie auf das **Erstellen**-Symbol ( ), um das Dialogfeld „Angepasstes Profil erstellen“ anzuzeigen.
4. Auf der Registerkarte **Allgemein**:
   a. Geben Sie einen Namen für das Profil ein, z. B. `Angepasstes Windows für Japanisch-Profil`.
   b. Verwenden Sie den Standardwert für das Feld **Angepasste Daten und Dateipfad**.
   c. Wählen Sie für den Anpassungstyp **Nur Unattend-Dateien** aus.
   d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Registerkarte **Treiberoptionen** auf **Weiter**. Die Treiber für die In-Box-Einheitentreiber sind standardmäßig enthalten.
6. Wählen Sie auf der Registerkarte **Boot-Dateien** die angepasste Boot-Datei aus (z. B. `WinPE_64_ja`) und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Registerkarte **Software** auf **Weiter**.
8. Wählen Sie auf der Registerkarte **Unattend-Dateien** die angepasste Unattend-Datei aus (z. B. `Windows_locale_customUnattend.xml`) und klicken Sie auf **Weiter**.
9. Klicken Sie auf der Registerkarte **Installationsskripts** auf **Weiter**.
10. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.



11. Klicken Sie auf **Anpassen**, um das angepasste BS-Image-Profil zu erstellen.

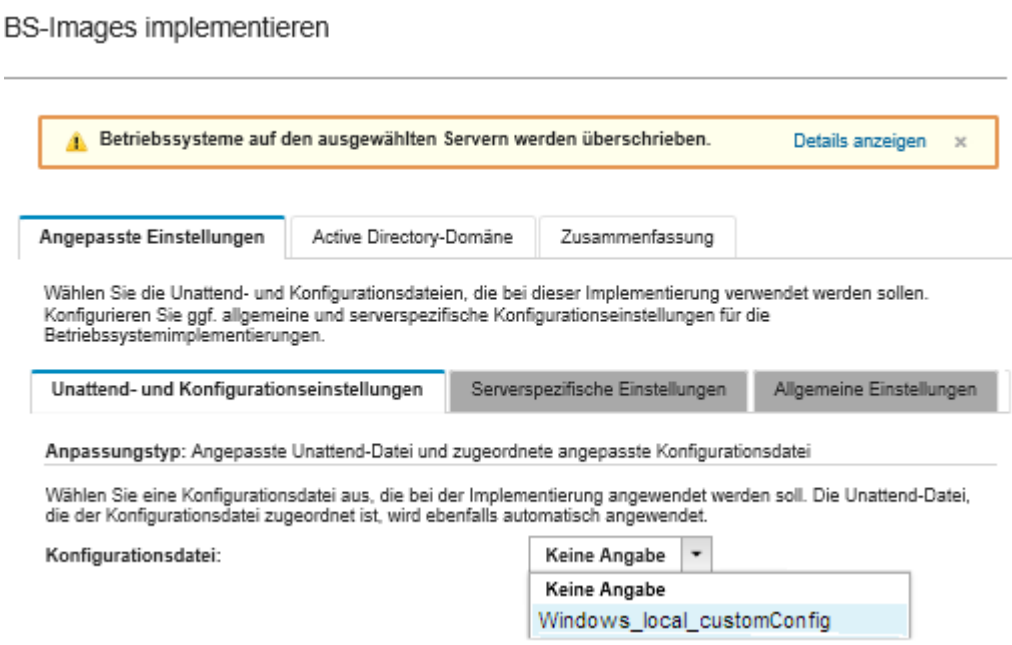
Schritt 6. Implementieren Sie das angepasste BS-Image-Profil auf den Zielservern. Weitere Informationen finden Sie unter Ein Betriebssystem-Image implementieren.

1. Klicken Sie auf der Menüleiste von XClarity Administrator auf **Bereitstellung → BS-Images implementieren**, um die Seite Betriebssystem implementieren: BS-Images implementieren anzuzeigen.
2. Für jeden Zielserver:
   a. Wählen Sie den Server aus.
   b. Klicken Sie auf **Ausgewählte ändern → Netzwerkeinstellungen** und geben Sie Hostname, IP-Adresse, Subnetzmaske, Gateway, DNS, MTU und VLAN-Einstellungen für den Server an.

      Tipp: VLAN-Einstellungen sind nur verfügbar, wenn der VLAN-Modus unter **Globale Einstellungen → IP-Zuordnung → VLANs verwenden** festgelegt wurde.
   c. Wählen Sie das angepasste BS-Image-Profil (z. B. <*Basis_BS*>|<*Zeitstempel*>_`Angepasstes Windows für Japanisch-Profil`) aus der Dropdown-Liste der Spalte **Zu implementierendes Image** aus.

      Anmerkung: Stellen Sie sicher, dass alle Zielserver dasselbe angepasste Profil verwenden.
   d. (Optional) Klicken Sie auf das Symbol **Lizenzschlüssel** () und geben Sie den Lizenzschlüssel an, mit dem das Betriebssystem nach der Installation aktiviert werden soll.
   e. Wählen Sie in der Spalte **Speicher** die bevorzugte Speicherposition aus, an der das Betriebssystem-Image implementiert werden soll.

      Anmerkung: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom verwalteten Server.
   f. Überprüfen Sie, ob als Implementierungsstatus für den ausgewählten Server **Bereitstellung** angegeben ist.
3. Wählen Sie alle Zielserver aus und klicken Sie auf das Symbol **Image implementieren** (), um die Betriebssystemimplementierung einzuleiten.
4. Klicken Sie auf der Registerkarte **Angepasste Einstellungen** auf die Unterregisterkarte **Unattend- und Konfigurationseinstellungen** und wählen Sie die angepasste Unattend-Datei aus (z. B. `Windows_locale_customUnattend.xml`).



5. (Optional) Geben Sie auf der Registerkarte **Active Directory-Domäne** die Informationen zum Verknüpfen einer Active Directory-Domäne im Rahmen einer Windows-Image-Implementierung an (siehe In Windows Active Directory integrieren
6. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Einstellungen.
7. Klicken Sie auf **Implementieren**, um das Betriebssystem zu implementieren.

   Der Windows-Installationsdialog wird in Japanisch angezeigt.

Nach Abschluss der Installation wird die Windows-Anmeldeseite auch in Japanisch angezeigt.


Administrator
パスワード
パスワードのリセット

Kapitel 16. End-to-End-Szenarien für das Einrichten neuer Einheiten

Verwenden Sie diese End-to-End-Szenarien, um Lenovo XClarity Administrator zum einheitlichen und leicht wiederholbaren Einrichten neuer Einheiten zu verwenden.

ESXi auf einem lokalen Festplattenlaufwerk implementieren

Verwenden Sie dieses Verfahren, um VMware ESXi 5.5 auf einem lokal installierten Festplattenlaufwerk auf Flex System x240 Rechenknoten zu implementieren. Es wird gezeigt, wie Sie ein Servermuster von einem vorhandenen Server übernehmen, das zugehörige Kategoriemuster für erweiterte UEFI-Einstellungen ändern und VMware ESXi installieren.

VMware ESXi 5.5 erfordert, dass im Speicher abgebildeter E/A-Platz (MMIO; memory-mapped I/O) innerhalb der ursprünglichen 4 GB des Systems konfiguriert wird. Je nach verwendeter Konfiguration versuchen bestimmte Systeme, mehr Hauptspeicher als 4 GB zu verwenden, was Fehler verursachen kann. Sie können das Problem beheben, indem Sie über das Setup Utility für jeden Server, auf dem VMware ESXi 5.5 installiert wird, den Wert der Option „MM Config“ auf 3 GB erhöhen.

Alternativ können Sie auch ein Servermuster implementieren, das eins der für die Virtualisierung bestimmten, vordefinierten erweiterten UEFI-Kategoriemuster enthält. Dadurch wird die Option „MM Config“ festgelegt und die PCI-64-Bit-Ressourcenzuordnung deaktiviert.

Ein vordefiniertes Virtualisierungsmuster implementieren

Ein Kategoriemuster definiert bestimmte Firmwareeinstellungen, die in mehreren Servermustern wiederverwendet werden können. Um ein vordefiniertes Virtualisierungsmuster zu implementieren, erstellen Sie ein Servermuster. Dann wenden Sie ein vordefiniertes erweitertes UEFI-Muster auf dieses Servermuster an. Dieses Servermuster kann auf mehrere Server desselben Typs angewendet werden, zum Beispiel auf Flex System x240 Rechenknoten oder Flex System x880 X6 Rechenknoten.

Zu dieser Aufgabe

Beim Erstellen eines Servermusters können Sie auswählen, ob Sie die Konfiguration selbst durchführen möchten oder ob die Musterattribute von einem vorhandenen, bereits eingerichteten Server übernommen werden sollen. Wenn Sie ein neues Muster von einem vorhandenen Server übernehmen, sind die meisten Musterattribute bereits definiert.

Weitere Informationen zu Server- und Kategoriemustern finden Sie unter Mit Servermustern arbeiten.

Vorgehensweise

Gehen Sie wie folgt vor, um ein neues Muster von einem vorhandenen Server zu übernehmen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Servermuster**.

Schritt 3. Klicken Sie auf das Symbol **Erstellen** ( ). Der Assistent für neue Servermuster wird angezeigt.

Schritt 4. Klicken Sie auf **Neues Muster auf Basis eines vorhandenen Servers erstellen**. Sie können auswählen, ob ein komplett neues Muster erstellt werden soll. Allerdings ist es meist effizienter, ein Muster von einem vorhandenen Server zu erstellen, der die gewünschte Konfiguration besitzt.

Wenn Sie ein Servermuster von einem vorhandenen Server erstellen, übernimmt XClarity Administrator die Einstellungen von einem verwalteten Server (einschließlich der Einstellungen für den erweiterten Anschluss, UEFI und Baseboard Management Controller) und erstellt dynamisch Kategoriemuster für diese Einstellungen. Bei einem völlig neuen Server übernimmt XClarity Administrator die werkseitigen Voreinstellungen. Wenn der Server bereits verwendet wird, übernimmt XClarity Administrator die angepassten Einstellungen. Sie können die Einstellungen anschließend gezielt für den Server ändern, auf dem das Muster implementiert wird.

Schritt 5. Wählen Sie den Server aus, der beim Erstellen des Musters als Basiskonfiguration verwendet werden soll.

Anmerkung: Beachten Sie, dass der ausgewählte Server dasselbe Modell wie die Server aufweisen muss, auf denen Sie das Servermuster implementieren möchten. Dieses Szenario basiert auf der Auswahl von Flex System x240 Rechenknoten.

Schritt 6. Geben Sie den Namen des neuen Musters ein und stellen Sie eine Beschreibung bereit.

Beispiele:

- Name: **x240_ESXi_deployment**
- Beschreibung: **Muster mit erweiterten UEFI-Einstellungen, die zur Implementierung von VMware ESXi geeignet sind**

Schritt 7. Klicken Sie auf **Weiter**, um die Informationen vom ausgewählten Server zu laden.

Schritt 8. Wählen Sie auf der Registerkarte **Lokaler Speicher** die Option **Speicherkonfiguration angeben** aus und legen Sie dann einen Speichertyp fest. Klicken Sie anschließend auf **Weiter**.

Weitere Informationen zu den Einstellungen für den lokalen Speicher finden Sie unter Lokalen Speicher definieren.

Schritt 9. Geben Sie auf der Registerkarte **E/A-Adapter** Informationen zu den Adaptern ein, die sich auf den Servern befinden, auf denen VMware ESXi installiert werden soll.

Es werden alle Adapter angezeigt, die auf dem als Basis verwendeten Server vorhanden sind.

Wenn alle Flex System x240 Rechenknoten in Ihrer Installation über dieselben Adapter verfügen, müssen Sie auf dieser Registerkarte keine Einstellungen ändern.

Weitere Informationen zu den Einstellungen für E/A-Adapter finden Sie unter E/A-Adapter definieren.

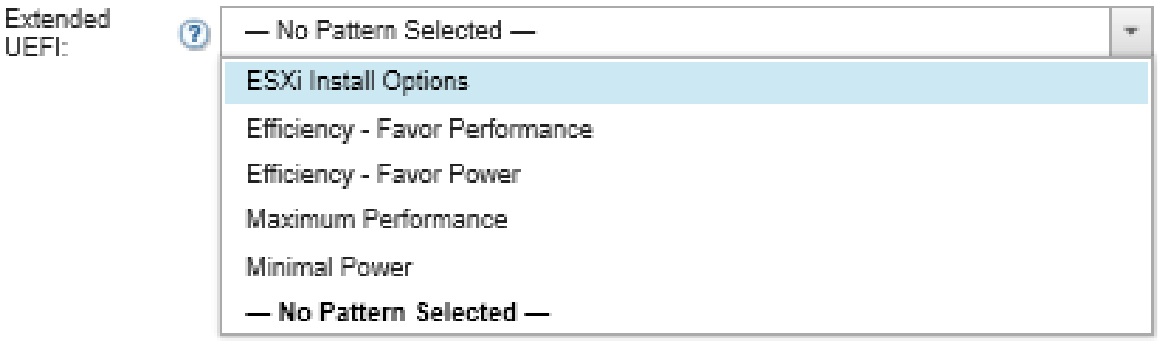
Schritt 10. Klicken Sie zum Fortfahren auf **Weiter**.

Schritt 11. Konfigurieren Sie auf der Registerkarte **Boot** die Einstellungen für ausschließlich traditionelle Bootumgebungen und SAN-Bootumgebungen. Sofern Sie keine dieser Umgebungen verwenden, übernehmen Sie die Standardeinstellung **Bootmodus für ausschließlich UEFI-Betriebssysteme** und klicken Sie auf **Weiter**.

Weitere Informationen zu den Booteinstellungen finden Sie unter Bootoptionen definieren.

Schritt 12. Geben Sie auf der Registerkarte **Firmwareeinstellungen** die Management-Controller- und UEFI-Firmwareeinstellungen an, die bei der Implementierung dieses Musters für Zielserver verwendet werden sollen. (Wählen Sie z. B. **x240 Virtualisierung** aus.)

Auf dieser Registerkarte können Sie eines der vordefinierten erweiterten UEFI-Muster auswählen:



Weitere Informationen zu den Firmwareeinstellungen finden Sie unter Firmwareeinstellungen definieren.

Schritt 13. Klicken Sie auf **Speichern und implementieren**, um das Muster in XClarity Administrator zu speichern und es auf den Servern zu implementieren, auf denen VMware ESXi installiert werden soll.

Nach dieser Aufgabe

Nachdem das Servermuster auf allen Servern implementiert wurde, können Sie das Betriebssystem auf diesen Servern installieren.

VMware ESXi auf Flex System x240 Rechenknoten implementieren

Verwenden Sie dieses Verfahren als Beispiel, um den Prozess für die Implementierung des ESXi-Betriebssystems auf Flex System x240 Rechenknoten zu veranschaulichen.

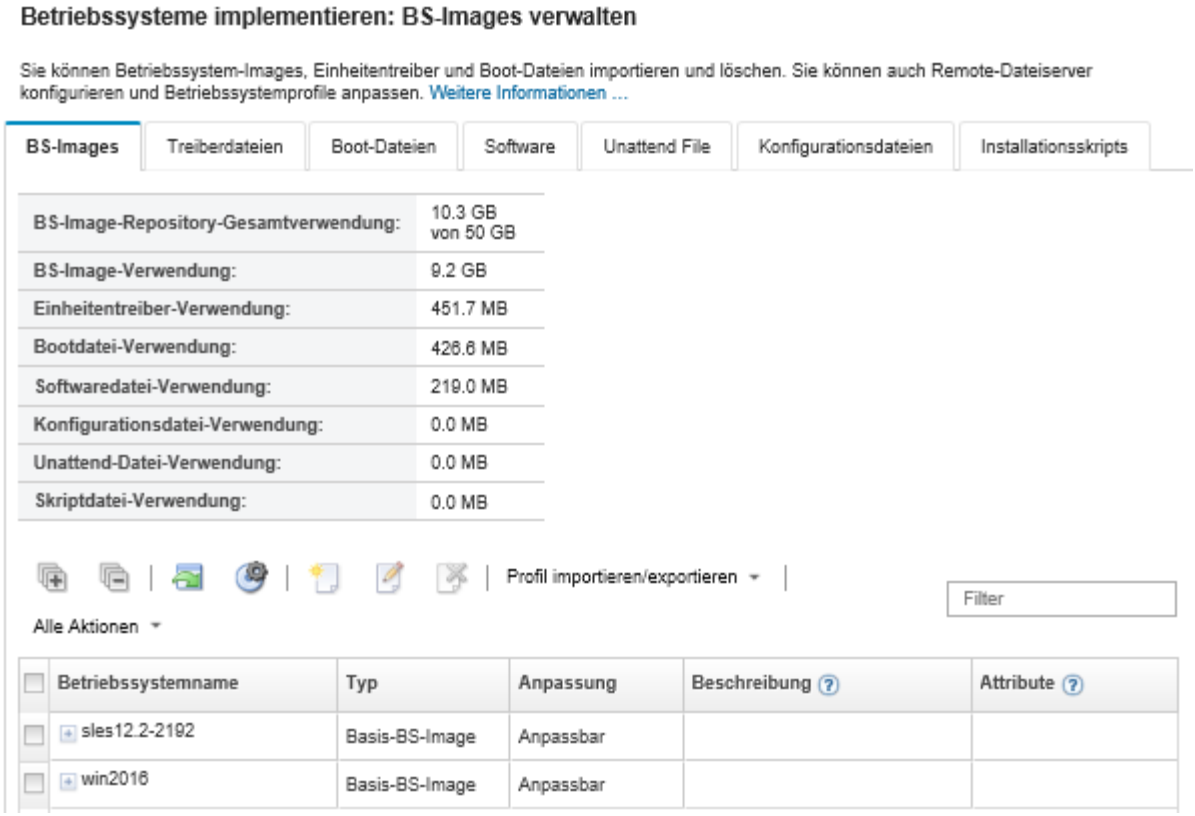
Vorbereitende Schritte

Bevor Sie diesen Vorgang starten, müssen Sie sicherstellen, dass Lenovo XClarity Administrator das Gehäuse verwaltet, in dem Flex System x240 Rechenknoten installiert ist.

Vorgehensweise

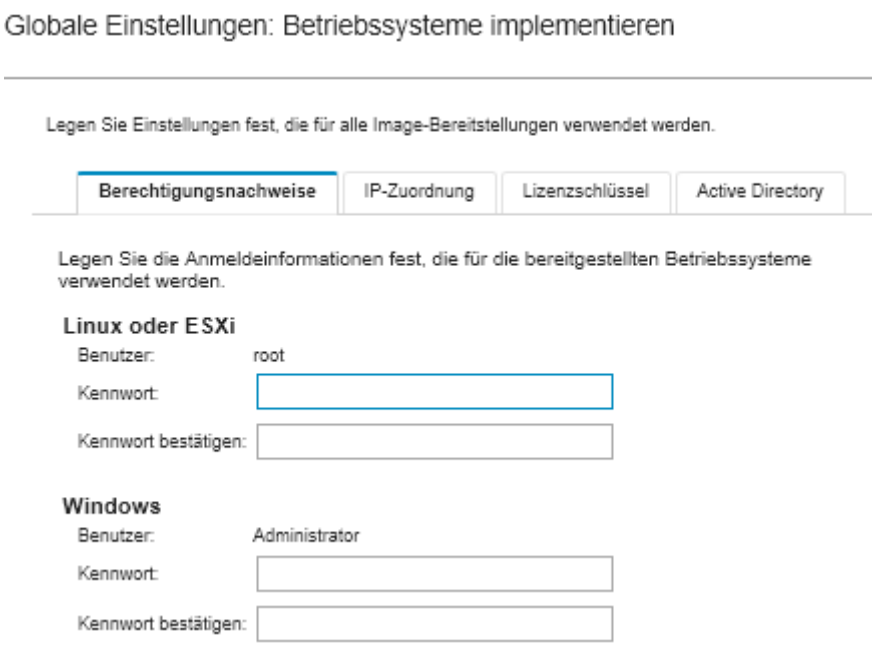
Gehen Sie wie folgt vor, um das ESXi-Betriebssystem auf Flex System x240 Rechenknoten zu implementieren.

Schritt 1. Stellen Sie sicher, dass das zu implementierende Image bereits im BS-Images-Repository geladen ist, indem Sie durch Klicken auf **Alle Aktionen → BS-Images verwalten** eine Liste mit allen verfügbaren Images anzeigen.



Schritt 2. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → BS-Images implementieren**. Die Seite BS-Images implementieren wird angezeigt.

Schritt 3. Legen Sie globale Einstellungen fest, die als Standardeinstellungen für alle Image-Implementierungen verwendet werden sollen. Klicken Sie dazu auf **Alle Aktionen → Globale Einstellungen**, um das Dialogfenster „Globale Einstellungen“ anzuzeigen.



a. Geben Sie auf der Registerkarte **Anmeldeinformationen** das Kennwort ein, das für die Anmeldung des Administratoraccount am Betriebssystem verwendet werden soll.

b. Geben Sie auf der Registerkarte **IP-Zuordnung** an, wie die IP-Adresse für das Betriebssystem auf dem Server zugeordnet wird.

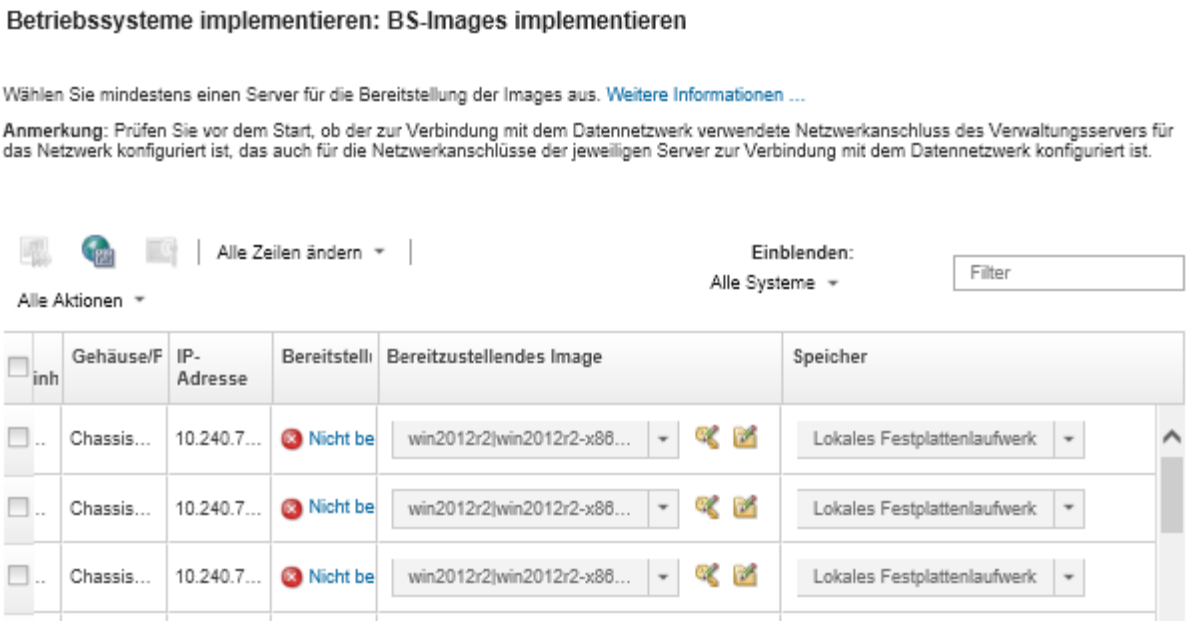
   Wenn Sie für die Zuordnung der IP-Adressen die Option **Dynamic Host Configuration Protocol (DHCP) verwenden** auswählen, werden die IP-Adressinformationen nicht im Dialogfenster Netzwerkeinstellungen ändern angezeigt (siehe Schritt Schritt 8 9 auf Seite 644). Wenn Sie **Statische IP-Adresse (IPv4) zuordnen** auswählen, können Sie für jede Implementierung eine IP-Adresse, ein Subnetz und ein Gateway angeben.

c. Geben Sie bei Bedarf auf der Registerkarte **Lizenzschlüssel** einen Lizenzschlüssel für die Massenaktivierung ein.

d. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Schritt 4. Stellen Sie sicher, dass der Server für die Betriebssystembereitstellung bereit ist. Wählen Sie dazu den Server aus, auf dem das Betriebssystem implementiert werden soll. Zunächst wird als Implementierungsstatus für den möglicherweise „Nicht bereit“ angezeigt. Erst wenn als Implementierungsstatus „Bereitstellung“ angegeben ist, können Sie ein Betriebssystem auf einem Server implementieren.

Tipp: Sie können mehrere Server in verschiedenen Flex System-Gehäusen auswählen, wenn Sie dasselbe Betriebssystem auf allen Servern implementieren möchten. Sie können bis zu 28 Server auswählen.



Schritt 5. Klicken Sie auf die Spalte **Zu implementierendes Image** und wählen Sie VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**) aus.

Schritt 6. Klicken Sie in derselben Spalte auf das **Lizenzschlüssel**symbol ( ), um den Lizenzschlüssel für diese Implementierung einzugeben.

Tipp: Sie können auch auswählen, dass der Massenaktivierungsschlüssel verwendet wird, den Sie im Dialogfenster „Globale Einstellungen“ eingegeben haben.

Schritt 7. Stellen Sie sicher, dass in der Spalte „Speicher“ die Option **Lokale Festplatte** ausgewählt wurde.

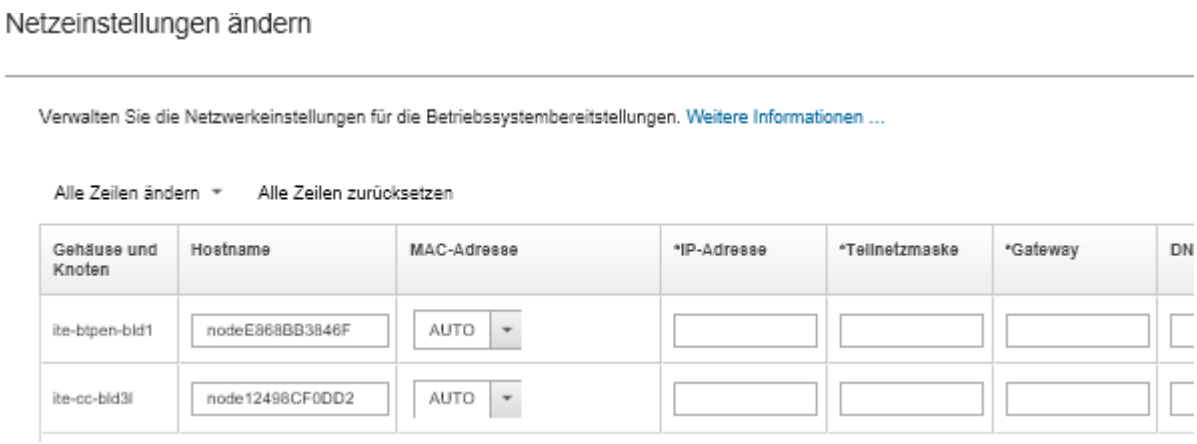
Schritt 8. Klicken Sie in der Spalte **Netzwerkeinstellungen** in der Zeile für den Server auf **Bearbeiten**, um die Netzwerkeinstellungen für diese Implementierung zu konfigurieren. Die Seite „Netzwerkeinstellungen ändern“ wird angezeigt.

Machen Sie in folgenden Feldern die erforderlichen Angaben:

- Hostname
- MAC-Adresse für den Port auf dem Host, auf dem das Betriebssystem installiert wird
- DNS-Server (falls erforderlich)
- MTU-Geschwindigkeit

Anmerkungen: Wenn Sie im Dialogfenster „Globale Einstellungen“ die Option **Statische IP-Adresse (IPv4) zuordnen** ausgewählt haben (siehe Schritt Schritt 3 4 auf Seite 642), müssen Sie auch die folgenden Informationen eingeben:

- IPv4-Adresse
- Teilnetzmaske
- Gateway



Schritt 9. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Stellen Sie sicher, dass der Implementierungsstatus für den Server auf der Seite BS-Images implementieren „Bereitstellung“ lautet.

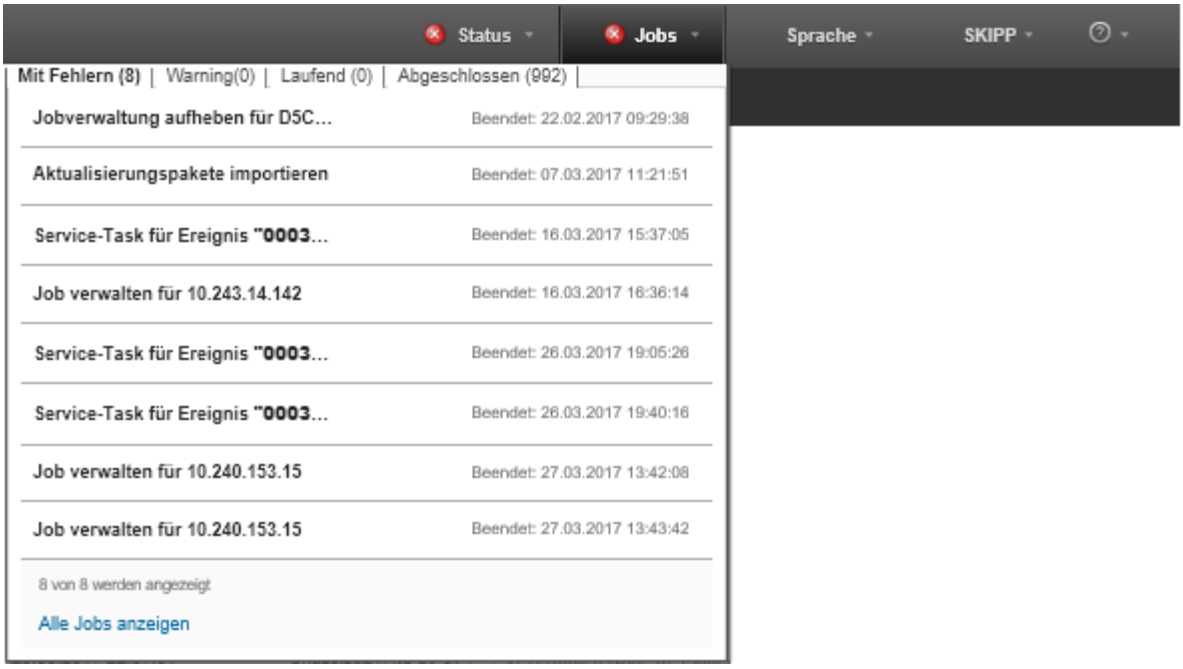
Schritt 10. Klicken Sie zum Implementieren des Betriebssystems auf **Alle Aktionen → Images implementieren**.

Schritt 11. Klicken Sie auf der Bestätigungsseite auf **Implementieren**, um das Image zu implementieren.

Wenn auf dem Server bereits ein Betriebssystem installiert ist, werden Sie gewarnt, dass das aktuelle Betriebssystem durch die Implementierung des Image überschrieben wird.

Tipp: Sie können eine Fernsteuerungssitzung einrichten, um den Fortschritt der Installation zu beobachten. Klicken Sie auf **Alle Aktionen → Fernsteuerung**, um eine Fernsteuerungssitzung für den Server zu starten.

Wenn Sie das Betriebssystem implementieren, startet Lenovo XClarity Administrator einen Job zur Implementierungsverfolgung. Um den Status des Implementierungsjobs anzuzeigen, klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Jobs**. Klicken Sie dann auf die Registerkarte **Laufend**.

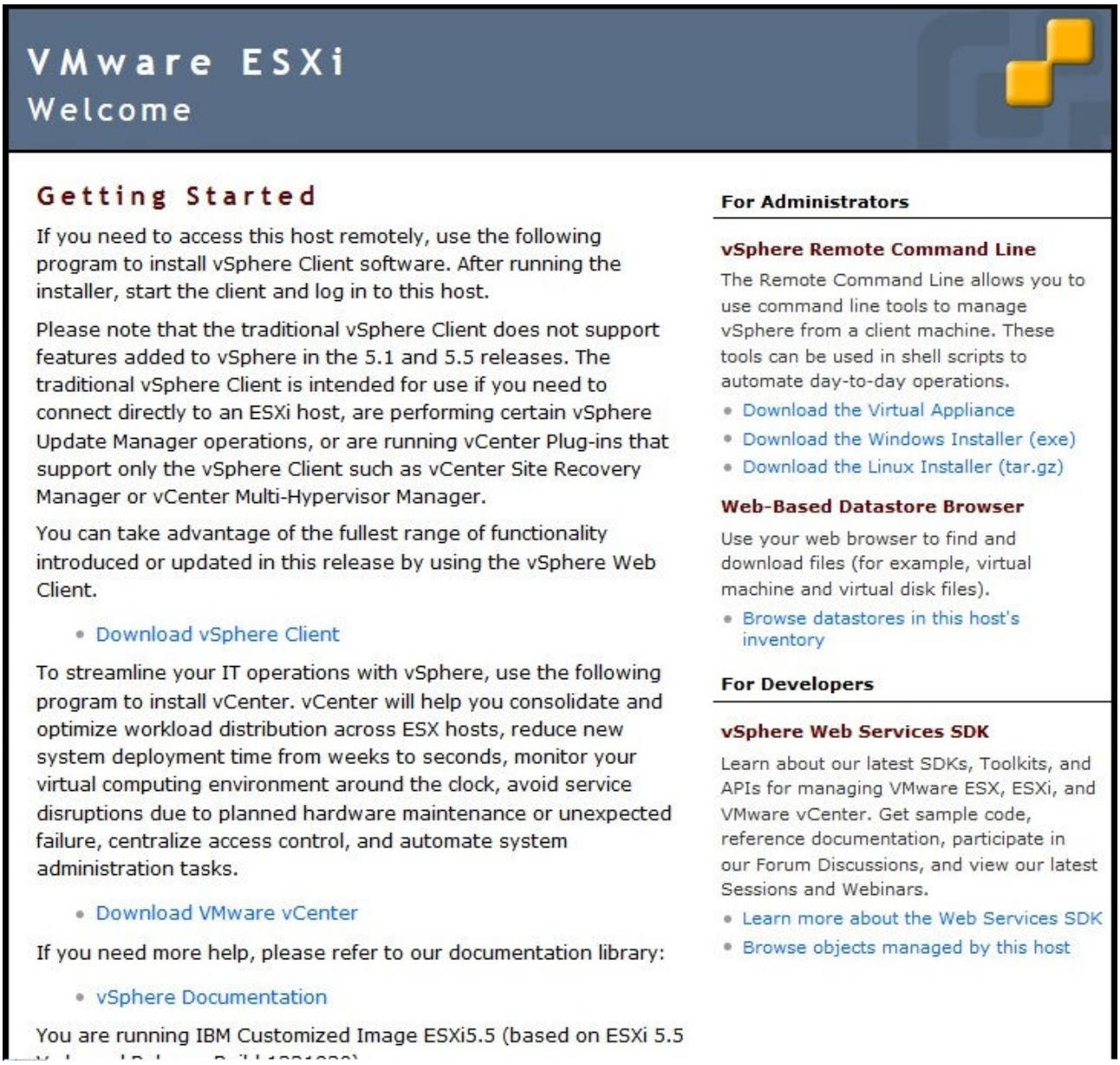


Bewegen Sie den Mauszeiger über den laufenden Job, um Details anzuzeigen, beispielsweise den Prozentsatz des Job-Fortschritts.

Ergebnisse

Wenn die Betriebssystembereitstellung abgeschlossen ist, melden Sie sich bei der IP-Adresse an, die Sie auf der Seite „Netzwerkeinstellungen ändern“ angegeben haben. Dann wird der Konfigurationsprozess fortgesetzt.

Anmerkung: 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.



ESXi auf SAN-Speicher implementieren

Verwenden Sie dieses Verfahren, um VMware ESXi 5.5 auf SAN-Datenträgern zu implementieren, die mit Servern verbunden sind.

Wenn Sie ein Betriebssystem auf einem SAN implementieren, wird das Betriebssystem auf dem ersten SAN-Bootziel implementiert, das über ein Servermuster konfiguriert wurde. Ein lokales Festplattenlaufwerk kann nicht auf dem Server aktiviert werden, der über ein SAN bootet. Er muss deaktiviert oder entfernt werden, wenn ein Festplattenlaufwerk vorhanden ist.

Servermuster zur Unterstützung des SAN-Bootvorgangs implementieren

Wenn Sie ein Servermuster erstellen und implementieren, um das Booten eines Systems über SAN-Speicher zu unterstützen, müssen Sie das SAN-Bootziel und die Adapter identifizieren, die zum Server gehören.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Servermuster zu erstellen und zu implementieren, das die Implementierung des Betriebssystems auf SAN-Speicher unterstützt.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Muster**. Die Seite Konfigurationsmuster: Muster wird angezeigt.

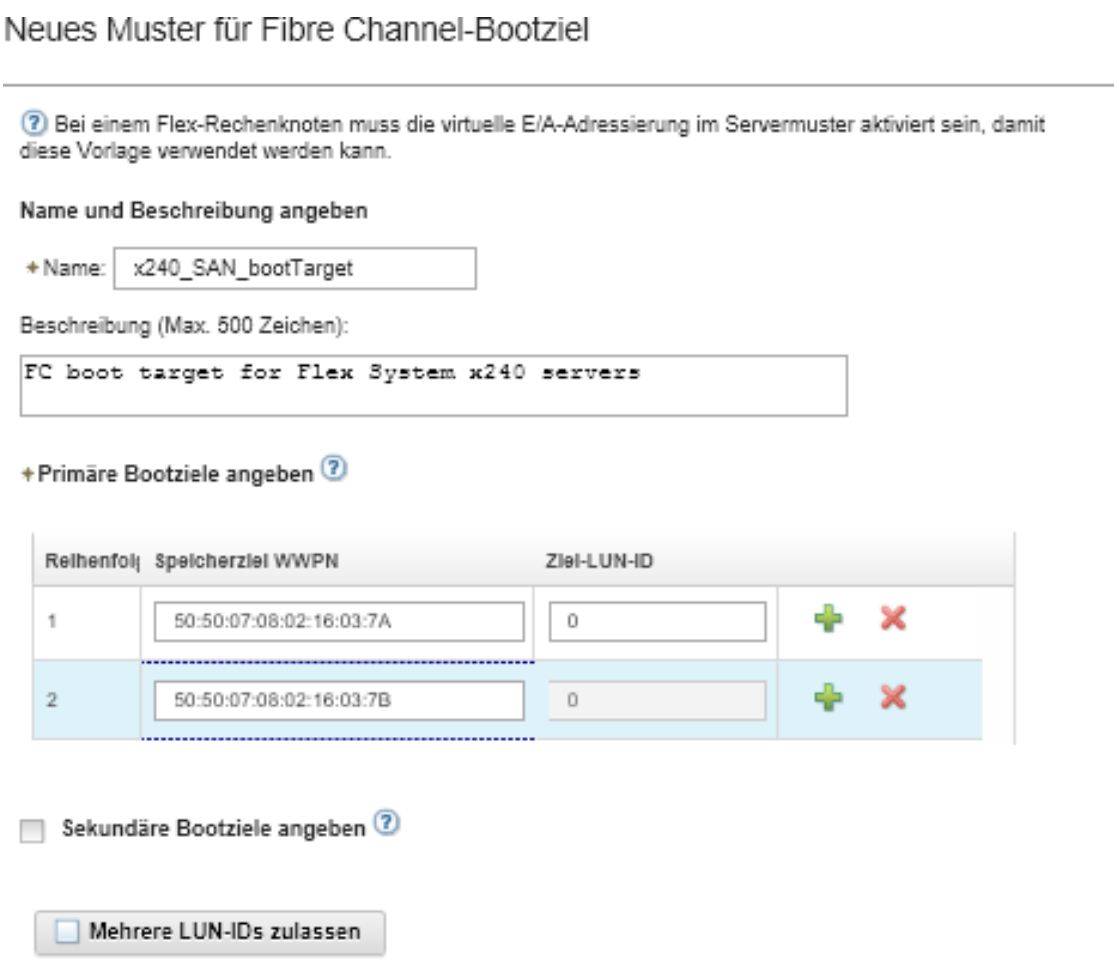
Schritt 2. Erstellen Sie ein Kategoriemuster, um durch das Identifizieren des weltweiten Portnamens (WWPN) und der LUNs der Speicherdatenträger festzulegen, wo das Betriebssystem implementiert werden soll.

a. Klicken Sie auf die Registerkarte **Kategoriemuster**.

b. Klicken Sie auf **Fibre Channel-Bootziel-Muster** und dann auf das Symbol für **Erstellen** ( ).

c. Geben Sie den WWPN des Speicherziels ein.

Anmerkung: Klicken Sie auf **Mehrere LUN-IDs zulassen**, um mehrere LUN-IDs auf denselben Speicherdatenträgern als Ziel zuzuweisen.



d. Klicken Sie auf **Create**, um das Muster zu erstellen. Das Ziel wird in der Liste der Fibre Channel-Bootziel-Muster angezeigt.

Schritt 3. Klicken Sie auf die Registerkarte **Servermuster**, um ein Muster zu erstellen.

Schritt 4. Klicken Sie auf das Symbol **Erstellen** ( ). Der Assistent für neue Servermuster wird angezeigt.

Schritt 5. Klicken Sie auf **Völlig neues Muster erstellen**.

Schritt 6. Auf der Registerkarte **Allgemein**:

- Wählen Sie **Flex Compute Node** für die Abmessungen aus.

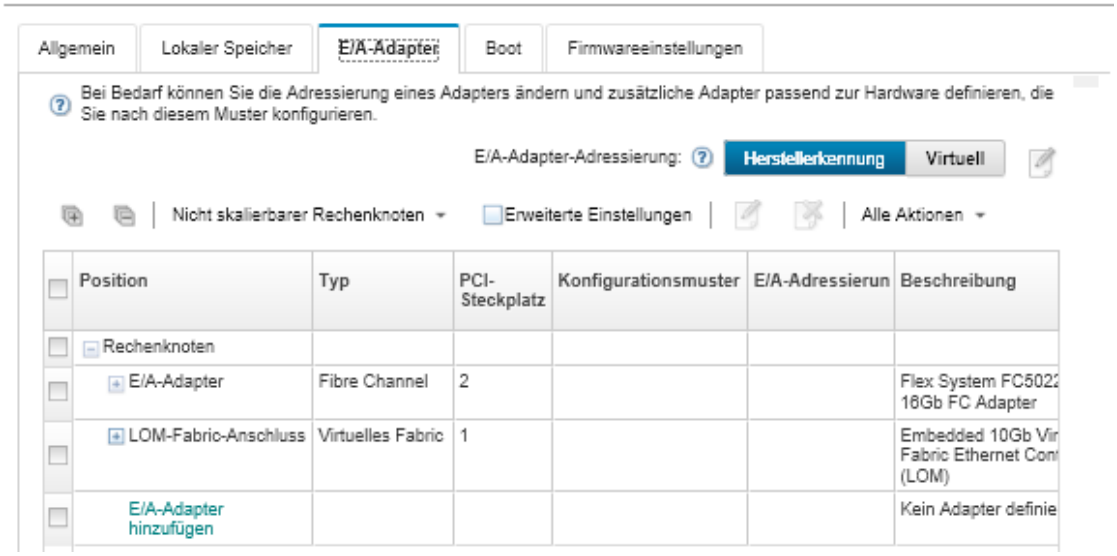
- Geben Sie einen Musternamen (**x240_san_boot**) und eine Beschreibung an.
- Klicken Sie auf **Weiter**.

Schritt 7. Zum Verbessern der Bootzeiten, die mit der Suche nach lokalen Laufwerken zusammenhängen, müssen Sie auf der Registerkarte **Lokaler Speicher** unter Umständen den lokalen Speicheradapterdeaktivieren, wenn Sie ein System ohne Datenträger verwenden. Klicken Sie anschließend auf **Weiter**.

Schritt 8. Fügen Sie auf der Registerkarte **E/A-Adapter** die Ethernet- und Fibre Channel-Adapter hinzu. Stellen Sie sicher, dass sie sich in den richtigen PCI-Steckplätzen befinden.

a. Klicken Sie für jeden Adapter auf **E/A-Adapter hinzufügen**. Geben Sie den PCI-Steckplatz an, in dem sich der Adapter befindet, und wählen Sie den Adapter aus.

Anmerkung: Geben Sie einen Ethernet- und einen Fibre Channel-Adapter an.



b. Als E/A-Adapter-Adressierung muss **Virtuell** festgelegt sein. Klicken Sie auf das Symbol für **Bearbeiten**  , um die Konfiguration anzugeben, die für die virtuelle Ethernet-MAC-Adressierung und die virtuelle Fibre Channel-WWN-Adressierung verwendet werden soll.

Anmerkung: Auf der Seite Virtuelle Adressierung bearbeiten können Sie auswählen, ob die vom Hersteller festgelegte MAC-Adresse für den Ethernet-Adapter verwendet werden soll. Deaktivieren Sie dazu die virtuelle Adressierung. Wenn Sie jedoch ein Fibre Channel-Bootziel-Muster zur Verwendung auswählen möchten, müssen Sie die virtuelle Adressierung für den Fibre Channel-Adapter verwenden.

c. Klicken Sie auf **Weiter**.

Schritt 9. Fügen Sie auf der Registerkarte **Boot** das zuvor erstellte SAN-Bootzielmuster hinzu.

a. Wählen Sie auf der Registerkarte **SAN-Boot** das definierte Bootzielmuster aus.

b. Klicken Sie auf **Weiter**.

Schritt 10. Auf der Registerkarte **Firmwareeinstellungen** definieren Sie alle zusätzlichen Kategoriemuster für dieses Servermuster. Sie können die folgenden Kategoriemuster definieren.

- **Systeminformationen**. (Weitere Informationen finden Sie unter Systeminformationseinstellungen definieren.)

- **Verwaltungsschnittstelle**. (Weitere Informationen finden Sie unter Verwaltungsschnittstelleneinstellungen definieren.)
- **Einheiten- und E/A-Anschlüsse** (Weitere Informationen finden Sie unter Einheiten- und E/A-Anschlusseinstellungen definieren.)
- **Erweitertes BMC**. Sie können unter den zuvor erfassten Baseboard Management Controller-Einstellungen auswählen. (Weitere Informationen finden Sie unter Erweiterte Management-Controller-Einstellungen definieren.)
- **Erweiterte UEFI**. Sie können unter den vordefinierten Einstellungen oder den zuvor erfassten UEFI-Einstellungen auswählen. (Weitere Informationen finden Sie unter Erweiterte UEFI-Einstellungen definieren.)

Schritt 11. Klicken Sie auf **Speichern und implementieren**, um das Muster in Lenovo XClarity Administrator zu speichern und es auf den Servern zu implementieren, auf denen VMware ESXi installiert werden soll.

Nach dieser Aufgabe

Führen Sie ggf. die folgenden Schritte aus, nachdem das Servermuster auf allen Servern implementiert wurde.

1. Fügen Sie die neu erstellten virtualisierten WWPN-Adressen in der Speicherzone hinzu, damit der Server auf die definierten Speicher-LUNs zugreifen kann.

   Tipp: Nach der Implementierung des Serverprofils finden Sie die virtuellen WWPN-Adressen im Serverprofil.

   a. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → Serverprofile**.

   b. Klicken Sie auf das implementierte Serverprofil (z. B. **x240_SAN_boot**). Auf der Registerkarte **Virtuelle Adressenzuordnung** wird die Liste mit Adressen angezeigt.

2. Implementieren Sie das Betriebssystem auf dem Server.

VMware ESXi auf SAN-Speicher implementieren

Verwenden Sie dieses Verfahren als Beispiel, um den Prozess für die Implementierung des ESXi-Betriebssystems auf mit einem Server verbundenem SAN-Speicher zu veranschaulichen.

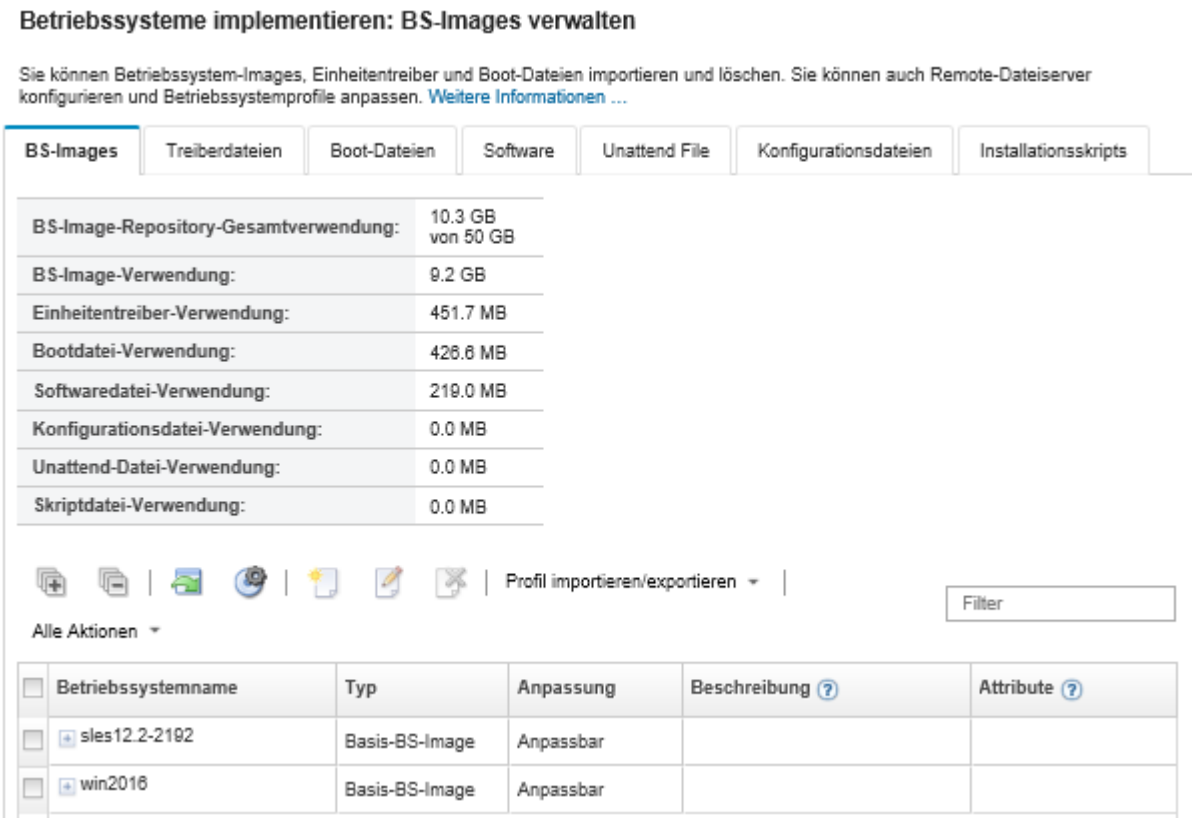
Vorbereitende Schritte

Bevor Sie diesen Vorgang starten, müssen Sie sicherstellen, dass Lenovo XClarity Administrator das Gehäuse verwaltet, in dem Flex System x220 Rechenknoten installiert ist.

Vorgehensweise

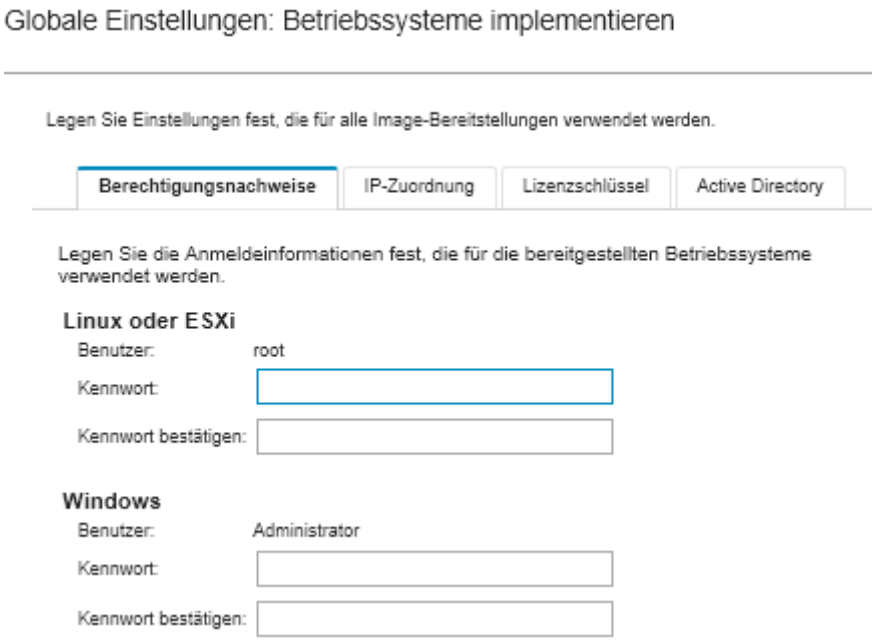
Gehen Sie wie folgt vor, um das ESXi-Betriebssystem auf Flex System x222 Rechenknoten zu implementieren.

Schritt 1. Stellen Sie sicher, dass das zu implementierende Image bereits im BS-Images-Repository geladen ist, indem Sie auf **Alle Aktionen → BS-Images verwalten** klicken.



Schritt 2. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Bereitstellung → BS-Images implementieren**.

Schritt 3. Legen Sie globale Einstellungen fest, die als Standardeinstellungen für alle Image-Implementierungen verwendet werden sollen. Klicken Sie dazu auf **Alle Aktionen → Globale Einstellungen**, um das Dialogfenster Globale Einstellungen: Betriebssysteme implementieren anzuzeigen.



a. Geben Sie auf der Registerkarte **Anmeldeinformationen** das Kennwort ein, das für die Anmeldung des Administratoraccount am Betriebssystem verwendet werden soll.

b. Geben Sie auf der Registerkarte **IP-Zuordnung** an, wie die IP-Adresse für das Betriebssystem auf dem „Server“ zugeordnet werden soll.

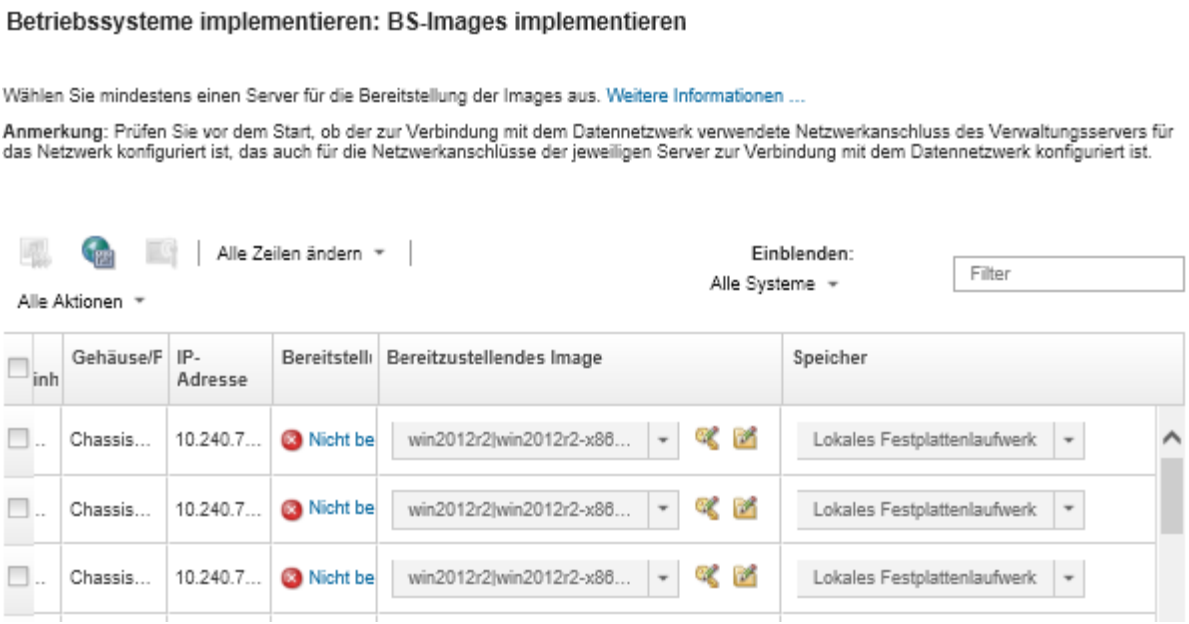
   Wenn Sie für die Zuordnung der IP-Adressen die Option **Dynamic Host Configuration Protocol (DHCP) verwenden** auswählen, werden die IP-Adressinformationen nicht im Dialogfenster Netzwerkeinstellungen ändern angezeigt (siehe Schritt Schritt 8 9 auf Seite 653). Wenn Sie **Statische IP-Adresse (IPv4) zuordnen** auswählen, können Sie für jede Implementierung eine IP-Adresse, ein Subnetz und ein Gateway angeben.

c. Geben Sie bei Bedarf auf der Registerkarte **Lizenzschlüssel** einen Lizenzschlüssel für die Massenaktivierung ein.

d. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Schritt 4. Stellen Sie sicher, dass der Server für die Betriebssystembereitstellung bereit ist. Wählen Sie dazu den Server aus, auf dem das Betriebssystem implementiert werden soll. Zunächst wird als Implementierungsstatus für den möglicherweise „Nicht bereit“ angezeigt. Erst wenn als Implementierungsstatus „Bereitstellung“ angegeben ist, können Sie ein Betriebssystem auf einem Server implementieren.

Tipp: Sie können mehrere Server in verschiedenen Flex System-Gehäusen auswählen, wenn Sie dasselbe Betriebssystem auf allen Servern implementieren möchten. Sie können bis zu 28 Server auswählen.



Schritt 5. Klicken Sie auf die Spalte **Zu implementierendes Image** und wählen Sie VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**) aus.

Schritt 6. Klicken Sie in derselben Spalte auf das **Lizenzschlüssel**symbol ( ), um den Lizenzschlüssel für diese Implementierung einzugeben.

Tipp: Sie können auch auswählen, dass der Massenaktivierungsschlüssel verwendet wird, den Sie im Dialogfenster Globale Einstellungen: Betriebssysteme implementieren eingegeben haben.

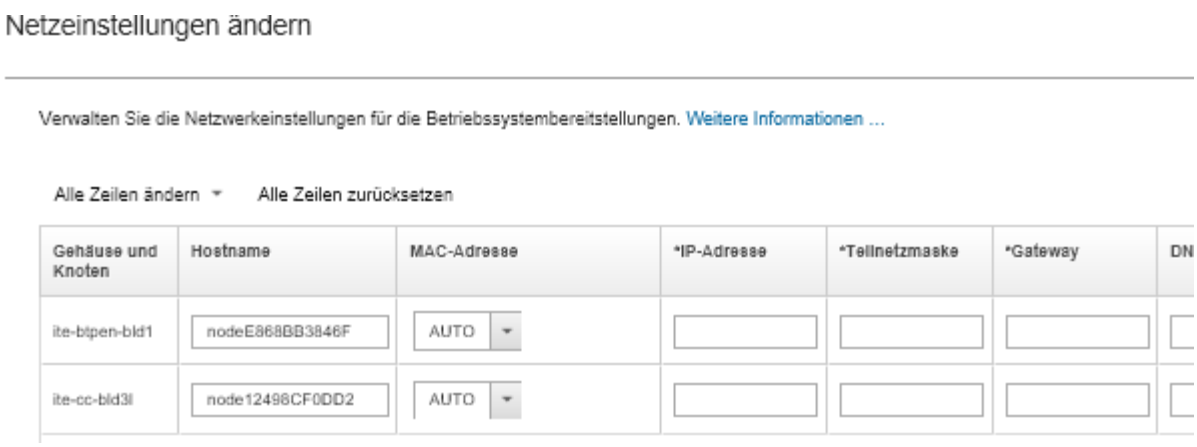
Schritt 7. Wählen Sie in der Spalte **Speicher** den SAN-Speicher aus, auf dem das Betriebssystem implementiert werden soll.

Der Speicher wird folgendermaßen angegeben:
`LUN: <LUN_VALUE>  WWPN: <WWPN_VALUE>`

Schritt 8. Klicken Sie in der Spalte **Netzwerkeinstellungen** in der Zeile für den Server auf **Bearbeiten**, um die Netzwerkeinstellungen für diese Implementierung zu konfigurieren. Die Seite „Netzwerkeinstellungen ändern“ wird angezeigt.

Machen Sie in folgenden Feldern die erforderlichen Angaben:
- Hostname
- MAC-Adresse für den Port auf dem Host, auf dem das Betriebssystem installiert wird
- DNS-Server (falls erforderlich)
- MTU-Geschwindigkeit

Anmerkungen: Wenn Sie im Dialogfenster Globale Einstellungen: Betriebssysteme implementieren die Option **Statische IP-Adresse (IPv4) zuordnen** ausgewählt haben (siehe Schritt Schritt 3 4 auf Seite 651), müssen Sie auch die folgenden Informationen eingeben:
- IPv4-Adresse
- Teilnetzmaske
- Gateway



Schritt 9. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Der Implementierungsstatus für den Server auf der Seite BS-Images implementieren lautet nun „Bereitstellung“.

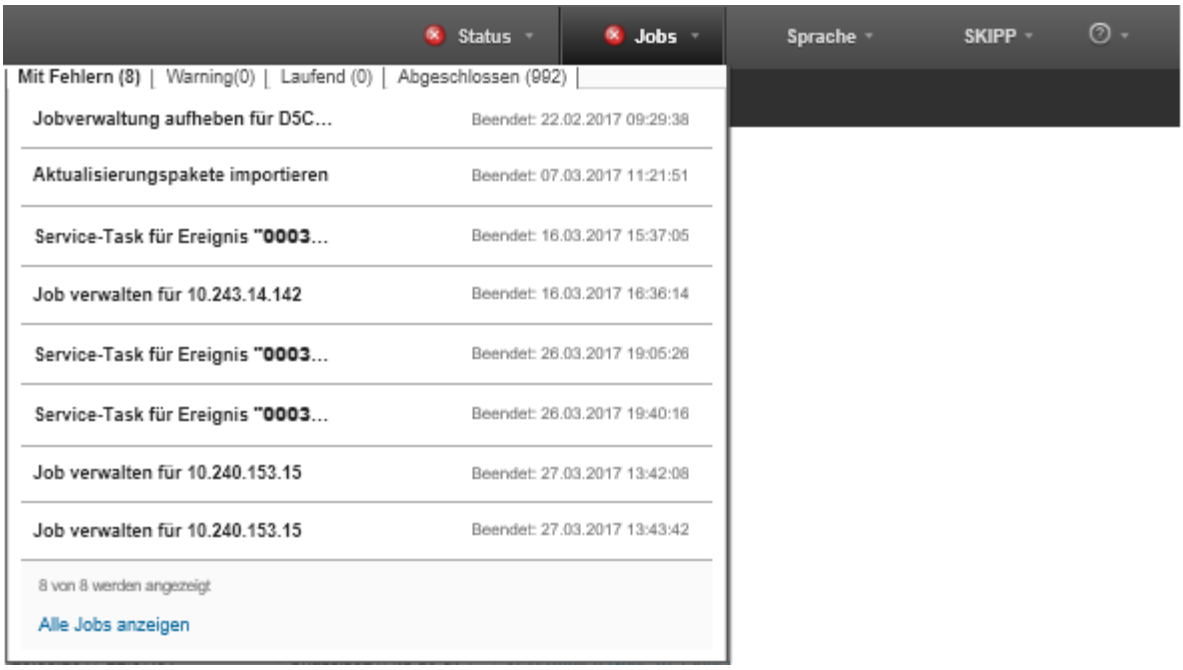
Schritt 10. Klicken Sie zum Implementieren des Betriebssystems auf **Alle Aktionen → Images implementieren**.

Schritt 11. Klicken Sie auf der Bestätigungsseite auf **Implementieren**, um das Image zu implementieren.

Wenn auf dem Server bereits ein Betriebssystem installiert ist, werden Sie gewarnt, dass das aktuelle Betriebssystem durch die Implementierung des Image überschrieben wird.

Tipp: Sie können eine Fernsteuerungssitzung einrichten, um den Fortschritt der Installation zu beobachten. Klicken Sie auf **Alle Aktionen → Fernsteuerung**, um eine Fernsteuerungssitzung für den Server zu starten.

Wenn Sie das Betriebssystem implementieren, startet Lenovo XClarity Administrator einen Job zur Implementierungsverfolgung. Um den Status des Implementierungsjobs anzuzeigen, klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Jobs**. Klicken Sie dann auf die Registerkarte **Laufend**.

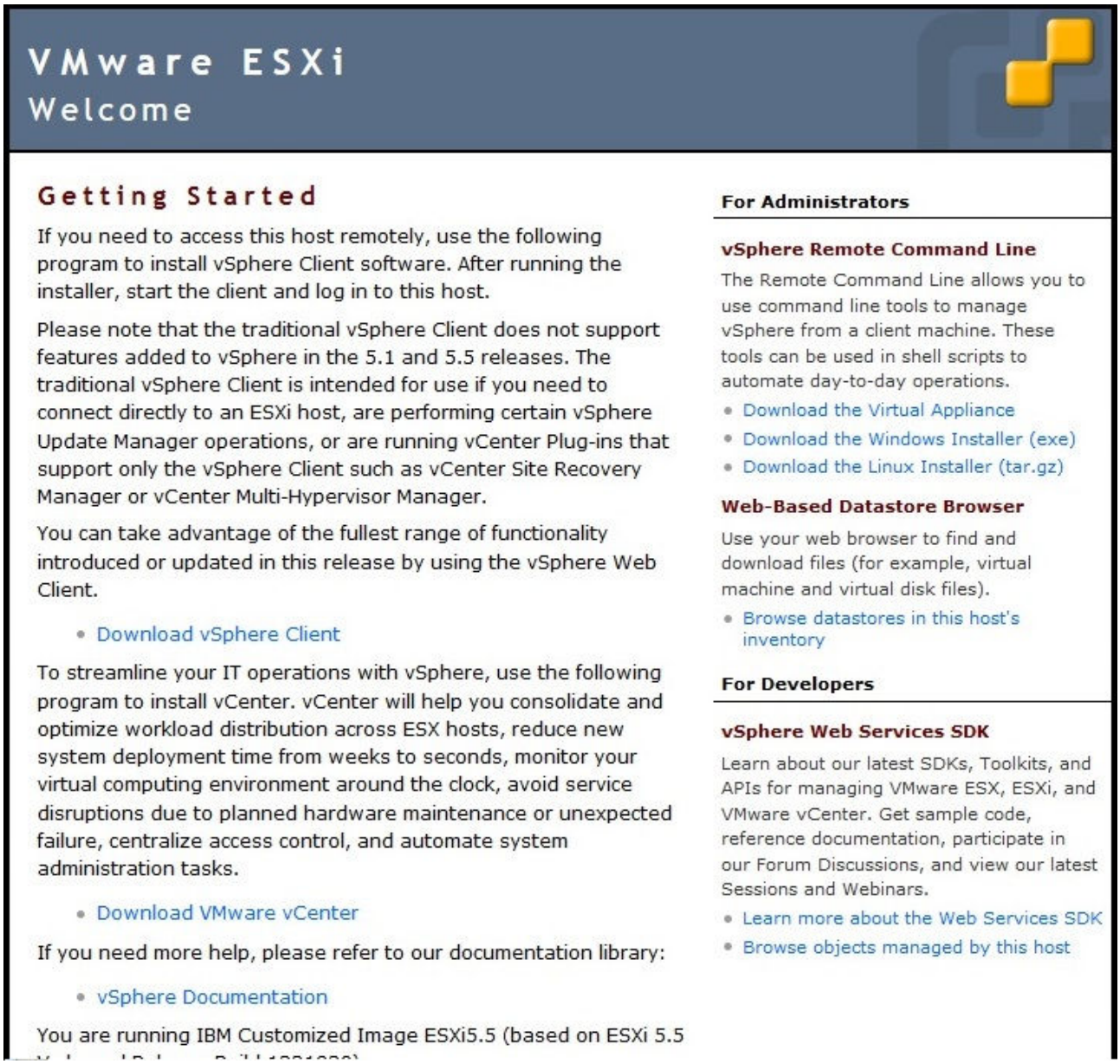


Bewegen Sie den Mauszeiger über den laufenden Job, um Details anzuzeigen, beispielsweise den Prozentsatz des Job-Fortschritts.

Ergebnisse

Wenn die Betriebssystembereitstellung abgeschlossen ist, melden Sie sich bei der IP-Adresse an, die Sie auf der Seite Netzwerkeinstellungen ändern angegeben haben. Dann wird der Konfigurationsprozess fortgesetzt.

Anmerkung: 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.


VMware ESXi
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.
You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
If you need more help, please refer to our documentation library:
vSphere Documentation
You are running IBM Customized Image ESXi5.5 (based on ESXi 5.5
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in this host's inventory
For Developers
vSphere Web Services SDK
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.
Learn more about the Web Services SDK
Browse objects managed by this host

Hinweise

Möglicherweise bietet Lenovo die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim Lenovo Ansprechpartner erhältlich.

Hinweise auf Lenovo Lizenzprogramme oder andere Lenovo Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von Lenovo verwendet werden können. Anstelle der Lenovo Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von Lenovo verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es Lenovo Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Dokuments sind kein Angebot und keine Lizenz unter Patenten oder Patentanmeldungen verbunden. Anfragen sind schriftlich an die nachstehende Adresse zu richten:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO STELLT DIESE VERÖFFENTLICHUNG IN DER VORLIEGENDEN FORM (AUF „AS-IS“-BASIS) ZUR VERFÜGUNG UND ÜBERNIMMT KEINE GARANTIE FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE FREIHEIT DER RECHTE DRITTER. Einige Rechtsordnungen erlauben keine Garantieausschlüsse bei bestimmten Transaktionen, sodass dieser Hinweis möglicherweise nicht zutreffend ist.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Lenovo kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Die in diesem Dokument beschriebenen Produkte sind nicht zur Verwendung bei Implantationen oder anderen lebenserhaltenden Anwendungen, bei denen ein Nichtfunktionieren zu Verletzungen oder zum Tode führen könnte, vorgesehen. Die Informationen in diesem Dokument beeinflussen oder ändern nicht die Lenovo Produktspezifikationen oder Garantien. Keine Passagen in dieser Dokumentation stellen eine ausdrückliche oder stillschweigende Lizenz oder Anspruchsgrundlage bezüglich der gewerblichen Schutzrechte von Lenovo oder von anderen Firmen dar. Alle Informationen in dieser Dokumentation beziehen sich auf eine bestimmte Betriebsumgebung und dienen zur Veranschaulichung. In anderen Betriebsumgebungen werden möglicherweise andere Ergebnisse erzielt.

Werden an Lenovo Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses Lenovo Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten überprüfen, welche Daten für ihre jeweilige Umgebung maßgeblich sind.

Marken

Lenovo