



Lenovo ThinkAgile  
SXM Serie  
Administratorhandbuch



## **Hinweise**

### **Anmerkung**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts lesen Sie die Sicherheitsinformationen und -hinweise, die unter der folgenden Adresse verfügbar sind:

[https://pubs.lenovo.com/safety\\_documentation/pdf\\_files](https://pubs.lenovo.com/safety_documentation/pdf_files)

Außerdem müssen Sie sicherstellen, dass Sie mit den Geschäftsbedingungen der Lenovo Warranty für Ihre Lösung vertraut sind, die Sie unter der folgenden Adresse finden:

<http://datacentersupport.lenovo.com/warrantylookup>

**Sechste Ausgabe (November 2023)**

**© Copyright Lenovo 2017, 2023.**

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

---

# Inhaltsverzeichnis

<b>Inhaltsverzeichnis</b> . . . . .	<b>i</b>
<b>Abbildungen</b> . . . . .	<b>.iii</b>
<b>Tabellen</b> . . . . .	<b>v</b>
<b>Kapitel 1. ThinkAgile SXM Serie Lösungen verwalten</b> . . . . .	<b>1</b>
ThinkAgile SXM – Hinweise zur Verwaltung . . . . .	1
<b>Kapitel 2. Produktverwaltung und -änderungen</b> . . . . .	<b>3</b>
Standardverwaltung . . . . .	3
IDs und Kennwörter verwalten . . . . .	4
<b>Kapitel 3. ThinkAgile SXM Serie Lösungsfirmware aktualisieren</b> . . . . .	<b>5</b>
Firmwarewartung und optimale Vorgehensweise . . . . .	5
Vorbedingungen . . . . .	5
Aktualisierung der Firmware für ThinkAgile SXM vorbereiten . . . . .	6
XClarity Administrator für eine bestimmte optimale Vorgehensweise konfigurieren . . . . .	6
XClarity Administrator aktualisieren . . . . .	7
Firmwareaktualisierungspakete importieren . . . . .	9
Firmwarekonformitätsrichtlinie importieren . . . . .	11
Firmwarekonformitätsrichtlinie zuordnen . . . . .	13
ThinkAgile SXM OEM Extension Package aktualisieren . . . . .	15
Vorbedingungen . . . . .	16
LXCA-Details für Azure Stack Hub bereitstellen . . . . .	16
Aktuelle Versionen bestimmen . . . . .	18
Speichercontainer für Aktualisierung erstellen . . . . .	19
OEM Extension Package hochladen . . . . .	20
Aktualisierung durchführen . . . . .	23
Aktualisierung und Azure Stack Hub- Funktionalität überprüfen . . . . .	25
ThinkAgile SXM Switch-Firmware aktualisieren (nur Lenovo Switches) . . . . .	25
Vorbedingungen . . . . .	26
XClarity Administrator für Aktualisierung von Switch-Firmware vorbereiten . . . . .	26
Lenovo TOR-Switch-Firmware aktualisieren . . . . .	27
Lenovo BMC-Switch-Firmware aktualisieren . . . . .	42

Rückstellung . . . . .	53
Aktualisierte CNOS-Befehlssyntax. . . . .	54

## **Kapitel 4. Hinweise zum Warten und Austauschen von Komponenten. . . . . 55**

Server austauschen . . . . .	55
Serverteile austauschen . . . . .	56

## **Anhang A. XClarity Administrator implementieren und konfigurieren . . . . . 59**

Aktuelle LXCA-Installation stilllegen . . . . .	59
LXCA implementieren und konfigurieren . . . . .	65
Statische IP-Adresse für LXCA konfigurieren . . . . .	67
Aufgabe „Lenovo XClarity Administrator- Lizenzvereinbarung lesen und akzeptieren“ . . . . .	70
Aufgabe „Benutzeraccount erstellen“ . . . . .	71
Aufgabe „Netzwerkzugriff konfigurieren“ . . . . .	74
Aufgabe „Einstellungen für Datum und Uhrzeit konfigurieren“ . . . . .	78
Aufgabe „Einstellungen für Service und Support konfigurieren“ . . . . .	79
Aufgabe „Weitere Sicherheitseinstellungen konfigurieren“ . . . . .	83
Aufgabe „Systemverwaltung starten“ . . . . .	84
LXCA Pro-Lizenz übernehmen . . . . .	85
LXCA-Aktualisierungspaket übernehmen . . . . .	85
Knoten verwalten . . . . .	88
Servermuster importieren und übernehmen . . . . .	91

## **Anhang B. ThinkAgile SXM Serie Switches mit der CLI aktualisieren (nur Lenovo Switches) . . . . . 95**

Vorbedingungen . . . . .	95
Switch-Image-Dateien vorbereiten . . . . .	95
Zustand von Azure Stack Hub überprüfen . . . . .	97
Lenovo TOR-Switch-Firmware mit der CLI aktualisieren . . . . .	97
TOR-Switch-Konfiguration sichern . . . . .	97
CNOS auf TOR-Switches mit der CLI aktualisieren . . . . .	98
BMC-Switch-Firmware mit der CLI aktualisieren . . . . .	101
BMC-Switch-Konfiguration sichern . . . . .	101
BMC-Switch mit der CLI aktualisieren . . . . .	102



# Abbildungen

1.	<b>Menü „Verwaltung“ → Verwaltungsserver aktualisieren</b>	7
2.	LXCA-Aktualisierungspaket hochladen	8
3.	Aktualisierung des Verwaltungsservers durchführen	8
4.	Neustartmeldung nach XClarity Administrator-Aktualisierung	9
5.	Anforderungsmeldung zu XClarity Administrator-Aktualisierung	9
6.	Firmwareaktualisierungs-Repository von XClarity Administrator	10
7.	Auswählen von Dateien für den Import.	10
8.	Status des Firmwareimports	11
9.	Produktkatalog mit neuen Aktualisierungen	11
10.	Firmwareaktualisierungen: Fenster „Konformitätsrichtlinien“	12
11.	Firmwarekonformitätsrichtlinie importieren	12
12.	Importierte Firmwarekonformitätsrichtlinie	13
13.	Fenster „Firmwareaktualisierungen: Übernehmen/Aktivieren“	14
14.	Fenster „Globale Einstellungen: Firmwareaktualisierungen“	14
15.	Firmwarekonformitätsrichtlinie, die nicht konforme Knoten zeigt	15
16.	Anmeldeinformationen, die für die Anmeldung bei LXCA verwendet werden	18
17.	Überprüfung der aktuell ausgeführten Versionen von Azure Stack Hub	19
18.	Navigieren zum Speichercontainer „updateadminaccount“	19
19.	Navigieren zum Speichercontainer „Blobs“	20
20.	Erstellen des neuen Containers	20
21.	Auswählen des Speichercontainers zum Hochladen	21
22.	Auswählen des Steuerelements „Hochladen“	21
23.	Auswählen der Aktualisierungspaketdateien zum Hochladen	22
24.	Hochladen der Aktualisierungspaketdateien	22
25.	Überprüfen, ob Uploads erfolgreich abgeschlossen wurden	23
26.	Initiieren der Aktualisierung	23
27.	Anzeigen zum Aktualisierungsfortschritt	24
28.	Installationsdetails	24
29.		27
30.	Überprüfen des Azure Stack Hub-Zustands vor der Aktualisierung	27
31.	Auswählen beider TOR-Switches	28
32.	Sichern der TOR-Konfigurationsdatei	28
33.	Dialogfeld „Konfigurationsdatei sichern“	29

34.	Ergebnisse der Konfigurationsdateisicherung	29
35.	Auswahl der gesicherten Konfigurationsdatei zum Download auf einen lokalen PC	30
36.	Auswählen des TOR1-Switches für die Aktualisierung	31
37.	Auswählen von Optionen in der TOR1-Aktualisierungszusammenfassung	32
38.	Aktualisierungsfortschritt auf der Jobs-Seite	33
39.	Aktive und Standby-Images	34
40.	PuTTY-Sicherheitshinweis	35
41.	Alert-Überprüfung im Azure Stack Hub-Administratorportal	41
42.	Überprüfen der Firmwareaktualisierungen der TOR-Switches auf Vollständigkeit	42
43.	Auswahl des BMC-Switches für die Sicherung	43
44.	Überprüfen und Kommentieren des BMC-Switches für die Sicherung	43
45.	Auswahl der gesicherten Konfigurationsdatei zum Download	44
46.	Auswählen von BMC-Aktualisierungs- und -Aktivierungsregeln	45
47.	Überwachen des BMC-Aktualisierungsfortschritts auf der Jobs-Seite	46
48.	Überprüfen der neuen ausgeführten BMC-Firmware im aktiven Image	47
49.	LXCA-IPv4-Einstellungen, die notiert werden müssen	60
50.	Auswählen der zu deaktivierenden LXCA-Serverprofile	61
51.	Zurücksetzen der BMC-Identitätseinstellungen	62
52.	Aufheben der Knotenverwaltung	63
53.	Auswahl der erzwungenen Verwaltungsaufhebung von Knoten	64
54.	Fenster „Verbindung der virtuellen Maschine“	68
55.	Parameter der virtuellen Maschine	69
56.	Seite „LXCA-Ersteinrichtung“	70
57.	Fenster „Lenovo XClarity Administrator-Lizenzvereinbarung lesen und akzeptieren“	71
58.	Fenster „Neuen Supervisor-Benutzer erstellen“	72
59.	Fenster „Lokale Benutzerverwaltung“	73
60.	Fenster „Lokale Benutzerverwaltung“ mit Backup-Benutzer	74
61.	Fenster „Netzwerkzugriff bearbeiten“	75
62.	Einstellungen-Registerkarte „DNS & Proxy“	76
63.	Deaktivieren der IPv6-Einstellungen	77
64.	Speichern von Änderungen in der Registerkarte „IP-Einstellungen“	77
65.	Seite „Erstkonfiguration“ mit abgehakten abgeschlossenen Aufgaben	78

66. Fenster „Datum und Uhrzeit bearbeiten“ . . . . .	79	79. Gespeicherte Anmeldeinformationen verwalten . . . . .	89
67. Registerkarte „Service und Support – Regelmäßiger Daten-Upload“ . . . . .	80	80. Erstellen neuer gespeicherter Anmeldeinformationen . . . . .	89
68. Registerkarte „Call-Home-Konfiguration“ von Service und Support. . . . .	80	81. Auswählen neuer gespeicherter Anmeldeinformationen für die Verwaltung . . . . .	90
69. Registerkarte „Lenovo Upload-Funktionalität“ von Service und Support. . . . .	81	82. Herstellen von Verwaltungsverbindungen mit jedem XClarity Controller . . . . .	90
70. Registerkarte „Garantie“ von Service und Support. . . . .	82	83. Alle Server anzeigen . . . . .	91
71. Seite „Kennwort zur Service-Wiederherstellung“ . . . . .	83	84. Bestandserfassung abgeschlossen . . . . .	91
72. Fenster „Erstkonfiguration“ mit einer unerledigten Aufgabe . . . . .	84	85. Implementieren eines Musters . . . . .	92
73. Auswählen von „Nein, Demodaten nicht einbeziehen“ im Fenster „Systemverwaltung starten“ . . . . .	84	86. Implementieren des Musters mit vollständiger Aktivierung . . . . .	93
74. Seite „Lizenzverwaltung“ mit angezeigter gültiger LXCA Pro-Lizenz . . . . .	85	87. Steuerelement „Zu Profile wechseln“ . . . . .	93
75. Auswählen von LXCA-FixPack-Dateien . . . . .	86	88. Serverprofile mit Status „Aktiv“ . . . . .	94
76. Auswählen des Aktualisierungspakets und Aktualisierung . . . . .	87	89. Broadwell-basierte ThinkAgile SXM Switch-Firmwareaktualisierungspakete . . . . .	96
77. Finale Status des Aktualisierungspakets . . . . .	87	90. Inhalt des Switch-Firmwareaktualisierungsarchivs . . . . .	96
78. Vier Knoten, die zur Verwaltung ausgewählt sind . . . . .	88	91. ThinkAgile SXM Switch-Firmware-IMGS-Image-Dateien . . . . .	97
		92. Überprüfen des Zustands von Azure Stack Hub . . . . .	97
		93. Alert-Überprüfung im Azure Stack Hub-Administratorportal . . . . .	101

---

# Tabellen





---

# Kapitel 1. ThinkAgile SXM Serie Lösungen verwalten

Diese Dokumentation bezieht sich auf die folgenden Produkte:

- SXM4400
- SXM6400
- SXM4600

---

## ThinkAgile SXM – Hinweise zur Verwaltung

Die folgenden Hinweise und Einschränkungen gelten für ThinkAgile SXM Lösungen.

### Einschränkungen bei automatisierten Serviceanforderungen (Call-Home-Funktion)

Da ThinkAgile SXM-Produkte auf Rackebene gewartet und unterstützt werden, empfehlen wir Ihnen, die Call-Home-Funktion für die Komponenten nicht zu aktivieren. Wenn Sie sich zur Aktivierung der Call-Home-Funktion entscheiden, beachten Sie, dass Ihre Berechtigung möglicherweise nicht erkannt wird.

### Firmware und Einhaltung der optimalen Vorgehensweise

Lenovo veröffentlicht eine „optimale Vorgehensweise“ für die Firmware von ThinkAgile SXM, in der die unterstützten Ebenen der verschiedenen Komponenten identifiziert werden. Jede Firmware, die sich über oder unter der in der optimalen Vorgehensweise genannten Version befindet, wird nicht unterstützt und wirkt sich möglicherweise auf die Fähigkeit von Lenovo aus, Probleme mit der entsprechenden Komponente zu unterstützen. Weitere Informationen finden Sie unter [„Firmwarewartung und optimale Vorgehensweise“ auf Seite 5](#).

### ThinkAgile SXM-Berechtigung

ThinkAgile SXM Lösungen besitzen eine Berechtigung auf Rackebene.

Wenn Sie Support für das Produkt oder seine Komponenten oder die integrierte Software benötigen, verwenden Sie unbedingt die Seriennummer Ihres Racks, die dem Maschinentyp 9565 zugeordnet ist. Wenn Sie die Komponentenummer oder die Softwareseriennummer verwenden, erkennt der ThinkAgile Advantage Support möglicherweise nicht sofort die korrekte Berechtigung, was eine ordnungsgemäße Verarbeitung des Vorgangs verzögern kann. Sie finden die Seriennummer auf dem Racketikett.



---

## Kapitel 2. Produktverwaltung und -änderungen

Aufgrund der Komplexität von ThinkAgile SXM Serie Lösungen müssen bestimmte Änderungen sorgfältig geplant werden.

### Änderungen mit hohen Auswirkungen

Die folgenden Änderungen (oder die Nichteinhaltung von Bestimmungen) können sich erheblich auf die Funktionalität der Lösung auswirken.

- Die Punkt-zu-Punkt-Verkabelung aus der Erstkonfiguration ändern
- Firmware, Software oder Betriebssystem (einschließlich CNOS, ENOS und Cumulus Linux) auf Versionen ändern, die nicht in der optimalen Vorgehensweise genannt sind

Siehe „[Firmwarewartung und optimale Vorgehensweise](#)“ auf [Seite 5](#) für weitere Informationen.

- Das IPv4-Netzwerkschema, wie Adressen und Subnetze, ändern
- Die IPv4-Adressen für Server oder Switches ändern
- Den Verwaltungsstapel außerhalb der empfohlenen Versionen aktualisieren
- Das IMM, XCC oder UEFI auf die anfänglichen werkseitigen Standardwerte zurücksetzen
- Einen Netzwerk-Switch auf seine Erstkonfiguration zurücksetzen

---

## Standardverwaltung

Nach der ersten Einrichtung und Konfiguration der ThinkAgile SXM Serie Lösung durch Lenovo Professional Services sollten Sie das System regelmäßig mit der folgenden Software verwalten können.

### Lenovo XClarity Administrator

Verwenden Sie [Lenovo XClarity Administrator](#), um die Hardware überwachen und verwalten zu können. Zu den typischen Anwendungsszenarien zählen die folgenden:

- UEFI-Einstellungen (gemäß der ThinkAgile SXM Musterdatei)
- Firmware- und Gerätetreiberaktualisierungen (gemäß der optimalen Vorgehensweise für ThinkAgile SXM) über den Patch- und Update-Prozess von Microsoft Azure Stack Hub
- Hardware-Alerts und Problembeseitigung

Relevante Links finden Sie unter [https://pubs.lenovo.com/thinkagile-sxm/printable\\_doc](https://pubs.lenovo.com/thinkagile-sxm/printable_doc).

### Microsoft Azure Stack Hub-Portale

Microsoft Azure Stack Hub aktiviert die Verwaltung über die folgenden Portale:

- Administratorportal

Ein Administrator kann folgende Aufgaben ausführen:

- Verwaltungs-Tasks ausführen
- Ressourcen und Ressourcengruppen anzeigen
- VMs, Pläne und Angebote erstellen
- Die Lösungsintegrität überwachen

- Tenant-Portal

Ein Tenant kann folgende Aufgaben ausführen:

- Verfügbare Ressourcen zur Durchführung von Arbeiten verwenden
- VMs, Pläne und Angebote verwenden, die von einem Administrator erstellt wurden

Relevante Links finden Sie unter [https://pubs.lenovo.com/thinkagile-sxm/printable\\_doc](https://pubs.lenovo.com/thinkagile-sxm/printable_doc).

---

## IDs und Kennwörter verwalten

Eine ordnungsgemäße Aufbewahrung von IDs und Kennwörtern ist wichtig für die Sicherheit der Komponenten und das gesamte Produkt. Der Prüfungsausschuss zur Softwaresicherheit von Lenovo betont mit äußerstem Nachdruck, dass Kunden alle Anmeldeinformationen für Produkte gemäß den hier genannten Empfehlungen verwalten sollten.

### Anfängliche IDs und Kennwörter

Gültige IDs und Kennwörter werden während der Lenovo Professional Services-Bereitstellungsphase festgelegt oder geändert. Lenovo Professional Services stellt in der Dokumentation, die dem Kunden bei der Lösungsübergabe zur Verfügung gestellt wird, eine Liste aller Anmeldeinformationen für die Implementierung und Verwaltung der ThinkAgile SXM Serie Lösung zur Verfügung. Lenovo Professional Services stellt in der Dokumentation, die dem Kunden bei der Lösungsübergabe zur Verfügung gestellt wird, eine Liste aller Anmeldeinformationen für die Implementierung und Verwaltung der ThinkAgile SXM Serie Lösung zur Verfügung.

### Kennwörter ändern

Die Verfahren zum Ändern von Kennwörtern finden Sie in der Dokumentation der entsprechenden Komponente. Siehe [https://pubs.lenovo.com/thinkagile-sxm/printable\\_doc](https://pubs.lenovo.com/thinkagile-sxm/printable_doc). Insbesondere die folgende Microsoft-Webseite bietet einen Überblick und detaillierte Anweisungen zum Rotieren von Geheimnissen in der Azure Stack Hub-Umgebung:

<https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets>

**Wichtig:** Wenn Sie einige IDs oder Kennwörter ohne ordnungsgemäße Planung ändern (z. B. die IMM/XCC-Anmeldeinformationen auf einem der Skalierungseinheit Knoten), kann sich dies auf die Gesamtkonfiguration der Lösung auswirken und dazu führen, dass die Knoten nicht über XClarity Administrator verwaltet werden können.

### Kennwortkriterien

Die folgenden Kennwortkriterien werden vom Prüfungsausschuss zur Softwaresicherheit von Lenovo dringend empfohlen:

- Nicht weniger als zwanzig (20) Zeichen
- Enthält Buchstaben, insbesondere Groß- und Kleinschreibung
- Enthält Nummern
- Enthält Interpunktion
- Enthält keine wiederholten Zeichen

Zusätzlich wird die Verwendung eines Generators für zufällige Kennwörter empfohlen. Ein Beispiel hierfür ist der [Norton Identity Safe Password Generator](#). Siehe folgende Website:

<https://identitysafe.norton.com/password-generator>

---

## Kapitel 3. ThinkAgile SXM Serie Lösungsfirmware aktualisieren

Die folgenden Abschnitte enthalten erforderliche Schritte zum Aktualisieren von Firmware, Gerätetreibern und Software auf den Knoten und Netzwerk-Switches einer laufenden ThinkAgile SXM Serie Lösung, basierend auf der aktuellen lösungsspezifischen optimalen Vorgehensweise.

Die aktuelle optimale Vorgehensweise für ThinkAgile SXM finden Sie unter der folgenden URL:

<https://datacentersupport.lenovo.com/us/en/solutions/HT505122>

Der vollständige Aktualisierungsprozess der System-Firmware umfasst die folgenden Hauptaktivitäten und kann je nach der aktuell ausgeführten Version des Azure Stack Hub Builds geringfügig abweichen.

---

### Firmwarewartung und optimale Vorgehensweise

ThinkAgile SXM Serie Lösungen verwenden eine „optimale Vorgehensweise“, um die unterstützten Firmwareversionen für das Produkt zu identifizieren.

Informationen zur optimalen Vorgehensweise von ThinkAgile SXM Serie erhalten Sie auf der folgenden Website:

<https://datacentersupport.lenovo.com/solutions/ht505122>

#### Einhaltung der optimalen Vorgehensweise und Auswirkungen auf den Support

Die optimalen Vorgehensweisen für ThinkAgile SXM Serie umfassen Firmwareversionen der Komponente, die in einer entsprechenden Umgebung getestet wurden. Jede Firmware, die sich über oder unter der in der optimalen Vorgehensweise genannten Version befindet, wird nicht unterstützt und wirkt sich möglicherweise auf die Fähigkeit von Lenovo aus, Probleme mit der entsprechenden Komponente oder der gesamten Lösung unterstützen zu können.

#### Firmware aktualisieren

Links zu relevanten Dokumentationen finden Sie unter [https://pubs.lenovo.com/thinkagile-sxm/printable\\_doc](https://pubs.lenovo.com/thinkagile-sxm/printable_doc).

---

### Vorbedingungen

Stellen Sie vor Beginn des Prozesses sicher, dass Sie die folgenden Elemente zur Verfügung haben:

- Anmeldeinformationen für den Zugriff auf das Azure Stack Hub-Administratorportal
- Anmeldeinformationen für den Zugriff auf XClarity Administrator auf dem HLH
- USB-Stick mit:
  - Lenovo ThinkAgile SXM-Firmwareaktualisierungsdateien für die entsprechende optimale Vorgehensweise
  - XClarity Administrator-Firmwareaktualisierungsrichtlinien-Datei für die entsprechende optimale Vorgehensweise
  - Lenovo OEM Extension Package für die entsprechende optimale Vorgehensweise

**Anmerkung:** Die obigen Elemente finden Sie im ThinkAgile SXM-Repository unter der folgenden URL:

---

## Aktualisierung der Firmware für ThinkAgile SXM vorbereiten

Gehen Sie wie folgt vor, um die ThinkAgile SXM Firmwareaktualisierung vorzubereiten.

Schritt 1. Greifen Sie über <https://thinkagile.lenovo.com/SXM> auf das ThinkAgile SXM Aktualisierungs-Repository zu.

Auf der obersten Ebene befinden sich Verzeichnisse basierend auf bestimmten optimalen Vorgehensweisen für ThinkAgile SXM. Jedes Verzeichnis enthält einen vollständigen Satz Dateien, die für eine bestimmte optimale Vorgehensweise und Hardwareplattform erforderlich sind.

Schritt 2. Klicken Sie auf den Link für das Verzeichnis mit der aktuellen optimalen Vorgehensweise.

Schritt 3. Laden Sie erforderlichen Dateien für Ihre Umgebung basierend auf folgenden Kriterien herunter:

- Laden Sie die folgenden Dateien für alle Umgebungen herunter:
  - AzureStackRecoveryHelper.ps1
  - LXCA\_<date>.zip
  - OEM Extension Package für die optimale Vorgehensweise
- Wenn Ihre Lösung eine SXM4400 oder SXM6400 ist, laden Sie **PurleyFirmware\_SXMBR<yyyy>.zip** herunter (yyyy ist die Version der optimalen Vorgehensweise für die Lösung). Dieses einzelne Archiv enthält die Firmwareaktualisierungs-Nutzdatendateien für die SR650 Knoten.
- Wenn Ihre Lösung eine SXM4600 ist, laden Sie **EGSFirmware\_SXMBR<yyyy>.zip** herunter (yyyy ist die Version der optimalen Vorgehensweise für die Lösung). Dieses einzelne Archiv enthält die Firmwareaktualisierungs-Nutzdatendateien für die SR650 V3 Knoten.

Schritt 4. Entpacken Sie alle ZIP-Archive und kopieren Sie die entpackten Inhalte auf einen USB-Stick.

Schritt 5. Kopieren Sie die entpackten Inhalte folgendermaßen vom USB-Stick auf den Hardware Lifecycle Host (HLH):

1. Kopieren Sie die Skriptdatei AzureStackRecoveryHelper.ps1 nach D:\Lenovo\Scripts.
2. Kopieren Sie die **Inhalte** (nicht das Verzeichnis selbst) des Verzeichnisses LXCA\_<date> nach D:\Lenovo\LXCA. Dadurch werden alle Dateien oder Verzeichnisse mit demselben Namen ersetzt, die sich bereits im Verzeichnis befinden.
3. Kopieren Sie das Verzeichnis, das die heruntergeladenen Inhalte der Systemfirmwareaktualisierung enthält, nach D:\Lenovo\LXCA.

---

## XClarity Administrator für eine bestimmte optimale Vorgehensweise konfigurieren

Eine der Hauptaufgaben von XClarity Administrator in einer ThinkAgile SXM Serie Lösung ist die Bereitstellung einer einfachen Methode zur Verwaltung von Firmwareaktualisierungen auf den Knoten der Azure Stack Hub-Skalierungseinheit. Firmwareaktualisierungen müssen in XClarity Administrator importiert werden, bevor sie bei einem verwalteten System angewendet werden können. Da auf den Azure Stack Hub Knoten Firmwareversionen gemäß den [optimalen Vorgehensweisen](#) für die jeweilige Firmware ausgeführt werden müssen, werden die entsprechenden Firmwareaktualisierungspakete für jede veröffentlichte optimale Vorgehensweise in einem einzigen Verzeichnis bereitgestellt.

Sobald XClarity Administrator für eine optimale Vorgehensweise vorbereitet wurde, kann die Firmwareaktualisierung jederzeit stattfinden.

Gehen Sie für die Vorbereitung von XClarity Administrator zum Verwalten von Firmwareaktualisierungen wie folgt vor:

## XClarity Administrator aktualisieren

Mithilfe der Schritte in diesem Abschnitt können Sie XClarity Administrator bei Bedarf aktualisieren (prüfen Sie die aktuelle optimale Vorgehensweise), bevor Sie mit den restlichen Anweisungen fortfahren.

Befolgen Sie die Schritte in diesem Abschnitt, um XClarity Administrator zu aktualisieren. Die Aktualisierung von LXCA erfolgt normalerweise in zwei Schritten. Zuerst wird LXCA auf eine neue „Basisversion“ aktualisiert und anschließend wird ein „FixPack“ angewendet. Um LXCA beispielsweise auf v2.6.6 zu aktualisieren, wird das LXCA v2.6.0-Aktualisierungspaket auf eine beliebige frühere v2.x-Version von LXCA angewendet und anschließend wird das FixPack v2.6.6 auf LXCA v2.6.0 angewendet.

Die folgenden Beispiele zeigen den Prozess zum Aktualisieren von XClarity Administrator v2.1.0 auf v2.4.0. Sie gelten für die Aktualisierung auf eine beliebige Version.

- Schritt 1. Kopieren Sie das Verzeichnis des LXCA-Aktualisierungspakets nach D:\Lenovo\LXCA auf dem HLH.
- Schritt 2. Melden Sie sich auf dem HLH-Server bei XClarity Administrator an.
- Schritt 3. Navigieren Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle zu **Verwaltung** → **Verwaltungsserver aktualisieren**.

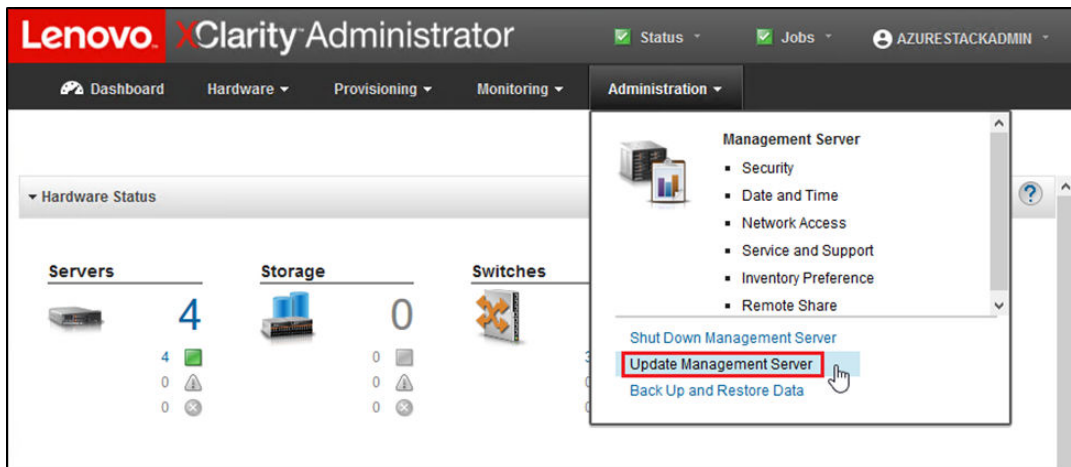


Abbildung 1. Menü „Verwaltung“ → Verwaltungsserver aktualisieren

- Schritt 4. Klicken Sie auf die Schaltfläche **Importieren** (  ).
- Schritt 5. Klicken Sie auf **Dateien auswählen**.
- Schritt 6. Navigieren Sie zu D:\Lenovo\LXCA\LXCA Update Package, wählen Sie alle vier Dateien im Verzeichnis aus und klicken Sie dann auf **Öffnen**. Die folgende Beispielabbildung zeigt die Aktualisierungspaketdateien für XClarity Administrator v2.4.0, die je nach der in der aktuellen optimalen Vorgehensweise angegebenen Version von XClarity Administrator variieren können.

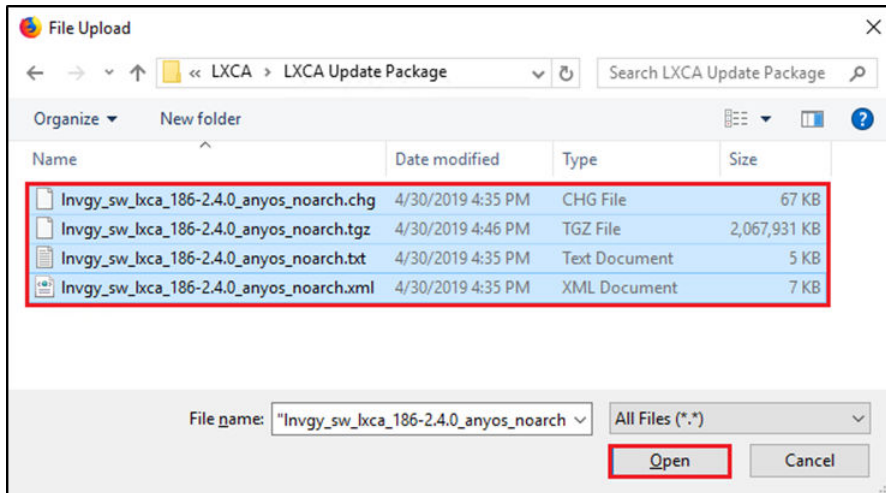



Abbildung 2. LXCA-Aktualisierungspaket hochladen

Schritt 7. Klicken Sie im Fenster „Importieren“ auf **Importieren**.

Schritt 8. Während des Importvorgangs wird der Status angezeigt. Überprüfen Sie nach Abschluss, ob in der Spalte „Downloadstatus“ für das XClarity Administrator-Aktualisierungspaket „Heruntergeladen“ angezeigt wird.

Schritt 9. Wählen Sie das Aktualisierungspaket aus, indem Sie auf das Optionsfeld links neben dem Paketnamen und dann auf die Schaltfläche **Aktualisierung durchführen** (  ) klicken.

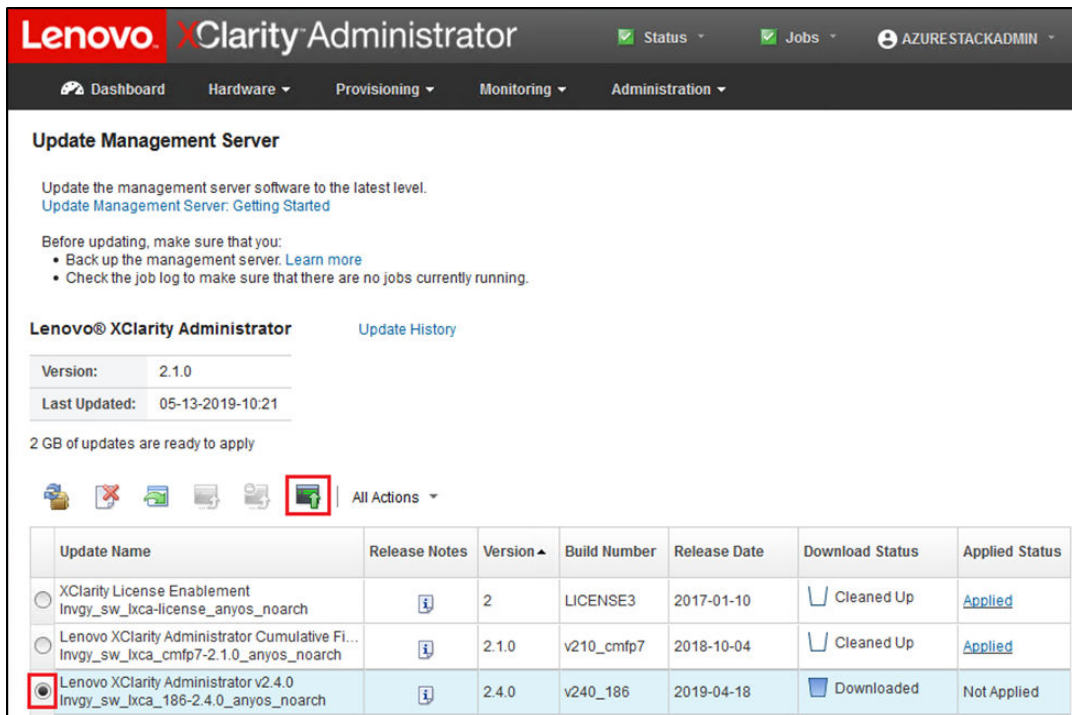


Abbildung 3. Aktualisierung des Verwaltungsservers durchführen

Schritt 10. Klicken Sie im angezeigten Bestätigungsfenster auf **Neu starten**.



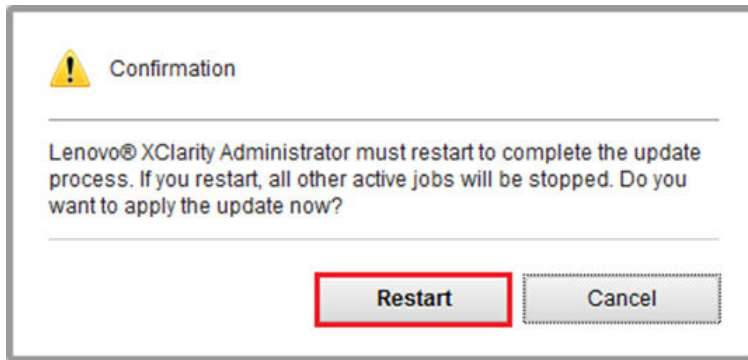


Abbildung 4. Neustartmeldung nach XClarity Administrator-Aktualisierung

Schritt 11. Nach einigen Sekunden wird die XClarity Administrator-Browser-Schnittstelle durch die folgende Meldung ersetzt:

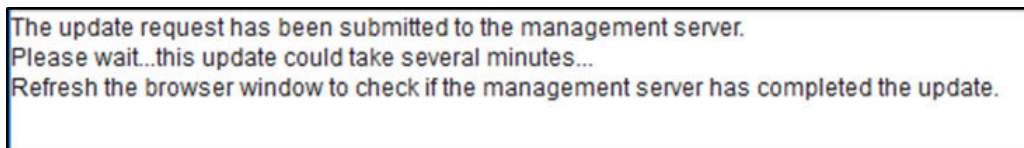


Abbildung 5. Anforderungsmeldung zu XClarity Administrator-Aktualisierung

Schritt 12. Sobald XClarity Administrator wieder online ist, stellen Sie die Verbindung wieder her und melden Sie sich bei der XClarity Administrator-Browser-Schnittstelle an. Nach der Anmeldung kann es mehrere Minuten dauern, bis alle Server und Switches korrekt in der XClarity Administrator-Schnittstelle angezeigt werden. Zunächst wird der Status möglicherweise als „Getrennt“ angezeigt.

## Firmwareaktualisierungspakete importieren

Gehen Sie zum Importieren von Firmwareaktualisierungen wie folgt vor:

Schritt 1. Wählen Sie im Hauptmenü von XClarity Administrator **Bereitstellung** → **Repository** aus. Zunächst ist das Firmware-Repository möglicherweise leer (z. B. wenn Sie XClarity Administrator gerade installiert und konfiguriert haben), was von der blauen Informationsmeldung in der folgenden Abbildung gezeigt wird.

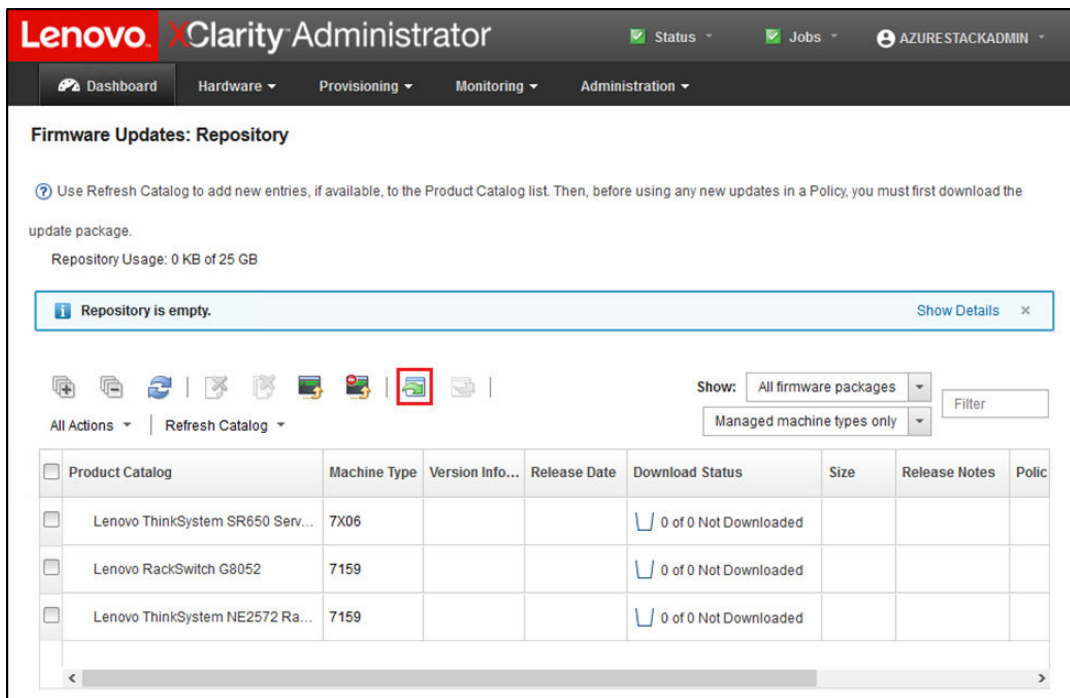


Abbildung 6. Firmwareaktualisierungs-Repository von XClarity Administrator

- Schritt 2. Klicken Sie auf das Symbol **Importieren** () und dann auf **Dateien auswählen ....**
- Schritt 3. Navigieren Sie zum entsprechenden Firmwareverzeichnis in D:\Lenovo\XCA, wie oben beschrieben, wählen Sie alle Dateien im Verzeichnis aus und klicken Sie auf **Öffnen**.

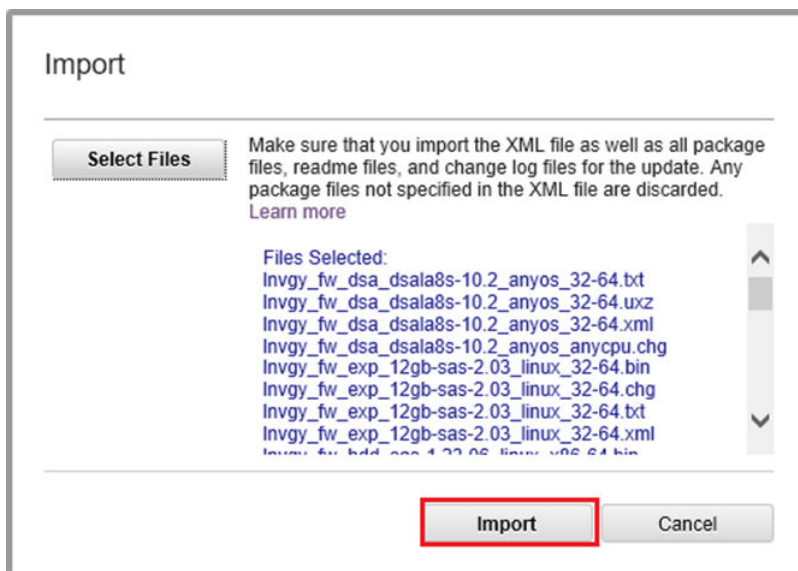


Abbildung 7. Auswählen von Dateien für den Import

- Schritt 4. Klicken Sie auf **Importieren**. Während Import und Validierung wird oben im Fenster eine Statusleiste angezeigt.

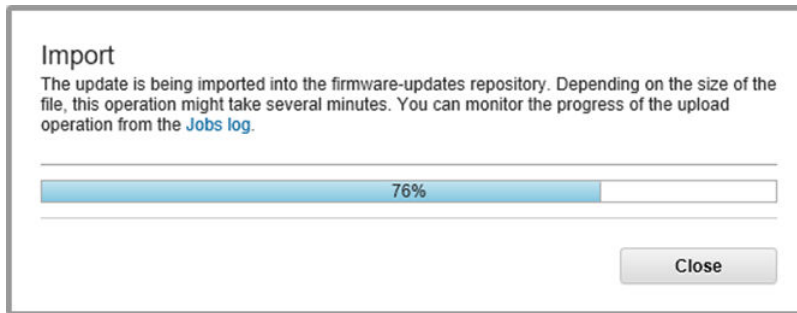


Abbildung 8. Status des Firmwareimports

Sie können den Produktkatalog nun erweitern, um die Firmwareaktualisierungsversion jeder Komponente anzuzeigen, die im Repository enthalten ist.

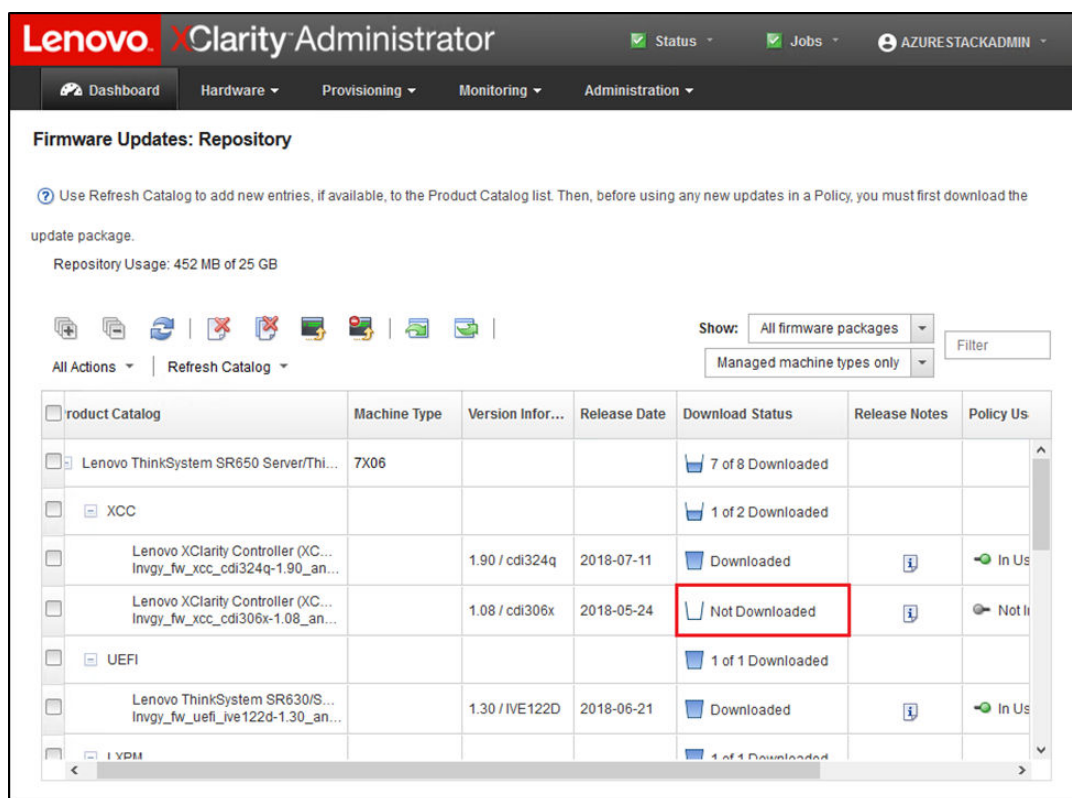


Abbildung 9. Produktkatalog mit neuen Aktualisierungen

## Firmwarekonformitätsrichtlinie importieren

Die Konformitätsrichtlinien von XClarity Administrator im LXCA\_<date>.zip-Archiv aus dem ThinkAgile SXM Aktualisierungs-Repository haben einen Namen im folgenden Format, damit Sie leicht erkennen können, für welche optimale Vorgehensweise sie bestimmt sind:

<Plattform>Policy\_SXMBRyyyy

wo <Plattform> entweder „Purley“ oder „EGS“ und yyyy die Version der optimalen Vorgehensweise für ThinkAgile SXM ist.

Gehen Sie wie folgt vor, um die XClarity Administrator-Firmwarekonformitätsrichtlinie zu importieren:

Schritt 1. Wählen Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle **Bereitstellung** → **Konformitätsrichtlinien** aus. Ähnlich wie beim Firmware-Repository werden möglicherweise bereits Firmwareaktualisierungsrichtlinien angezeigt. Diese Liste wird im Laufe der Zeit länger, wenn zusätzliche Richtlinien für neue optimale Vorgehensweisen hinzugefügt werden. Im folgenden Beispiel-Screenshot sehen Sie drei vorherige Richtlinien für optimale Vorgehensweisen SXMBR1903, SXMBR1905 und SXMBR1910 für die Purley-Plattform. Wir fahren mit diesem Beispiel fort und bereiten XClarity Administrator für die optimale Vorgehensweise SXMBR2002 für die Purley-Plattform vor.

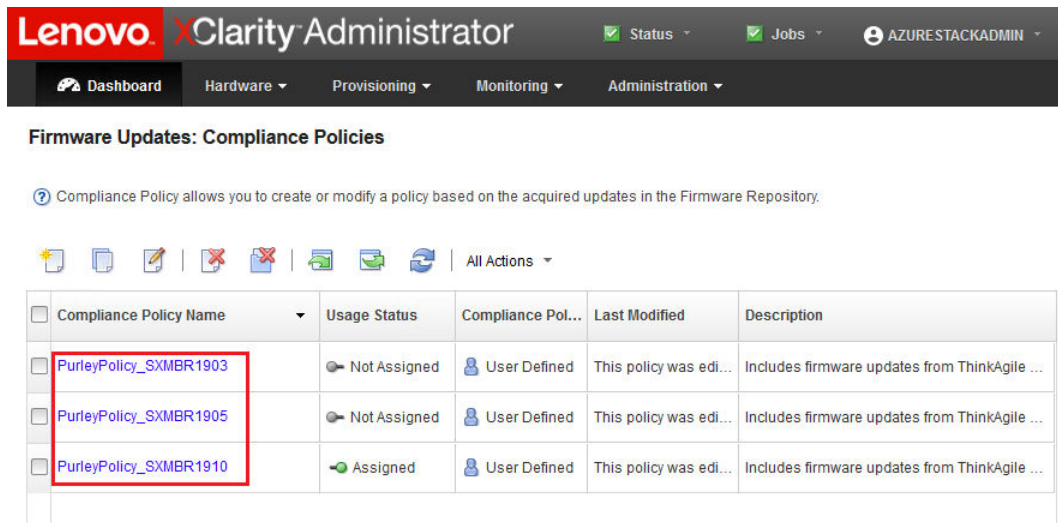


Abbildung 10. Firmwareaktualisierungen: Fenster „Konformitätsrichtlinien“

Schritt 2. Klicken Sie auf das Symbol **Importieren** (  ) und dann auf **Dateien auswählen ....**

Schritt 3. Navigieren Sie zu D:\Lenovo\XCA, wählen Sie die Datei mit dem Titel <Platform>Policy\_SXMBRyyy.xml aus und klicken Sie dann auf **Importieren**. Wie zuvor angegeben, steht „<Platform>“ im Dateinamen je nach Lösung entweder für „Purley“ oder „EGS“, und „yyy“ spiegelt die Version der optimalen Vorgehensweise für ThinkAgile SXM wider, für die die Richtliniendatei erstellt wurde. Nachdem die Richtlinie importiert wurde, wird sie auf der Seite „Firmwareaktualisierungen: Konformitätsrichtlinien“ angezeigt.

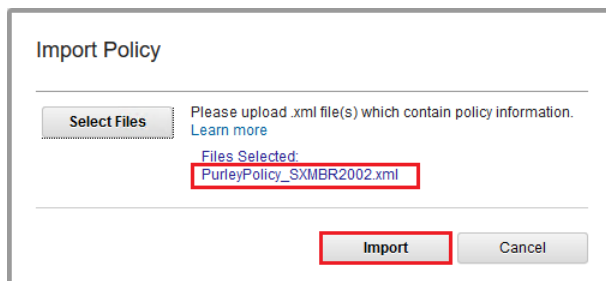


Abbildung 11. Firmwarekonformitätsrichtlinie importieren

### Firmware Updates: Compliance Policies

Compliance Policy allows you to create or modify a policy based on the acquired updates in the Firmware Repository.

All Actions

<input type="checkbox"/>	Compliance Policy Name	Usage Status	Compliance Pol...	Last Modified	Description
<input type="checkbox"/>	PurleyPolicy_SXMBR1903	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
<input type="checkbox"/>	PurleyPolicy_SXMBR1905	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
<input type="checkbox"/>	PurleyPolicy_SXMBR1910	Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
<input type="checkbox"/>	PurleyPolicy_SXMBR2002	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...

Abbildung 12. Importierte Firmwarekonformitätsrichtlinie

## Firmwarekonformitätsrichtlinie zuordnen

Nachdem das Repository mit Firmwareaktualisierungspaketen befüllt und die Firmwarekonformitätsrichtlinie importiert wurden, kann die Richtlinie den Knoten der Skalierungseinheit zugewiesen werden. Gehen Sie dazu wie folgt vor:

- Schritt 1. Wählen Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle **Bereitstellung** → **Übernehmen/Aktivieren** aus. Zunächst zeigt die zugeordnete Konformitätsrichtlinie für jedes System möglicherweise „Keine Zuordnung“ oder eine Richtlinie von einer vorherigen optimalen Vorgehensweise. In der folgenden Beispielabbildung wurde allen vier Knoten bereits die Richtlinie der optimalen Vorgehensweise SXMBR1910 zugeordnet. Darüber hinaus werden alle vier Knoten als „Konform“ mit dieser Richtlinie angezeigt.

### Firmware Updates: Apply / Activate

To update firmware on a device, assign a compliance policy and select Perform Updates.

Update with Policy
Update without Policy

+ + + + + +

All Actions

Filter By

Critical Release Information
Show: All Devices

<input type="checkbox"/>	Device	Power	Installed Version	Assigned Compliance Policy	Compliance Target
<input type="checkbox"/>	Lenovo-01 10.30.8.3	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> Compliant	PurleyPolicy_SXMBR1910	
<input type="checkbox"/>	Lenovo-02 10.30.8.4	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> Compliant	PurleyPolicy_SXMBR1910	
<input type="checkbox"/>	Lenovo-03 10.30.8.5	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> Compliant	PurleyPolicy_SXMBR1910	
<input type="checkbox"/>	Lenovo-04 10.30.8.6	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> Compliant	PurleyPolicy_SXMBR1910	

Abbildung 13. Fenster „Firmwareaktualisierungen: Übernehmen/Aktivieren“

- Schritt 2. Vor dem Zuordnen der Firmwareaktualisierungsrichtlinie zu den Knoten müssen die globalen Einstellungen für Firmwareaktualisierungen festgelegt werden. Klicken Sie dazu auf **Alle Aktionen** und wählen Sie dann in der Dropdown-Liste **Globale Einstellungen** aus.
- Schritt 3. Aktivieren Sie im neu geöffneten Fenster „Globale Einstellungen: Firmwareaktualisierungen“ die Kontrollkästchen alle drei Optionen und klicken Sie auf **OK**.

#### Global Settings: Firmware Updates

**Enhanced Support for Down-Level Devices**  
Down-level firmware might prevent a device from appearing in inventory or reporting full version information. When you select this option, all policy-based packages are available for you to apply (the default). If you do not select this option, only detected devices are shown.

**Alerts for Non-Compliant Devices**  
If this option is enabled, you will see alerts for all devices that do not meet the requirements of their assigned firmware compliance policies. These alerts are listed under Monitoring > Alerts

**Disable Auto Policy Assignment**  
If this option is enabled, firmware compliance policies are not assigned automatically to managed devices that have no assigned policy.

**Report Non-Compliant for Firmware Without Target**  
If this option is enabled, devices will be shown as non-compliant when a firmware component has no target associated to it in the policy, such as some legacy hardware module that has no firmware released for it for a while.

Abbildung 14. Fenster „Globale Einstellungen: Firmwareaktualisierungen“

- Schritt 4. Nachdem die globalen Einstellungen konfiguriert wurden, ändern Sie die zugeordnete Konformitätsrichtlinie auf der Seite „Firmwareaktualisierungen: Übernehmen/Aktivieren“ in die



Richtlinie, die gerade importiert wurde. Beachten Sie in der folgenden Beispielabbildung einer Purley-Lösung mit 4 Knoten, dass die Richtlinie geändert wurde, sodass die optimale Vorgehensweise SXMBR2002 für Purley-Lösungen unterstützt wird und alle Knoten nun als „Nicht konform“ (siehe rote Felder) angezeigt werden, da die Firmware noch nicht auf SXMBR2002-Ebene aktualisiert wurde. Wenn außerdem ein Server aufgrund der konfigurierten globalen Einstellungen als nicht konform gekennzeichnet wird, zeigt auch das Symbol **Status** in der oberen Leiste von XClarity Administrator (siehe gelbes Feld) eine Warnung an. Es kann ein paar Minuten dauern, bis dieses Warnsymbol aktualisiert wird.

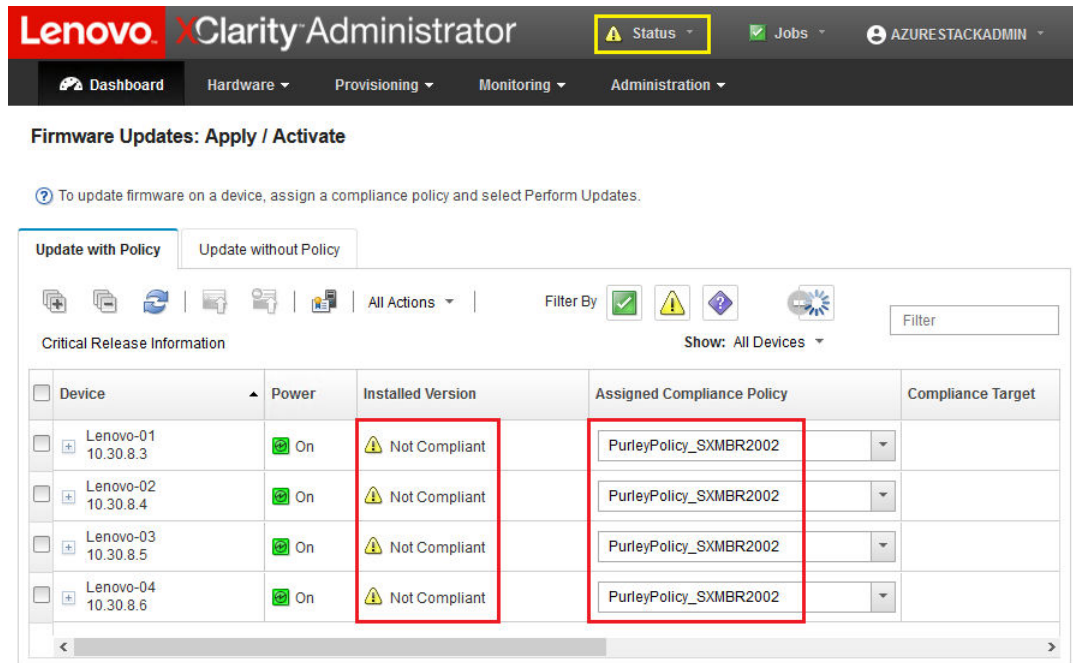


Abbildung 15. Firmwarekonformitätsrichtlinie, die nicht konforme Knoten zeigt

XClarity Administrator ist nun bereit zum Durchführen von Firmwareaktualisierungen auf der ThinkAgile SXM Serie Lösung. Fahren Sie mit „[ThinkAgile SXM OEM Extension Package aktualisieren](#)“ auf Seite 15 am Anfang des Fensters „Planmäßige Wartung“ fort, um die Firmware der Lösung zu aktualisieren.

## ThinkAgile SXM OEM Extension Package aktualisieren

In diesen Abschnitten wird der Vorgang zum Übernehmen einer OEM Extension Package-Aktualisierung auf eine laufende ThinkAgile SXM Serie Lösung detailliert beschrieben. Das OEM Extension Package ist ein Paket von Microsoft, das Einheitentreiber für alle Komponenten in den Azure Stack Hub-Knoten enthält. Daher wurde es dafür entwickelt, mit der Systemfirmware einer optimalen Vorgehensweise von ThinkAgile SXM zu funktionieren. Aus diesem Grund wird das OEM Extension Package in jeder optimalen Vorgehensweise aufgeführt.

OEM Extension Packages befinden sich in einem ZIP-Archiv mit dem folgenden Namensformat:

OEMv<x>\_SXMBR<yyyy>, wobei <x> entweder „2.2“ oder „3.0“ ist und yyyy die Version der optimalen Vorgehensweise ist, für die es gedacht ist.

Laden Sie zur Vorbereitung auf die Aktualisierung des OEM Extension Package das entsprechende ZIP-Archiv aus dem Repository herunter.

Die allgemeinen Aktivitäten beim Aktualisieren des OEM Extension Package sind:

- „LXCA-Details für Azure Stack Hub bereitstellen“ auf Seite 16
- „Aktuelle Versionen bestimmen“ auf Seite 18
- „Speichercontainer für Aktualisierung erstellen“ auf Seite 19
- „OEM Extension Package hochladen“ auf Seite 20
- „Aktualisierung durchführen“ auf Seite 23
- „Aktualisierung und Azure Stack Hub-Funktionalität überprüfen“ auf Seite 25

Microsoft empfiehlt, die aktuelle Version von Azure Stack Hub auszuführen.

## Vorbedingungen

Stellen Sie zunächst sicher, dass Sie einen USB-Stick mit dem entsprechenden OEM Extension Package zur Verfügung haben.

Versuchen Sie außerdem nicht, das OEM Extension Package zu aktualisieren, bis LXCA vorbereitet wurde, wie in „XClarity Administrator für eine bestimmte optimale Vorgehensweise konfigurieren“ auf Seite 6 beschrieben.

## LXCA-Details für Azure Stack Hub bereitstellen

Die Patch- und Update-Funktion (PnU) von Azure Stack Hub erfordert, dass IP-Adresse und Anmeldeinformationen von LXCA in einer bestimmten Variablen im Azure Stack Hub-Fabric gespeichert werden, damit alle Firmwareaktualisierungsanfragen an LXCA übermittelt und die jeweilige Authentifizierung angewendet werden können.

### Anmerkungen:

- Die Schritte in diesem Abschnitt müssen abgeschlossen sein, bevor die erste PnU-Firmwareaktualisierung ausgeführt wird. Bei jeder Änderung der LXCA-Anmeldeinformationen sollten diese Schritte erneut ausgeführt werden.

Es wurde ein Hilfsskript erstellt, um diesen Prozess zu vereinfachen. Gehen Sie wie folgt vor, um das Skript zu verwenden:

Schritt 1. Kopieren Sie AzureStackManagerCredsHelper.ps1 nach D:\Lenovo\Scripts auf dem HLH.

Schritt 2. Öffnen Sie eine neue Instanz von PowerShell ISE als Administrator und öffnen Sie dann das Hilfsskript. Das Skript enthält Kommentare, die Sie bei der Verwendung unterstützen.

```
# Set the variables used by the rest of the lines
#
# <EmergencyConsoleIPAddresses> is the IP address of a PEP
$ip = "<EmergencyConsoleIPAddresses>"

# <Password> is the password for the Azure Stack Hub Administrator account
$pwd = ConvertTo-SecureString "<Password>" -AsPlainText -Force

# <DomainFQDN> is the domain name of the Skalierungseinheit
# <UserID> is the UserID of the Azure Stack Hub admin account (often "CloudAdmin")
$cred = New-Object System.Management.Automation.PSCredential ("<DomainFQDN>\<UserID>", $pwd)
Enter-PSSession -ComputerName $ip -ConfigurationName PrivilegedEndpoint -Credential $cred

# The following command will pop up a window for LXCA Credentials
# <LXCAIPAddress> is the IP Address of LXCA
Set-OEMExternalVM -VMType HardwareManager -IPAddress "<LXCAIPAddress>"
```



Dieses Skript enthält in Klammern gesetzte Parameter, die durch echte Werte aus Ihrer Umgebung ersetzt werden müssen. Diese Werte finden Sie in der Tabelle im Dokument **Lenovo ThinkAgile SXM – Customer Deployment Summary** (Implementierungszusammenfassung für Kunde), das Sie erhalten haben und was auf den HLH kopiert wurde (D:\Lenovo\Azure Stack Deployment Details), nachdem Azure Stack Hub zum ersten Mal in Ihrem Rechenzentrum implementiert wurde. Ersetzen Sie die in Klammern gesetzten Parameter wie folgt:

- *<EmergencyConsoleIPAddresses>* ist die IP-Adresse eines privilegierten Endpunkts (PEP), die im Abschnitt *Emergency Recovery Console Endpoints* (Konsolenendpunkte für Notfallwiederherstellung) der Tabelle zu finden ist. Alle drei IP-Adressen können verwendet werden.
- *<Password>* ist das Kennwort für den Azure Stack Hub Administratoraccount, das im Abschnitt *Azure Stack Infrastructure* (Azure Stack-Infrastruktur) der Tabelle zu finden ist. Dies ist das Kennwort, mit dem Sie sich beim Azure Stack Hub-Administratorportal anmelden.
- *<DomainFQDN>* ist der Domänenname der Skalierungseinheit, der im Abschnitt *Azure Stack Hub Infrastructure* (Azure Stack-Infrastruktur) der Tabelle zu finden ist.
- *<UserID>* ist die UserID des Azure Stack Hub Administratoraccounts, die im Abschnitt *Azure Stack Infrastructure* (Azure Stack-Infrastruktur) der Tabelle zu finden ist. Dies ist die UserID, mit der Sie sich beim Azure Stack Hub-Administratorportal anmelden.
- *<LXCAIPAddress>* ist die IP-Adresse der virtuellen LXCA-Maschine, die im Abschnitt *LXCA* der Tabelle zu finden ist.

Schritt 3. Speichern Sie das Skript, nachdem Sie alle Parameter in Klammern durch echte Werte ersetzt haben, damit es in Zukunft wiederverwendet werden kann, wenn die LXCA-Anmeldeinformationen geändert werden.

Schritt 4. Wählen Sie alle Zeilen im Skript mit Ausnahme der letzten drei Zeilen aus und führen Sie den ausgewählten Teil aus, indem Sie auf die Schaltfläche **Abschnitt ausführen** (📄) klicken. Es ist normal, dass eine orangefarbene Warnmeldung mit dem folgenden Text angezeigt wird:

**Die Namen einiger importierter Befehle auf dem Modul „ECEClient“ enthalten nicht genehmigte Verben, sodass deren Auffindbarkeit erschwert werden kann. Wenn Sie die Befehle mit nicht genehmigten Verben finden möchten, führen Sie den Import-Module-Befehl erneut mit dem Verbose-Parameter aus. Sie können durch Eingeben von „Get-Verb“ eine Liste der genehmigten Verben anzeigen.**

Schritt 5. Es öffnet sich ein Popup-Fenster, in dem Sie nach Anmeldeinformationen gefragt werden. **Geben Sie die Anmeldeinformationen ein, die für die Anmeldung bei LXCA verwendet werden.** Die Anmeldeinformationen zum Zeitpunkt der Implementierung von Azure Stack Hub finden Sie in der oben bereits erwähnten Tabelle im Abschnitt **LXCA**.

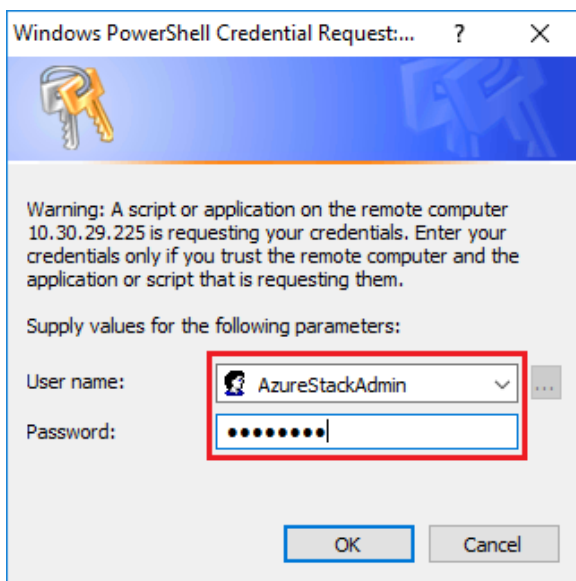


Abbildung 16. Anmeldeinformationen, die für die Anmeldung bei LXCA verwendet werden

Es dauert einige Minuten, bis der Befehl ausgeführt wird. PowerShell wird regelmäßig mit den folgenden Verbose-Statusmeldungen aktualisiert:

VERBOSE:

Overall action status: 'Running'

VERBOSE:

VERBOSE: Step 'OEM Hardware Manager password update' status: 'InProgress'

VERBOSE:

Nach Abschluss des Vorgangs sehen Sie eine letzte Statusaktualisierung (VERBOSE: DONE), bevor eine Zusammenfassung der durchgeführten Aufgaben angezeigt wird.

Damit sind die erforderlichen Schritte zum Bereitstellen von XClarity Administrator-Details für Skalierungseinheit abgeschlossen. Fahren Sie mit „[Aktuelle Versionen bestimmen](#)“ auf Seite 18 fort.

## Aktuelle Versionen bestimmen

Gehen Sie wie folgt vor, um Ihre Version von Microsoft Azure Stack Hub zu überprüfen.

Überprüfen Sie das Dashboard im Azure Stack Hub-Administratorportal, um sicherzustellen, dass keine aktuellen Alerts angezeigt werden. Alle Alerts müssen behoben werden, bevor Sie eine Aktualisierung mit dem OEM Extension Package oder Azure Stack Hub Build durchführen. Andernfalls wartet der Aktualisierungsprozess einfach darauf, dass die Skalierungseinheit im fehlerfreien Zustand ist, bevor die Aktualisierung beginnt.

Überprüfen Sie die aktuelle Version, um festzustellen, ob eine Aktualisierung erforderlich ist. Melden Sie sich dazu beim Azure Stack Hub-Administratorportal an. Klicken Sie auf die Kachel „Aktualisieren“, um den Aktualisierungs-Blade zu öffnen und die Version des OEM Extension Package zu finden, die derzeit von der Lösung verwendet wird.

Die Version des OEM Extension Package, die derzeit von der Lösung verwendet wird, wird als „Aktuelle OEM-Version“ angezeigt (siehe folgende Abbildung). Notieren Sie sich die gefundenen Versionen, um sie später mit den aktuellen Versionen vergleichen zu können. Im folgenden Beispiel-Screenshot werden auf der

Lösung Azure Stack Hub Build 1910 (siehe gelbes Feld) und OEM Extension Package Version 2.1.1910.503 (siehe hellblaues Feld) ausgeführt.

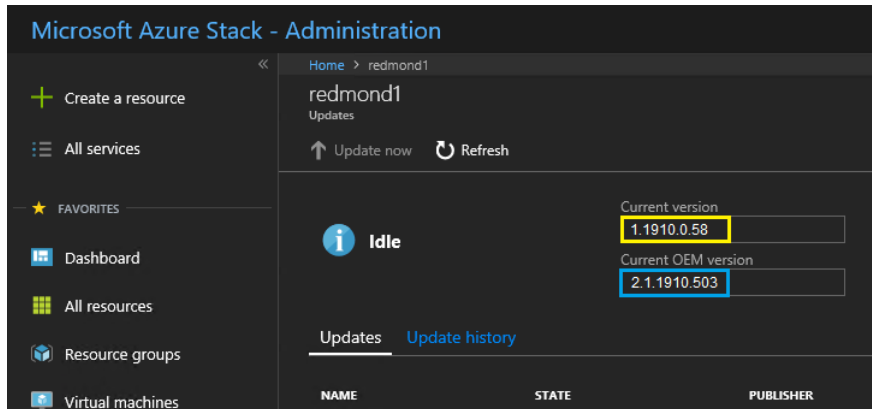


Abbildung 17. Überprüfung der aktuell ausgeführten Versionen von Azure Stack Hub

## Speichercontainer für Aktualisierung erstellen

Befolgen Sie dieses Verfahren zum Erstellen eines Speichercontainers in Azure Stack Hub, um das Aktualisierungspaket zu importieren.

Damit ein OEM Extension Package bei Azure Stack Hub angewendet werden kann, muss es in einen bestimmten Speichercontainer in Azure Stack Hub importiert werden. Dieser Container muss wie folgt erstellt werden:

- Schritt 1. Melden Sie sich beim Azure Stack Hub-Administratorportal an.
- Schritt 2. Navigieren Sie im Azure Stack Hub-Administratorportal zu **Alle Dienste** → **Speicher-Konten** (zu finden unter DATEN + SPEICHER).
- Schritt 3. Geben Sie im Filterfeld update ein und wählen Sie **updateadminaccount** aus.

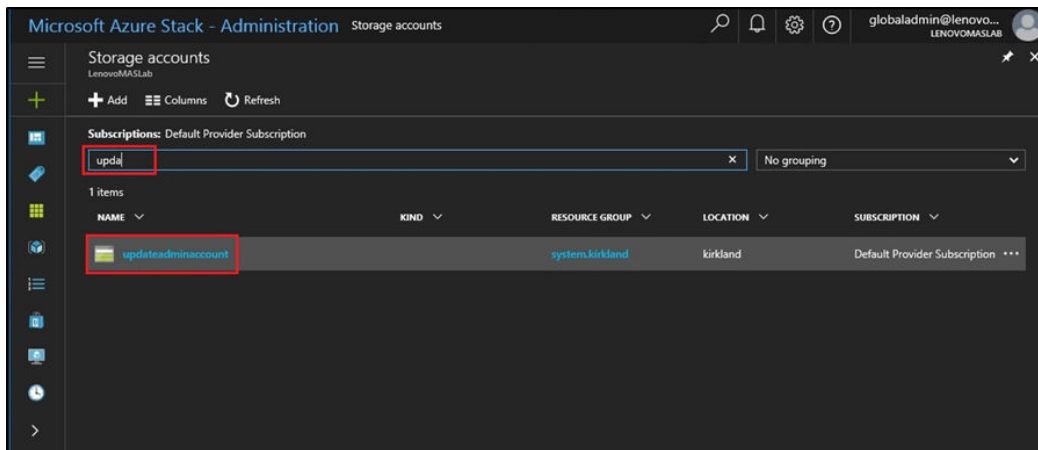


Abbildung 18. Navigieren zum Speichercontainer „updateadminaccount“

- Schritt 4. Wählen Sie in den Details des Speicher-Kontos „updateadminaccount“ unter Services die Option **Blobs** aus.

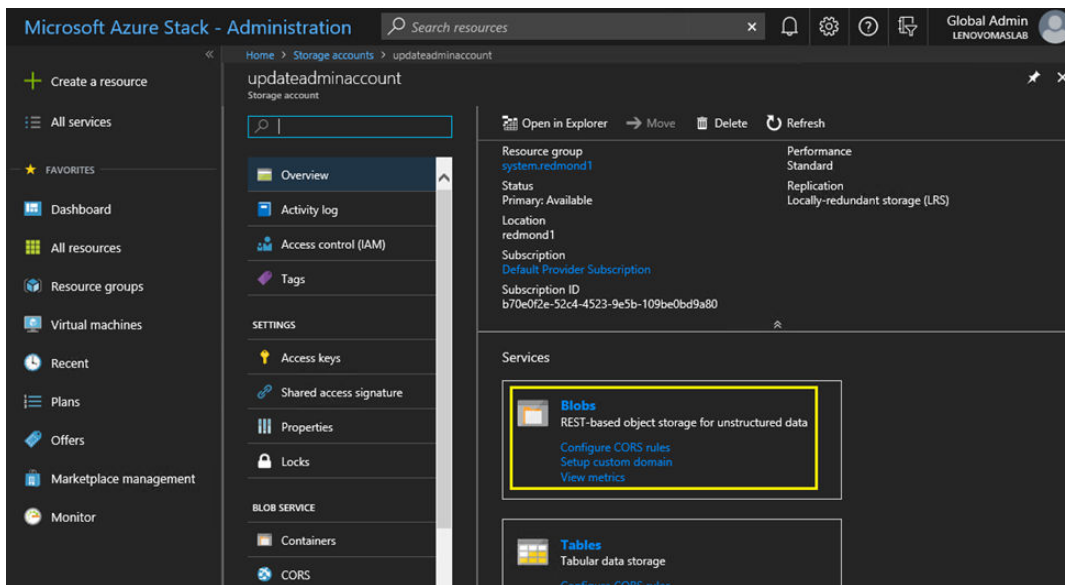


Abbildung 19. Navigieren zum Speichercontainer „Blobs“

Schritt 5. Klicken Sie auf der Kachel Blob-Service auf **+ Container**, um einen Container zu erstellen, geben Sie einen Namen für den Container ein (z. B. **oem-update-2002**) und klicken Sie auf **OK**.

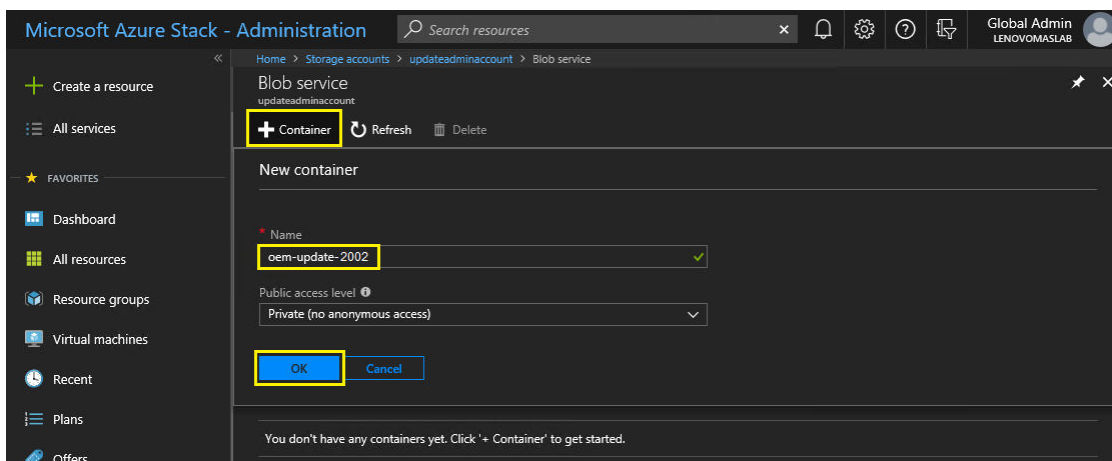


Abbildung 20. Erstellen des neuen Containers

## OEM Extension Package hochladen

Nach Erstellung des Speichercontainers müssen die Aktualisierungspaketdateien in den Container hochgeladen werden. Gehen Sie dazu wie folgt vor:

Schritt 1. Wählen Sie den Container nach seiner Erstellung aus, um eine neue Kachel zu öffnen.

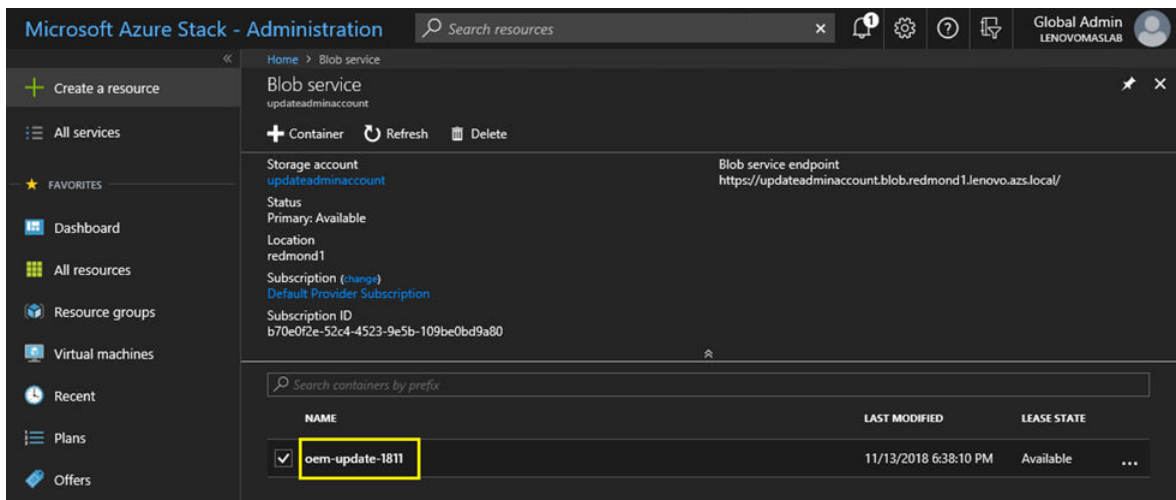


Abbildung 21. Auswählen des Speichercontainers zum Hochladen

Schritt 2. Klicken Sie auf **Hochladen**.

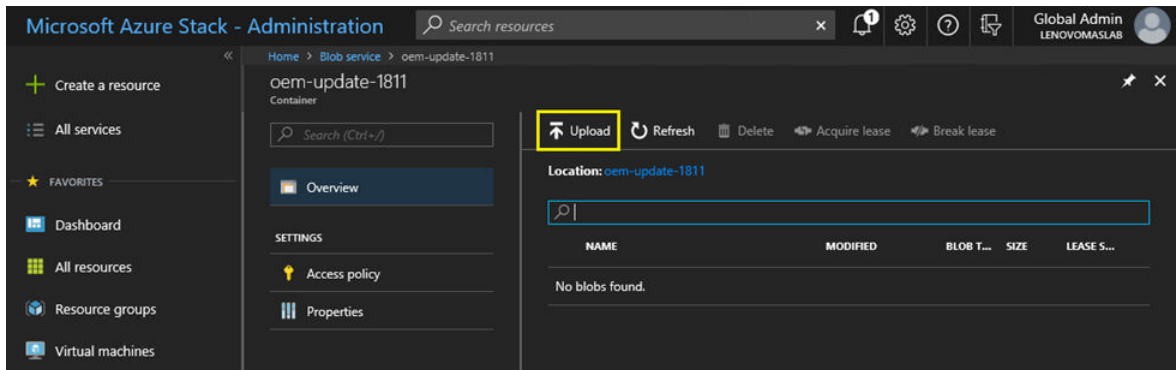


Abbildung 22. Auswählen des Steuerelements „Hochladen“

Schritt 3. Navigieren Sie zum Aktualisierungspaket, wählen Sie beide Paketdateien aus und klicken Sie im Datei-Explorer auf **Öffnen**.

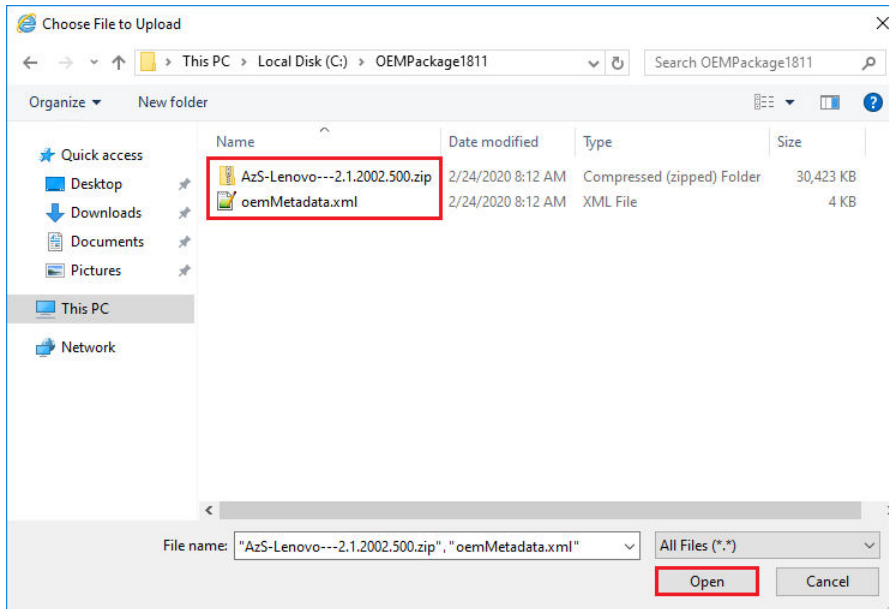


Abbildung 23. Auswählen der Aktualisierungspaketdateien zum Hochladen

Schritt 4. Klicken Sie im Administratorportal auf **Hochladen**.

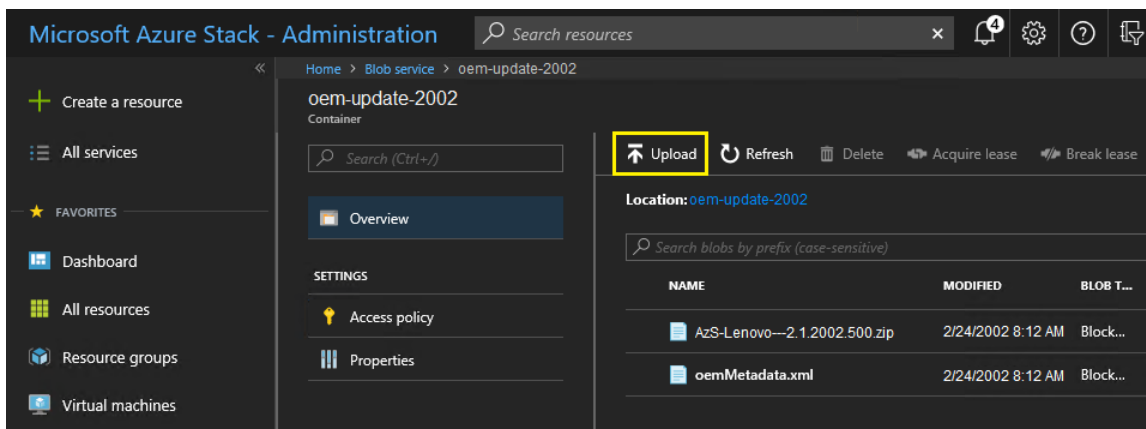


Abbildung 24. Hochladen der Aktualisierungspaketdateien

Wenn das Hochladen abgeschlossen ist, werden alle Paketdateien im Container aufgeführt. Im Bereich Benachrichtigungen (🔔) können Sie überprüfen, dass jeder Upload abgeschlossen wurde.

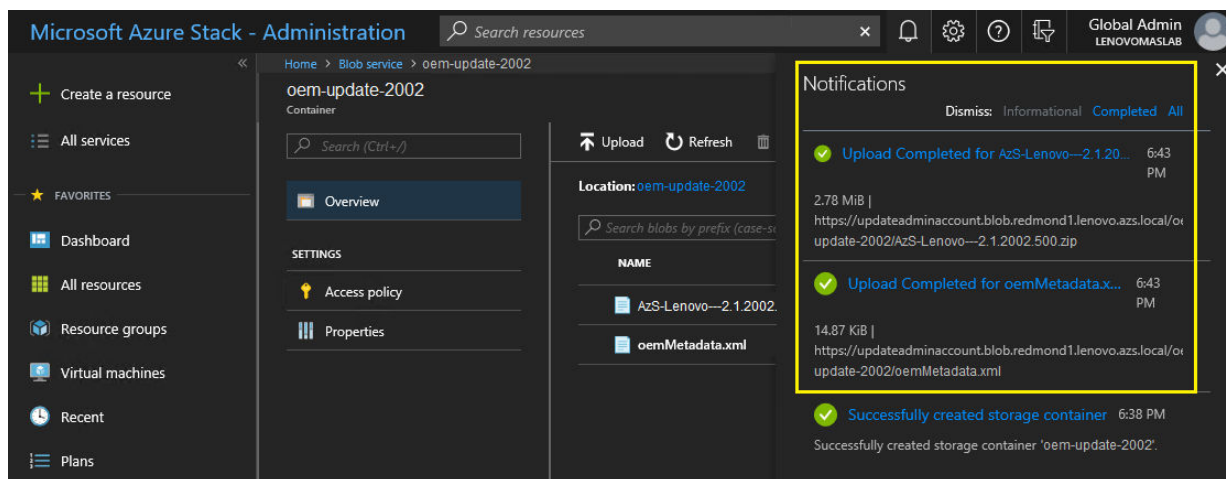


Abbildung 25. Überprüfen, ob Uploads erfolgreich abgeschlossen wurden

## Aktualisierung durchführen

Kehren Sie zur Dashboard-Ansicht zurück, wenn die OEM Extension Package-Dateien in ihren Container hochgeladen wurden. Die Kachel Aktualisieren zeigt jetzt „Verfügbare Aktualisierung“ an. Die OEM Extension Package-Aktualisierung kann jetzt wie folgt angewendet werden:

- Schritt 1. Wählen Sie **Aktualisieren** aus, um das neu hinzugefügte Aktualisierungspaket mit Versionsnummer zu überprüfen.
- Schritt 2. Wählen Sie zum Installieren der Aktualisierung die OEM Extension Package-Aktualisierung aus, die als **Bereit** markiert ist. Beachten Sie, dass eine verfügbare Azure Stack Hub-Aktualisierung zusammen mit der OEM Extension Package-Aktualisierung aufgeführt wird und einen vollständig separaten Aktualisierungsprozess erfordert. Stellen Sie sicher, dass Sie vor dem Fortfahren die richtige Aktualisierung auswählen.

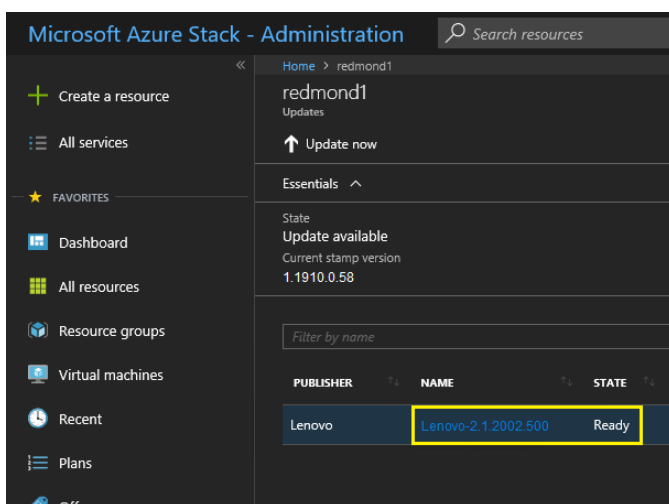


Abbildung 26. Initiieren der Aktualisierung

- Schritt 3. Klicken Sie bei ausgewählter OEM Extension Package-Aktualisierung entweder mit der rechten Maustaste und wählen Sie **Jetzt aktualisieren** aus oder klicken Sie auf **Jetzt aktualisieren** in der Befehlsleiste oben im Fenster, um die Aktualisierung zu starten. Der Status der Aktualisierung

unten im Portal ändert sich zu „Wird ausgeführt“ und der Status aller anderen verfügbaren Aktualisierungen ändert sich zu „Nicht zutreffend“, da nun eine Aktualisierung ausgeführt wird.

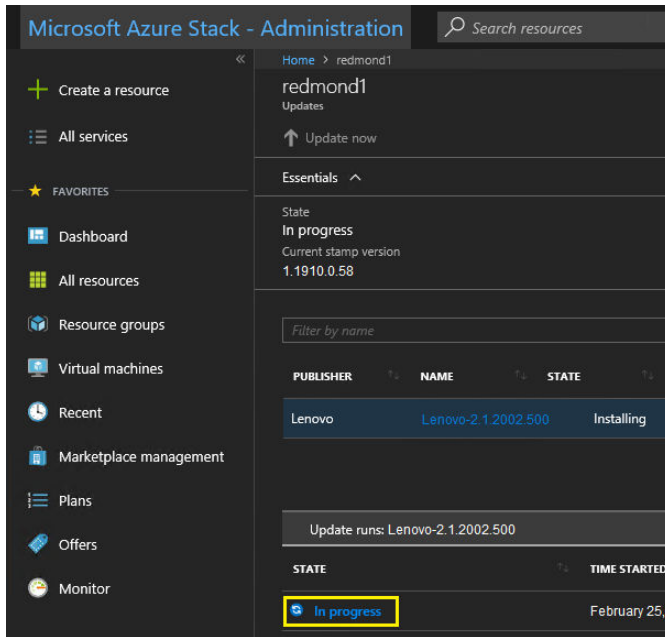


Abbildung 27. Anzeigen zum Aktualisierungsfortschritt

Schritt 4. Klicken Sie auf die Anzeige **Wird ausgeführt**, um die Kachel Ausführungsdetails aktualisieren zu öffnen und Details zum aktuell installierten Aktualisierungspaket anzuzeigen.

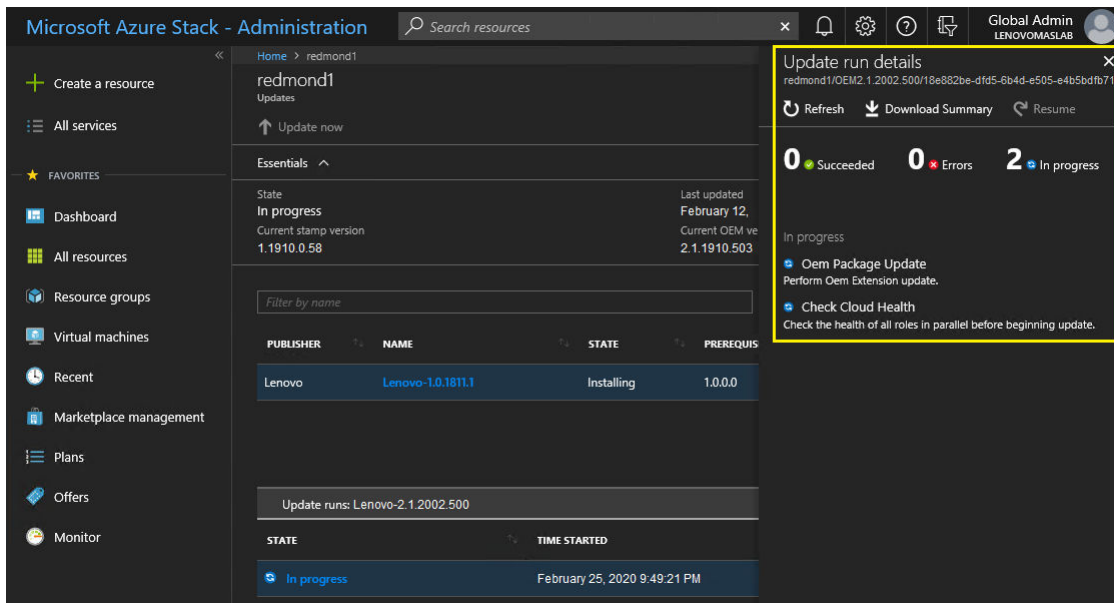


Abbildung 28. Installationsdetails

Schritt 5. Der gesamte Aktualisierungsvorgang kann sehr lange dauern, da jeder Knoten geleert, von Bare-Metal erneut implementiert und während des Vorgangs wiederaufgenommen wird. Wenn die Aktualisierung abgeschlossen ist, wird die STATUS-Spalte zu „Erfolgreich“ aktualisiert und die



Kachel „Ausführungsdetails aktualisieren“ auf der rechten Seite des Portals zeigt keine laufenden Aktualisierungen mehr an.

## Aktualisierung und Azure Stack Hub-Funktionalität überprüfen

Wenn die Aktualisierung erfolgreich angewendet wurde, kann es einige Zeit (zwei Stunden oder länger) dauern, bis Azure Stack Hub sich „beruhigt“ hat und wieder normal funktioniert. Während des Aktualisierungsprozesses und dieser Beruhigungszeit werden basierend auf der Verfügbarkeit von Komponenten der Infrastruktur möglicherweise Alerts angezeigt.

Sie können überprüfen, ob die Aktualisierung angewendet wurde, indem Sie die Version der aktuellen Umgebung im Azure Stack Hub-Administratorportal überprüfen. Kehren Sie zum Dashboard zurück und klicken Sie auf **Aktualisieren**, um den Aktualisierungs-Blade zu öffnen. Überprüfen Sie, ob die aktuelle OEM-Version wie erwartet ist.

Das Azure Stack Hub-Überprüfungstool (**Test-AzureStack**) ist ein PowerShell-Cmdlet, mit dem Sie eine Reihe von Tests auf Ihrem System ausführen können, um vorliegende Fehler zu identifizieren. Es wird empfohlen, das Test-AzureStack-Cmdlet nach jeder Aktualisierung auszuführen. Hier finden Sie die aktuellen Anweisungen von Microsoft zur Durchführung dieses Tests: <https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-diagnostic-test>.

---

## ThinkAgile SXM Switch-Firmware aktualisieren (nur Lenovo Switches)

Aktuelle ThinkAgile SXM Serie Lösungen werden nicht mehr mit Lenovo Netzwerk-Switches geliefert. In diesem Abschnitt werden die erforderlichen Schritte zum Aktualisieren von Lenovo BMC- und TOR-Switches in einer laufenden Lenovo ThinkAgile SXM Serie Lösung vorgestellt, die mit Lenovo Switches geliefert wurde. Dabei sind Schritte enthalten, mit denen Sie die Switch-Konfigurationen sichern, das Netzwerkbetriebssystem (NOS) auf jedem Switch aktualisieren und sicherstellen können, dass die Switches ordnungsgemäß funktionieren.

### Einführung

Sobald eine ThinkAgile SXM Serie Lösung implementiert wurde und Workloads ausführt, muss die Produktionsumgebung so störungsfrei wie möglich gestaltet werden. Es ist erforderlich, jederzeit eine aktive Netzwerkverbindung zu erhalten, selbst bei Aktualisierungen von Netzwerkbetriebssystemen und Konfigurationen. Das Azure Stack Hub-Netzwerkdesign verfügt über zwei redundante TOR-Switches, um Hochverfügbarkeit zu erzielen.

In diesen Themen enthalten die Schritte die Eingabe von Switch-Anmeldeinformationen in der Form „admin/<password>“. Sie müssen die tatsächlichen Anmeldeinformationen für alle Switches einsetzen, um diesen Prozess abzuschließen. Sie finden diese Anmeldeinformationen im Dokument „Customer Deployment Summary“ (Implementierungszusammenfassung für Kunde), das Sie bei der Implementierung der Lösung erhalten haben. Sie können Kennwörter ändern, nachdem Sie den Switch erfolgreich aktualisiert haben.

Der Aktualisierungsprozess für die Switch-Firmware umfasst die folgenden Aktivitäten:

- XClarity Administrator für Aktualisierung von Switch-Firmware vorbereiten
- TOR-Switch-Konfiguration sichern
- TOR-Switch aktualisieren
- TOR-Switch-Funktionalität überprüfen
- BMC-Switch-Konfiguration sichern
- BMC-Switch aktualisieren
- BMC-Switch-Funktionalität überprüfen

## Vorbedingungen

Befolgen Sie die Anweisungen in diesem Abschnitt, bevor Sie mit der Aktualisierung der Switch-Firmware beginnen.

Stellen Sie vor Beginn des Prozesses sicher, dass Sie die folgenden Elemente zur Verfügung haben:

- Anmeldeinformationen für den Zugriff auf das Azure Stack Hub-Administratorportal
- Anmeldeinformationen für den Zugriff auf XClarity Administrator auf dem HLH
- Falls eine direkte serielle Verbindung zu einem Switch für die Fehlerbehebung erforderlich ist:
  - Für Lenovo spezifisches serielles Kabel (Mini-USB RJ-45 seriell), mit dem Switch mitgeliefert
  - USB-zu-seriell-Kabel
  - USB-Stick mit:
    - Lenovo ThinkAgile SXM-Firmwareaktualisierungsdateien für die entsprechende optimale Vorgehensweise
    - XClarity Administrator-Firmwareaktualisierungsrichtlinien-Datei für die entsprechende optimale Vorgehensweise

**Anmerkung:** Die obigen Dateien finden Sie im ThinkAgile SXM Repository unter der folgenden URL:

<https://thinkagile.lenovo.com/SXM>

- In diesem Handbuch wird vorausgesetzt, dass auf Ihrer ThinkAgile SXM Serie Lösung Lenovo XClarity Administrator Version 2.x auf dem HLH ausgeführt wird, um Firmwareaktualisierungen auf den ThinkAgile SXM Netzwerk-Switches durchzuführen. Wenn XClarity Administrator Version 2.x auf dem HLH ausgeführt wird, kann sie anhand der Anweisungen im Abschnitt [XClarity Administrator aktualisieren](#) problemlos auf jede andere Version 2.x aktualisiert werden.
- Der minimal erforderlichen Switch-NOS-Versionen für die Verwendung von XClarity Administrator für Aktualisierungen sind CNOS v10.6.1.0 (auf den TOR-Switches und dem NE0152T BMC-Switch) und ENOS v8.4.8.0 (auf dem G8052 BMC-Switch). Wenn auf einem Switch eine frühere Version ausgeführt wird, können Sie XClarity Administrator nicht zum Aktualisieren des NOS auf dem Switch verwenden. In dieser Situation finden Sie unter [Anhang B „ThinkAgile SXM Serie Switches mit der CLI aktualisieren \(nur Lenovo Switches\)“ auf Seite 95](#) Anweisungen zur Verwendung der Switch-CLI-Methode zum Aktualisieren der Switch-Firmware.
- Schaffen Sie ein Wartungsfenster für die Lösung, in dem Sie davon ausgehen, dass die Lösung möglicherweise nicht verfügbar ist. Lenovo empfiehlt ein Wartungsfenster von mindestens 2 Stunden für alle drei Switches.

## XClarity Administrator für Aktualisierung von Switch-Firmware vorbereiten

Befolgen Sie die Anweisungen in diesem Abschnitt, um XClarity Administrator auf die Aktualisierung der Lenovo Switch-Firmware vorzubereiten.

Die Verwendung von XClarity Administrator zum Aktualisieren der Lenovo Switch-Firmware ist einfach und schnell. Vor der Aktualisierung müssen die Switches von XClarity Administrator verwaltet werden. Um zu überprüfen, dass XClarity Administrator die Switches verwaltet, navigieren Sie im Hauptmenü von XClarity Administrator zu **Hardware** → **Switches**. Wenn Sie nicht alle Switches der Lösung wie im folgenden Screenshots dargestellt sehen, lesen Sie den Abschnitt „Switches verwalten“ in [Anhang A „XClarity Administrator implementieren und konfigurieren“ auf Seite 59](#), um Schritte zur Switch-Verwaltung zu erhalten.

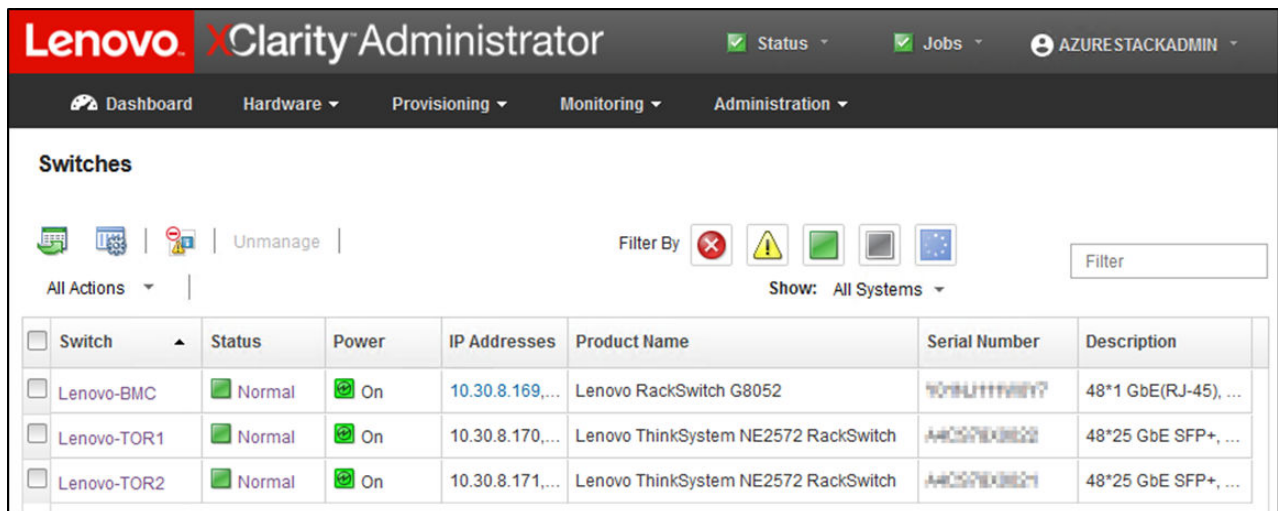


Abbildung 29.

XClarity Administrator muss genau so auf die Durchführung der Switch-Firmwareaktualisierungen vorbereitet werden, wie es für die Aktualisierung von Knoten-Firmware vorbereitet wird. Falls noch nicht geschehen, lesen Sie [„Aktualisierung der Firmware für ThinkAgile SXM vorbereiten“](#) auf Seite 6 und [„XClarity Administrator für eine bestimmte optimale Vorgehensweise konfigurieren“](#) auf Seite 6, um XClarity Administrator auf die Aktualisierung der Switch-Firmware vorzubereiten.

Sobald XClarity Administrator für die Aktualisierung der Firmware auf den Switches vorbereitet wurde, müssen Sie sicherstellen, dass die Azure Stack Hub-Umgebung fehlerfrei ist. Melden Sie sich bei Azure Stack Hub-Administratorportal an und stellen Sie sicher, dass keine Alerts angezeigt werden. Im Laufe des Prozesses werden wir den Allgemeinzustand der Lösung immer wieder im Portal überprüfen.

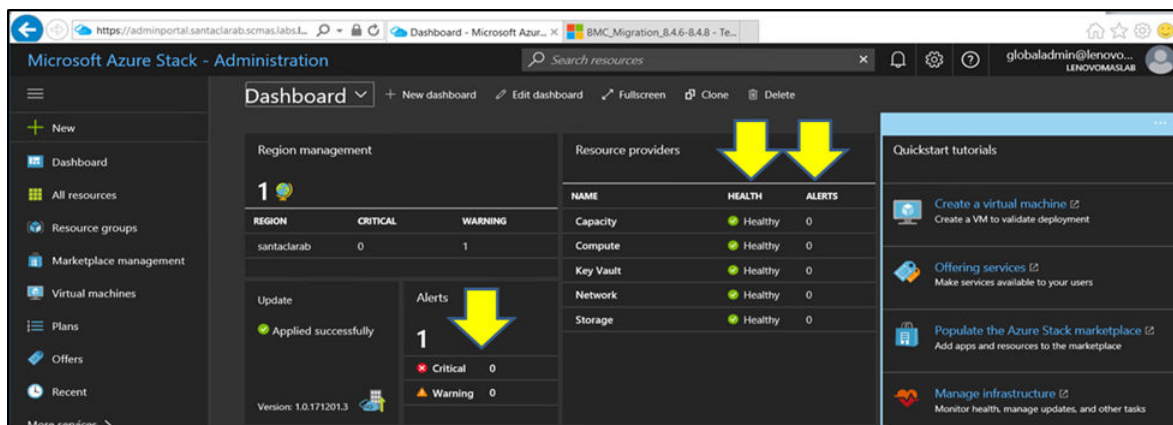


Abbildung 30. Überprüfen des Azure Stack Hub-Zustands vor der Aktualisierung

## Lenovo TOR-Switch-Firmware aktualisieren

In diesem Abschnitt werden die erforderlichen Schritte zur Aktualisierung des CNOS-Image der TOR-Switches beschrieben.

### Lenovo TOR-Switch-Konfigurationen sichern

Stellen Sie vor Beginn des Aktualisierungsverfahrens sicher, dass beide Lenovo TOR-Switch-Konfigurationen gesichert wurden.

Sie können die Switch-Konfiguration der TOR-Switches ganz einfach mit wenigen Klicks in XClarity Administrator sichern. Gehen Sie wie folgt vor:

- Schritt 1. Wählen Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle **Hardware** → **Switches** aus.
- Schritt 2. Wählen Sie beide TOR-Switches aus, indem Sie das Kontrollkästchen links neben den Switches aktivieren.

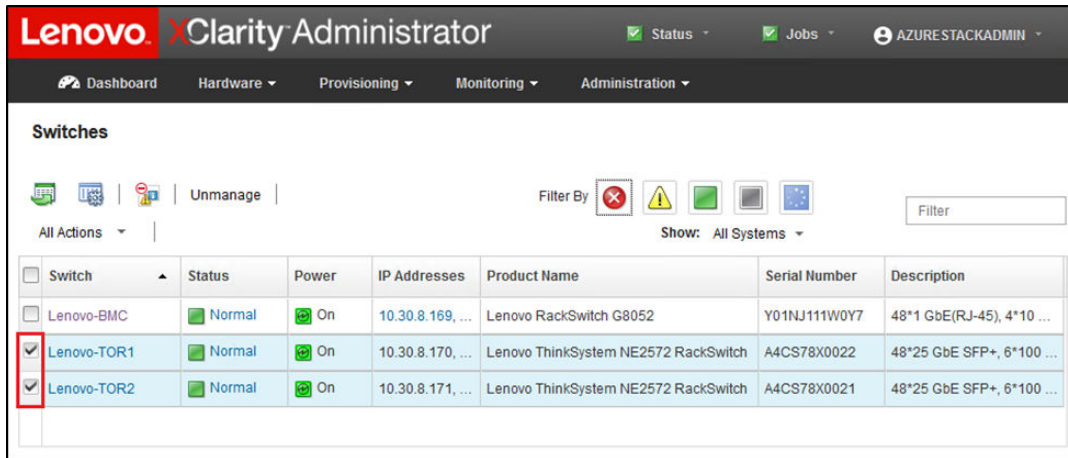


Abbildung 31. Auswählen beider TOR-Switches

- Schritt 3. Navigieren Sie zu **Alle Aktionen** → **Konfiguration** → **Konfigurationsdatei sichern**.

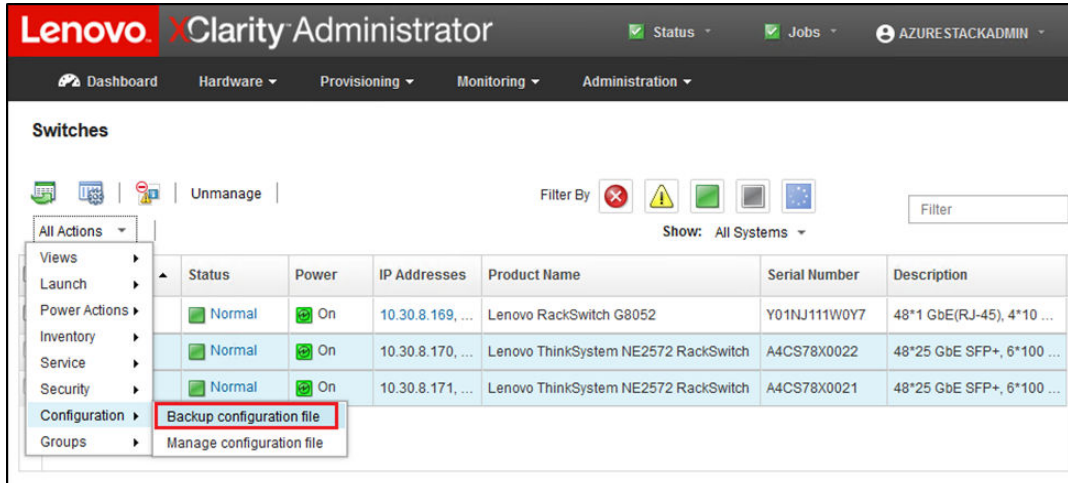


Abbildung 32. Sichern der TOR-Konfigurationsdatei

- Schritt 4. Überprüfen Sie, ob beide TOR-Switches im Feld **Ausgewählte Switches** angezeigt werden. Geben Sie eine Beschreibung für die Sicherung ein und klicken Sie auf **Sicherung**.

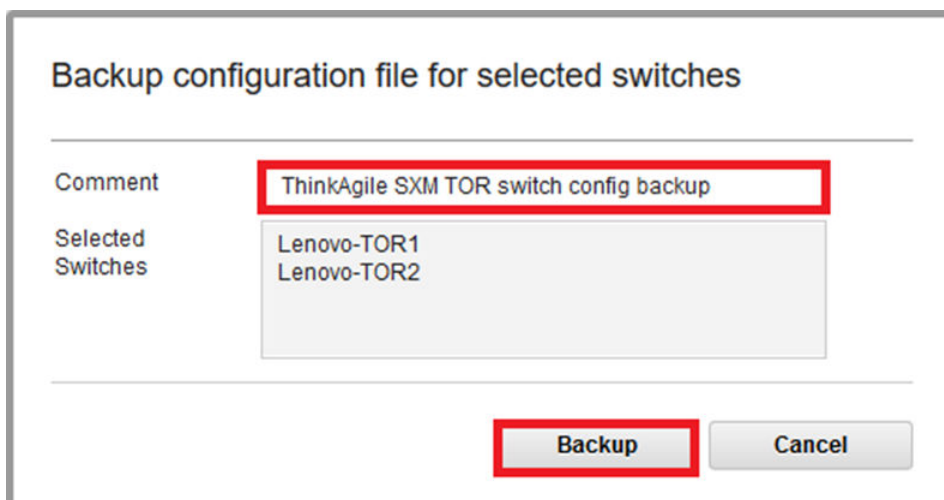


Abbildung 33. Dialogfeld „Konfigurationsdatei sichern“

Schritt 5. Das Fenster sollte die erfolgreiche Sicherung bestätigen. Klicken Sie auf **Schließen**, um dieses Fenster zu schließen.

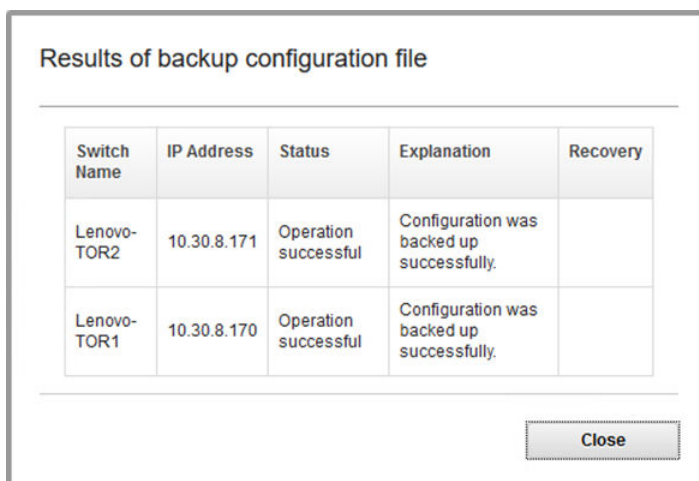


Abbildung 34. Ergebnisse der Konfigurationsdateisicherung

Schritt 6. Die Backup-Switch-Konfigurationsdateien werden intern in XClarity Administrator gespeichert, aber es ist ratsam, eine besser verfügbare Kopie zu speichern. Um eine Kopie auf dem HLH zu speichern, klicken Sie auf einen Switch, um eine detaillierte Ansicht des Switches zu öffnen.

Schritt 7. Wählen Sie im linken Bereich **Konfigurationsdateien** aus und aktivieren Sie das Kontrollkästchen links vom Dateinamen, um die gesicherte Konfigurationsdatei auszuwählen.

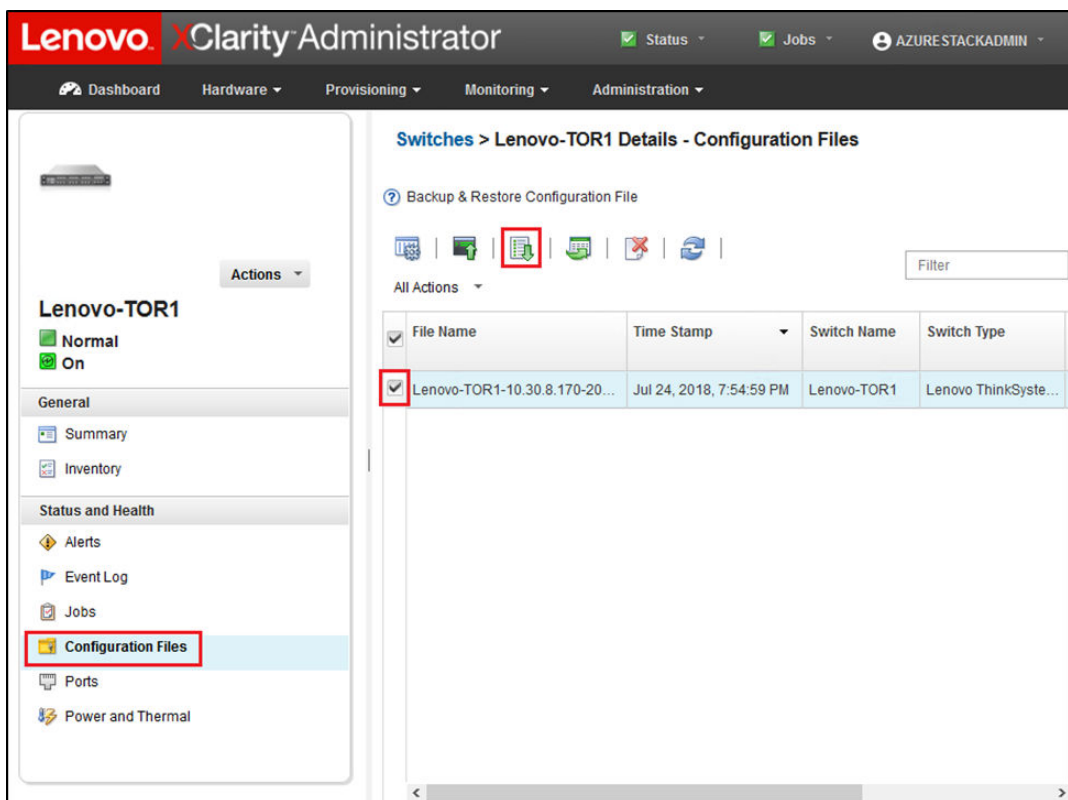


Abbildung 35. Auswahl der gesicherten Konfigurationsdatei zum Download auf einen lokalen PC

Schritt 8. Klicken Sie auf die Schaltfläche **Konfigurationsdatei aus XClarity auf lokalen PC herunterladen**



Schritt 9. Geben Sie je nach verwendetem Browser einen Downloadspeicherort an und speichern Sie die Datei. Der Standarddateiname von XClarity Administrator hat das folgende Format:  
 <SwitchHostname>-<IPAddress>-<Date>-<Time>.cfg

Schritt 10. Wiederholen Sie die Schritte 6 bis 9 für den anderen TOR-Switch.

Schritt 11. Wenn es noch nicht vorhanden ist, erstellen Sie das Verzeichnis D:\Lenovo\SwitchConfigBackups auf dem HLH und verschieben Sie die gesicherten TOR-Konfigurationsdateien in dieses Verzeichnis.

## CNOS auf Lenovo TOR-Switches aktualisieren

Verwenden Sie bei gesicherten Switch-Konfigurationsdateien XClarity Administrator zum Aktualisieren der Lenovo TOR-Switch-Firmware.

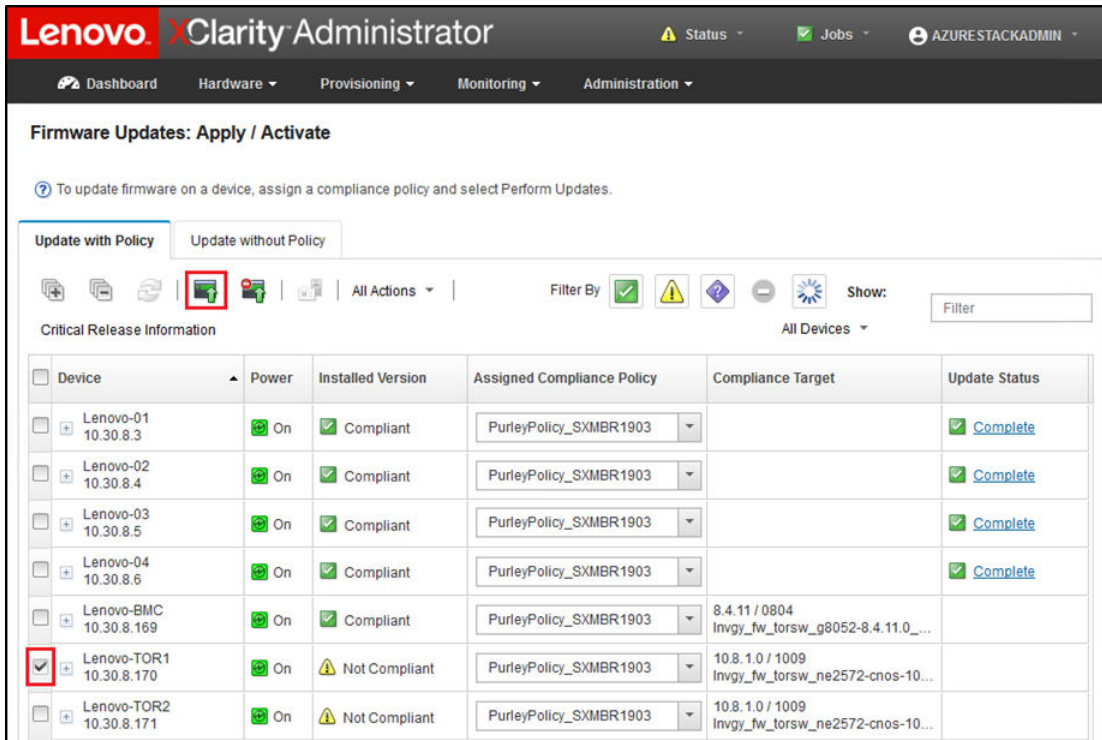
Der Prozess beinhaltet das Aktualisieren der Firmware auf beiden TOR-Switches und Überprüfen der TOR-Switch-Funktionalität. Gehen Sie zur Aktualisierung des ersten TOR-Switches wie folgt vor:

Schritt 1. Verwenden Sie das Hauptmenü von XClarity Administrator, um zu **Bereitstellung** → **Übernehmen/Aktivieren** zu navigieren.

Schritt 2. Stellen Sie sicher, dass die TOR-Switches als „Nicht konform“ für die Firmwareaktualisierungsrichtlinie mit optimaler Vorgehensweise angezeigt werden, die ihnen zugeordnet ist. Im folgenden Beispiel-Screenshot sind die TOR-Switches nicht konform, aber der BMC-Switch wird als „Konform“ angezeigt, sodass er nicht aktualisiert werden muss.



Schritt 3. Wählen Sie den TOR1-Switch durch Aktivieren des Kontrollkästchens auf der linken Seite und klicken Sie auf **Aktualisierungen durchführen** (  ).



The screenshot shows the 'Firmware Updates: Apply / Activate' page in the Lenovo XClarity Administrator. The interface includes a navigation bar with 'Dashboard', 'Hardware', 'Provisioning', 'Monitoring', and 'Administration'. Below the navigation bar, there are tabs for 'Update with Policy' (selected) and 'Update without Policy'. A toolbar contains various icons, including a green arrow icon highlighted with a red box. Below the toolbar, there is a table of devices with columns for 'Device', 'Power', 'Installed Version', 'Assigned Compliance Policy', 'Compliance Target', and 'Update Status'. The table lists several devices, including 'Lenovo-TOR1' which is selected with a red box around its checkbox and has a 'Not Compliant' status.

Device	Power	Installed Version	Assigned Compliance Policy	Compliance Target	Update Status
Lenovo-01 10.30.8.3	On	Compliant	PurleyPolicy_SXMBR1903		Complete
Lenovo-02 10.30.8.4	On	Compliant	PurleyPolicy_SXMBR1903		Complete
Lenovo-03 10.30.8.5	On	Compliant	PurleyPolicy_SXMBR1903		Complete
Lenovo-04 10.30.8.6	On	Compliant	PurleyPolicy_SXMBR1903		Complete
Lenovo-BMC 10.30.8.169	On	Compliant	PurleyPolicy_SXMBR1903	8.4.11 / 0804 Invgy_fw_torsw_g8052-8.4.11.0_...	
<input checked="" type="checkbox"/> Lenovo-TOR1 10.30.8.170	On	Not Compliant	PurleyPolicy_SXMBR1903	10.8.1.0 / 1009 Invgy_fw_torsw_ne2572-cn0s-10...	
Lenovo-TOR2 10.30.8.171	On	Not Compliant	PurleyPolicy_SXMBR1903	10.8.1.0 / 1009 Invgy_fw_torsw_ne2572-cn0s-10...	

Abbildung 36. Auswählen des TOR1-Switches für die Aktualisierung

Schritt 4. Legen Sie im Fenster Aktualisierungszusammenfassung die folgenden Optionen fest und wählen Sie **Aktualisierung durchführen** aus:

- Aktualisierungsregel: **Alle Aktualisierungen bei einem Fehler anhalten**
- Aktivierungsregel: **Sofortige Aktivierung**

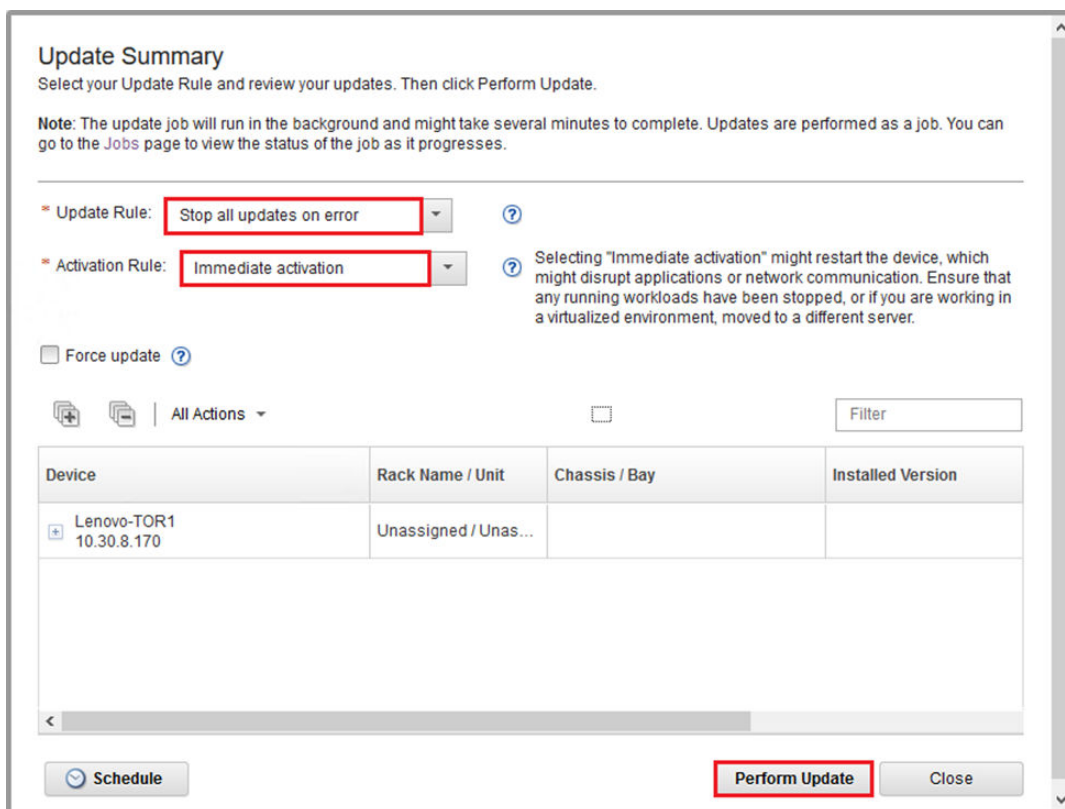


Abbildung 37. Auswählen von Optionen in der TOR1-Aktualisierungszusammenfassung

Schritt 5. Öffnen Sie die Jobs-Seite, um den Aktualisierungsfortschritt zu überwachen.



Lenovo XClarity Administrator

Dashboard Hardware Provisioning Monitoring Administration

Jobs Page > Firmware Updates

Job	Start	Complete	Targets	Status
✱ Firmware Updates	January 9, 2019 at 15:08:26		Lenovo-TOR1	Executing - 64.00%
✱ Lenovo-TOR1	January 9, 2019 at 15:08:26		Lenovo-TOR1	Executing - 64.00%
✓ RackSwitch Readiness Check	January 9, 2019 at 15:08:26	January 9, 2019 at 15:08:26	Lenovo-TOR1	Complete
✱ Applying RackSwitch firmware	January 9, 2019 at 15:08:28		Lenovo-TOR1	Executing - 28.00%

Summary for *Firmware Updates* job and sub-jobs

No summary available

Lenovo XClarity Administrator

Dashboard Hardware Provisioning Monitoring Administration

Jobs Page > Firmware Updates


Job	Start	Complete	Targets	Status
✓ Firmware Updates	January 9, 2019 at 15:08:26	January 9, 2019 at 15:13:20	Lenovo-TOR1	Complete
✓ Lenovo-TOR1	January 9, 2019 at 15:08:26	January 9, 2019 at 15:13:20	Lenovo-TOR1	Complete
✓ RackSwitch Readiness Check	January 9, 2019 at 15:08:26	January 9, 2019 at 15:08:26	Lenovo-TOR1	Complete
✓ Applying RackSwitch firmware	January 9, 2019 at 15:08:28	January 9, 2019 at 15:13:20	Lenovo-TOR1	Complete

Summary for *Applying RackSwitch firmware* job and sub-jobs

Severity: i Informational  
 Description: The task has completed successfully.  
 Action: No action required for this task.

Abbildung 38. Aktualisierungsfortschritt auf der Jobs-Seite

Schritt 6. Kehren Sie zur Seite Firmwareaktualisierungen: Übernehmen/Aktivieren in XClarity Administrator zurück, um zu überprüfen, ob die neue Switch-Firmware nun auf dem aktiven Image des TOR-

Switches ausgeführt wird. Möglicherweise müssen Sie auf **Aktualisieren** () klicken, um korrekte Details zu erhalten.

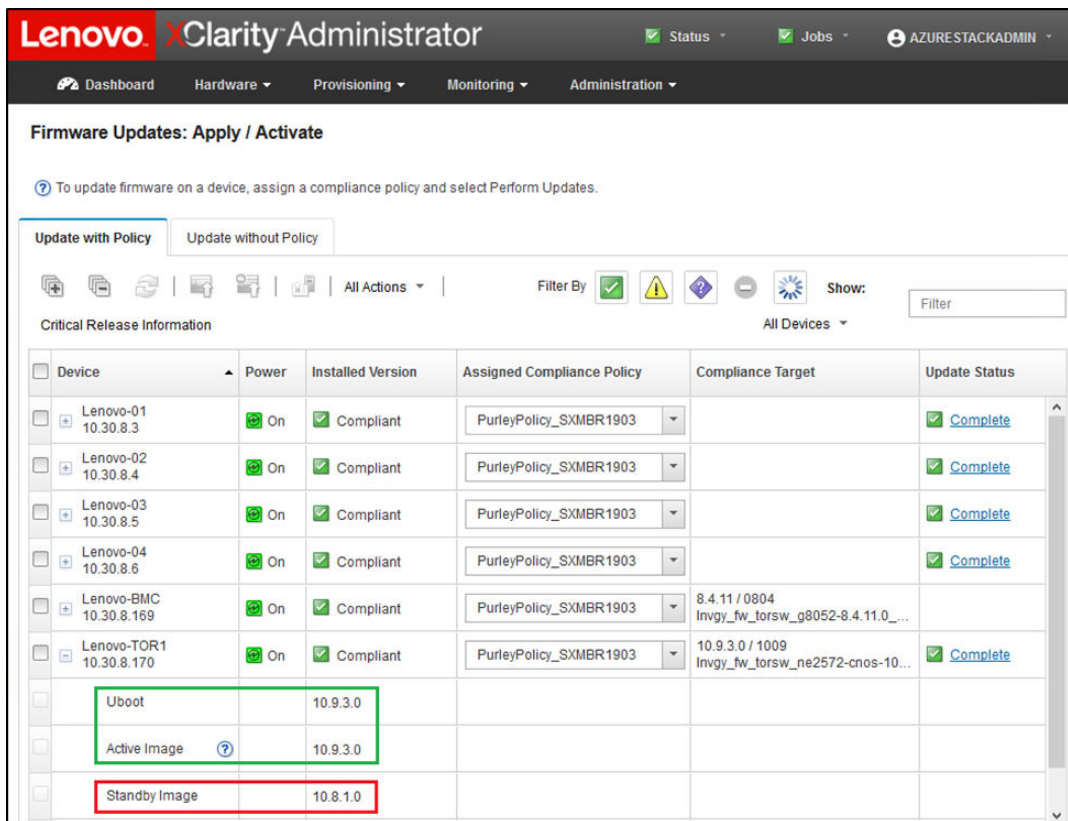


Abbildung 39. Aktive und Standby-Images

**Anmerkung:** Für die TOR-Switches, auf denen CNOS ausgeführt wird, aktualisiert XClarity Administrator nur das Uboot- und Standby-Image und macht es vor dem Laden des Switches zum aktiven Image. Daher ist die „N-1“-Switch-Firmwareversion im Hinblick auf eine optimale Vorgehensweise immer als das Standby-Image verfügbar. Im obigen Screenshot wird auf dem Uboot- und aktiven Image die neue Firmware (im grünen Feld angezeigt) ausgeführt und auf dem Standby-Image wird weiterhin die vorherige Firmware (im roten Feld angezeigt) ausgeführt.

Schritt 7. Geben Sie in einer SSH-Sitzung mit dem gerade aktualisierten TOR-Switch (Sie können PuTTY verwenden, das auf dem HLH verfügbar ist) den folgenden Befehl aus, um die laufende Konfiguration in der Startkonfiguration zu speichern.

```
write
```

## Lenovo TOR-Switch-Funktionalität überprüfen

Stellen Sie nach der Aktualisierung des Lenovo TOR-Switches basierend auf der Lösungskonfiguration sicher, dass der Switch voll funktionsfähig ist.

Zusätzlich zum Vergleich der ausgeführten Konfiguration des Switches mit der gesicherten Konfigurationsdatei, die vor der Aktualisierung der Switch-Firmware gespeichert wurde, helfen die folgenden Prüfungsverfahren bei der Überprüfung dieser Fakten:

- Switch-NOS ist aktualisiert und zum Booten festgelegt
- vLAG ISL ist intakt und betriebsbereit
- BGP-Verbindungen sind aktiv und Sitzungen wurden hergestellt
- VRRP-Master und -Sicherung sind aktiv und leiten weiter

- Alle Links sind aktiv und die IP-Adressen sind zugewiesen
- ACLs sind vorhanden und Zähler zählen hoch

Gehen Sie wie folgt vor, um vor dem Fortfahren sicherzustellen, dass der aktualisierte TOR-Switch ordnungsgemäß funktioniert. Verwenden Sie PuTTY auf dem HLH, um eine Verbindung mit dem TOR-Switch herzustellen. Wählen Sie im angezeigten PuTTY-Sicherheitshinweis **Ja** aus.

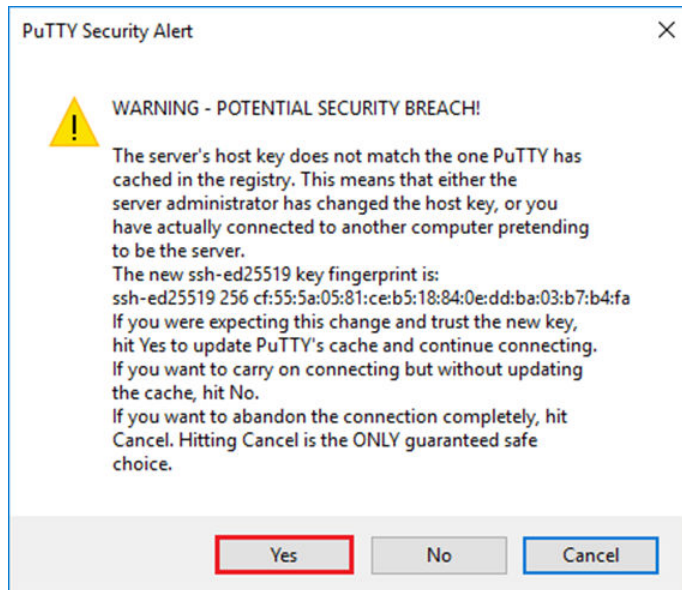


Abbildung 40. PuTTY-Sicherheitshinweis

### Lenovo TOR-Switch-Aktualisierung überprüfen

Geben Sie den folgenden Befehl ein, um zu überprüfen, dass die NOS-Aktualisierung des Lenovo TOR-Switches angewendet wurde:

```
Show version
```

## Beispiel

```
Lenovo-TOR1#show version
Lenovo Networking Operating System (NOS) Software
Technical Assistance Center: http://www.lenovo.com
Copyright (C) Lenovo, 2016. All rights reserved.

Software:
  Bootloader version: 10.8.1.0
  System version: 10.8.1.0
  System compile time: Jul 18 17:06:53 PDT 2018
Hardware:
  NE2572 ("48x25GE + 6x100GE")
  Intel(R) Celeron(R) CPU with 8192 MB of memory

  Device name: Lenovo-TOR1
  Boot Flash: 16 MB

Kernel uptime is 0 day(s), 0 hour(s), 6 minute(s), 46 second(s)

Last Reset Reason: Power Cycle
Lenovo-TOR1#

2019-01-09T23:18:00.924+00:00 Lenovo-TOR1(cnos:default) %VLAG-5-OS_MISMATCH: vLAG OS version mismatch,
local OS version is 10.8.x.x peer OS version is 10.6.x.x
2019-01-09T23:18:10.924+00:00 Lenovo-TOR1(cnos:default) %VLAG-5-OS_MISMATCH: vLAG OS version mismatch,
local OS version is 10.8.x.x peer OS version is 10.6.x.x
```

**Anmerkung:** Möglicherweise werden Ihnen in regelmäßigen Abständen Informationsnachrichten angezeigt, wie am Ende des obigen Beispiels sichtbar, die angeben, dass die Betriebssysteme der beiden TOR-Switches nicht übereinstimmen. Dies entspricht dem erwarteten Verhalten zu diesem Zeitpunkt des Prozesses. Diese Nachrichten sollten nicht mehr angezeigt werden, nachdem der zweite TOR-Switch aktualisiert wurde.

## Boot-Image überprüfen

Geben Sie den folgenden Befehl ein, um zu überprüfen, dass der TOR-Switch mit dem neuen Firmware-Image (das nun das aktive Image ist) gebootet werden soll:

```
show boot
```

## Beispiel

```
Lenovo-TOR1#show boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.8.1.0, downloaded 00:33:35 PST Thu Jan 10 2019
  standby image: version 10.6.1.0, downloaded 18:24:35 PST Fri Jan 12 2018
  Grub: version 10.8.1.0, downloaded 23:09:14 PST Wed Jan 9 2019
  BIOS: version 020AB, release date 02/14/2018
  Secure Boot: Enabled
  ONIE: version unknown, downloaded unknown
Currently set to boot software active image
Current port mode:
  Port Ethernet1/37 is set in 10G mode
  Port Ethernet1/38 is set in 10G mode
  Port Ethernet1/39 is set in 10G mode
  Port Ethernet1/40 is set in 10G mode
  Port Ethernet1/45 is set in 10G mode
  Port Ethernet1/46 is set in 10G mode
  Port Ethernet1/47 is set in 10G mode
  Port Ethernet1/48 is set in 10G mode
Next boot port mode:
  Port Ethernet1/37 is set in 10G mode
  Port Ethernet1/38 is set in 10G mode
  Port Ethernet1/39 is set in 10G mode
  Port Ethernet1/40 is set in 10G mode
  Port Ethernet1/45 is set in 10G mode
  Port Ethernet1/46 is set in 10G mode
  Port Ethernet1/47 is set in 10G mode
  Port Ethernet1/48 is set in 10G mode
Currently scheduled reboot time: none
```

## Links überprüfen

Führen Sie den folgenden Befehl aus, um zu überprüfen, dass alle Links aktiv sind und IP-Adressen zugewiesen wurden:

```
show interface brief | include up
```

## Beispiel

```
Lenovo-TOR1#show interface brief | include up
Ethernet1/1      7      eth trunk up none          25000  --
Ethernet1/2      7      eth trunk up none          25000  --
Ethernet1/3      7      eth trunk up none          25000  --
Ethernet1/4      7      eth trunk up none          25000  --
Ethernet1/40     --     eth routed up none          10000  --
Ethernet1/43     --     eth routed up none          25000  --
Ethernet1/44     --     eth routed up none          25000  --
Ethernet1/47     --     eth routed up none          10000  --
Ethernet1/48     --     eth routed up none          10000  --
Ethernet1/49     99     eth trunk up none          100000 101
Ethernet1/50     99     eth trunk up none          100000 101
po101            99     eth trunk up none          100000 lacp
mgmt0 management up      10.30.8.170          1000 1500
Vlan7            --     up --
Vlan107          --     up --
loopback0        up      Loopback0_Rack1_TOR1
```

**Anmerkung:** Der Status der Ethernet-Schnittstellen 1/5 bis 1/16 hängt von der Anzahl der Knoten in der Skalierungseinheit ab. Das obige Beispiel stammt von einer SXM4400 Lösung mit vier Knoten.

### VLAG ISL überprüfen

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der vLAG ISL intakt und betriebsbereit ist:

```
show vlag information
```

#### Beispiel

```
Lenovo-TOR1#show vlag information
Global State:          enabled
VRRP active/active mode: enabled
vLAG system MAC:      08:17:f4:c3:dd:63
ISL Information:
  PCH    Ifindex      State      Previous State
  -----+-----+-----+-----
  101    100101        Active     Inactive

Mis-Match Information:
           Local                Peer
  -----+-----+-----+-----
Match Result : Match                Match
Tier ID      : 100                  100
System Type  : NE2572                NE2572
OS Version   : 10.8.x.x              10.8.x.x

Role Information:
           Local                Peer
  -----+-----+-----+-----
Admin Role   : Primary                Secondary
Oper Role    : Secondary              Primary
Priority      : 0                      0
System MAC   : a4:8c:db:bb:0b:01      a4:8c:db:bb:0c:01

Consistency Checking Information:
State        : enabled
Strict Mode  : disabled
Final Result : pass
```

### BGP-Funktionalität überprüfen

Führen Sie den folgenden Befehl aus, um zu überprüfen, dass alle BGP-Verbindungen aktiv sind und Sitzungen erstellt wurden:

```
show ip bgp summary
```

### Beispiel

```
Lenovo-TOR1#show ip bgp summary
BGP router identifier 10.30.8.152, local AS number 64675
BGP table version is 74
2 BGP AS-PATH entries
0 BGP community entries
8 Configured ebgp ECMP multipath: Currently set at 8
8 Configured ibgp ECMP multipath: Currently set at 8

Neighbor      V      AS MsgRcv MsgSen TblVer InQ OutQ Up/Down State/PfxRcd
10.30.8.146   4  64675   72    74    74    0   0 01:09:14     5
10.30.8.158   4  64675   74    74    74    0   0 01:09:15    33
10.30.8.162   4  64675   74    74    74    0   0 01:09:24    33
10.30.29.12   4  64719  235   215    74    0   0 01:09:17    25
10.30.29.13   4  64719  235   214    74    0   0 01:09:17    25

Total number of neighbors 5

Total number of Established sessions 5
```

Beachten Sie, dass das obige Beispiel von einer statisch gerouteten Lösung stammt. Eine Lösung mit dynamischem Routing enthält außerdem zwei BGP-Sitzungen für Border-Switches (insgesamt sieben Sitzungen).

### VRRP-Funktionalität überprüfen

Führen Sie den folgenden Befehl auf jedem TOR-Switch aus, um sicherzustellen, dass VRRP-Master und -Sicherung aktiv sind und weiterleiten:

```
show vrrp vlag
```

### Beispiel

```
Lenovo-TOR1#show vrrp vlag
Flags: F - Forwarding enabled on Backup for vLAG
vLAG enabled, mode: vrrp active
Interface      VR IpVer Pri Time    Pre State VR IP addr
-----
(F)Vlan7       7  IPV4  100 100 cs Y Backup 10.30.29.1
(F)Vlan107     107 IPV4  100 100 cs Y Backup 10.30.28.1
```

```
Lenovo-TOR2#show vrrp vlag
Flags: F - Forwarding enabled on Backup for vLAG
vLAG enabled, mode: vrrp active
Interface      VR IpVer Pri Time    Pre State VR IP addr
-----
Vlan7          7  IPV4  100 100 cs Y Master 10.30.29.1
Vlan107        107 IPV4  100 100 cs Y Master 10.30.28.1
```

### Vorhandensein und Funktionalität von ALCs überprüfen

Führen Sie die folgenden Befehle aus, um zu überprüfen, dass ACLs vorhanden sind und die Zähler hochzählen:

```
show ip access-lists summary
show ip access-lists
```

## Beispiel

```
Lenovo-TOR-1#show ip access-lists summary
IPV4 ACL Rack01-CL01-SU01-Infra_IN
  statistics enabled
  Total ACEs Configured: 28
  Configured on interfaces:
    Vlan7 - ingress (Router ACL)
  Active on interfaces:
    Vlan7 - ingress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL Rack01-CL01-SU01-Infra_OUT
  statistics enabled
  Total ACEs Configured: 28
  Configured on interfaces:
    Vlan7 - egress (Router ACL)
  Active on interfaces:
    Vlan7 - egress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL Rack01-CL01-SU01-Stor_IN
  statistics enabled
  Total ACEs Configured: 6
  Configured on interfaces:
    Vlan107 - ingress (Router ACL)
  Active on interfaces:
    Vlan107 - ingress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL Rack01-CL01-SU01-Stor_OUT
  statistics enabled
  Total ACEs Configured: 6
  Configured on interfaces:
    Vlan107 - egress (Router ACL)
  Active on interfaces:
    Vlan107 - egress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL UPLINK_ROUTED_IN
  statistics enabled
  Total ACEs Configured: 4
  Configured on interfaces:
    Ethernet1/47 - ingress (Router ACL)
    Ethernet1/48 - ingress (Router ACL)
  Active on interfaces:
    Ethernet1/47 - ingress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL copp-system-acl-authentication
  Total ACEs Configured: 3
  Configured on interfaces:
  Active on interfaces:
  Configured and active on VRFs:
IPV4 ACL copp-system-acl-bgp
  Total ACEs Configured: 2
  Configured on interfaces:
  Active on interfaces:
  Configured and active on VRFs:
...
```



## Beispiel

```
Lenovo-TOR-1#show ip access-lists
IP access list Rack01-CL01-SU01-Infra_IN
    statistics per-entry
    500 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_R01-C01-SU01-INF
(10.20.25.0/24)"
    510 permit any 10.20.25.0/24 10.20.25.0/24 [match=70214264]
    520 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_azs-hlh-dvm00 (10
.20.3.61/32)"
    530 permit any 10.20.25.0/24 host 10.20.3.61 [match=11180]
    540 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_R01-C01-SU01-InVI
P (10.20.126.128/25)"
    550 permit any 10.20.25.0/24 10.20.126.128/25
    560 remark "Permit R01-C01-SU01-InVIP (10.20.126.128/25)_TO_R01-C01-SU01
-INF (10.20.25.0/24)"
    570 permit any 10.20.126.128/25 10.20.25.0/24 [match=27814360]
    580 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_pub-adm-vip (10.2
0.23.0/27)"
    590 permit any 10.20.25.0/24 10.20.23.0/27 [match=80158]
    600 remark "Permit pub-adm-vip (10.20.23.0/27)_TO_R01-C01-SU01-INF (10.2
0.25.0/24)"
    610 permit any 10.20.23.0/27 10.20.25.0/24 [match=76824]
    620 remark "Permit 112 any (0.0.0.0/0)_to_Multicast (224.0.0.18/32)"
    630 permit 112 any host 224.0.0.18 [match=62576]
    640 remark "Permit UDP any_TO_any(BOOTP) port 67"
    650 permit udp any any eq bootps [match=443]
...
```

## Netzwerkverbindung der Lösung überprüfen

Sobald die Basissystem-Konvergenz im aktualisierten Lenovo TOR-Switch überprüft wurde, gehen Sie wie folgt vor, um die Lösungsverbindung zu testen:

1. Navigieren Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle zu **Verwaltung** → **Netzwerkzugriff**.
2. Klicken Sie oben in der Browser-Schnittstelle auf die Schaltfläche **Verbindung testen**.
3. Geben Sie im Feld **Host** 8.8.8.8 ein und klicken Sie auf **Verbindung testen**.
4. Ein Erfolgsfenster wird angezeigt. Klicken Sie auf **Schließen**, um dieses Fenster zu schließen.
5. Melden Sie sich als zusätzlichen Verifizierungsschritt im Azure Stack Hub-Administratorportal an.
6. Stellen Sie im Azure Stack Hub-Administratorportal sicher, dass derzeit keine Alerts sichtbar sind.

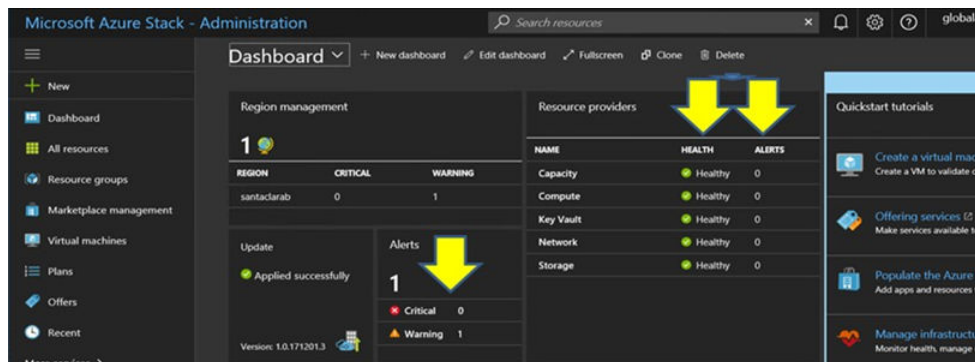


Abbildung 41. Alert-Überprüfung im Azure Stack Hub-Administratorportal

Warten Sie, bis Netzwerkverkehr und Erreichbarkeit vollständig rekonvergiert sind und sich die Systeme stabilisiert haben. Überprüfen Sie außerdem das Azure Stack Hub-Administratorportal, um sicherzustellen, dass die Statusanzeigen aller Komponenten als fehlerfrei angezeigt werden. Wenn sich die Lösung stabilisiert hat, kehren Sie zum Abschnitt „CNOS auf TOR-Switches aktualisieren“ zurück und wiederholen Sie den Vorgang auf dem anderen TOR-Switch. Nachdem beide TOR-Switches aktualisiert wurden und ihre Funktionalität und Stabilität überprüft wurde, fahren Sie mit der Aktualisierung des BMC-Switches fort.

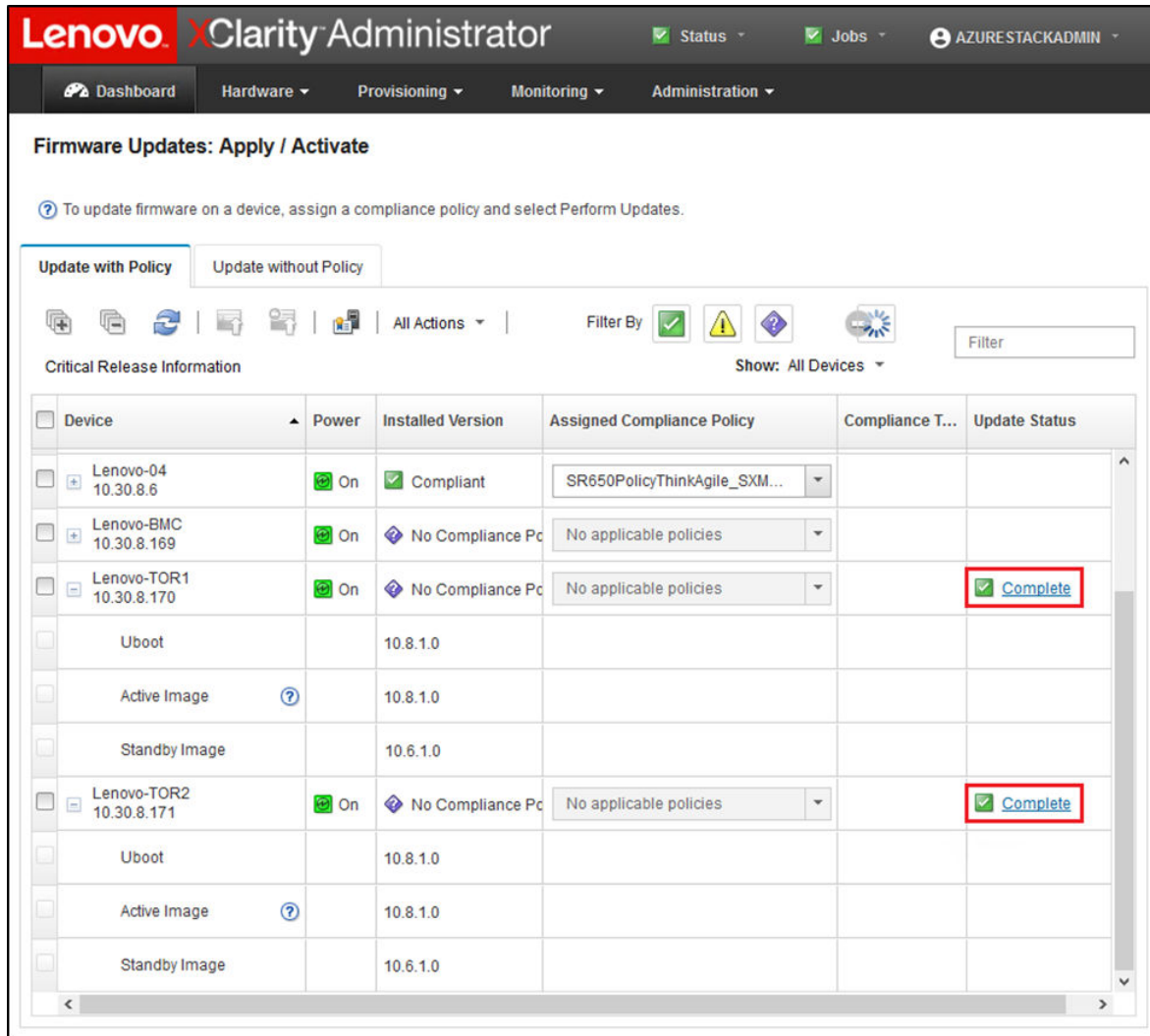


Abbildung 42. Überprüfen der Firmwareaktualisierungen der TOR-Switches auf Vollständigkeit

## Lenovo BMC-Switch-Firmware aktualisieren

In diesem Abschnitt werden die erforderlichen Schritte zur Aktualisierung des Firmware-Image auf einem Lenovo BMC-Switch beschrieben.

**Anmerkung:** Wenn der Lenovo ThinkSystem NE0152T RackSwitch nicht von LXCA verwaltet wird, verwenden Sie die Schritte in „BMC-Switch-Firmware mit der CLI aktualisieren“ auf Seite 101 zur Aktualisierung dieses Switches, falls er in Ihrer Lösung vorhanden ist.

### BMC-Switch-Konfiguration sichern

Stellen Sie vor Beginn des Aktualisierungsverfahrens sicher, dass die BMC-Switch-Konfiguration gesichert wurde.

**Anmerkung:** Wenn der Lenovo ThinkSystem NE0152T RackSwitch nicht von LXCA verwaltet wird, verwenden Sie die Schritte in „[BMC-Switch-Firmware mit der CLI aktualisieren](#)“ auf Seite 101 zur Aktualisierung dieses Switches, falls er in Ihrer Lösung vorhanden ist.

Sie können die Switch-Konfigurationsdateien eines Lenovo BMC-Switches ganz einfach in XClarity Administrator sichern. Gehen Sie wie folgt vor:

Schritt 1. Wählen Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle **Hardware** → **Switches** aus.

Schritt 2. Aktivieren Sie das Kontrollkästchen, um den BMC-Switch auszuwählen.



Abbildung 43. Auswahl des BMC-Switches für die Sicherung

Schritt 3. Navigieren Sie zu **Alle Aktionen** → **Konfiguration** → **Konfigurationsdatei sichern**.

Schritt 4. Prüfen Sie im angezeigten Fenster, dass der BMC-Switch im Feld **Ausgewählte Switches** angezeigt wird. Geben Sie eine Beschreibung für die Sicherung ein und klicken Sie auf **Sicherung**.

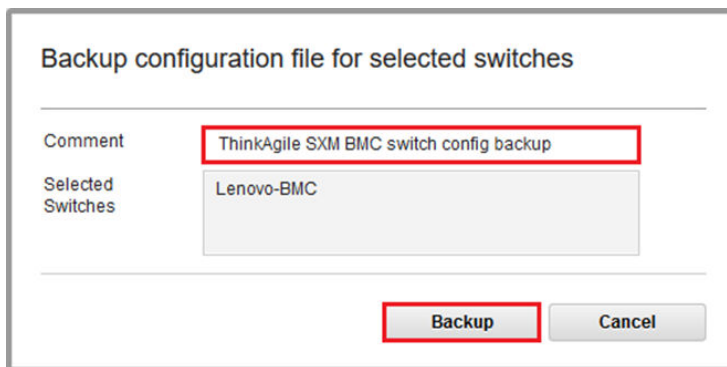


Abbildung 44. Überprüfen und Kommentieren des BMC-Switches für die Sicherung

Schritt 5. Eine Meldung zur erfolgreichen Sicherung wird angezeigt. Klicken Sie auf **Schließen**, um diese Meldung zu schließen.

Schritt 6. Die Backup-Switch-Konfigurationsdateien werden intern in XClarity Administrator gespeichert, aber wir müssen eine besser verfügbare Kopie bereitstellen. Um eine Kopie auf dem HLH zu speichern, klicken Sie auf einen Switch, um eine detaillierte Ansicht des Switches zu öffnen.

Schritt 7. Wählen Sie im linken Bereich **Konfigurationsdateien** aus und aktivieren Sie das Kontrollkästchen neben dem Dateinamen, um die gesicherte Konfigurationsdatei auszuwählen.

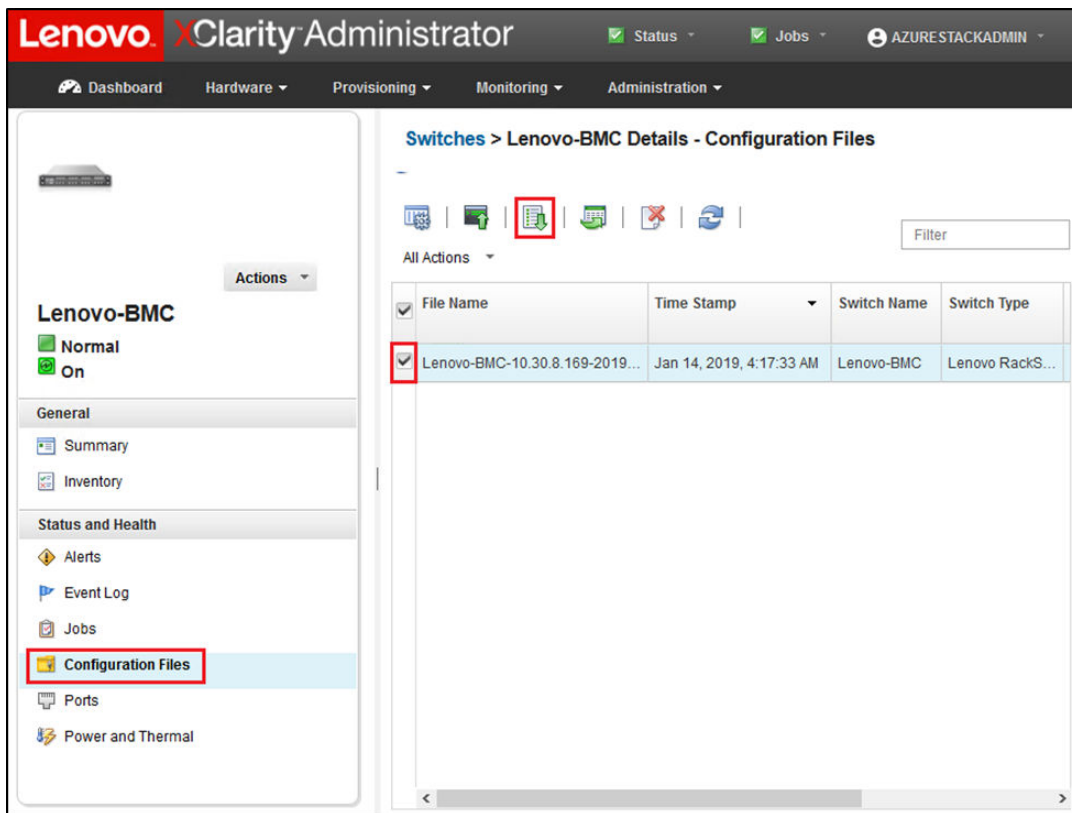


Abbildung 45. Auswahl der gesicherten Konfigurationsdatei zum Download

Schritt 8. Klicken Sie auf die Schaltfläche **Konfigurationsdatei aus XClarity auf lokalen PC herunterladen**



Schritt 9. Geben Sie je nach verwendetem Browser einen Downloadspeicherort an und speichern Sie die Datei. Der Standarddateiname von XClarity Administrator hat das folgende Format:

<SwitchHostname>-<IPAddress>-<Date>-<Time>.cfg

Schritt 10. Verschieben Sie die gesicherte BMC-Konfigurationsdatei in das Verzeichnis D:\Lenovo\Switch Config Backups auf dem HLH.

## Lenovo BMC-Switch aktualisieren

Verwenden Sie bei gesicherter Switch-Konfigurationsdatei XClarity Administrator zum Aktualisieren der BMC-Switch-Firmware.


**Anmerkung:** Wenn der Lenovo ThinkSystem NE0152T RackSwitch nicht von LXCA verwaltet wird, verwenden Sie die Schritte in „[BMC-Switch-Firmware mit der CLI aktualisieren](#)“ auf Seite 101 zur Aktualisierung dieses Switches, falls er in Ihrer Lösung vorhanden ist.

Der Prozess beinhaltet das Aktualisieren der Firmware auf dem BMC-Switch und Überprüfen der BMC-Switch-Funktionalität. Gehen Sie zur Aktualisierung eines Lenovo BMC-Switches wie folgt vor:

Schritt 1. Melden Sie sich ggf. bei XClarity Administrator an und navigieren Sie im Hauptmenü zu **Bereitstellung → Übernehmen/Aktivieren**.

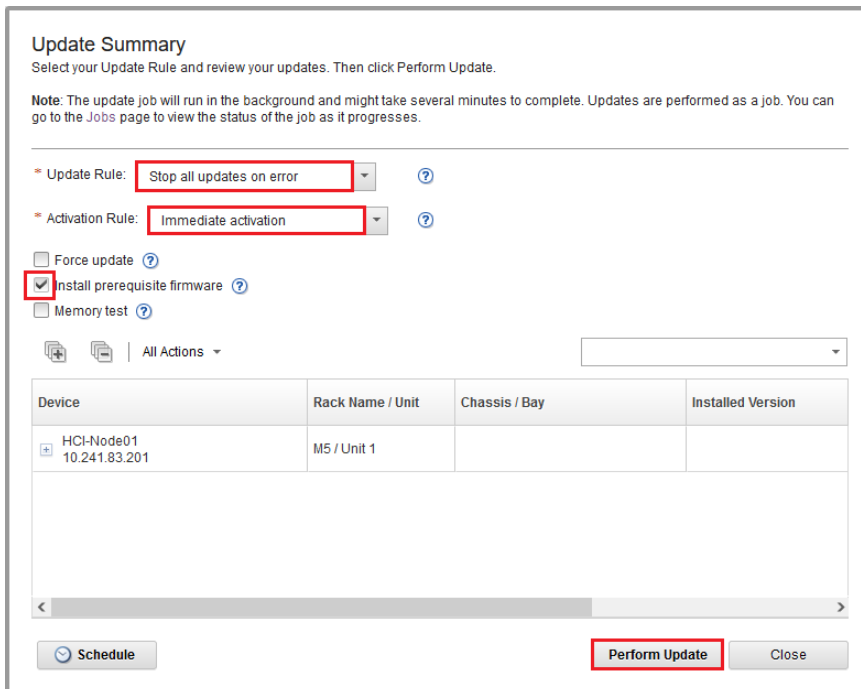
Schritt 2. Stellen Sie sicher, dass der BMC-Switch als „Nicht konform“ für die Firmwareaktualisierungsrichtlinie mit optimaler Vorgehensweise angezeigt wird, die ihm

zugeordnet ist. Wenn der Switch als „Konform“ angezeigt wird, ist keine Aktualisierung erforderlich.

Schritt 3. Wenn der Switch nicht konform ist, wählen Sie den BMC-Switch durch Aktivierung des Kontrollkästchens links davon aus und klicken Sie auf die Schaltfläche **Aktualisierungen durchführen** (  ).

Schritt 4. Legen Sie im neu geöffneten Fenster Aktualisierungszusammenfassung die folgenden Optionen fest und klicken Sie auf **Aktualisierung durchführen**:

- **Aktualisierungsregel: Alle Aktualisierungen bei einem Fehler anhalten**
- **Aktivierungsregel: Sofortige Aktivierung**
- **Erforderliche Firmware installieren**



**Update Summary**  
Select your Update Rule and review your updates. Then click Perform Update.

**Note:** The update job will run in the background and might take several minutes to complete. Updates are performed as a job. You can go to the Jobs page to view the status of the job as it progresses.

\* Update Rule:  ?

\* Activation Rule:  ?

Force update ?

Install prerequisite firmware ?

Memory test ?

All Actions ▾


Device	Rack Name / Unit	Chassis / Bay	Installed Version
 HCI-Node01 10.241.83.201	M5 / Unit 1		

Abbildung 46. Auswählen von BMC-Aktualisierungs- und -Aktivierungsregeln

Schritt 5. Öffnen Sie die Jobs-Seite, um den Aktualisierungsfortschritt zu überwachen.

**Lenovo XClarity Administrator** | Status | Jobs | AZURESTACKADMIN

Dashboard | Hardware | Provisioning | Monitoring | Administration

**Jobs Page > Firmware Updates**

Job	Start	Complete	Targets	Status
❄️ Firmware Updates	January 14, 2019 at 12:50:55		Lenovo-BMC	Executing - 64.00%
❄️ Lenovo-BMC	January 14, 2019 at 12:50:55		Lenovo-BMC	Executing - 64.00%
✅ RackSwitch Readiness Check	January 14, 2019 at 12:50:55	January 14, 2019 at 12:50:56	Lenovo-BMC	Complete
❄️ Applying RackSwitch firmware	January 14, 2019 at 12:50:57		Lenovo-BMC	Executing - 28.00%

**Summary for Firmware Updates job and sub-jobs**  
No summary available

**Lenovo XClarity Administrator** | Status | Jobs | AZURESTACKADMIN

Dashboard | Hardware | Provisioning | Monitoring | Administration

**Jobs Page > Firmware Updates**

Job	Start	Complete	Targets	Status
✅ Firmware Updates	January 14, 2019 at 12:50:55	January 14, 2019 at 12:54:51	Lenovo-BMC	Complete
✅ Lenovo-BMC	January 14, 2019 at 12:50:55	January 14, 2019 at 12:54:51	Lenovo-BMC	Complete
✅ RackSwitch Readiness Check	January 14, 2019 at 12:50:55	January 14, 2019 at 12:50:56	Lenovo-BMC	Complete
✅ Applying RackSwitch firmware	January 14, 2019 at 12:50:57	January 14, 2019 at 12:54:51	Lenovo-BMC	Complete

**Summary for Applying RackSwitch firmware job and sub-jobs**  
Severity: Informational  
Description: The task has completed successfully.  
Action: No action required for this task.

Abbildung 47. Überwachen des BMC-Aktualisierungsfortschritts auf der Jobs-Seite

Schritt 6. Kehren Sie zur Seite Firmwareaktualisierungen: Übernehmen/Aktivieren in XClarity Administrator zurück, um zu überprüfen, ob die neue Switch-Firmware auf dem aktiven Image des BMC-Switches ausgeführt wird. Möglicherweise müssen Sie auf die Schaltfläche **Aktualisieren** (🔄) klicken, um korrekte Details zu erhalten.



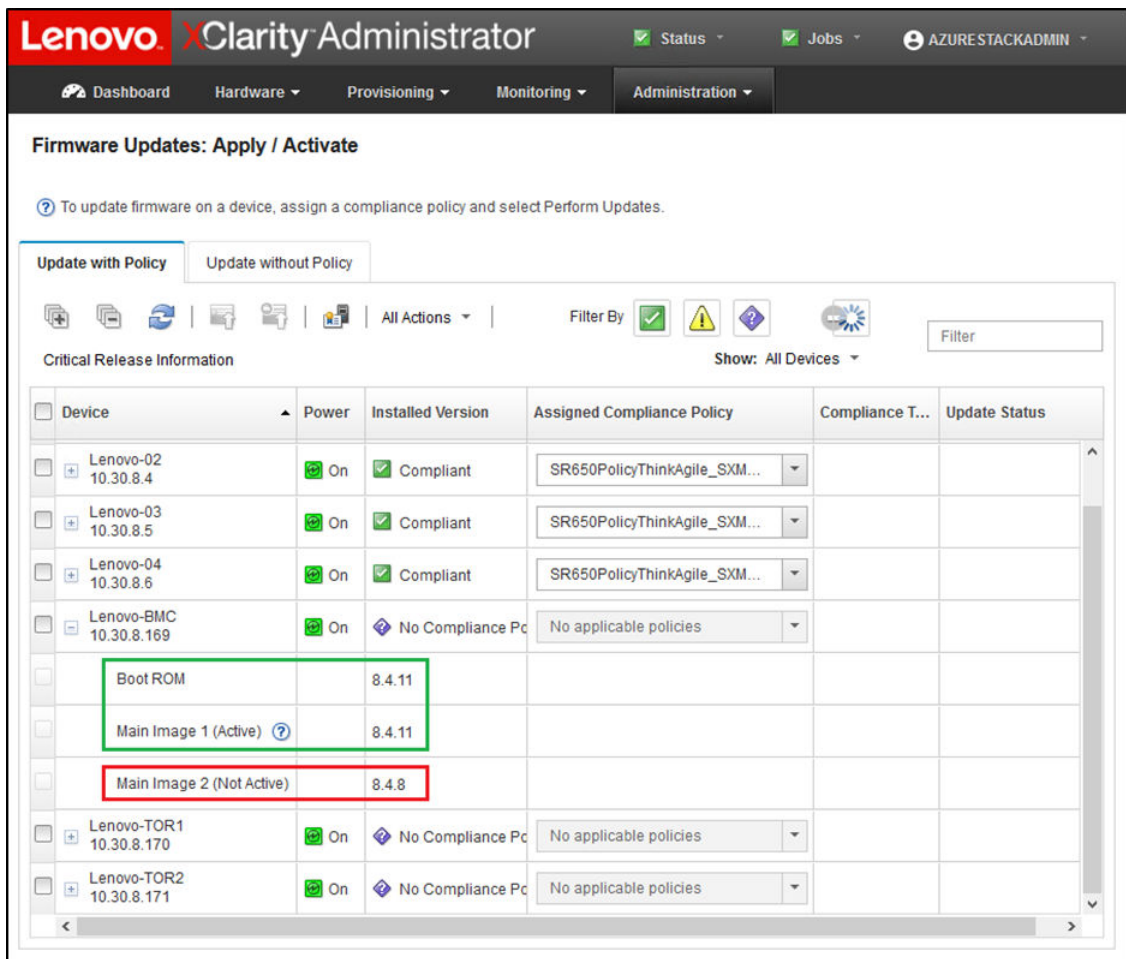


Abbildung 48. Überprüfen der neuen ausgeführten BMC-Firmware im aktiven Image

**Anmerkung:** Für einen Lenovo BMC-Switch, auf dem ENOS ausgeführt wird, aktualisiert XClarity Administrator nur das nicht aktive Image und macht dieses Image vor dem Laden des Switches zum aktiven Image. Daher ist die „N-1“-Switch-Firmwareversion im Hinblick auf eine optimale Vorgehensweise immer als das Standby-Image verfügbar. Im obigen Screenshot wird auf dem Boot-ROM und aktiven Image (Main Image 1/Haupt-Image 1) die neue Firmware ausgeführt (im grünen Feld angezeigt). Auf dem nicht aktiven Image (Main Image 2/Haupt-Image 2) wird weiterhin die vorherige Firmware ausgeführt (im roten Feld angezeigt).

Schritt 7. Geben Sie in einer SSH-Sitzung mit dem BMC-Switch (Sie können PuTTY verwenden, das auf dem HLH verfügbar ist) den folgenden Befehl aus, um die laufende Konfiguration in der Startkonfiguration zu speichern.

```
copy running-config startup-config
```

## BMC-Switch-Funktionalität überprüfen

Stellen Sie nach der Aktualisierung des BMC-Switches basierend auf der Lösungskonfiguration sicher, dass der Switch voll funktionsfähig ist.

Zusätzlich zum Vergleich der ausgeführten Konfiguration des Switches mit der gesicherten Konfigurationsdatei, die vor der Aktualisierung der Switch-Firmware gespeichert wurde, helfen diese Prüfungsverfahren bei der Überprüfung dieser Fakten:

- Switch-NOS ist aktualisiert und zum Booten festgelegt
- Alle Links sind aktiv und die IP-Adressen sind zugewiesen
- BGP-Verbindungen sind aktiv und Sitzungen wurden hergestellt
- ACLs sind vorhanden und Zähler zählen hoch

Gehen Sie wie folgt vor, um vor dem Fortfahren sicherzustellen, dass der aktualisierte BMC-Switch ordnungsgemäß funktioniert.

### **BMC-Switch-Aktualisierung überprüfen**

Melden Sie sich beim BMC-Switch an und führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Switch-NOS-Aktualisierung durchgeführt wurde und der Switch zum aktualisierten Image bootet:

```
show boot
```

#### **Beispiel**

```
Lenovo-BMC#show boot
Current running image version: 8.4.11
Currently set to boot software image1, active config block.
NetBoot: disabled, NetBoot tftp server: , NetBoot cfgfile:
Current boot Openflow protocol version: 1.0
USB Boot: disabled
Currently profile is default, set to boot with default profile next time.
Current FLASH software:
  image1: version 8.4.11, downloaded 12:52:04 Mon Jan 14, 2019
           NormalPanel, Mode Stand-alone
  image2: version 8.4.8, downloaded 10:26:19 Mon Jan 14, 2019
           NormalPanel, Mode Stand-alone
  boot kernel: version 8.4.11
              NormalPanel
  bootloader : version 8.4.11
Currently scheduled reboot time: none
```

### **Links überprüfen**

Führen Sie den folgenden Befehl aus, um zu überprüfen, dass alle Links aktiv sind und IP-Adressen zugewiesen wurden:

```
show interface link state up
```



### Beispiel

```
Lenovo-BMC#show interface link state up
```

Alias	Port	Speed	Duplex	Flow Ctrl	Link	Description
				--TX--	--RX--	
1	1	1000	full	no	no	up BMC Mgmt Ports
2	2	1000	full	no	no	up BMC Mgmt Ports
3	3	1000	full	no	no	up BMC Mgmt Ports
4	4	1000	full	no	no	up BMC Mgmt Ports
8	8	1000	full	no	no	up BMC Mgmt Ports
46	8	1000	full	no	no	up BMC Mgmt Ports
47	47	1000	full	no	no	up Switch Mgmt Ports
48	48	1000	full	no	no	up Switch Mgmt Ports
XGE1	49	10000	full	no	no	up BMC Mgmt Ports
XGE2	50	10000	full	no	no	up BMC Mgmt Ports
XGE3	51	10000	full	no	no	up P2P_Rack1/TOR1_To_Rack1/BMC TOR Port 46
XGE4	52	10000	full	no	no	up P2P_Rack1/TOR2_To_Rack1/BMC TOR Port 46

**Anmerkung:** Der Status der Ports 1 bis 16 hängt von der Anzahl der Knoten in der Lösung ab. Das obige Beispiel stammt von einer Lösung mit vier Knoten.

Ein weiterer hilfreicher Befehl zum Überprüfen von IP-Konfiguration und Status:

```
show interface ip
```

### Beispiel

```
Lenovo-BMC#show interface ip
```

```
Interface information:
```

```
5: IP4 10.30.8.169 255.255.255.248 10.30.8.175, vlan 5, up
6: IP4 10.30.1.1 255.255.255.128 10.30.8.151, vlan 6, up
```

```
Routed Port Interface Information:
```

```
XGE3: IP4 10.30.8.146 255.255.255.252 10.30.8.147, routed, up
XGE4: IP4 10.30.8.150 255.255.255.252 10.30.8.151, routed, up
```

```
Loopback interface information:
```

```
lo1: 10.30.30.26 255.255.255.255 10.30.30.26, up
```

### BGP-Funktionalität überprüfen

Führen Sie den folgenden Befehl aus, um zu überprüfen, dass alle BGP-Verbindungen aktiv sind und Sitzungen erstellt wurden:

```
show ip bgp neighbor summary
```

### Beispiel

```
Lenovo-BMC#show ip bgp neighbor summary
```

```
BGP ON
```

```
BGP router identifier 10.30.8.154, local AS number 64675
```

```
BGP thid 21, allocs 1168, frees 301, current 147124, largest 5784
```

```
BGP Neighbor Summary Information:
```

Peer	V	AS	MsgRcvd	MsgSent	Up/Down	State
1: 10.30.8.145	4	64675	106	104	01:41:23	established
2: 10.30.8.149	4	64675	106	104	01:41:23	established

## Vorhandensein und Funktionalität von ALCs überprüfen

Führen Sie den folgenden Befehl aus, um zu überprüfen, dass ACLs vorhanden sind und die Zähler hochzählen:

```
show access-control
show access-control group
show access-control counters
```

### Beispiel

```
Lenovo-BMC#show access-control
Current access control configuration:
```

```
Filter 200 profile:
```

```
IPv4
```

```
- SRC IP      : 10.20.3.0/255.255.255.192
- DST IP      : 10.20.3.0/255.255.255.192
```

```
Meter
```

```
- Set to disabled
- Set committed rate : 64
- Set max burst size : 32
```

```
Re-Mark
```

```
- Set use of TOS precedence to disabled
```

```
Actions      : Permit
```

```
Statistics   : enabled
```

```
Installed on vlan 125 in
```

```
ACL remark note
```

```
- "Permit R01-bmc (10.20.3.0/26)_TO_R01-bmc (10.20.3.0/26)"
```

```
Filter 202 profile:
```

```
IPv4
```

```
- SRC IP      : 10.20.3.0/255.255.255.192
- DST IP      : 10.20.30.40/255.255.255.248
```

```
Meter
```

```
- Set to disabled
- Set committed rate : 64
- Set max burst size : 32
```

```
Re-Mark
```

```
- Set use of TOS precedence to disabled
```

```
Actions      : Permit
```

```
Statistics   : enabled
```

```
Installed on vlan 125 in
```

```
ACL remark note
```

```
- "Permit R01-bmc (10.20.3.0/26)_TO_R01-SwitchMgmt (10.20.30.40/29)"
```

```
Filter 204 profile:
```

```
IPv4
```

```
- SRC IP      : 10.20.3.61/255.255.255.255
- DST IP      : 0.0.0.0/0.0.0.0
```

```
...
```

### Beispiel

```
Lenovo-BMC#show access-control group
Current ACL group Information:
-----
ACL group 1 (14 filter level consumed):

- ACL 200
- ACL 202
- ACL 204
- ACL 206
- ACL 208
- ACL 210
- ACL 212
- ACL 214
- ACL 216
- ACL 218
- ACL 220
- ACL 222
- ACL 224
- ACL 226
ACL group 2 (50 filter level consumed):

- ACL 228
- ACL 230
- ACL 232

...
```

### Beispiel

```
Lenovo-BMC#show access-control counters
ACL stats:
Hits for ACL 200  vlan 125    in          1357392
Hits for ACL 202  vlan 125    in          60229537
Hits for ACL 204  vlan 125    in          237099377
Hits for ACL 206  vlan 125    in           0
Hits for ACL 208  vlan 125    in           0
Hits for ACL 210  vlan 125    in           0
Hits for ACL 212  vlan 125    in           0
Hits for ACL 214  vlan 125    in           24
Hits for ACL 216  vlan 125    in           0
Hits for ACL 218  vlan 125    in          573818
Hits for ACL 220  vlan 125    in          800950
Hits for ACL 222  vlan 125    in           0
Hits for ACL 224  vlan 125    in           0
Hits for ACL 226  vlan 125    in          447369
Hits for ACL 228  vlan 125    in          1389622
Hits for ACL 230  vlan 125    in          59570795
Hits for ACL 232  vlan 125    in          174516137

...
```

### Netzwerkverbindung der Lösung überprüfen

Sobald die Basissystem-Konvergenz im aktualisierten BMC-Switch überprüft wurde, testen Sie die Verbindung auf Folgendes:

- Ping von BMC-Switch zu verbundenen TOR-Switch-IP-Schnittstellen

### Beispiel

```
Lenovo-BMC#ping 10.30.8.130
[host 10.30.8.130, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.130: #1 ok, RTT 7 msec.
10.30.8.130: #2 ok, RTT 0 msec.
10.30.8.130: #3 ok, RTT 0 msec.
10.30.8.130: #4 ok, RTT 0 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.134
[host 10.30.8.134, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.134: #1 ok, RTT 0 msec.
10.30.8.134: #2 ok, RTT 0 msec.
10.30.8.134: #3 ok, RTT 0 msec.
10.30.8.134: #4 ok, RTT 0 msec.
Ping finished.
```

- Ping von BMC-Switch zu TOR-Verwaltungs-IP-Adressen

### Beispiel

```
Lenovo-BMC#ping 10.30.8.170
[host 10.30.8.170, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.170: #1 ok, RTT 1 msec.
10.30.8.170: #2 ok, RTT 0 msec.
10.30.8.170: #3 ok, RTT 0 msec.
10.30.8.170: #4 ok, RTT 0 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.171
[host 10.30.8.171, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.171: #1 ok, RTT 0 msec.
10.30.8.171: #2 ok, RTT 0 msec.
10.30.8.171: #3 ok, RTT 0 msec.
10.30.8.171: #4 ok, RTT 0 msec.
Ping finished.
```

- Ping von BMC-Switch zu Knoten-IMMs/XCCs

## Beispiel

```
Lenovo-BMC#ping 10.30.8.3
[host 10.30.8.3, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.3: #1 ok, RTT 1 msec.
10.30.8.3: #2 ok, RTT 0 msec.
10.30.8.3: #3 ok, RTT 0 msec.
10.30.8.3: #4 ok, RTT 0 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.4
[host 10.30.8.4, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.4: #1 ok, RTT 0 msec.
10.30.8.4: #2 ok, RTT 1 msec.
10.30.8.4: #3 ok, RTT 1 msec.
10.30.8.4: #4 ok, RTT 1 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.5
[host 10.30.8.5, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.5: #1 ok, RTT 0 msec.
10.30.8.5: #2 ok, RTT 1 msec.
10.30.8.5: #3 ok, RTT 0 msec.
10.30.8.5: #4 ok, RTT 1 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.6
[host 10.30.8.6, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.6: #1 ok, RTT 1 msec.
10.30.8.6: #2 ok, RTT 1 msec.
10.30.8.6: #3 ok, RTT 1 msec.
10.30.8.6: #4 ok, RTT 1 msec.
Ping finished.
```

## Rückstellung

Wenn ein Problem verhindert, dass ein Switch aktualisiert werden kann, müssen alle Switches in ihren ursprünglichen Status zurückgesetzt werden.

Das Rückstellungsverfahren enthält dahingehend allgemeine Schritte. Generell können die Befehle in diesem Dokument zur Durchführung von Switch-Aktualisierungen auch verwendet werden, um Switches in ihren ursprünglichen Status zurückzusetzen.

1. Wenn die Aktualisierung eines Switches fehlschlägt, fahren Sie nicht mit einem anderen Switch fort. Wenn XClarity Administrator einen Fehler beim Versuch meldet, die Image-Dateien auf den Switch zu übertragen, finden Sie unter [Anhang B „ThinkAgile SXM Serie Switches mit der CLI aktualisieren \(nur Lenovo Switches\)“ auf Seite 95](#) Anweisungen zur Verwendung der Switch-CLI-Methode zum Aktualisieren der Switch-Firmware.
2. Die ursprüngliche Switch-Firmware ist im „Standby“-Image-Slot für alle Switches in der ThinkAgile SXM Serie Lösung verfügbar. Der RackSwitch G8052 BMC-Switch stellt eine Ausnahme dar. Für diesen Switch steht die ursprüngliche Switch-Firmware im nicht aktiven Image-Slot zur Verfügung, der „image1“ oder „image2“ sein kann. Wenn eine Switch-Aktualisierung fehlschlägt, kann der Switch mit der folgenden Befehlssyntax zur ursprünglichen Firmware zurückgesetzt werden:

Alle Switches außer G8052: `boot image <standby | active`

RackSwitch G8052 BMC-Switch: `boot image <image1 | image2`

**Wichtig:** Auf den TOR-Switches dürfen keine verschiedenen Firmwareversionen ausgeführt werden. Einzige Ausnahme ist der Zeitraum, in dem TOR1 aktualisiert wird und die Aktualisierung von TOR2 ansteht. Falls TOR1 nicht korrekt aktualisiert wird, dürfen Sie TOR2 nicht aktualisieren. Wenn außerdem die Aktualisierung von TOR2 fehlschlägt, muss die vorherige Firmware von TOR1 wiederhergestellt werden, bis das Problem behoben werden kann.

- Die Konfigurationsdatei von jedem Switch wird gesichert, bevor die Switches aktualisiert werden. Diese Dateien werden auch unter D:\Lenovo\SwitchConfigBackups auf dem HLH gespeichert. Jeder Switch kann auf eine gesicherte Konfiguration zurückgesetzt werden, um den Switch mit einer vorherigen Konfiguration wiederherzustellen.

## Aktualisierte CNOS-Befehlssyntax

Mit der Veröffentlichung der Lenovo Switch-Firmware CNOS v10.7.1.0 wurden verschiedene CLI-Befehlsschlüsselwörter aus Gründen der Konsistenz geändert.

Die linke Tabellenspalte zeigt das Schlüsselwort aus CNOS Version 10.6.x und früher. Die rechte Spalte zeigt das aktualisierte Schlüsselwort aus CNOS Version 10.7.x und später.

Altes CLI-Schlüsselwort	Neues CLI-Schlüsselwort
configure device	configure terminal
routing-protocol	router
bridge-port	switchport
port-aggregation	port-channel
aggregation-group	channel-group
cancel	abort
startup	boot
remove	clear
cp	copy
apply	set
display	show
save	write
dbg	debug

Ab CNOS v10.7.1.0 bot das NOS nur neue Formate an (Endbenutzerdokumentation, Hilfszeichenfolgen usw.). In einem begrenzten Zeitraum akzeptiert und verarbeitet das NOS jedoch alte und neue Formate. Daher enthalten die neuen NOS-Images Nachrichten, dass das alte Format in zukünftigen Versionen nicht mehr unterstützt wird.

Beachten Sie aber, dass obwohl CNOS v10.7.1.0 und höher zwar alte CLI-Befehle akzeptiert und verarbeitet, die Informationsanzeige nur die neue Syntax anzeigt. Beispielsweise werden beim laufenden Switch oder Startkonfigurationen alle „routing-protocol“-Einstellungen jetzt im Abschnitt „router“ angezeigt.

Die Informationen in einer gespeicherten Konfigurationsdatei sind nicht betroffen und bleiben mit den alten Befehlen intakt. Zum Speichern der Befehle in einer Datei im neuen Format müssen Sie nach dem erneuten Laden des Switches auf ein v10.7.1.0 oder höheres Image explizit `save/write` für jeden TOR-Switch ausführen.

Kopieren Sie die neu gespeicherte Konfiguration von allen Switches zum HLH, um später darauf zugreifen zu können. Wenn XClarity Administrator v2.1 oder höher installiert und für die Verwaltung der Switches konfiguriert ist, können Sie außerdem alle Switch-Konfigurationen mithilfe von XClarity Administrator sichern.

---

## Kapitel 4. Hinweise zum Warten und Austauschen von Komponenten

Die Komponenten der ThinkAgile SXM Serie wurden genau konfiguriert, um die erforderliche Funktionalität für die Lösungsebene bereitzustellen. Bevor Sie versuchen, Hardware- und Softwarekomponenten zu warten, auszutauschen oder erneut zu installieren, sollten Sie sich das relevante Thema durchlesen, um sicherzustellen, dass Sie die speziellen Verfahren oder Anforderungen kennen.

---

### Server austauschen

ThinkAgile SXM Serie Lösungen erfordern eine spezifische Konfiguration des HLH und der Knoten der Skalierungseinheit. Verwenden Sie die folgenden Tipps, um den erfolgreichen Austausch des Servers sicherzustellen.

#### HLH-System austauschen

Gehen Sie beim Austausch des HLH-Systems wie folgt vor:

1. Wenn Sie immer noch Zugriff auf Lenovo XClarity Administrator haben, heben Sie die Verwaltung aller Azure Stack Hub-Skalierungseinheit Knoten und Netzwerk-Switches auf.
2. Falls Sie immer noch auf das HLH-BS zugreifen können, kopieren Sie den Ordner D:\lenovo zur Wiederherstellung auf einen USB-Stick.
3. Stellen Sie nach dem Austausch der HLH-Hardware sicher, dass die Firmwareversion und die UEFI-Einstellungen gemäß der optimalen Vorgehensweise von ThinkAgile SXM konfiguriert werden. Weitere Informationen finden Sie unter „[Firmwarewartung und optimale Vorgehensweise](#)“ auf Seite 5.
4. Übernehmen Sie alle Sicherheitseinstellung der Plattform.
5. Konfigurieren Sie die IMM- oder XCC-IPv4-Adresse gemäß dem Arbeitsblatt, das während der ersten Implementierung erstellt wurde.
6. Konfigurieren Sie erneut das Konto auf Supervisor-Ebene.
7. Entfernen Sie den standardmäßigen USERID-Account aus dem IMM oder XCC.
8. Falls verfügbar, kopieren Sie die Dateien vom Sicherungs-USB-Stick (aus [2 auf Seite 55](#) oben) nach D:\Lenovo auf dem Ersatz-HLH-System.
9. Installieren Sie Lenovo XClarity Administrator erneut. (Siehe [Anhang A „XClarity Administrator implementieren und konfigurieren“](#) auf Seite 59.)

#### Knoten der Azure Stack Hub-Skalierungseinheit austauschen

Gehen Sie beim Austausch des Knotens einer Azure Stack Hub-Skalierungseinheit wie folgt vor:

1. Wenn das System noch reagiert, verwenden Sie das Azure Stack Hub-Administratorportal, um den zu ersetzenden Knoten der Skalierungseinheit zu leeren.
2. Heben Sie die Verwaltung des Knotens in LXCA auf.
3. Tauschen Sie die Skalierungseinheit-Knotenhardware aus.
4. Schließen Sie die Netzwerk- und Netzkabel wieder an.
5. Konfigurieren Sie die IMM/XCC-IPv4-Adresse gemäß dem Arbeitsblatt, das während der ersten Implementierung erstellt wurde.
6. Konfigurieren Sie den Account Supervisor-Ebene auf dem IMM/XCC neu, das von LXCA verwaltet werden soll, und verwenden Sie dabei dieselben Anmeldeinformationen, die derzeit für die anderen Knoten verwendet werden.
7. Entfernen Sie den standardmäßigen USERID-Account aus dem IMM/XCC.

8. Stellen Sie sicher, dass die Firmwareversionen auf dem Ersatzknoten gemäß der optimalen Vorgehensweise von ThinkAgile SXM konfiguriert sind, die derzeit für die Lösung verwendet wird.

Weitere Informationen finden Sie unter „[Firmwarewartung und optimale Vorgehensweise](#)“ auf Seite 5.

9. Verwenden Sie Lenovo XClarity Administrator, um die Microsoft Azure Stack Hub UEFI-Mustereinstellungen zu übernehmen. Weitere Informationen finden Sie unter „[Servermuster importieren und übernehmen](#)“ auf Seite 91.
10. Konfigurieren Sie das Bootdatenträger als RAID-1-Mirror.

---

## Serverteile austauschen

ThinkAgile SXM Serie Lösungen erfordern eine bestimmte Serverkonfiguration. Verwenden Sie die folgenden Tipps, um den erfolgreichen Austausch von Teilen sicherzustellen.

### Anforderung für produktspezifisches Server-Motherboard

Um die funktionalen Anforderungen zu erfüllen, benötigen die ThinkAgile SXM Serie Lösungen ein bestimmtes Motherboard als FRU-Komponente für die Knoten der Skalierungseinheit und das HLH-System. Stellen Sie vor der Wartung von Knoten der Skalierungseinheit sicher, dass Ihr Supporttechniker über Folgendes informiert ist:

- Verwenden Sie keine allgemeinen Ersatzteile für Server-Motherboards.
- Prüfen Sie immer die ThinkAgile SXM Serie-Support-Informationen im Internet auf die korrekte FRU-Teilenummer für das Motherboard.

### Server-Hot-Swap-Lüfter

Die ThinkAgile SXM Serie-Racks besitzen keine Kabelträger. Um einen Hot-Swap-Lüfter auf dem HLH oder Knoten der Skalierungseinheit auszutauschen, muss der Server ausgeschaltet und aus dem Rack herausgezogen sein. Stellen Sie immer sicher, dass Sie einen Knoten der Skalierungseinheit mithilfe des Azure Stack Hub-Administratorportals leeren, bevor Sie ihn aus irgendeinem Grund ausschalten.

### RAID-Adapter für Bootdatenträger

Der RAID-Adapter unterstützt nur den BS-Bootdatenträger und nicht die Speichergeräte, aus denen der Lösungsspeicherpool besteht.

1. Verwenden Sie Lenovo XClarity Administrator, um die Adapterfirmware auf dieselbe Version der optimalen Vorgehensweise zu aktualisieren, die derzeit für die Lösung verwendet wird. (Siehe „[Firmwarewartung und optimale Vorgehensweise](#)“ auf Seite 5.)
2. Stellen Sie die RAID-Konfiguration wieder auf den Laufwerken her.

### Mellanox-Netzwerkadapter

1. Schließen Sie die Kabel wieder gemäß den Punkt-zu-Punkt-Diagrammen und Tabellen im entsprechenden Abschnitt an:
  - SXM4400/SXM6400 Lösungen siehe [https://pubs.lenovo.com/thinkagile-sxm/sxm\\_r2\\_network\\_cabling](https://pubs.lenovo.com/thinkagile-sxm/sxm_r2_network_cabling)
  - SXM4600 Lösungen siehe [https://pubs.lenovo.com/thinkagile-sxm/sxm\\_r3\\_network\\_cabling](https://pubs.lenovo.com/thinkagile-sxm/sxm_r3_network_cabling)
2. Verwenden Sie Lenovo XClarity Administrator, um die Adapterfirmware auf dieselbe Version der optimalen Vorgehensweise zu aktualisieren, die derzeit für die Lösung verwendet wird. (Siehe „[Firmwarewartung und optimale Vorgehensweise](#)“ auf Seite 5.)



**Speicher**

Nach dem Austausch ist keine lösungsspezifische Konfiguration erforderlich.

**CPU**

Nach dem Austausch ist keine lösungsspezifische Konfiguration erforderlich.



---

## Anhang A. XClarity Administrator implementieren und konfigurieren

Normalerweise ist es nicht erforderlich, XClarity Administrator (LXCA) für die Verwendung mit ThinkAgile SXM Serie Lösungen von Grund auf neu zu installieren und zu konfigurieren. Trotzdem enthält dieses Dokument Anweisungen dazu, falls dies aus irgendeinem Grund erforderlich sein sollte. Dieses Dokument enthält zudem Anweisungen zum Aktualisieren von LXCA auf die Version in der aktuellen optimalen Vorgehensweise der ThinkAgile SXM Serie.

---

### Aktuelle LXCA-Installation stilllegen

Wenn LXCA v2.x oder höher auf dem HLH implementiert ist, ist es normalerweise nicht erforderlich, LXCA stillzulegen. Aktualisieren Sie in diesem Fall einfach LXCA auf die Version in der aktuellen optimalen Vorgehensweise. Wenn jedoch LXCA v1.x auf dem HLH implementiert ist, gehen Sie wie hier gezeigt vor, um die vorhandene Installation von LXCA stillzulegen. Fahren Sie dann anhand der folgenden Abschnitte damit fort, LXCA von Grund auf neu zu implementieren.

Wenn LXCA v1.x auf dem HLH implementiert ist, gehen Sie wie folgt vor, um die vorhandene Installation von LXCA stillzulegen.

- Schritt 1. Verwenden Sie auf dem HLH den Internet Explorer, um sich bei LXCA anzumelden.
- Schritt 2. Navigieren Sie in der LXCA-Menüleiste oben auf dem Bildschirm zu **Verwaltung** → **Netzwerkzugriff**.
- Schritt 3. Notieren Sie zur späteren Konfiguration einer neuen LXCA-Implementierung die IPv4-Einstellungen der aktuellen LXCA-Umgebung anhand der Parameter, die in der folgenden Abbildung hervorgehoben sind. Wenn Sie aus irgendeinem Grund nicht auf LXCA zugreifen können, finden Sie diese Parameter im Dokument „Customer Deployment Summary“ (Implementierungszusammenfassung für Kunde), das Kunden nach der Erstimplementierung der Lösung erhalten.

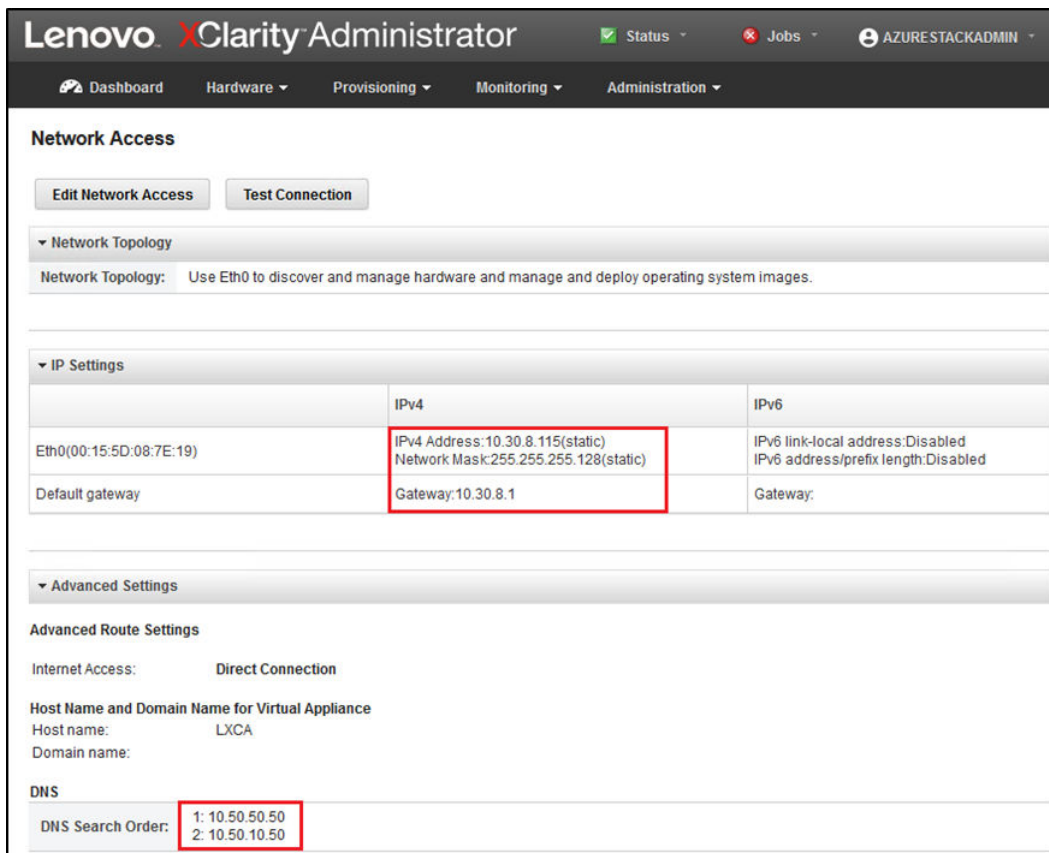



Abbildung 49. LXCA-IPv4-Einstellungen, die notiert werden müssen

Notieren Sie die Einstellungen in der folgenden Tabelle:

	Lenovo LXCA-IPv4-Einstellungen
IPv4-Adresse	
Netzwerkmaske	
Gateway	
DNS-Server 1	
DNS-Server 2 (optional)	

Schritt 4. Navigieren Sie in der LXCA-Menüleiste oben auf dem Bildschirm zu **Bereitstellung** → **Serverprofile**.

Schritt 5. Wählen Sie alle angezeigten Serverprofile aus und klicken Sie auf das Symbol **Serverprofile deaktivieren** ()

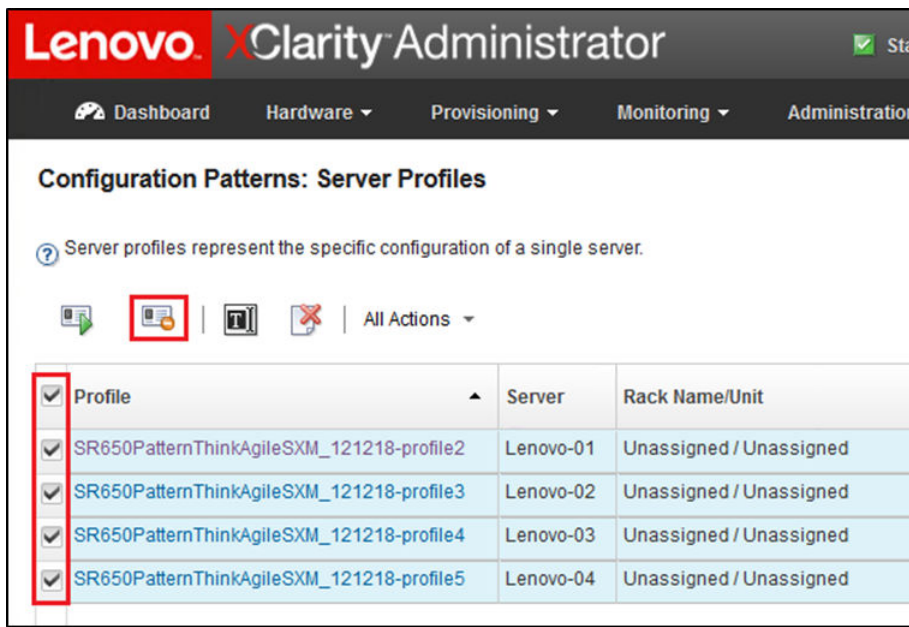


Abbildung 50. Auswählen der zu deaktivierenden LXCA-Serverprofile

Schritt 6. Heben Sie im angezeigten Fenster die Auswahl der Option „BMC-Identitätseinstellungen aufheben“ auf, falls sie vorher aktiviert war, und klicken Sie auf **Deaktivieren**.

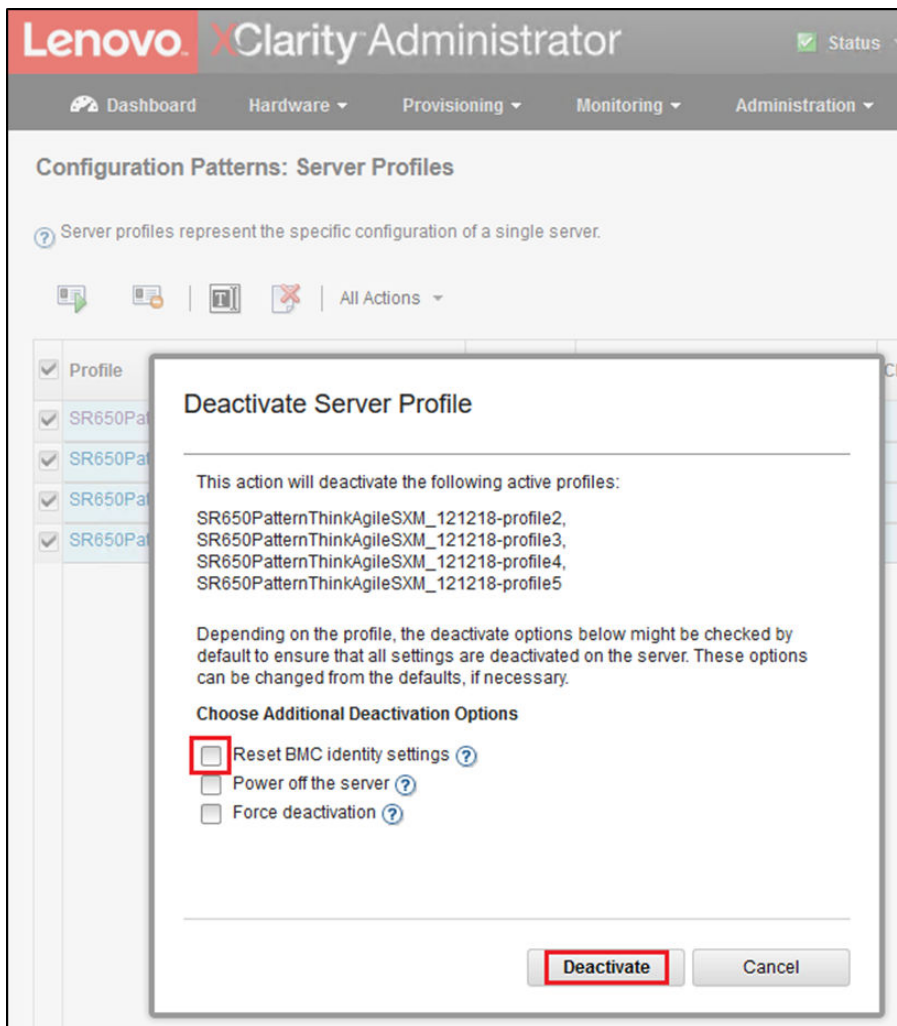


Abbildung 51. Zurücksetzen der BMC-Identitätseinstellungen

Schritt 7. Navigieren Sie in der LXCA-Menüleiste oben auf dem Bildschirm zu **Hardware** → **Server**.

Schritt 8. Wählen Sie alle Knoten aus und klicken Sie auf **Verwaltung aufheben**.

The screenshot shows the Lenovo XClarity Administrator interface. At the top, there is a navigation bar with 'Dashboard', 'Hardware', 'Provisioning', 'Monitoring', and 'Administration'. Below this, the 'Servers' section is active. A toolbar contains various icons for server management, including a red 'Unmanage' button which is highlighted with a red box. To the right of the toolbar, there are filter options and a 'Filter' input field. Below the toolbar is a table with the following columns: Server, Status, Power, IP Addresses, Product Name, Type-Model, and Firmware (UEFI/BIOS). The table contains four rows of server data, all of which are selected with checkmarks in the first column.

Server	Status	Power	IP Addresses	Product Name	Type-Model	Firmware (UEFI/BIOS)
Lenovo-01	Normal	On	10.30.8.3, 1...	ThinkSystem SR650	7X06-CTO1WW	IVE126O / 1.41 (Oct 29, 2018, 5:00:00 PM)
Lenovo-02	Normal	On	10.30.8.4, 1...	ThinkSystem SR650	7X06-CTO1WW	IVE126O / 1.41 (Oct 29, 2018, 5:00:00 PM)
Lenovo-03	Normal	On	10.30.8.5, 1...	ThinkSystem SR650	7X06-CTO1WW	IVE126O / 1.41 (Oct 29, 2018, 5:00:00 PM)
Lenovo-04	Normal	On	10.30.8.6, 1...	ThinkSystem SR650	7X06-CTO1WW	IVE126O / 1.41 (Oct 29, 2018, 5:00:00 PM)

Abbildung 52. Aufheben der Knotenverwaltung

Schritt 9. Aktivieren Sie im neu geöffneten Fenster die Option **Verwaltungsaufhebung erzwingen, selbst wenn das Gerät nicht erreichbar ist** und klicken Sie auf **Verwaltung aufheben**.

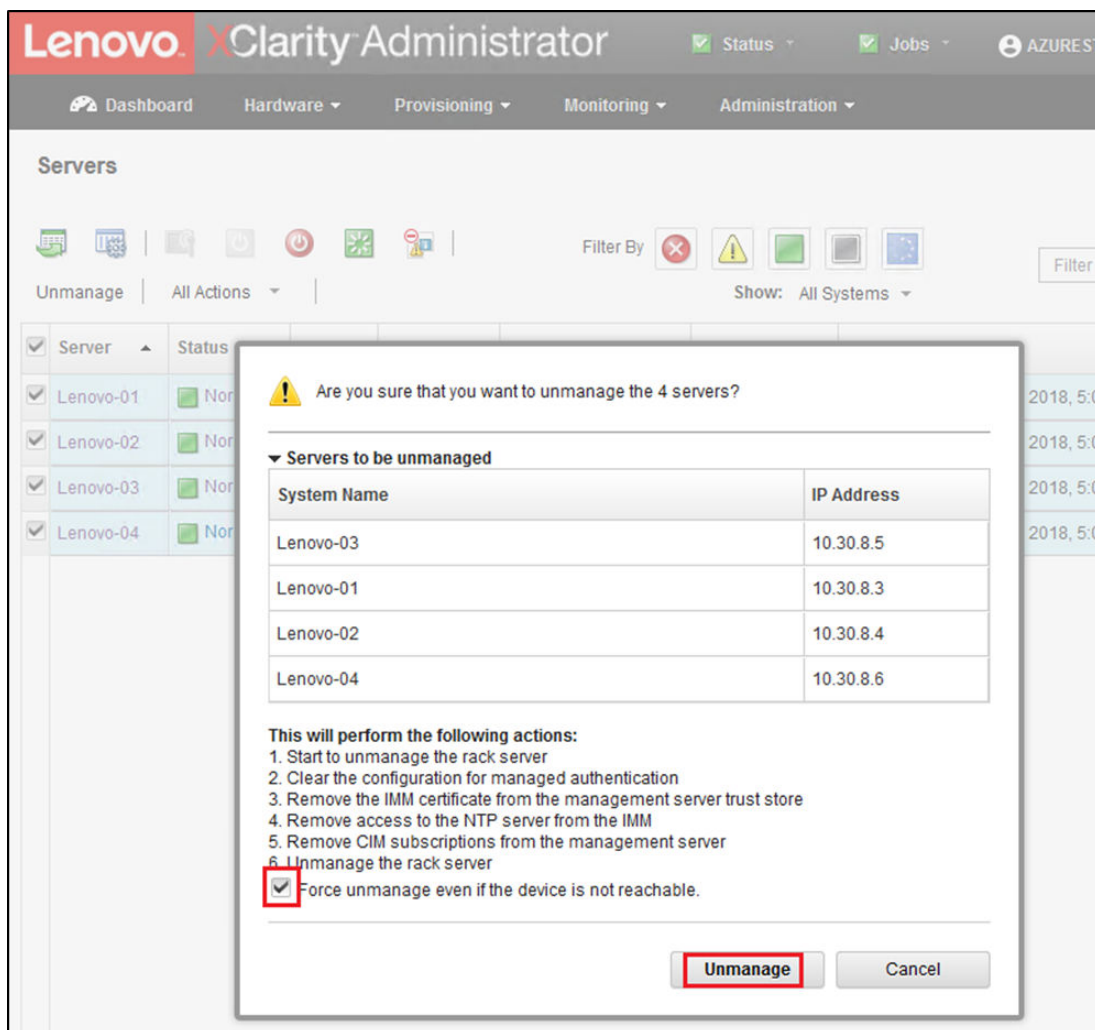


Abbildung 53. Auswahl der erzwungenen Verwaltungsaufhebung von Knoten

Schritt 10. Navigieren Sie in der LXCA-Menüleiste oben auf dem Bildschirm zu **Hardware → Switches**.

Schritt 11. Wenn Switches angezeigt werden, wählen Sie alle Switches aus und klicken Sie auf **Verwaltung aufheben**.

Schritt 12. Aktivieren Sie im neu geöffneten Fenster die Option **Verwaltungsaufhebung erzwingen, selbst wenn das Gerät nicht erreichbar ist** und klicken Sie auf **Verwaltung aufheben**.

Schritt 13. Nachdem die Verwaltung von allen verwalteten Servern und Switches aufgehoben wurde, fahren Sie den LXCA-Server herunter, indem Sie in der Menüleiste zu **Verwaltung → Verwaltungsserver herunterfahren** navigieren.

Schritt 14. Stellen Sie im neu geöffneten Fenster sicher, dass keine Jobs aktiv sind, und klicken Sie auf **Herunterfahren**.

Schritt 15. Klicken Sie im Bestätigungsfenster auf **OK**.

Schritt 16. Öffnen Sie auf dem HLH den Hyper-V Manager und warten Sie darauf, dass die virtuelle LXCA-Maschine den Status „Aus“ anzeigt.

Sobald die virtuelle LXCA-Maschine ausgeschaltet ist, können Sie mit der Implementierung und Konfiguration einer neuen Version von LXCA auf dem HLH beginnen.



## LXCA implementieren und konfigurieren

Zur Vorbereitung einer neuen Implementierung von LXCA müssen die entsprechenden Dateien von [ThinkAgile SXM Serie Aktualisierungs-Repository](#) heruntergeladen werden. Dazu gehören die Archivdatei „LXCA\_SXMBR<xyy>.zip“ und die vollständige LXCA-VHD-Image-Datei, die einen Dateinamen im Format „Invgv\_sw\_lxca\_<version>\_winsrvr\_x86-64.vhd“ hat und sich im aktuellen Verzeichnis für optimale Vorgehensweisen auf der Website befindet.



### Lenovo ThinkAgile SXM Series Updates Repository

September 2023 ThinkAgile SXM Series update release (SXMBR2309)

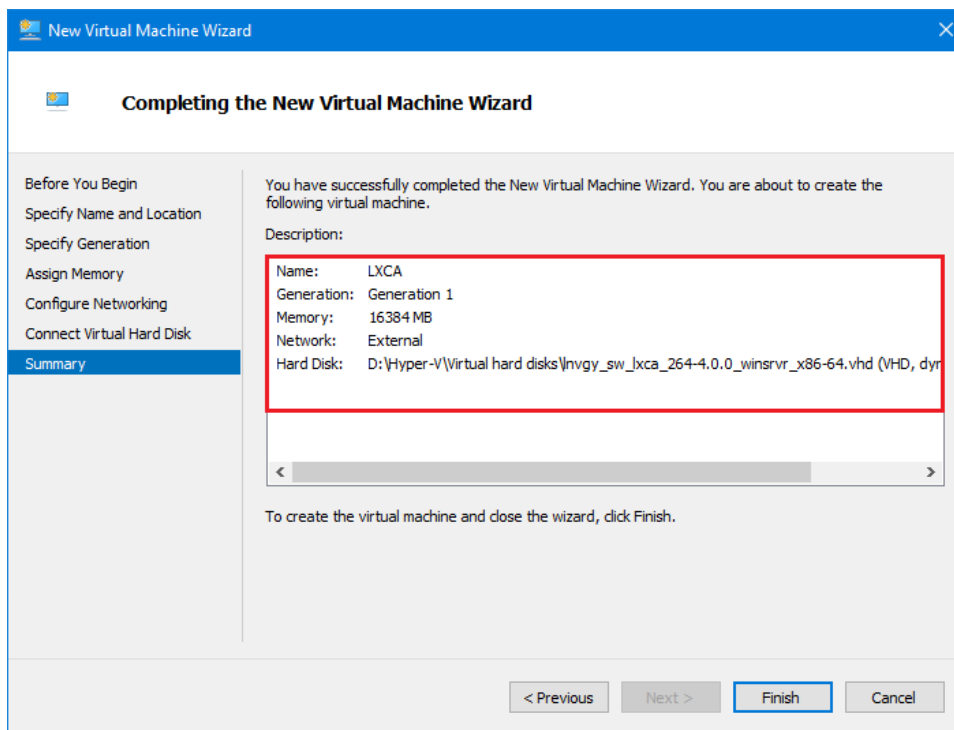
**Important:** The OEM Extension Packages in this Best Recipe include functionality to perform an attempt to update to this OEM Extension Package until LXCA has been prepared to perform system Administrator for a specific Best Recipe topic in the [ThinkAgile SXM Series Information Center](#) for

File Name	Date Modified
Parent Directory	
<a href="#">HelperScripts.zip</a>	09/29/2023
<a href="#">Invgv_sw_lxca_264-4.0.0_winsrvr_x86-64.vhd</a>	09/29/2023
<a href="#">LXCA_SXMBR2309.zip</a>	
SHA256 Hash: fc833a189538e3b930270d3fa70a794bc77ac4b7d0ee7eb6c581df892a2bdae7 MD5 Hash: 114f1376d28d3242f2141d89d2dc9bda	09/29/2023
<a href="#">OEMv2.2_SXMBR2309-EGS.zip</a>	
SHA256 Hash:	

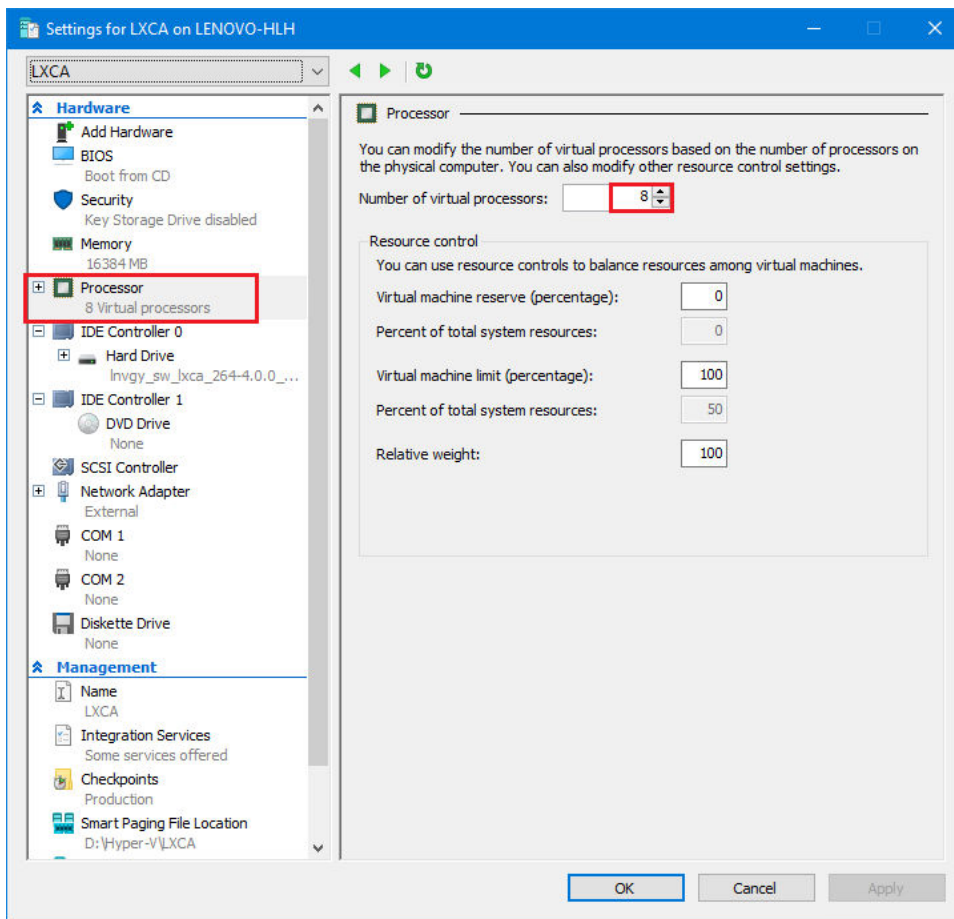
Gehen Sie wie folgt vor, nachdem alle Dateien aus dem ThinkAgile SXM Serie Aktualisierungs-Repository heruntergeladen und auf einen USB-Stick kopiert wurden:

- Schritt 1. Entpacken Sie die Archivdatei „LXCA\_SXMBR<xyy>.zip“ auf dem USB-Stick.
- Schritt 2. Kopieren Sie die VHD-Datei und den entpackten Archivinhalt (nicht das Verzeichnis selbst) des Archivs auf D:\LXCA auf dem Hardware Lifecycle Host (HLH). Ersetzen Sie alle Dateien oder Verzeichnisse mit demselben Namen, die sich bereits im Verzeichnis befinden.
- Schritt 3. Kopieren Sie die LXCA-VHD-Datei von **D:\Lenovo\LXCA** zu **D:\Hyper-V\Virtual hard disks** auf dem HLH. Falls erforderlich, müssen Sie die angegebenen Verzeichnisse erstellen. Achten Sie darauf, die Datei zu kopieren und nicht zu verschieben, damit das Original als Sicherung verwendet werden kann, falls Sie LXCA später wieder installieren müssen.
- Schritt 4. Öffnen Sie Hyper-V Manager und wählen Sie im linken Navigationsbereich **Lenovo-HLH** aus.
- Schritt 5. Navigieren Sie im Bereich Aktionen auf der rechten Seite zu **Neu → Virtuelle Maschine ...**
- Schritt 6. Klicken Sie auf der Seite „Vorbereitende Schritte“ auf **Weiter**.

- Schritt 7. Geben Sie auf der Seite „Name und Standort angeben“ einen Namen für die VM ein, z. B. „LXCA“, aktivieren Sie das Kontrollkästchen „Virtuelle Maschine an einem anderen Ort speichern“, geben Sie „D:\Hyper-V“ als Standort ein und klicken Sie dann auf **Weiter**.
- Schritt 8. Lassen Sie auf der Seite „Generation angeben“ die Option „Generation 1“ ausgewählt und klicken Sie auf **Weiter**.
- Schritt 9. Geben Sie auf der Seite „Hauptspeicher zuweisen“ „16384“ als Startspeicher ein und klicken Sie dann auf **Weiter**.
- Schritt 10. Wählen Sie auf der Seite „Netzwerk konfigurieren“ in der Dropdown-Liste „Verbindung“ die Option „Extern“ aus und klicken Sie dann auf **Weiter**.
- Schritt 11. Klicken Sie auf der Seite „Virtuelle Festplatte verbinden“ auf die Option „Vorhandene virtuelle Festplatte verwenden“, klicken Sie auf **Durchsuchen ...** und navigieren Sie dann zur LXCA-VHD-Datei unter **D:\Hyper-V\Virtual hard disks** auf dem HLH. Klicken Sie nach dem Auswählen der VHD-Datei auf „Weiter“.
- Schritt 12. Überprüfen Sie auf der Seite „Zusammenfassung“, dass alle Parameter ordnungsgemäß angezeigt werden, bevor Sie auf **Fertig stellen** klicken, um die virtuelle Maschine zu erstellen.




- Schritt 13. Sobald die VM erstellt wurde, wird sie bei Hyper-V Manager im Bereich „Virtuelle Maschinen“ angezeigt. Wählen Sie die VM aus und klicken Sie dann im rechten Bereich auf **Einstellungen ....**
- Schritt 14. Wählen Sie auf der neu geöffneten Seite im linken Bereich „Prozessor“ aus, erhöhen Sie die Anzahl der virtuellen Prozessoren auf 8 und klicken Sie dann auf „OK“.



## Statische IP-Adresse für LXCA konfigurieren

Gehen Sie wie folgt vor, um die statische IP-Adresse von LXCA für Ihre ThinkAgile SXM Serie Lösung zu konfigurieren.

- Schritt 1. Wählen Sie im Hyper-V Manager die virtuelle LXCA-Maschine im mittleren Bereich aus und klicken Sie dann rechts auf **Verbinden ....**
- Schritt 2. Klicken Sie im Fenster „Verbindung der virtuellen Maschine“ auf die Schaltfläche **Starten** () , um die virtuelle LXCA-Maschine zu starten.
- Schritt 3. Überwachen Sie den Boot-Vorgang, bis die folgenden Informationen angezeigt werden. Geben Sie dann „1“ ein und drücken Sie die Eingabetaste.

```
-----  
Lenovo LXCA - Version 4.0.0 build 264  
-----  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 metric 1  
      inet6 fe80::215:5dff:fe2a:b416 prefixlen 64 scopeid 0x20<link>  
      ether 00:15:5d:2a:b4:16 txqueuelen 1000 (Ethernet)  
      RX errors 0 dropped 0 overruns 0 frame 0  
  
eth1:      Disabled  
  
=====
```

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

Abbildung 54. Fenster „Verbindung der virtuellen Maschine“

Schritt 4. Geben Sie die erforderlichen Parameter (siehe gelbe Felder der folgenden Abbildung). Beziehen Sie sich auf die Tabelle, die Sie in „Aktuelle LXCA-Installation stilllegen“ auf Seite 59 ausgefüllt haben.

```

=====
=====
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

... .. [ 50.079250] hu_balloon: Received INFO_TYPE_MAX_PAGE_CNT
[ 50.083244] hu_balloon: Data Size is 8
1

ATTENTION: ***
Perform this action only when the Lenovo XClarity Administrator virtual
appliance is initially deployed. If you change the virtual appliance IP
address after managing devices, Lenovo XClarity Administrator will not be
able to connect to those managed devices and the devices will appear to
be offline.

For more information, see 'Configuring network settings' in the Lenovo
XClarity Administrator online documentation.

Gather all required IP information before proceeding. You have 60 secs
to enter the information for each prompt.
- For ipv4 protocol: IP address, subnetmask and gateway IP address
- For ipv6 protocol: IP address and prefix length.

Do you want to continue? (enter y or Y for Yes, n for No) Y

Enter the appropriate static IP settings for the XClarity virtual
appliance eth0 port when prompted and then press Enter, OR just press
Enter to proceed to next prompt without providing any input to the
current prompt.

IP protocol(specify ipv4 or ipv6): ipv4
IP address: 10.30.8.115
netmask: 255.255.255.128
gateway: 10.30.8.1
DNS1 IP (optional): 10.50.50.50
DNS2 IP (optional): 10.50.10.50

Processing ... ..
IP protocol: ipv4
IP addr: 10.30.8.115
netmask: 255.255.255.128
gateway: 10.30.8.1
DNS1: 10.50.50.50
DNS2: 10.50.10.50
Do you want to continue? (enter y or Y for Yes, n for No) Y

Status: Running

```

Abbildung 55. Parameter der virtuellen Maschine

Schritt 5. Stellen Sie sicher, dass alle Parameter ordnungsgemäß eingegeben wurden, geben Sie dann „Y“ ein und drücken Sie die Eingabetaste.

Schritt 6. Öffnen Sie den Internet Explorer und greifen Sie auf die Seite „LXCA-Ersteinrichtung“ zu: <https://<IPv4Address>/ui/login.html>

wo <IPv4Address> die IP-Adresse von LXCA ist, die gerade konfiguriert wurde.

Die Seite „Erstkonfiguration“ wird angezeigt. Wenn Sie zum ersten Mal auf LXCA zugreifen, müssen Sie bestimmte Schritte zur Erstkonfiguration ausführen.

Führen Sie für die Ersteinrichtung von LXCA jede der sieben auf der Seite „Ersteinrichtung“ gezeigten Aufgaben durch und schließen Sie sie gemäß den Anweisungen in den folgenden Abschnitten ab.

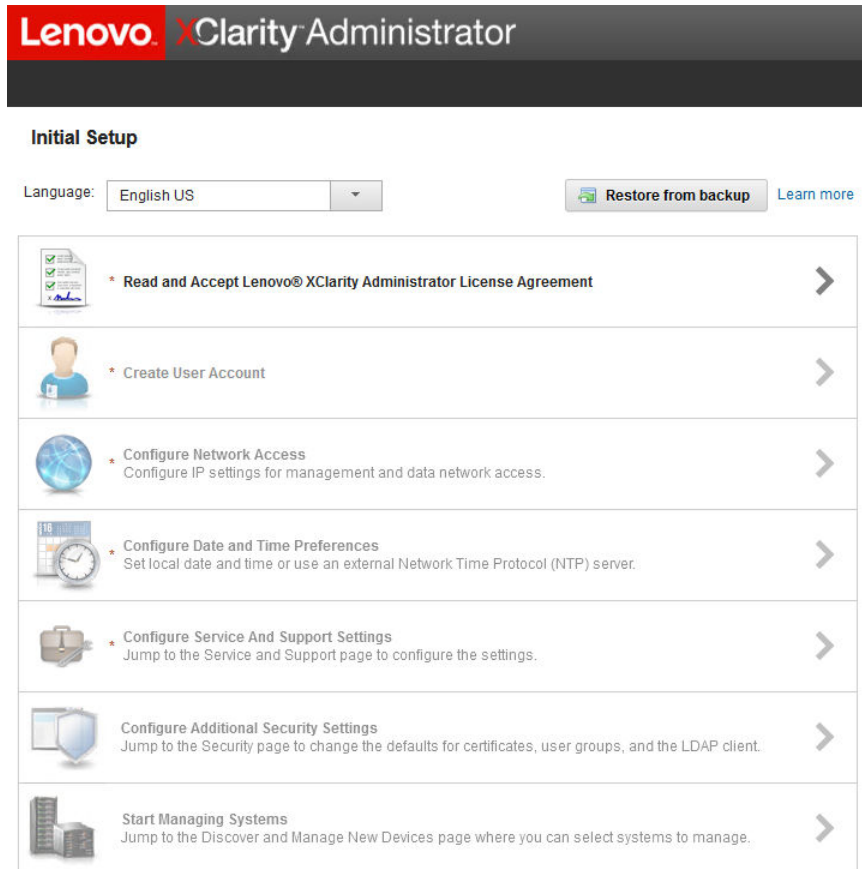


Abbildung 56. Seite „LXCA-Ersteinrichtung“

## Aufgabe „Lenovo XClarity Administrator-Lizenzvereinbarung lesen und akzeptieren“

Verfahren zum Ausführen der Lizenzvereinbarungs-Aufgabe im Rahmen der LXCA-Erstkonfiguration.

Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf **Lizenzvereinbarung für Lenovo® XClarity Administrator lesen und akzeptieren**. Die Lizenzvereinbarung wird angezeigt.



Abbildung 57. Fenster „Lenovo XClarity Administrator-Lizenzvereinbarung lesen und akzeptieren“

Schritt 2. Klicken Sie auf **Accept**. Die erste Startseite zeigt nun ein grünes Häkchen für diese Aufgabe.

Fahren Sie mit der Aufgabe „[Benutzeraccount erstellen](#)“ auf Seite 71 fort.

---

## Aufgabe „Benutzeraccount erstellen“

Verfahren zum Ausführen der Aufgabe „Benutzeraccount erstellen“ im Rahmen der Erstkonfiguration von LXCA.

Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf **Benutzerkonto erstellen**.

Das Fenster Neuen Supervisor-Benutzer erstellen wird angezeigt.

Create New Supervisor User

\* Username: AzureStackAdmin

Description: Supervisor account used to m:

\* New password: ●●●●●●●●

\* Confirm new password: ●●●●●●●●

Password and password confirm values must match

Create Cancel

Abbildung 58. Fenster „Neuen Supervisor-Benutzer erstellen“

Schritt 2. Erstellen Sie einen Supervisor-Account, um auf LXCA zuzugreifen und die physischen Knoten von Azure Stack Hub zu verwalten. Nehmen Sie die folgenden Parameter auf:

- **Benutzername:** AzureStackAdmin (oder Ihren bevorzugten Benutzernamen)
- **Beschreibung:** <Description of your choice> (optional)
- **Kenntwort:** <Password>

Schritt 3. Klicken Sie auf **Erstellen**. Die Seite Lokale Benutzerverwaltung wird mit dem neuen Benutzer angezeigt. Die aktuelle aktive Sitzung wird nun mit diesem Account ausgeführt (obere rechte Ecke des folgenden Screenshots).



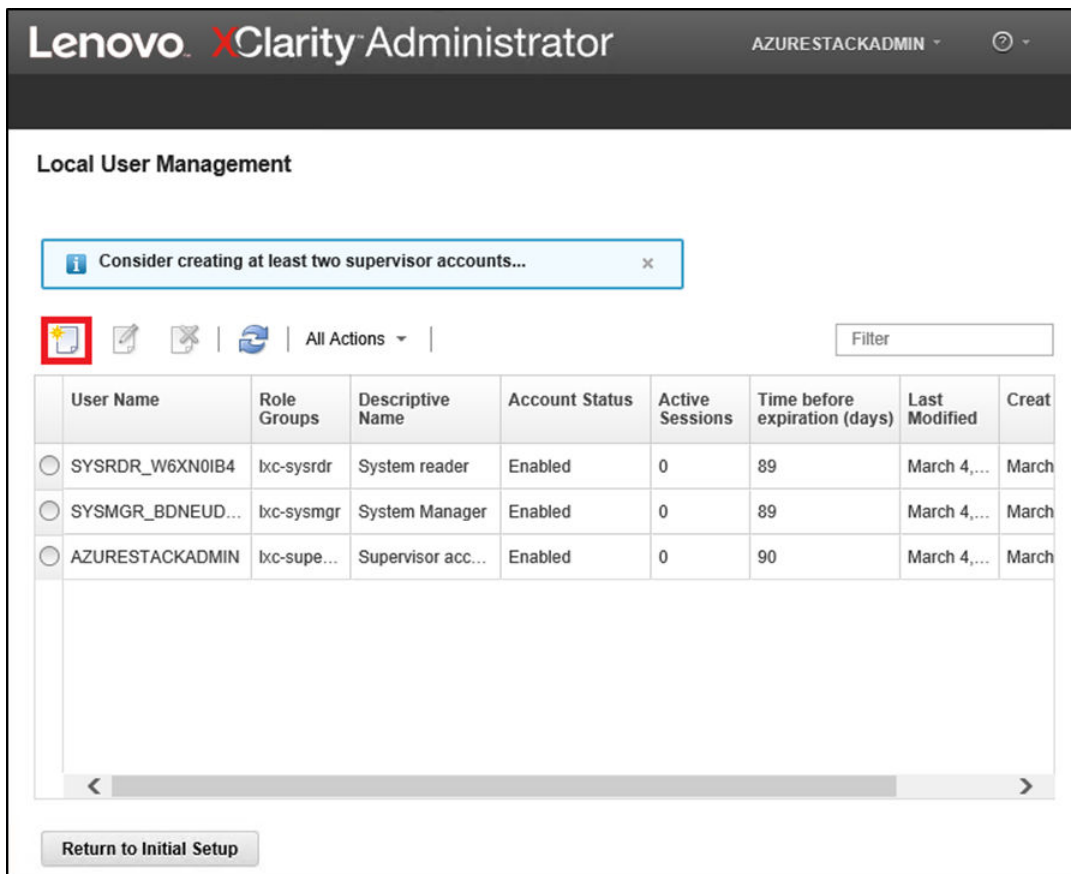


Abbildung 59. Fenster „Lokale Benutzerverwaltung“

Schritt 4. Es wird empfohlen, mindestens zwei Supervisor-Accounts zu erstellen. Falls das Kennwort für den gerade erstellten Account verloren oder vergessen wurde, kann der „failsafe“-Account zum Anmelden bei LXCA und Wiederherstellung des vergessenen Kennworts verwendet werden. Klicken Sie zum Erstellen eines zweiten Accounts auf das Symbol **Neuen Benutzer erstellen** (



), das im Screenshot oben rot umrandet ist.

Schritt 5. Wiederholen Sie Schritt 2, um einen zweiten Supervisor-Account zu erstellen. Nehmen Sie die folgenden Parameter auf:

- **Benutzername:** Backup (oder Ihren bevorzugten Benutzernamen)
- **Beschreibung:** <Description of your choice> (optional)
- **Kennwort:** <Password>

Schritt 6. Klicken Sie auf **Erstellen**. Die Seite Lokale Benutzerverwaltung wird mit dem zweiten neuen Benutzer angezeigt. Die zwei anderen aufgelisteten Accounts sind die internen Accounts, die von LXCA verwendet werden. Sie dürfen diese Accounts nicht bearbeiten oder entfernen.

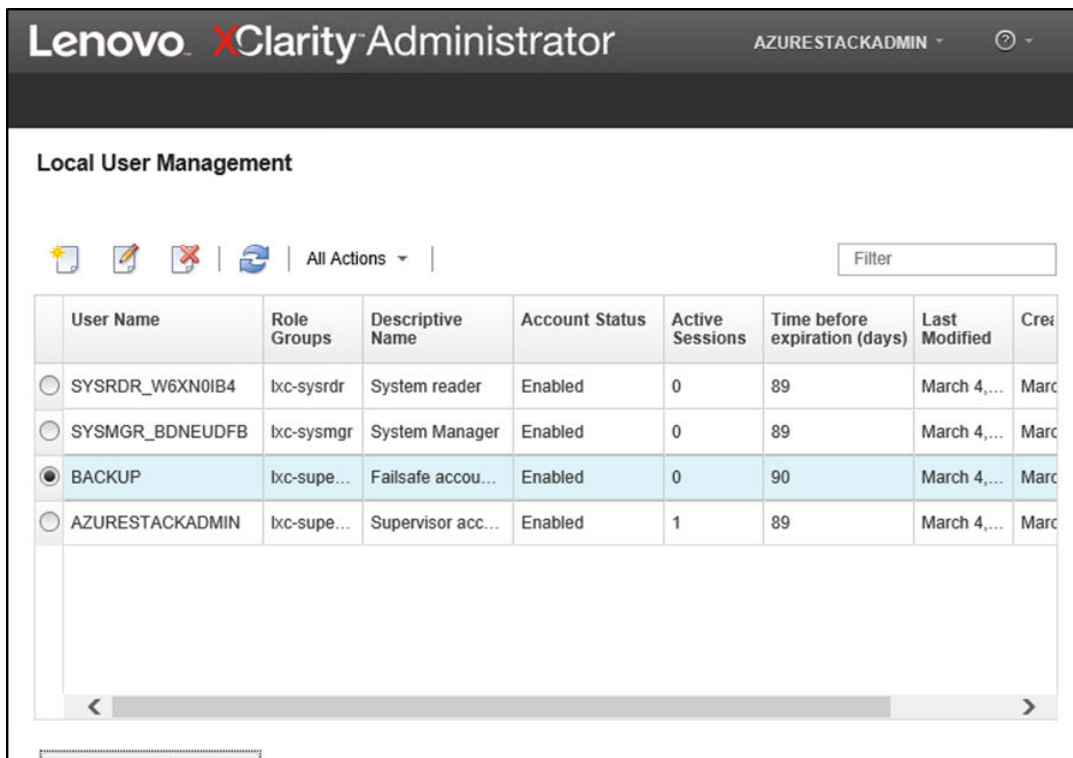


Abbildung 60. Fenster „Lokale Benutzerverwaltung“ mit Backup-Benutzer

Schritt 7. Notieren Sie alle LXCA-Anmeldeinformationen in der folgenden Tabelle, um Sie später zu Ihren Aufzeichnungen hinzuzufügen.

	Benutzername	Kennwort
Primärer Account		
Sekundärer Account		

Schritt 8. Klicken Sie im LXCA auf **Zu Erstkonfiguration zurückkehren**, um die Aufgabe „Benutzeraccount erstellen“ abzuschließen und zur Seite Erstkonfiguration zurückzukehren.

Fahren Sie mit „Aufgabe „Netzwerkzugriff konfigurieren““ auf Seite 74 fort.

## Aufgabe „Netzwerkzugriff konfigurieren“

Verfahren zum Konfigurieren des Netzwerkzugriffs als Teil der Erstkonfiguration von LXCA.

Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf **Netzwerkzugriff konfigurieren**.

Das Fenster Netzwerkzugriff bearbeiten wird angezeigt.

### Edit Network Access

IP Settings

Advanced Routing

DNS & Proxy

**IP Settings**

If you use DHCP and an external security certificate, make sure that the address leases for the management server on the DHCP server are permanent to avoid communication issues with managed resources when the management server IP address changes.

One network interface detected:

Eth0:  Enabled - used to discover and manage hardware only. ?

You will not be able to manage or deploy operating system images and update operating system drivers.

	IPv4	IPv6
	<span style="border: 1px solid #ccc; padding: 2px;">Use statically assigned IP address</span>	<span style="border: 1px solid #ccc; padding: 2px;">Use stateful address configuration (DHCPv6)</span>
<b>Eth0:</b>	* IP address: <span style="border: 1px solid #ccc; padding: 2px;">10.30.8.52</span> Network Mask: <span style="border: 1px solid #ccc; padding: 2px;">255.255.255.192</span>	IP address: <span style="border: 1px solid #ccc; padding: 2px;">0::0</span> Prefix Length: <span style="border: 1px solid #ccc; padding: 2px;">64</span>
<b>Default gateway:</b>	Gateway: <span style="border: 1px solid #ccc; padding: 2px;">10.30.8.1</span>	Gateway: <span style="border: 1px solid #ccc; padding: 2px;">DHCP</span>

Save IP Settings

Restart

Return to Initial Setup

Abbildung 61. Fenster „Netzwerkzugriff bearbeiten“

- Schritt 2. Überprüfen Sie auf der Seite Netzwerkzugriff bearbeiten in der Registerkarte IP-Einstellungen, dass die richtigen IPv4-Parameter bei den Feldern **IP-Adresse**, **Netzwerkmaske** und **Gateway** angezeigt werden.
- Schritt 3. Wechseln Sie zur Registerkarte DNS & Proxy und stellen Sie sicher, dass die DNS-Server korrekt eingegeben worden sind.
- Schritt 4. Geben Sie auf derselben Seite „LXCA“ im Feld **Hostname** ein, wie in der folgenden Abbildung dargestellt.

Edit Network Access

IP Settings   Advanced Routing   **DNS & Proxy**

**Names for this Virtual Appliance**

Host name:

Domain name:

**DNS Servers**

DNS Operating Mode:  ?

Order	DNS Server
<input type="text" value="1"/>	<input type="text" value="10.241.80.5"/>

**Proxy Setting**

Internet Access :  Direct Connection    HTTP Proxy

Abbildung 62. Einstellungen-Registerkarte „DNS & Proxy“

- Schritt 5. Klicken Sie auf **DNS & Proxy speichern** und anschließend im Bestätigungsfenster auf **Speichern**. Klicken Sie dann auf im Fenster Internet-/DNS-Einstellungen auf **Schließen**.
- Schritt 6. Kehren Sie zur Registerkarte IP-Einstellungen der Seite „Netzwerkzugriff bearbeiten“ zurück.
- Schritt 7. Wählen Sie unter der Spaltenüberschrift „IPv6“ **IPv6 deaktivieren** in der Dropdown-Liste aus. Klicken Sie auf **Schließen**, um das Popup-Fenster zu schließen, und klicken Sie dann auf **IP-Einstellungen speichern**.

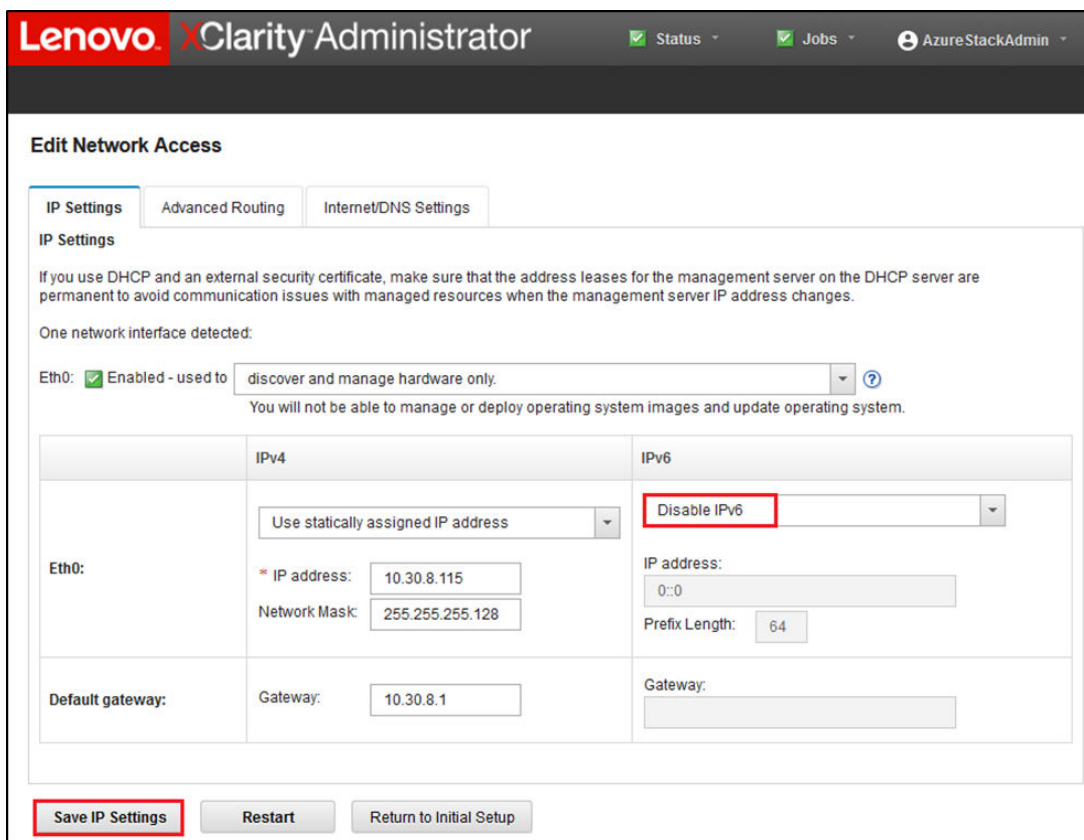


Abbildung 63. Deaktivieren der IPv6-Einstellungen

Schritt 8. Klicken Sie im Popup-Bestätigungsfenster auf **Speichern**.

Schritt 9. Im neu geöffneten Fenster werden Sie aufgefordert, den Verwaltungsserver zum Übernehmen dieser Änderungen neu zu starten. Klicken Sie auf **Neu starten** und klicken Sie dann im angezeigten Bestätigungsfenster auf **Schließen**.

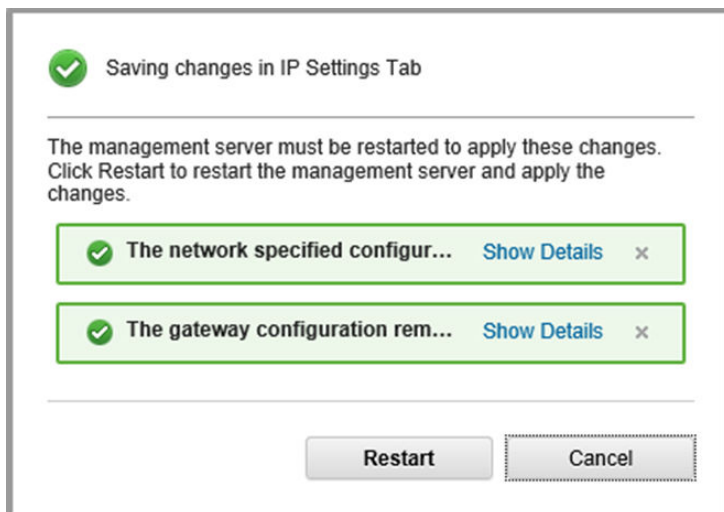


Abbildung 64. Speichern von Änderungen in der Registerkarte „IP-Einstellungen“

Schritt 10. Warten Sie auf den Neustart des Verwaltungsservers (ca. fünf Minuten). Während dieser Zeit wird ein Popup-Fenster mit der folgenden Nachricht angezeigt: „Die Verbindung mit dem Verwaltungsserver wurde unterbrochen. Es konnte keine Verbindung mit dem Server hergestellt werden.“ Diese Nachricht ist beim Neustart des Verwaltungsservers normal und kann ignoriert werden. Klicken Sie bei der Anzeige dieses Popup-Fensters auf **Schließen**. Für LXCA v4.0 und höher sollte nach dem Neustart des LXCA-Verwaltungsservers ein Anmeldebildschirm angezeigt werden.

Schritt 11. Falls erforderlich, aktualisieren Sie den Browser, um zur LXCA-Anmeldeseite zurückzukehren, und melden Sie sich dann mit dem zuvor erstellten primären Supervisor-Account an. Die Seite Erstkonfiguration wird angezeigt, wobei nun die ersten drei Aufgaben abgehakt sind.

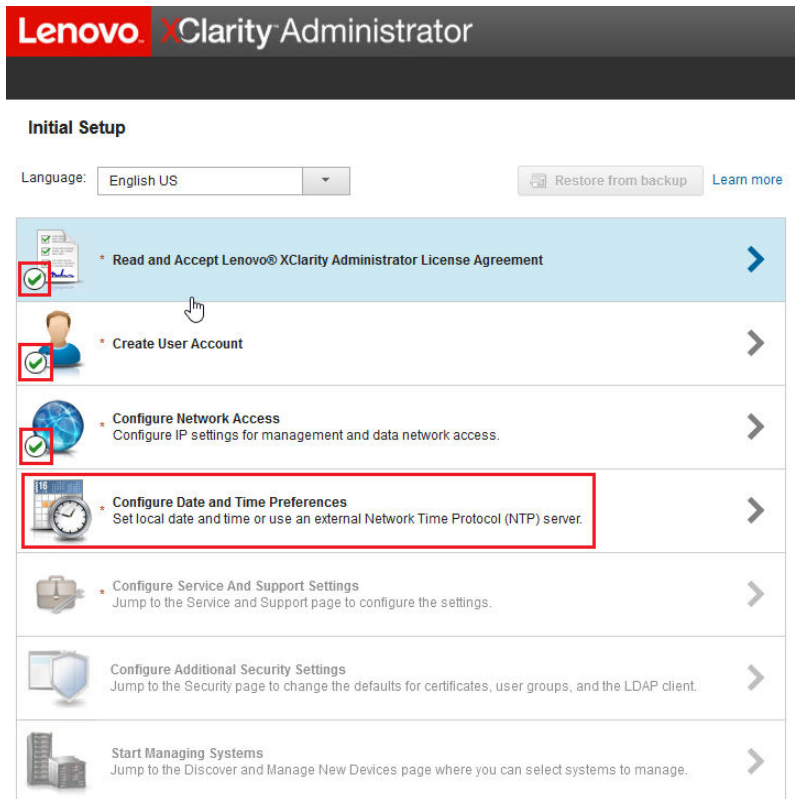


Abbildung 65. Seite „Erstkonfiguration“ mit abgehakten abgeschlossenen Aufgaben

Fahren Sie mit „Aufgabe „Einstellungen für Datum und Uhrzeit konfigurieren““ auf Seite 78 fort.

---

## Aufgabe „Einstellungen für Datum und Uhrzeit konfigurieren“

Verfahren zum Konfigurieren von Datums- und Uhrzeiteinstellungen im Rahmen der LXCA-Ersteinrichtung.

Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf **Einstellungen für Datum und Uhrzeit konfigurieren**.

Das Fenster Datum und Uhrzeit bearbeiten wird angezeigt.

### Edit Date and Time

Date and time will be automatically synchronized with the NTP server.

Time zone  ▾  
Daylight saving time is not observed in this time zone.

Edit clock settings (12 or 24 hours format):

NTP server host name or IP address:

NTP v3 Authentication:

Abbildung 66. Fenster „Datum und Uhrzeit bearbeiten“

Schritt 2. Geben Sie auf der Seite Datum und Uhrzeit bearbeiten die **Zeitzone** als „UTC -0:00, Coordinated Universal Time etc./UCT“ und **Hostname oder IP-Adresse des NTP-Servers** an, der bzw. die für Ihren Standort geeignet ist.

**Anmerkung:** LXCA unterstützt keine Windows-Zeitserver. Wenn Sie normalerweise einen Windows-Zeitserver verwenden, geben Sie stattdessen eine Adresse ein, die für Ihren Standort geeignet ist.

Schritt 3. Klicken Sie nach dem Eingeben der Parameter auf **Speichern**, um zur Seite Erstkonfiguration zurückzukehren.

Fahren Sie mit [„Aufgabe „Einstellungen für Service und Support konfigurieren““](#) auf Seite 79 fort.

---

## Aufgabe „Einstellungen für Service und Support konfigurieren“

Verfahren zum Konfigurieren von Service- und Supporteinstellungen als Teil der Erstkonfiguration von LXCA.

Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf die Aufgabe **Einstellungen für Service und Support konfigurieren**. Die Lenovo Datenschutzerklärung wird angezeigt. Klicken Sie auf „Akzeptieren“, um dieses Fenster zu schließen und zur Seite „Service und Support“ zu wechseln.

Schritt 2. Wählen Sie auf der Registerkarte Regelmäßiger Daten-Upload die gewünschten Optionen aus und klicken Sie auf **Übernehmen**.

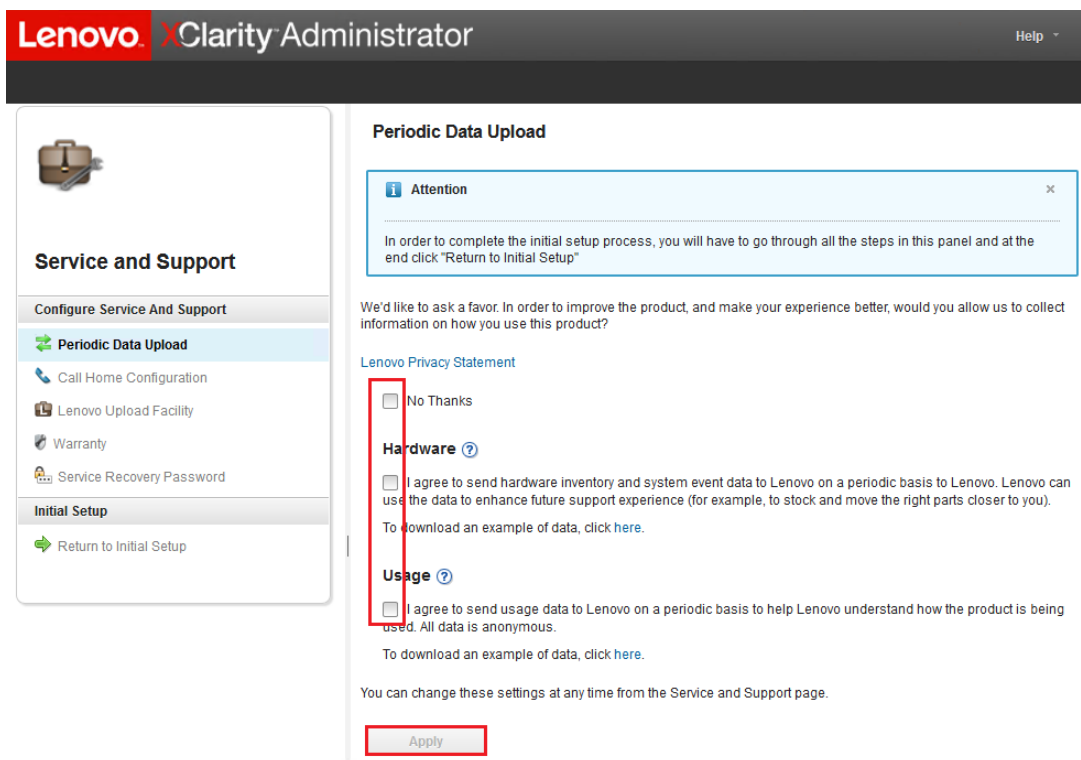


Abbildung 67. Registerkarte „Service und Support – Regelmäßiger Daten-Upload“

Schritt 3. Blättern Sie auf der Registerkarte Call-Home-Konfiguration ggf. nach ganz unten und wählen Sie **Schritt überspringen** aus (die Call-Home-Funktion wird nicht für ThinkAgile SXM Serie Lösungen verwendet).

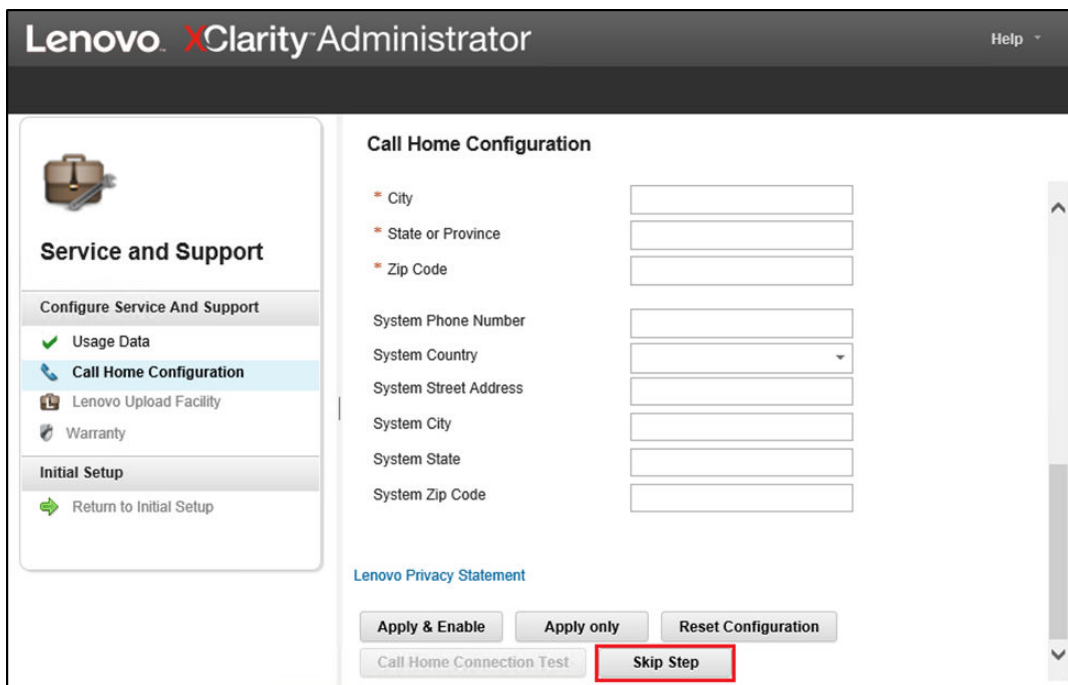


Abbildung 68. Registerkarte „Call-Home-Konfiguration“ von Service und Support



Schritt 4. Blättern Sie auf der Registerkarte Lenovo Upload-Funktionalität nach unten und klicken Sie auf **Schritt überspringen**.

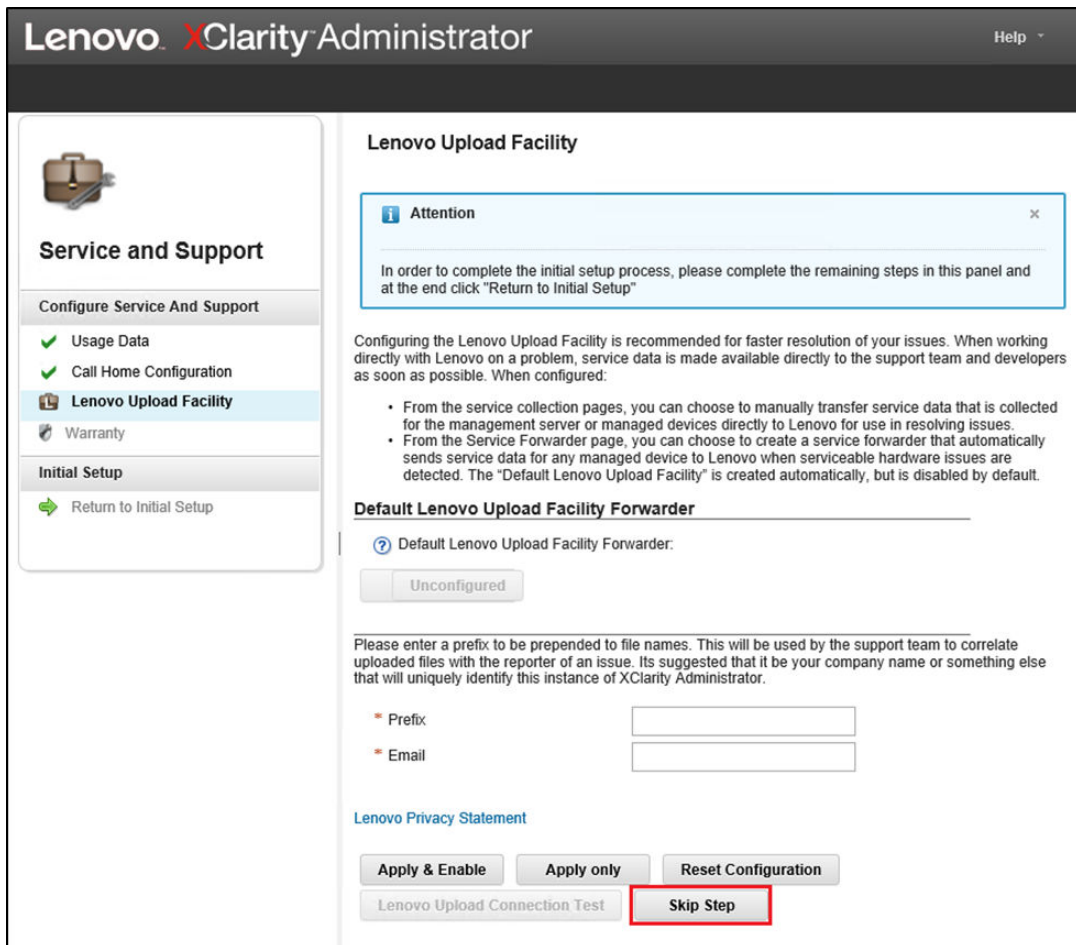


Abbildung 69. Registerkarte „Lenovo Upload-Funktionalität“ von Service und Support

Schritt 5. Stellen Sie auf der Registerkarte Garantie sicher, dass bei allen Dropdown-Listen **Deaktiviert** eingestellt ist, und klicken Sie auf **Übernehmen**. Da der Garantieanspruch für die ThinkAgile SXM Serie Lösung auf der Rack-Seriennummer basiert, wird diese LXCA-Funktion nicht unterstützt.

**Lenovo XClarity Administrator** Help

**Service and Support**

Configure Service And Support

- ✓ Periodic Data Upload
- ✓ Call Home Configuration
- ✓ Lenovo Upload Facility

**Warranty**

- Lenovo Bulletin Service
- Service Recovery Password

**Initial Setup**

- Return to Initial Setup

**Warranty**

**Attention**

In order to complete the initial setup process, please complete the remaining steps in this panel and at the end click "Return to Initial Setup"

The management server can automatically retrieve warranty information for your managed devices, if the appropriate external connections are enabled. This allows you to see when the warranties expire and to be notified when each device is getting close to the expiration date. Enabling the first two resources below is recommended for most parts of the world. For devices that were purchased in China, enabling the third resource is recommended. These resources are used to collect warranty information for managed devices. Ensure that there are no firewalls blocking the URLs.

⚠ Warranty servers are used to retrieve warranty information for all managed devices. These are external connections to Lenovo. If you don't require this information, the connections to these warranty servers can be disabled.

- Enable/Disable - Warranty server (all countries except China)
- Enable/Disable - Warranty server (China-only)

Online Resources	Status	Description
Lenovo Warranty Web Service	Disabled	This connection is used to retrieve wa...
Lenovo Warranty Database (China only)	Disabled	This connection is used to retrieve wa...

[Lenovo Privacy Statement](#)

**Apply** **Skip Step**

Abbildung 70. Registerkarte „Garantie“ von Service und Support

- Schritt 6. Klicken Sie im angezeigten Erfolgsfenster auf **Schließen**, wählen Sie aus, ob Sie Bulletins von Lenovo erhalten möchten, und klicken Sie dann auf **Übernehmen**.
- Schritt 7. Geben Sie auf der Registerkarte Kennwort zur Service-Wiederherstellung ein Kennwort für die LXCA-Wiederherstellung ein, bestätigen Sie es und klicken Sie auf **Übernehmen**. Notieren Sie sich das Kennwort zur späteren Verwendung.

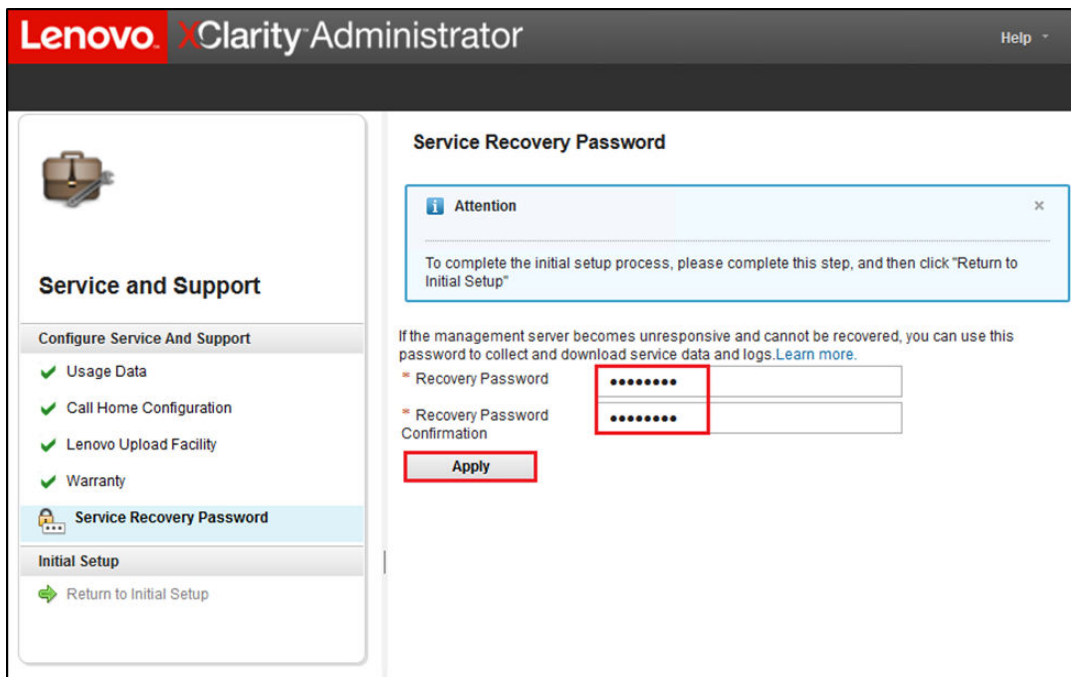


Abbildung 71. Seite „Kennwort zur Service-Wiederherstellung“

Schritt 8. Klicken Sie im angezeigten Erfolgsfenster auf **Schließen** und danach auf **Zu Erstkonfiguration zurückkehren**.

Fahren Sie mit „Aufgabe „Weitere Sicherheitseinstellungen konfigurieren““ auf Seite 83 fort.

## Aufgabe „Weitere Sicherheitseinstellungen konfigurieren“

Verfahren zum Konfigurieren zusätzlicher Sicherheitseinstellungen im Rahmen der LXCA-Ersteinrichtung.

- Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf **Weitere Sicherheitseinstellungen konfigurieren**. Die Seite Sicherheit wird angezeigt.
- Schritt 2. Da hier nichts geändert werden muss, klicken Sie auf **Zu Erstkonfiguration zurückkehren**.
- Schritt 3. Zu diesem Zeitpunkt ist LXCA bereit, mit der Verwaltung der Systeme zu beginnen. Stellen Sie sicher, dass alle Schritte auf der Seite Erstkonfiguration (bis auf den letzten) ein grünes Häkchen haben, wie im folgenden Screenshot dargestellt.

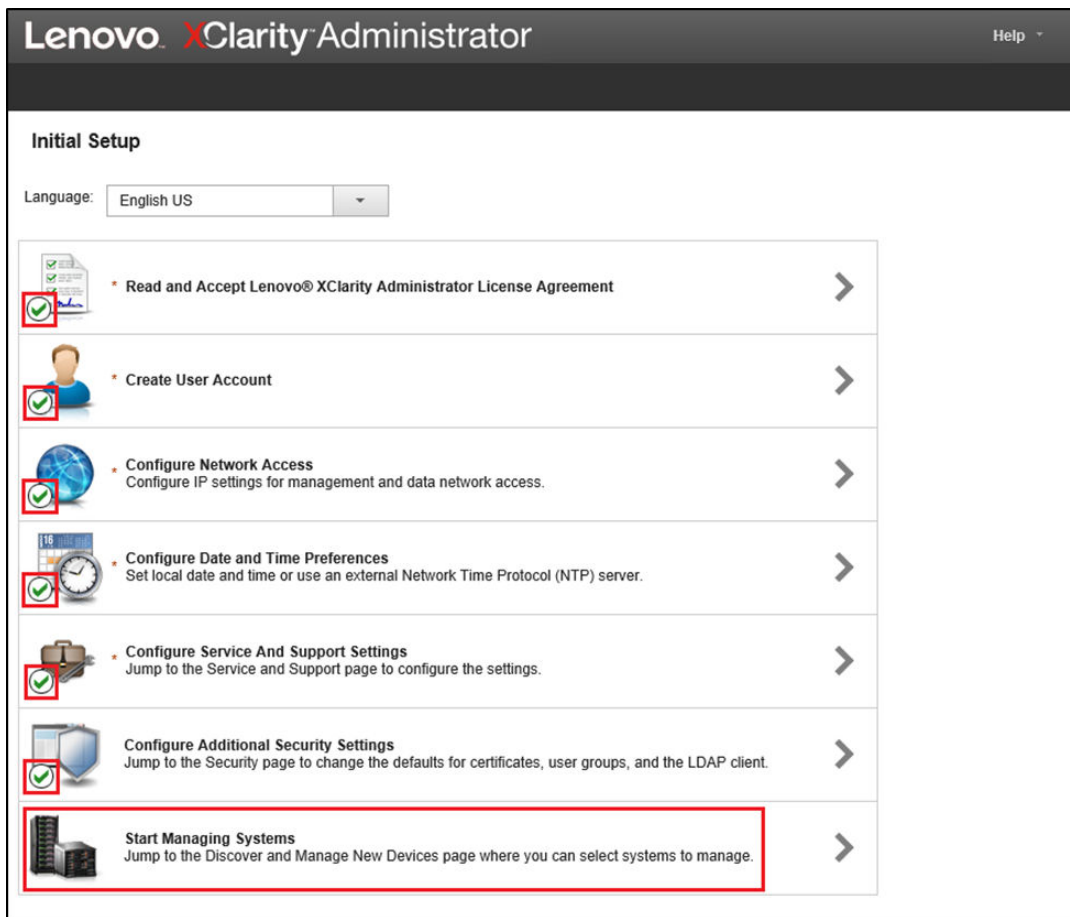


Abbildung 72. Fenster „Erstkonfiguration“ mit einer unerledigten Aufgabe

Fahren Sie mit „Aufgabe „Systemverwaltung starten““ auf Seite 84 fort.

## Aufgabe „Systemverwaltung starten“

Verfahren zur Verwaltung von Systemen in LXCA.

Schritt 1. Klicken Sie im Fenster Erstkonfiguration auf **Start Management Systems**. Die Seite Start Management Systems wird angezeigt.

Schritt 2. Klicken Sie auf **Nein, Demodaten nicht einbeziehen**.

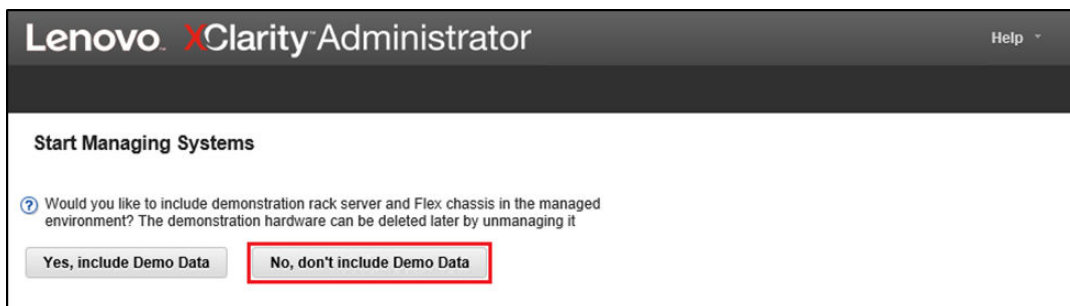


Abbildung 73. Auswählen von „Nein, Demodaten nicht einbeziehen“ im Fenster „Systemverwaltung starten“

Schritt 3. Klicken Sie im Popup-Bestätigungsfenster auf **Nein, danke**.

Schritt 4. Die Seite „Neue Einheiten ermitteln und verwalten“ wird angezeigt. Die automatische Ermittlung findet für das Subnetz statt, auf dem sich LXCA befindet. Da die BMCs in den Systemen, die zu Knoten im Azure Stack Hub-Skalierungseinheit werden, über IP-Adressen im selben Subnetz verfügen, sollten sie in der Tabelle angezeigt werden. Wenn Ihre Lösung Lenovo TOR-Switches verwendet, werden diese möglicherweise ebenfalls aufgeführt.

Wir verwalten zu diesem Zeitpunkt noch keine Systeme oder Switches. Wir kehren zur Verwaltung von Systemen zurück, nachdem der LXCA Pro-Lizenzschlüssel aktiviert und LXCA auf die in der aktuellen [Optimale Vorgehensweise für ThinkAgile SXM](#) angegebene Version aktualisiert wurde.

Fahren Sie mit „[LXCA Pro-Lizenz übernehmen](#)“ auf Seite 85 fort.

---

## LXCA Pro-Lizenz übernehmen

Vor der Verwendung von LXCA zum Verwalten von Systemen müssen Sie den LXCA Pro-Lizenzschlüssel importieren und übernehmen. Dieser Schlüssel dient insbesondere für die langfristige Verwendung der Musterfunktion. Gehen Sie zum Importieren und Anwenden des Lizenzschlüssels wie folgt vor:

Schritt 1. Navigieren Sie im Hauptmenü von LXCA zu **Verwaltung → Lizenzen**.

Schritt 2. Klicken Sie auf der Seite Lizenzverwaltung auf das Symbol **Importieren** ()

Schritt 3. Klicken Sie im neu geöffneten Fenster „Lizenzvereinbarung“ auf „Lizenz akzeptieren“ und dann auf **Dateien auswählen ...**

Schritt 4. Navigieren Sie zu D:\Lenovo\LXCA\LXCA License Files, wählen Sie die Datei im Verzeichnis aus und klicken Sie dann auf **Öffnen**.

Schritt 5. Klicken Sie im Fenster Importieren und übernehmen auf **Importieren und übernehmen** und dann im angezeigten Bestätigungsfenster auf **Ja**.

Schritt 6. Klicken Sie im angezeigten Erfolgsfenster auf **Schließen**.

Schritt 7. Bestätigen Sie auf der Seite Lizenzverwaltung, dass der LXCA Pro-Lizenzschlüssel erfolgreich angewendet wurde und der Status „Gültig“ lautet.

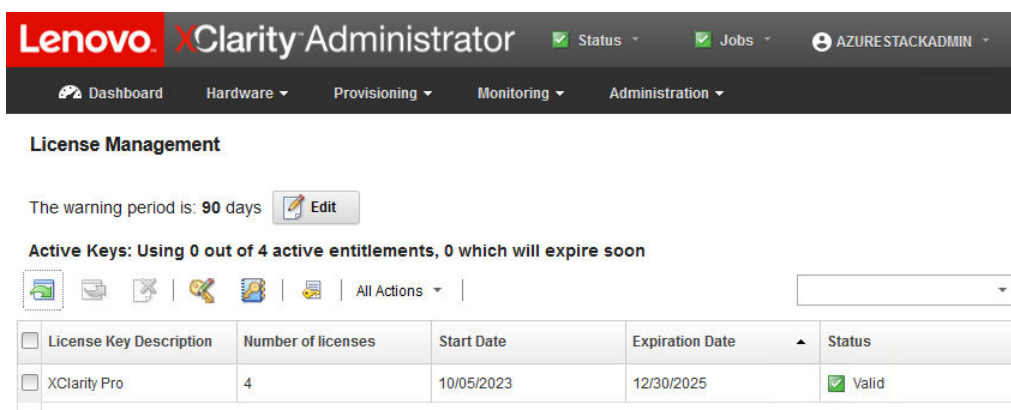


Abbildung 74. Seite „Lizenzverwaltung“ mit angezeigter gültiger LXCA Pro-Lizenz

---

## LXCA-Aktualisierungspaket übernehmen

Normalerweise sind zwei Arten von LXCA-Aktualisierungen verfügbar. Ein LXCA-Aktualisierungspaket wird auf ein Basis-VHD-Image angewendet, um auf die neueste Hauptversion zu aktualisieren (z. B. von v3.0.0 auf

v3.1.0 oder v3.2.0 oder v3.3.0 usw.). Ein LXCA-FixPack wird auf eine Hauptversion angewendet, um LXCA auf die neueste Nebenversion zu aktualisieren (z. B. von v3.6.0 auf v3.6.8). Gehen Sie wie folgt vor, um eine Aktualisierung auf LXCA anzuwenden:

Schritt 1. Navigieren Sie im Hauptmenü von LXCA zu **Verwaltung** → **Verwaltungsserver aktualisieren**.

Schritt 2. Klicken Sie auf das Symbol **Importieren** () und dann auf **Dateien auswählen ....**

Schritt 3. Navigieren Sie zum Verzeichnis mit dem entsprechenden Aktualisierungspaket oder FixPack in D:\Lenovo\LXCA\LXCA Update Packages. Wenn Sie beispielsweise die LXCA-Basis-VHD v3.4.5 auf v3.6.8 aktualisieren, verwenden Sie den Inhalt von Verzeichnis „LXCA v3.6.0 Update“, um auf v3.6.0 zu aktualisieren, und verwenden Sie dann den Inhalt von Verzeichnis „LXCA v3.6.8 FixPack“, um auf v3.6.8 aktualisieren. In unserem Beispiel unten aktualisieren wir LXCA v4.0.0 auf v4.0.14, was kein LXCA-Aktualisierungspaket, aber ein LXCA-FixPack erfordert.

Schritt 4. Wählen Sie alle vier Dateien im Verzeichnis aus und klicken Sie auf **Öffnen**.

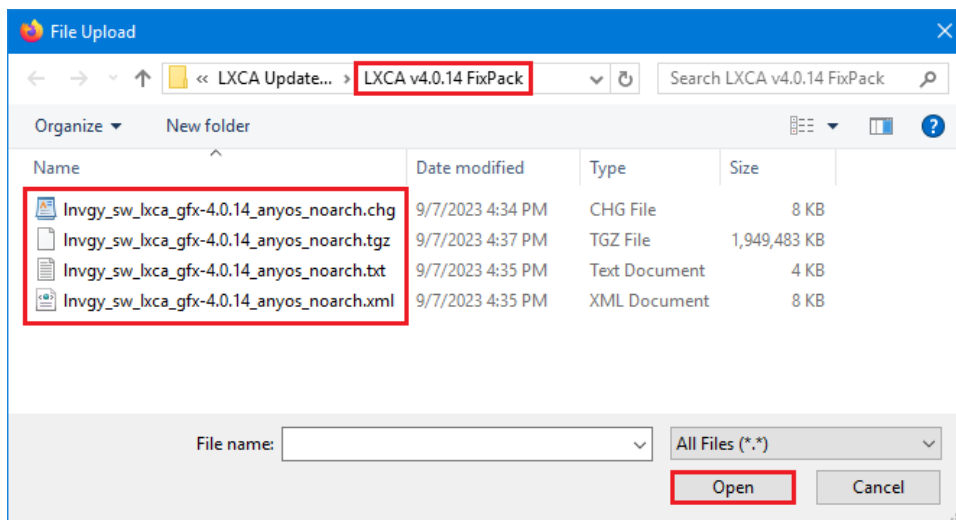



Abbildung 75. Auswählen von LXCA-FixPack-Dateien

Schritt 5. Klicken Sie im Fenster Importieren auf **Importieren**. Der Fortschritt wird angezeigt, bis der Import und die Überprüfung des Aktualisierungsinhalts abgeschlossen sind. Nach Abschluss des Vorgangs wird das Fenster Importieren geschlossen.

Schritt 6. Wählen Sie auf der Seite Verwaltungsserver aktualisieren den Aktualisierungsname für die Aktualisierung aus, die gerade importiert wurde, und klicken Sie dann auf die Schaltfläche

**Aktualisierung durchführen** (.

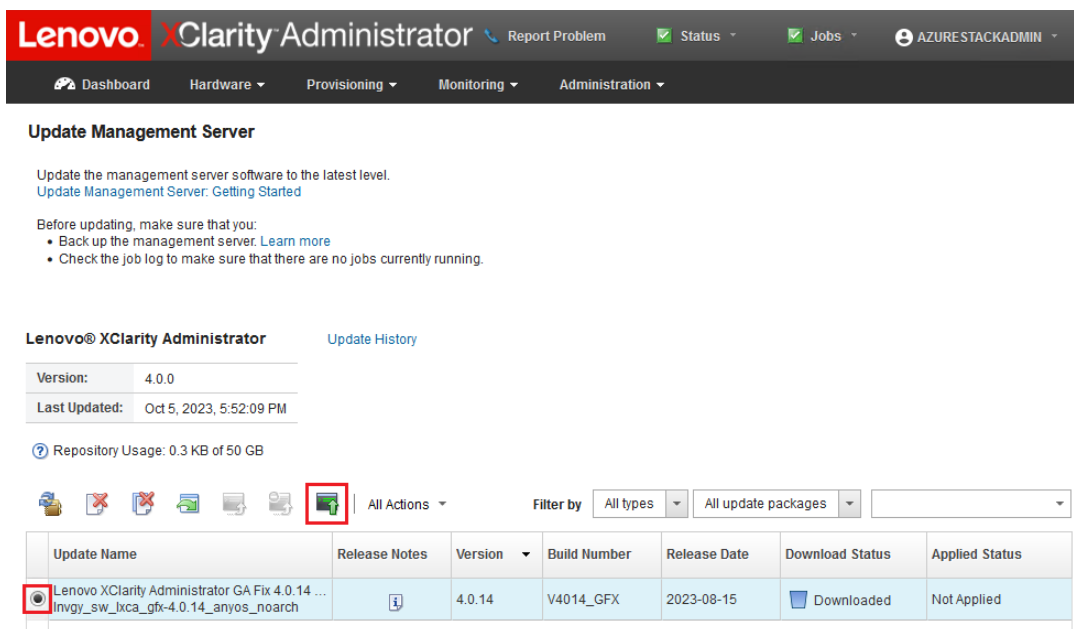


Abbildung 76. Auswählen des Aktualisierungspakets und Aktualisierung

Schritt 7. Klicken Sie im Popup-Bestätigungsfenster auf **Neu starten**.

Schritt 8. Warten Sie auf den Neustart des Verwaltungsservers. Dies kann einige Minuten dauern. Aktualisieren Sie ggf. den Browser, um zur LXCA-Anmeldeseite zurückzukehren, und melden Sie sich dann mit dem zuvor erstellten primären Supervisor-Account an.

Schritt 9. Kehren Sie zur Seite Verwaltungsserver aktualisieren zurück und warten Sie, bis der Downloadstatus zu „Bereinigt“ und der angewendete Status vor dem Fortfahren zu „Angewendet“ geändert wird. Möglicherweise müssen Sie die Seite aktualisieren, damit der letzte Status aktualisiert wird.

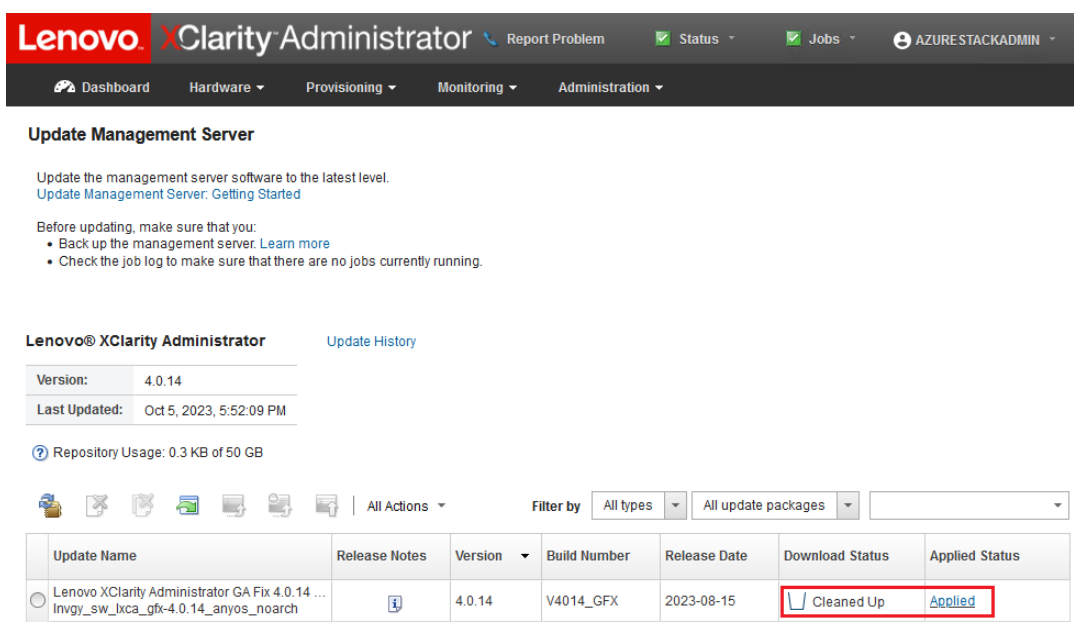


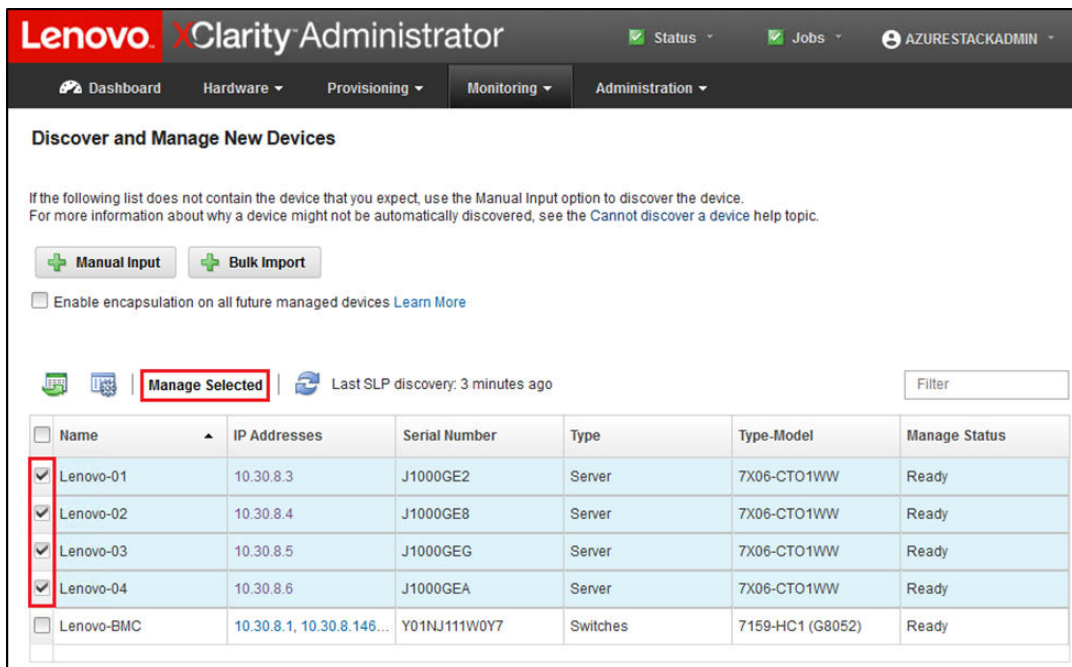
Abbildung 77. Finale Status des Aktualisierungspakets



## Knoten verwalten

Nach Abschluss der LXCA-Konfiguration kann sie die Knoten und Netzwerk-Switches in der Azure Stack Hub-Skalierungseinheit verwalten. Gehen Sie wie folgt vor, um die Knoten in der Azure Stack Hub-Skalierungseinheit zu verwalten:

- Schritt 1. Navigieren Sie im Hauptmenü von LXCA zu **Hardware** → **Neue Einheiten ermitteln und verwalten**.
- Schritt 2. Aktivieren sie zum Verwalten von Lenovo Servern das Kontrollkästchen links vom jeweiligen Server und klicken Sie auf **Ausgewählte verwalten**. Falls Switches und der HLH in der Liste enthalten sind, wählen Sie sie nicht aus.



The screenshot shows the 'Discover and Manage New Devices' section of the Lenovo XClarity Administrator. It includes a table of discovered devices with columns for Name, IP Addresses, Serial Number, Type, Type-Model, and Manage Status. Four server entries are selected with checkmarks in the 'Manage Status' column. A 'Manage Selected' button is highlighted with a red box above the table.

<input type="checkbox"/>	Name	IP Addresses	Serial Number	Type	Type-Model	Manage Status
<input checked="" type="checkbox"/>	Lenovo-01	10.30.8.3	J1000GE2	Server	7X06-CTO1WW	Ready
<input checked="" type="checkbox"/>	Lenovo-02	10.30.8.4	J1000GE8	Server	7X06-CTO1WW	Ready
<input checked="" type="checkbox"/>	Lenovo-03	10.30.8.5	J1000GEG	Server	7X06-CTO1WW	Ready
<input checked="" type="checkbox"/>	Lenovo-04	10.30.8.6	J1000GEA	Server	7X06-CTO1WW	Ready
<input type="checkbox"/>	Lenovo-BMC	10.30.8.1, 10.30.8.145...	Y01NJ111W0Y7	Switches	7159-HC1 (G8052)	Ready

Abbildung 78. Vier Knoten, die zur Verwaltung ausgewählt sind

- Schritt 3. Deaktivieren Sie im Fenster Verwalten das Kontrollkästchen **Verwaltete Authentifizierung** und klicken Sie auf **Gespeicherte Anmeldeinformationen verwalten**.



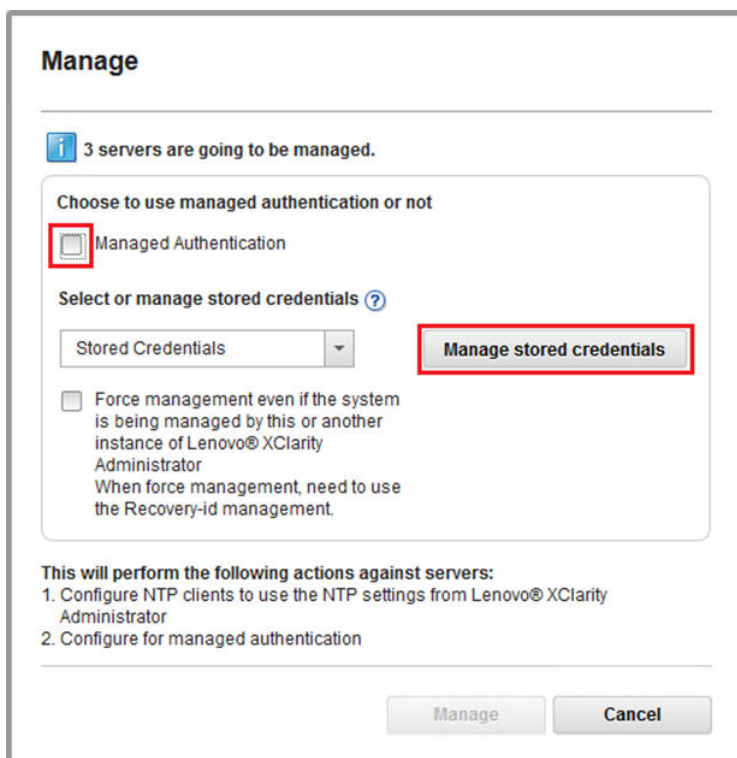


Abbildung 79. Gespeicherte Anmeldeinformationen verwalten

Schritt 4. Klicken Sie auf **Neue gespeicherte Anmeldeinformationen erstellen** (  ).

Schritt 5. Geben Sie die Anmeldeinformationen ein, die LXCA für die Kommunikation mit den XClarity Controllern auf den Knoten verwendet wird. Diese Anmeldeinformationen finden Sie im Dokument „Customer Deployment Summary“ (Implementierungszusammenfassung für Kunde), das Sie nach der ersten Implementierung der Lösung erhalten haben. Da die Anmeldeinformationen der beiden Knoten identisch sind, müssen sie nur einmal eingegeben werden. Geben Sie eine Beschreibung ein, die erklärt, dass dieser LXCA diese Anmeldeinformationen zur Verwaltung der Knoten verwendet. Klicken Sie nach dem Eingeben der Anmeldeinformationen auf **Gespeicherte Anmeldeinformationen erstellen**.

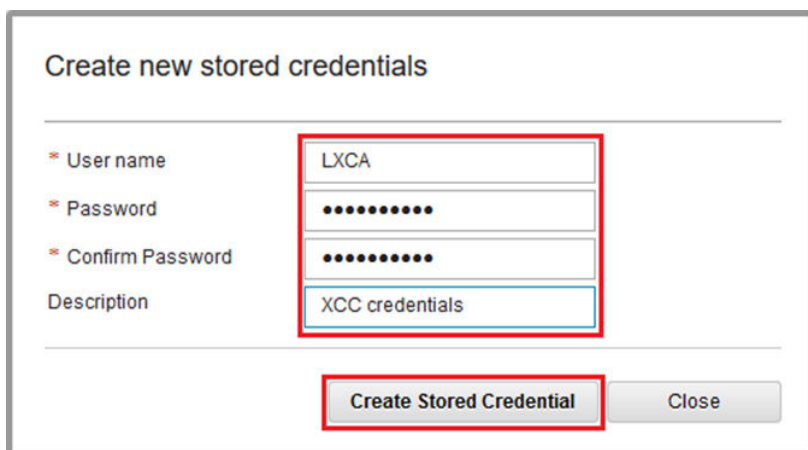


Abbildung 80. Erstellen neuer gespeicherter Anmeldeinformationen

Schritt 6. Wählen Sie im Fenster Verwaltung der gespeicherten Anmeldeinformationen die gerade erstellten Anmeldeinformationen aus und klicken Sie auf **Auswählen**.

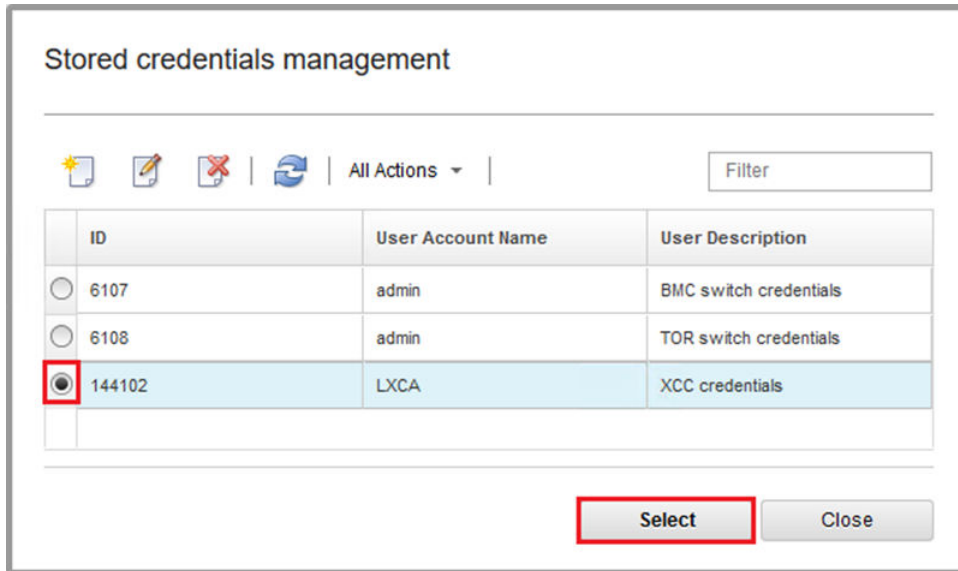


Abbildung 81. Auswählen neuer gespeicherter Anmeldeinformationen für die Verwaltung

Schritt 7. Klicken Sie im Fenster Verwalten auf **Verwalten**.

Schritt 8. Ein Statusfenster zeigt den Prozess zum Herstellen einer Verwaltungsverbindung mit jedem XClarity Controller an.

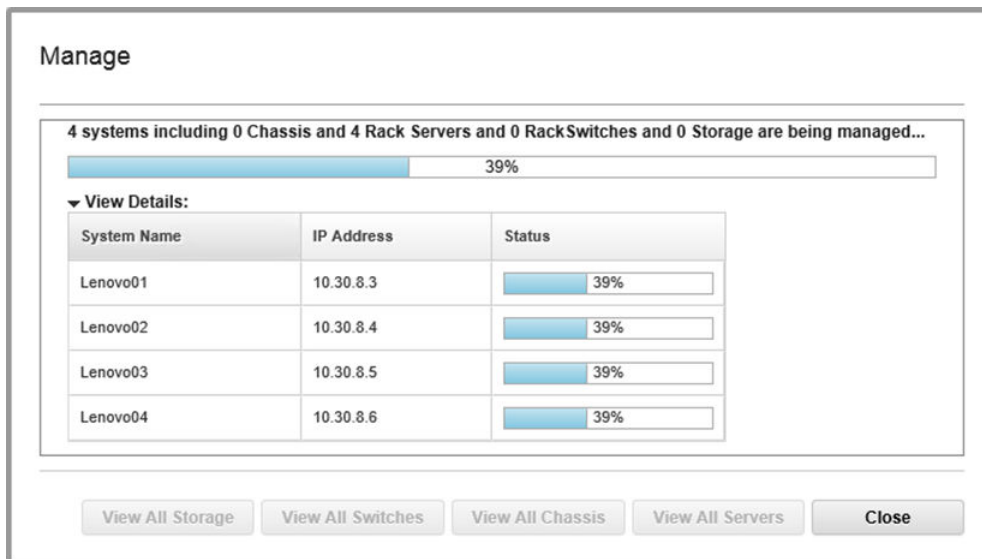


Abbildung 82. Herstellen von Verwaltungsverbindungen mit jedem XClarity Controller

Schritt 9. Klicken Sie nach Abschluss des Vorgangs auf **Alle Server anzeigen**, um das Fenster Verwalten zu schließen und zum Hauptfenster von LXCA zurückzukehren.

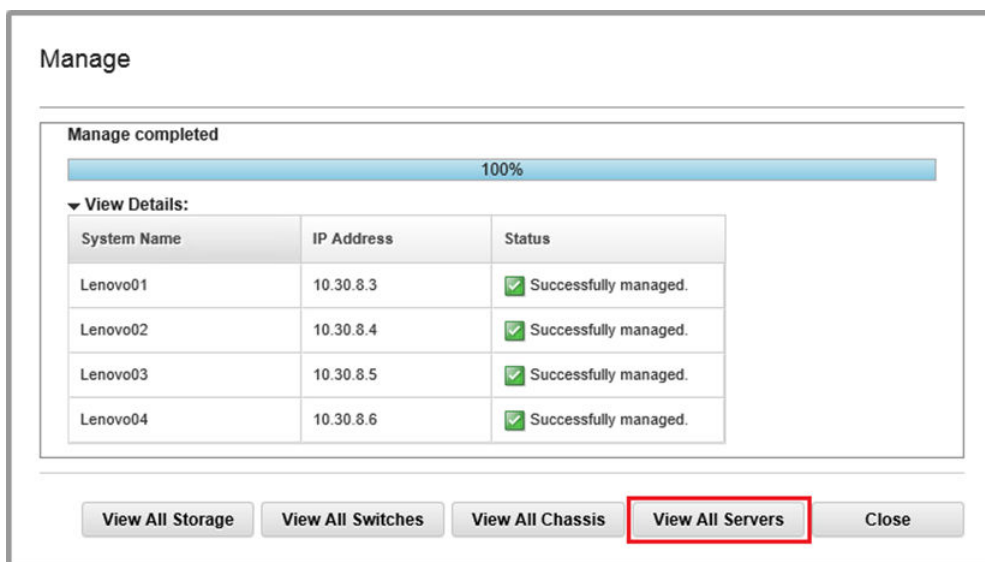


Abbildung 83. Alle Server anzeigen

Obwohl der Job erfolgreich abgeschlossen wird, kann die Bestandserfassung von den Knoten mindestens 20 Minuten in Anspruch nehmen. Während dieses Zeitraums sind einige Aufgaben (z. B. Servermuster oder Richtlinie anwenden) nicht zulässig. Ein Wartestatus weist darauf hin, dass die Bestandserfassung stattfindet.

Am Ende wird der Status aller Knoten als „Normal“ angezeigt.

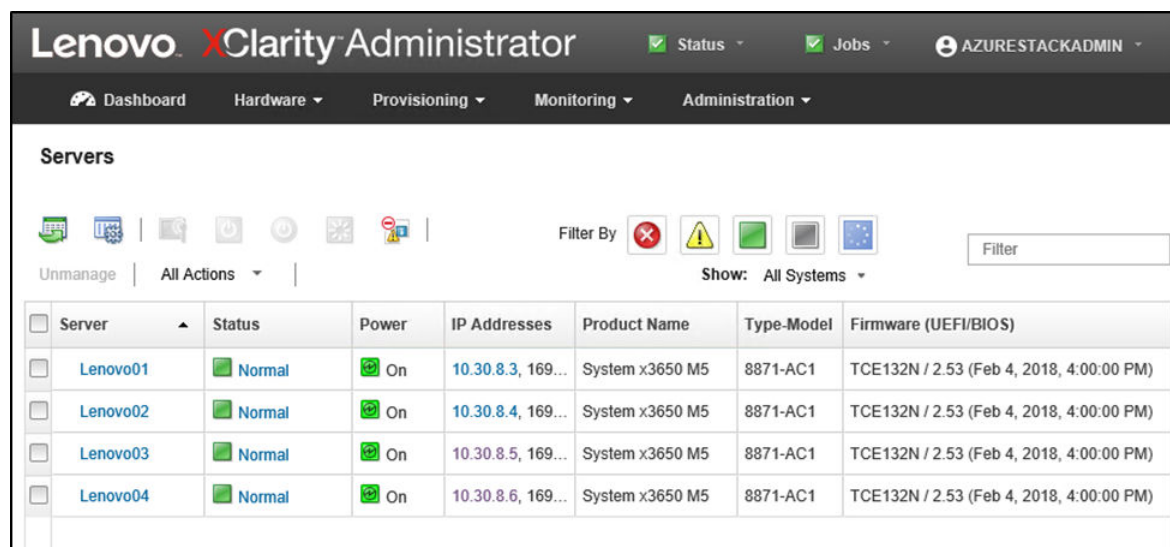


Abbildung 84. Bestandserfassung abgeschlossen


## Servermuster importieren und übernehmen

Ein Servermuster stellt eine Bare-Metal-Serverkonfiguration dar und kann auf mehreren Servern gleichzeitig angewendet werden.

Das entsprechende Servermuster finden Sie im Verzeichnis D:\Lenovo\XCA auf dem HLH.


Gehen Sie wie folgt vor, um das Lenovo ThinkAgile SXM Serie Servermuster zu importieren:

Schritt 1. Navigieren Sie im Hauptmenü der LXCA-Browser-Schnittstelle zu **Bereitstellung** → **Muster**.

Schritt 2. Klicken Sie auf der Seite „Konfigurationsmuster: Muster“ auf das Symbol **Importieren** () und dann auf **Dateien auswählen ...**.

Schritt 3. Navigieren Sie zu D:\Lenovo\LXCA, wählen Sie die für Ihre Lösung geeignete LXCA-Musterdatei aus und klicken Sie dann auf **Öffnen**.

Schritt 4. Klicken Sie auf **Importieren**. Wenn das Fenster zum erfolgreichen Import angezeigt wird, klicken Sie auf **Schließen**.

Schritt 5. Aktivieren Sie zum Implementieren des Musters das Kontrollkästchen links vom gerade importierten Muster aus und klicken Sie auf das Symbol **Muster bereitstellen** ()

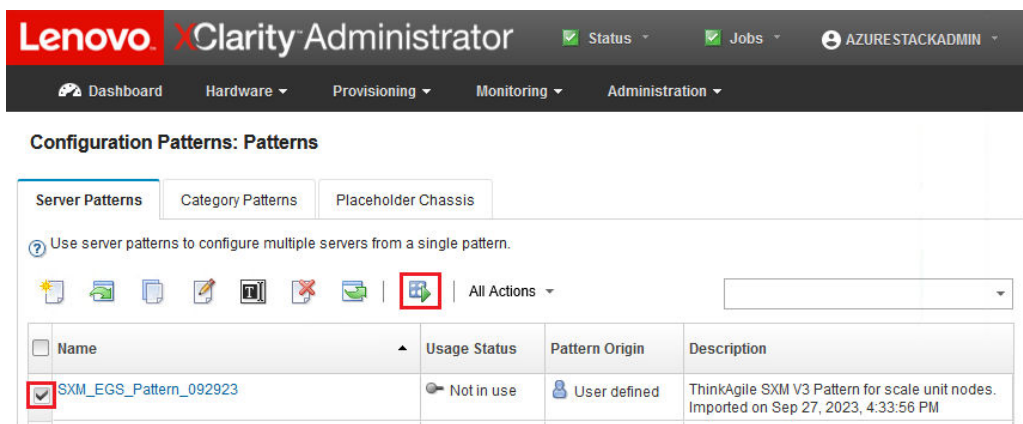


Abbildung 85. Implementieren eines Musters

Schritt 6. Stellen Sie sicher, dass das Optionsfeld **Teilweise – BMC-Einstellungen aktivieren, aber Server nicht neu starten ...** ausgewählt ist. Wählen Sie dann alle Knoten der Azure Stack Hub-Skalierungseinheit aus und klicken Sie auf **Implementieren**.

**Wichtig:** Stellen Sie sicher, dass die Option **Teilweise...** aktiviert ist, da NICHT alle Knoten gleichzeitig neu gestartet werden sollten.

### Deploy Server Pattern - SR650PatternThinkAgileSXM\_121218

Deploy the server pattern to one or more individual servers or groups of servers (for example, a chassis). During deployment, one server profile is created for each individual server.

\* Pattern To Deploy:

\* Activation ?

Full — Activate all settings and restart the server now.  
 Partial — Activate BMC settings but do not restart the server. UEFI and server settings will be active after the next restart.  
 Deferred — Generate a profile with the settings for review, but do not activate settings on the server.

Choose one or more servers to which to deploy the selected pattern.

Any Deploy Status

<input checked="" type="checkbox"/>	Name	Rack Name/Unit	Chassis/Bay	Deploy Status
<input checked="" type="checkbox"/>	Lenovo-01	Unassigned / Ur		✓ Ready
<input checked="" type="checkbox"/>	Lenovo-02	Unassigned / Ur		✓ Ready
<input checked="" type="checkbox"/>	Lenovo-03	Unassigned / Ur		✓ Ready
<input checked="" type="checkbox"/>	Lenovo-04	Unassigned / Ur		✓ Ready

Abbildung 86. Implementieren des Musters mit vollständiger Aktivierung

Schritt 7. Wählen Sie im angezeigten Popup-Fenster **Zu Profile-Seite wechseln** aus.

✓ Deployment request was submitted.

---

Job "Server Profile activation: Feb 27, 2018" has been created and started successfully. Changes are being propagated to the following servers or bays: Lenovo01, Lenovo02, Lenovo03, Lenovo04

You can monitor job progress from the Jobs pod in the banner above.

You can view the profile creation progress from the Server Profiles link that is located under the Provisioning menu in the menu bar. Profiles will not show up in the Server Profiles table until the profile has been created.

---

Abbildung 87. Steuerelement „Zu Profile wechseln“

Schritt 8. Warten Sie, bis alle Profile aktiv sind (siehe Spalte „Profilstatus“).

The screenshot shows the 'Configuration Patterns: Server Profiles' section in the Lenovo XClarity Administrator. It includes a navigation bar with 'Dashboard', 'Hardware', 'Provisioning', 'Monitoring', and 'Administration'. Below the navigation, there is a header for 'Configuration Patterns: Server Profiles' and a sub-header 'Server profiles represent the specific configuration of a single server.' There are also some icons and a dropdown menu for 'All Actions'. A table lists four server profiles, each with a 'Profile Status' of 'Active', which is highlighted with a red box in the original image.

Profile	Server	Rack Name/Unit	Chassis/Bay	Profile Status	Pattern
SR650PatternThinkAgileSXM_121218-profile6	Lenovo-01	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218
SR650PatternThinkAgileSXM_121218-profile7	Lenovo-02	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218
SR650PatternThinkAgileSXM_121218-profile8	Lenovo-03	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218
SR650PatternThinkAgileSXM_121218-profile9	Lenovo-04	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218

Abbildung 88. Serverprofile mit Status „Aktiv“

Damit ist die Implementierung und Konfiguration von LXCA abgeschlossen.

---

## Anhang B. ThinkAgile SXM Serie Switches mit der CLI aktualisieren (nur Lenovo Switches)

Wenn die Aktualisierung der ThinkAgile SXM Serie Switch-Firmware mit XClarity Administrator nicht funktioniert (z. B. wenn die aktuelle Version der Switch-Firmware keine Aktualisierung über XClarity Administrator zulässt), gehen Sie wie folgt vor, um die ThinkAgile SXM Serie Switch-Firmware über die CLI zu aktualisieren.

---

### Vorbedingungen

Befolgen Sie die Anweisungen in diesem Abschnitt, bevor Sie mit der Aktualisierung der Switch-Firmware mit CLI beginnen.

Stellen Sie zunächst sicher, dass Sie die folgenden Elemente zur Verfügung haben:

- Für Lenovo spezifisches serielles Kabel (Mini-USB RJ-45 seriell), mit dem Switch mitgeliefert
- USB-zu-seriell-Kabel
- USB-Stick (muss als FAT32 formatiert sein und darf max. 32 GB Kapazität haben)
- Geeignete Switch-Firmware-Images, basierend auf der optimalen Vorgehensweise für ThinkAgile SXM

---

### Switch-Image-Dateien vorbereiten

Bereiten Sie die Switch-Image-Dateien entsprechend der Anweisungen in diesem Abschnitt für die Aktualisierung der Switch-Firmware vor.

Die Switch-Firmware-Image-Dateien sind im Haupt-Firmwareaktualisierungsarchiv im ThinkAgile SXM Aktualisierungs-Repository enthalten. Der Titel dieses Archivs verwendet das Format `<Platform>Firmware_SXMBR<yyyy>.zip`, wobei `<Platform>` entweder „Broadwell“ oder „Purley“ und `yyyy` die Version der optimalen Vorgehensweise für ThinkAgile SXM ist. Gehen Sie wie folgt vor, um die Switch-Firmware-Image-Dateien für die Aktualisierung mithilfe der CLI-Methode vorzubereiten:

Schritt 1. Extrahieren Sie den gesamten Inhalt aus der Haupt-Firmwareaktualisierungsarchivdatei.

Schritt 2. Suchen Sie im extrahierten Verzeichnis nach den entsprechenden Switch-Firmwareaktualisierungsdateien. Das folgende Beispiel zeigt die Firmwareaktualisierungspakete für die Switches, die in Broadwell-basierten ThinkAgile SXM Lösungen enthalten sind.



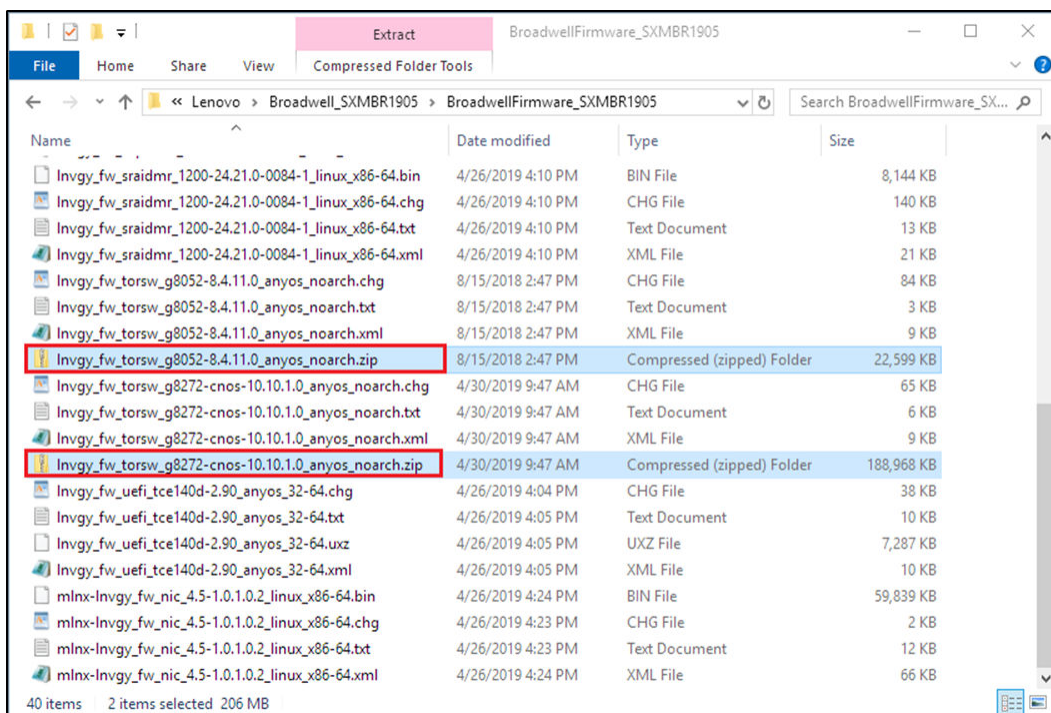


Abbildung 89. Broadwell-basierte ThinkAgile SXM Switch-Firmwareaktualisierungspakete

Schritt 3. Öffnen Sie für jeden zu aktualisierenden Switch die entsprechende ZIP-Archivdatei. Das folgende Beispiel zeigt den Inhalt des Archivs für die RackSwitch G8272 TOR-Switches, die in Broadwell-basierten ThinkAgile SXM Lösungen enthalten sind.

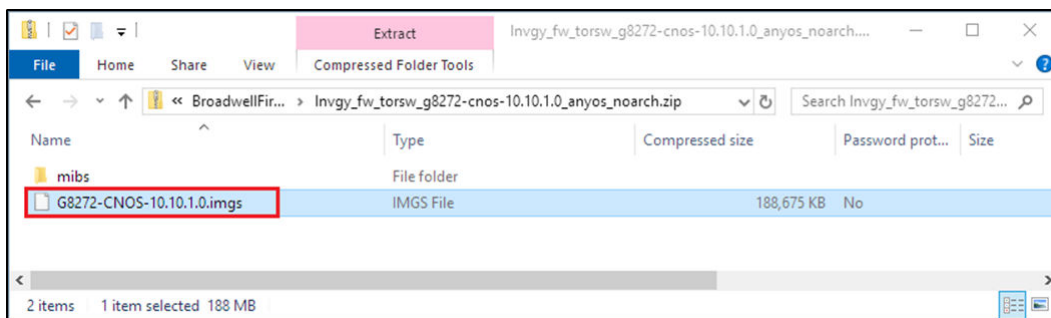


Abbildung 90. Inhalt des Switch-Firmwareaktualisierungsarchivs

Schritt 4. Wählen Sie die IMGS-Image-Dateien aus und kopieren Sie die Dateien. Beachten Sie, dass es für den BMC-Switch, auf dem ENOS ausgeführt wird, zwei IMGS-Dateien gibt, wie im folgenden Beispiel gezeigt.



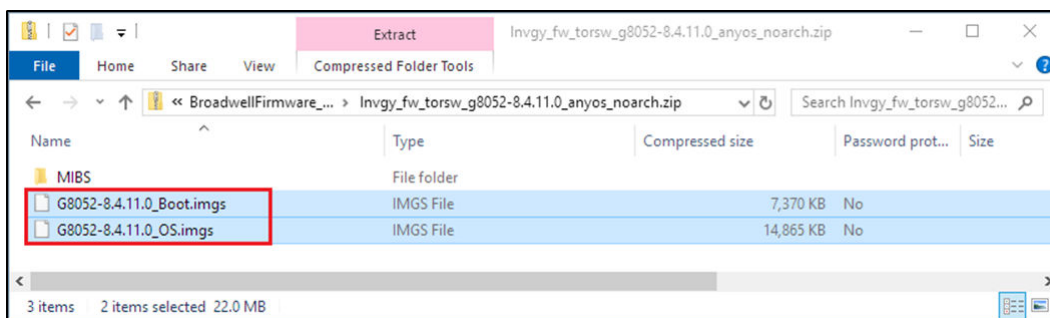


Abbildung 91. ThinkAgile SXM Switch-Firmware-IMGS-Image-Dateien

Schritt 5. Fügen Sie die Image-Dateien in das Stammverzeichnis des USB-Sticks ein.

Schritt 6. Wiederholen Sie diesen Vorgang, um alle anderen erforderlichen Switch-Image-Dateien auf den USB-Stick zu kopieren.

## Zustand von Azure Stack Hub überprüfen

Bevor Sie mit Switches arbeiten, müssen Sie zunächst sicherstellen, dass die Azure Stack Hub-Umgebung fehlerfrei ist.

Melden Sie sich dazu beim Azure Stack Hub-Administratorportal an und stellen Sie sicher, dass keine Alerts angezeigt werden. Ein Beispiel hierfür sehen Sie in der folgenden Abbildung. Im Laufe des Prozesses werden wir den Allgemeinzustand der Lösung immer wieder im Portal überprüfen.

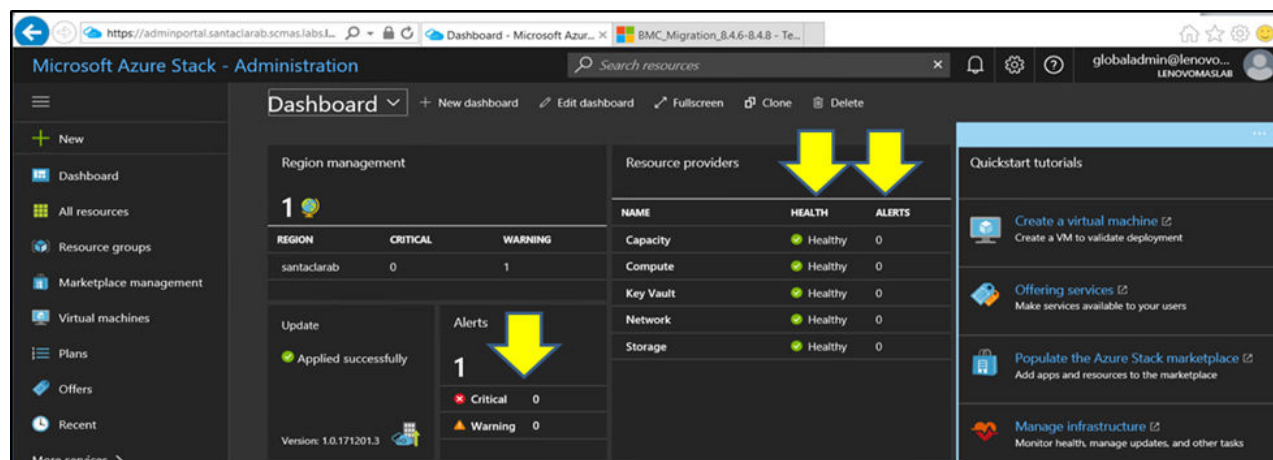


Abbildung 92. Überprüfen des Zustands von Azure Stack Hub

## Lenovo TOR-Switch-Firmware mit der CLI aktualisieren

In diesem Abschnitt werden die erforderlichen Schritte zur Aktualisierung des CNOS-Image der Lenovo TOR-Switches beschrieben. Der Prozess ist derselbe wie bei Lenovo G8272 RackSwitch-Switches in den Broadwell-Lösungen und Lenovo ThinkSystem NE2572 RackSwitch-Switches in Purley-Lösungen.

### TOR-Switch-Konfiguration sichern

Stellen Sie vor Beginn des Aktualisierungsverfahrens sicher, dass beide TOR-Switch-Konfigurationen gesichert wurden.

Die Sicherung der Switch-Konfiguration kann mit XClarity Administrator v2.1 und höher durchgeführt werden. Hier werden trotzdem Switch-CLI-Befehle bereitgestellt, da für die Schritte in diesem Anhang eine serielle Verbindung und ein USB-Stick verwendet werden.

Gehen Sie bei den zwei TOR-Switches, auf denen CNOS ausgeführt wird, wie folgt vor:

- Schritt 1. Stellen Sie über die serielle Konsole des HLH eine Verbindung zum TOR-1-Switch her.
- Schritt 2. Stecken Sie den USB-Stick in den TOR-1-Switch.
- Schritt 3. Melden Sie sich mit den Anmeldeinformationen `admin/<password>` beim TOR-1-Switch an.
- Schritt 4. Verwenden Sie die folgenden Befehle, um die aktuell ausgeführte Konfiguration in die Startkonfiguration zu kopieren und die Konfigurationsdatei im Stammverzeichnis des USB-Sticks zu speichern:

```
enable
cp running-config startup-config
cp startup-config usb1 TOR1StartupBackup.cfg
system eject-usb
```

- Schritt 5. Sie können den USB-Stick nun vom TOR-1-Switch entfernen.
- Schritt 6. Stellen Sie über die serielle Konsole des HLH eine Verbindung zum TOR-2-Switch her.
- Schritt 7. Stecken Sie den USB-Stick in den TOR-2-Switch.
- Schritt 8. Melden Sie sich mit den Anmeldeinformationen `admin/<password>` beim TOR-2-Switch an.
- Schritt 9. Verwenden Sie die folgenden Befehle, um die aktuell ausgeführte Konfiguration in die Startkonfiguration zu kopieren und die Konfigurationsdatei im Stammverzeichnis des USB-Sticks zu speichern:

```
enable
cp running-config startup-config
cp startup-config usb1 TOR2StartupBackup.cfg
system eject-usb
```

- Schritt 10. Sie können den USB-Stick nun vom TOR-2-Switch entfernen.

Die TOR-Switch-Konfigurationen werden jetzt auf dem USB-Stick gesichert, falls während der Switch-Aktualisierung Probleme auftreten und die Switches auf die aktuelle Konfiguration zurückgesetzt werden müssen.

## CNOS auf TOR-Switches mit der CLI aktualisieren

In dieser Vorgehensweise ist beschrieben, wie Sie das CNOS auf Ihren ThinkAgile SXM Serie TOR-Switches aktualisieren (Lenovo ThinkSystem NE2572 RackSwitch für Purley-basierte Lösungen und Lenovo RackSwitch G8272 für Broadwell-basierte Lösungen).

Die Beispiele in diesem Abschnitt zeigen möglicherweise leicht unterschiedliche Ergebnisse, je nachdem, mit welcher CNOS-Version die Befehle ausgeführt wurden. Wichtige Aspekte in den Beispielen werden hervorgehoben.

Um CNOS auf Ihren ThinkAgile SXM Serie TOR-Switches zu aktualisieren, gehen Sie auf dem TOR-1-Switch wie folgt vor und überprüfen Sie dann die Switch-Funktionalität, bevor Sie den Vorgang auf dem TOR-2-Switch wiederholen.

- Schritt 1. Stecken Sie den USB-Stick in den TOR-Switch.
- Schritt 2. Stellen Sie über die serielle Konsole des HLH eine Verbindung zum TOR-Switch her.

Schritt 3. Melden Sie sich mit den Anmeldeinformationen `admin/<password>` beim TOR-Switch an.

Schritt 4. Verwenden Sie die folgenden Befehle, um die neue Switch-Firmware-Image-Datei vom Stammverzeichnis des USB-Sticks zum Standby-Image-Slot auf dem TOR-Switch zu kopieren. Ersetzen Sie dabei das Element in Klammern durch den tatsächlichen Namen der Switch-Image-Datei:

```
enable
cp usb1 <ImageFileName>.imgs system-image all
```

#### Beispiel

```
TOR1 login: admin
Password:
...
TOR1#enable
TOR1#cp usb1 CNOS/G8272-CNOS-10.6.1.0.imgs system-image all
WARNING: This operation will overlay the currently booting image.
Confirm download operation (y/n)? y
TOR1#
```

Schritt 5. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Switch so eingestellt ist, dass er mit dem neuen Standby-Image neu startet:

```
display boot
```

#### Beispiel

```
TOR1#display boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.6.1.0, downloaded 20:49:51 UTC Tue Jan 16 2018
  standby image: version 10.8.1.0, downloaded 10:25:35 UTC Thu Jan 11 2018
  Uboot: version 10.8.1.0, downloaded 07:47:27 UTC Sun Jan 14 2018
  ONIE: empty
Currently set to boot software active image
Current port mode: default mode
Next boot port mode: default mode
Currently scheduled reboot time: none
```

Im obigen Beispiel gibt es zwei wichtige Details:

- Im Standby-Image ist neue Switch-Firmware verfügbar.
- Der Switch ist so eingestellt, dass er mit dem aktiven Image startet. Dies muss geändert werden.

Schritt 6. Führen Sie die folgenden Befehle aus, um das Image zu ändern, von dem der Switch startet:

```
configure
startup image standby
exit
```

### Beispiel

```
TOR1#configure
TOR1(config)# startup image standby
TOR1(config)#exit
TOR1#display boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.6.1.0, downloaded 20:49:51 UTC Tue Jan 16 2018
  standby image: version 10.8.1.0, downloaded 10:25:35 UTC Thu Jan 11 2018
  Uboot: version 10.8.1.0, downloaded 07:47:27 UTC Sun Jan 14 2018
  ONIE: empty
Currently set to boot software standby image
Current port mode: default mode
Next boot port mode: default mode
```

Im obigen Beispiel zeigt die erneute Ausführung des Befehls „display boot“, dass der Switch nun so eingestellt ist, dass er vom Standby-Image startet, das das neue Switch-Firmware-Image enthält.

- Schritt 7. Bevor Sie den TOR-Switch neu starten, um die Änderungen zu implementieren, empfiehlt es sich, alle Ports am Switch herunterzufahren und zu bestätigen, dass der andere TOR-Switch den Betrieb angewendet hat und den gesamten Netzwerkverkehr verarbeitet. Führen Sie die folgenden Befehle aus, um die Ports auf dem TOR-Switch herunterzufahren, der aktualisiert wird:

```
configure
interface ethernet 1/1-54
shutdown
exit
```

- Schritt 8. Überprüfen Sie nach dem Herunterfahren der Ports die Verbindung, um den Failover des Datenverkehrs zu TOR-2 sicherzustellen. Gehen Sie wie folgt vor:
- Navigieren Sie im Hauptmenü der XClarity Administrator-Browser-Schnittstelle zu **Verwaltung** → **Netzwerkzugriff**.
  - Klicken Sie oben in der Browser-Schnittstelle auf die Schaltfläche **Verbindung testen**.
  - Geben Sie im Feld **Host** 8.8.8.8 ein und klicken Sie dann auf **Verbindung testen**.
  - Ein Erfolgsfenster wird angezeigt. Klicken Sie auf **Schließen**, um dieses Fenster zu schließen.
  - Melden Sie sich als zusätzlichen Verifizierungsschritt im Azure Stack Hub-Administratorportal an.
  - Stellen Sie im Azure Stack Hub-Administratorportal sicher, dass derzeit keine Alerts sichtbar sind.

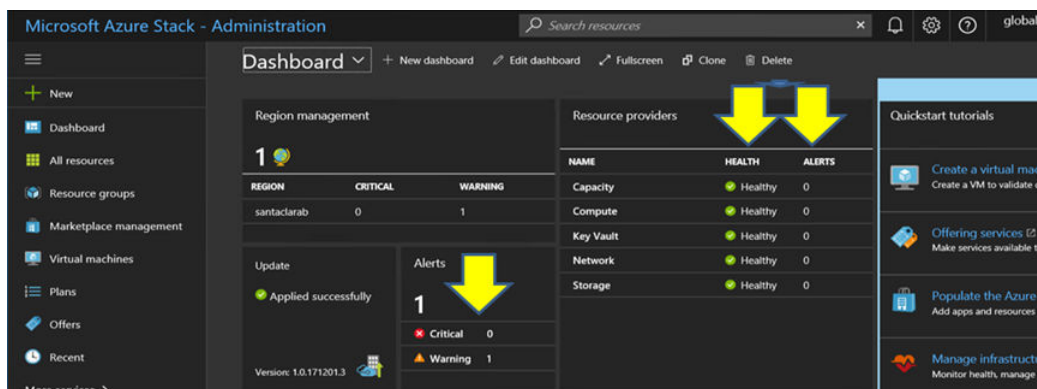


Abbildung 93. Alert-Überprüfung im Azure Stack Hub-Administratorportal

Schritt 9. Sobald das Switch-Failover abgeschlossen ist, starten Sie den TOR-Switch, der aktualisiert wird, mit dem folgenden Befehl neu: Reload

Es wird eine Warnung angezeigt, da alle Ports in der aktuell ausgeführten Konfiguration heruntergefahren sind, was sich von der aktuellen Startkonfiguration unterscheidet. Geben Sie `y` ein und drücken Sie die Eingabetaste, um fortzufahren.

**Wichtig:** Sie dürfen die ausgeführte Konfiguration zu diesem Zeitpunkt noch NICHT speichern, da sonst alle Ports nach dem Switch-Neustart heruntergefahren bleiben.

#### Beispiel

```
TOR1(config)#reload
WARNING: The running-config is different to startup-config.
Confirm operation without saving running-config to startup-config (y/n)? y
... After reload ...
TOR1 login: admin
Password:
...
TOR1#enable
```

Schritt 10. Sobald der Switch wieder online ist, melden Sie sich über die serielle Konsole am Switch an.

Schritt 11. Ziehen Sie den USB-Stick vom TOR-Switch ab.

Informationen zur ordnungsgemäßen Funktion des aktualisierten TOR-Switches finden Sie unter [„TOR-Switch-Funktionalität überprüfen“ auf Seite 34](#). Wiederholen Sie nach der Überprüfung den obigen Vorgang (einschließlich der Überprüfungsschritte) auf dem anderen TOR-Switch. Wenn der BMC-Switch ebenfalls aktualisiert werden muss, fahren Sie mit [„BMC-Switch-Firmware mit der CLI aktualisieren“ auf Seite 101](#) fort. Andernfalls ist der Switch-Firmwareaktualisierungsprozess nun abgeschlossen.

## BMC-Switch-Firmware mit der CLI aktualisieren

In diesem Abschnitt werden die erforderlichen Schritte zur Aktualisierung des ENOS-Image und der Konfiguration des BMC-Switches mit der Switch-CLI-Methode beschrieben. Obwohl der Prozess dem ähnelt, der für die TOR-Switches verwendet wird, unterscheiden sich die auf dem Switch ausgeführten Befehle, da der BMC-Switch ein anderes NOS als die TOR-Switches ausführt.

## BMC-Switch-Konfiguration sichern

Stellen Sie vor Beginn des Aktualisierungsverfahrens sicher, dass die BMC-Switch-Konfiguration gesichert wurde.

Gehen Sie wie folgt vor, um eine Sicherung der BMC-Switch-Konfigurationsdatei durchzuführen:

- Schritt 1. Stecken Sie einen USB-Stick in den BMC-Switch.
- Schritt 2. Stellen Sie über die serielle Konsole des HLH eine Verbindung zum BMC-Switch her.
- Schritt 3. Melden Sie sich mit den Anmeldeinformationen `admin/<password>` beim BMC-Switch an.
- Schritt 4. Verwenden Sie die folgenden Befehle, um die aktuell ausgeführte Konfiguration in die Startkonfiguration zu kopieren und dann die Startkonfiguration (Bootkonfiguration) im Stammverzeichnis des USB-Sticks zu speichern.

```
enable
copy running-config startup-config
usbcopy tusb BMCStartupBackup.cfg boot
```

Die BMC-Switch-Konfigurationsdatei wird jetzt auf dem USB-Stick gesichert, falls während der Switch-Aktualisierung Probleme auftreten und der Switch auf die aktuelle Konfiguration zurückgesetzt werden muss.

## BMC-Switch mit der CLI aktualisieren

In dieser Vorgehensweise ist beschrieben, wie Sie das Netzwerkbetriebssystem auf Ihrem ThinkAgile SXM Serie BMC-Switch aktualisieren.

Gehen Sie zur Aktualisierung des BMC-Switches wie folgt vor:

- Schritt 1. Stellen Sie über die serielle Konsole des HLH eine Verbindung zum BMC-Switch her.
- Schritt 2. Melden Sie sich mit den Anmeldeinformationen `admin/<password>` beim BMC-Switch an.
- Schritt 3. Verwenden Sie die folgenden Befehle, um die neue Switch-Betriebssystem-Image-Datei vom Stammverzeichnis des USB-Sticks in den „image2“-Slot auf dem BMC-Switch und die neue Switch-Boot-Image-Datei in den „boot“-Slot auf dem BMC-Switch zu kopieren:

```
enable
configure terminal
usbcopy fromusb <ImageFileName>_OS.imgs image2
usbcopy fromusb <ImageFileName>_Boot.imgs boot
```

### Beispiel

```
Enter login username: admin
Enter login password:
...
BMC#enable
BMC#configure terminal
BMC(config)#usbcopy fromusb G8052-8.4.8.0_OS.imgs image2
Switch to be booted with image1. (Y/N) : Y
BMC(config)#usbcopy fromusb G8052-8.4.8.0_Boot.imgs boot
```

- Schritt 4. Führen Sie die folgenden Befehle aus, um beim Switch festzulegen, dass er mit dem neuen Betriebssystem-Image im „image2“-Slot und dem passenden Boot-Image neu startet, und überprüfen Sie diese Einstellung anschließend:

```
boot image image2
exit
show boot
```

### Beispiel

```
BMC(config)#boot image image2
BMC(config)#exit
BMC#show boot
Current running image version: 8.4.8
Currently set to boot software image2, active config block.
NetBoot: disabled, NetBoot tftp server: , NetBoot cfgfile:
Current boot Openflow protocol version: 1.0
USB Boot: disabled
Currently profile is default, set to boot with default profile next time.
Current FLASH software:
  image1: version 8.4.8, downloaded 08:04:14 Fri Jan 19, 2018
           NormalPanel, Mode Stand-alone
  image2: version 8.4.11, downloaded 22:20:41 Thu Jan 18, 2018
           NormalPanel, Mode Stand-alone
  boot kernel: version 8.4.11
               NormalPanel
  bootloader : version 8.4.11
Currently scheduled reboot time: none
```

Schritt 5. Bevor Sie den BMC-Switch neu starten, um die Änderungen anzuwenden, sollten Sie alle Ports am Switch herunterfahren. Führen Sie die folgenden Befehle aus, um alle Ports am BMC-Switch herunterzufahren:

```
configure terminal
interface port 1-52
shutdown
exit
```

Schritt 6. Werfen Sie den USB-Stick aus dem BMC-Switch aus und führen Sie die folgenden Befehle aus, um ihn neu zu starten:

```
System usb-eject
reload
```

Es wird eine Warnung angezeigt, da alle Ports in der aktuell ausgeführten Konfiguration heruntergefahren sind, was sich von der aktuellen Startkonfiguration unterscheidet. Geben Sie `y` ein und drücken Sie die Eingabetaste, um fortzufahren.

**Wichtig:** Sie dürfen die ausgeführte Konfiguration zu diesem Zeitpunkt noch NICHT speichern, da sonst alle Ports nach dem Switch-Neustart heruntergefahren bleiben.

Schritt 7. Sobald der Switch wieder online ist, melden Sie sich über die serielle Konsole am Switch an.

Schritt 8. Ziehen Sie den USB-Stick vom BMC-Switch ab.

Informationen zur ordnungsgemäßen Funktion des aktualisierten BMC-Switches finden Sie unter „[BMC-Switch-Funktionalität überprüfen](#)“ auf Seite 47. Nach abgeschlossener Überprüfung ist die Switch-Firmwareaktualisierung abgeschlossen.







**Lenovo**