

Lenovo

Lenovo Hardware Management Pack für Microsoft System Center Operations Manager Installations- und Benutzerhandbuch



Version 7.6.0

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter Anhang D „Hinweise“ auf Seite 65 gelesen werden.

Fünfzehnte Ausgabe (April 2019)

© Copyright Lenovo 2014, 2019.

Portions © Copyright IBM Corporation 1999, 2014

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

Informationen über diese

Veröffentlichung iii

Konventionen und Terminologie iii

Webressourcen iii

Kapitel 1. Übersicht 1

Produktmerkmale 1

Vorteile 6

Hard- und Softwareanforderungen des
Verwaltungsservers 7

 Hardwarevoraussetzungen 7

 Softwarevoraussetzungen 8

Der Lenovo Hardware Ordner im Operations
Manager 8

Lenovo Systemgruppen im Operations Manager 9

Kapitel 2. Lenovo Hardware Management Pack installieren 11

Lenovo Hardware Management Pack
installieren 11

 Daten von der PostgreSQL-Datenbank zur
 SQL Server-Datenbank migrieren 13

 Datenbankinformationen anzeigen. 13

Lenovo Hardware Management Pack
deinstallieren 13

Lenovo XClarity Integrator Service deinstallieren 14

Lenovo Hardware Management Pack
aktualisieren 15

Kapitel 3. Server über den XClarity Integrator Service verwalten. 17

Den XClarity Integrator Service konfigurieren 17

 Bei XClarity Integrator Service anmelden 17

 Operations Management-Server
 registrieren 18

 Kennwort des XClarity Integrator Service
 ändern 19

 Den XClarity Integrator Service neu starten 19

XClarity Integrator Service auf dem Operations
Manager Server überwachen 19

Hohe Verfügbarkeit des XClarity Integrator
Service 19

Den BMC-Knoten ermitteln 20

 BMC-Knotenermittlung und
 -Authentifizierung 20

 Automatische Ermittlung und
 Authentifizierung von BMC-Knoten 21

 Nur BMC von Servern verwalten, die bereits
 vom Operations Manager verwaltet werden 22

Aktualisieren von BMC-Knotendaten 22

Systemstatus überprüfen 23

Energieverbrauchsbeschränkung festlegen 23

Einen BMC-Knoten entfernen 24

Einen oder mehrere BMC-Knoten entfernen 24

Kapitel 4. Server über XClarity Administrator verwalten 25

XClarity Administrator konfigurieren 25

ThinkServer-Daten aktualisieren 26

Systemstatus überprüfen 26

Einen ThinkServer-Server entfernen 27

Kapitel 5. Gehäuse über SNMP verwalten 29

Den SNMP-Agenten konfigurieren 29

 SNMPv1-Agent auf dem BladeCenter-
 Gehäuse konfigurieren 29

 SNMP auf dem Flex System Gehäuse
 konfigurieren 30

Ein Gehäuse ermitteln 32

Gehäuse-Status überwachen 33

 Status des BladeCenter-Gehäuses
 überwachen 33

 Status des Flex System Gehäuses
 überwachen 34

Die neuesten Informationen zum Gehäuse
abrufen 35

AMM/CMM-Webkonsole starten 35

Einen Bladeserver oder Rechenknoten hoch- oder
herunterfahren 36

Ein ermitteltes Gehäuse entfernen 36

Kapitel 6. Server über IBM Platform Agent verwalten 37

Einen Lenovo Server ermitteln 37

Serverstatus überwachen 38

Energieverbrauchsdaten der Client System x-
Server anzeigen. 39

Energieverbrauchsbeschränkung festlegen 39

Energieverbrauchsschwellenwert festlegen 40

Die neuesten Informationen für die Lenovo Server
abrufen 40

Kapitel 7. Mit XClarity Integrator Service-Sicherheitszertifikaten arbeiten 41

BMC-Kommunikationsprotokoll festlegen 41

Zertifikate generieren und hochladen 41

Zertifikate neu generieren 42

 Serverzertifikat neu generieren 42

 Stammzertifikat neu generieren 43

Zertifikate herunterladen	43
Das Serverzertifikat herunterladen	43
Stammzertifikat herunterladen	44
Kapitel 8. Protokolldaten	45
Protokolle für den XClarity Integrator Service	45
Protokollierungsstufe festlegen	45
Protokolldateien erfassen	45
Protokolle für das Lenovo Hardware Management Pack	45
Protokollierungsstufe festlegen	45
Das Protokoll in der Windows-Ereignisanzeige anzeigen.	46
Kapitel 9. Fehlerbehebung	47
Fehlerbehebung nach Symptom	47
Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden	48

Lenovo XClarity Forum und Lenovo XClarity Ideation verwenden.	49
---	----

Anhang A. Funktionen zur barrierefreien Bedienung 51

Anhang B. Bewährte Verfahren 53

Die Ursache eines Fehlers bestimmen	53
Alle BladeCenters erneut erkennen	56
Einen umbenannten Server erneut erkennen	56

Anhang C. Systemfirewalleinstellungen. 59

Anhang D. Hinweise. 65

Marken	66
Wichtige Anmerkungen.	66

Informationen über diese Veröffentlichung

Diese Veröffentlichung enthält die Anweisungen zum Installieren von Lenovo® Hardware Management Pack für Microsoft® System Center Operations Manager (nachfolgend Lenovo Hardware Management Pack genannt) in Microsoft System Center Operations Manager (nachfolgend Operations Manager genannt) und zur Verwendung der integrierten Funktionen zur Verwaltung der Systeme in Ihrer Umgebung.

Konventionen und Terminologie

Absätze, die mit den fettgedruckten Begriffen **Hinweis** oder **Wichtig** beginnen, sind Hinweise mit bestimmten Bedeutungen, in denen Schlüsselinformationen hervorgehoben werden.

Anmerkung: Diese Bemerkungen bieten wichtige Tipps, Anleitungen oder Ratschläge.

Wichtig: Diese Bemerkungen enthalten Informationen oder Empfehlungen, die Ihnen dabei helfen können, unangenehme oder schwierige Situationen zu vermeiden.

In der folgenden Tabelle werden einige Begriffe, Akronyme und Abkürzungen beschrieben, die in diesem Dokument verwendet werden.

Begriff, Akronym oder Abkürzung	Bedeutung
BMC	Baseboard Management Controller ist ein Serviceprozessor, der Serviceprozessor-Funktionen und einen Videocontroller in einem einzigen Chip vereint.
CMM	Chassis Management Module verwaltet das Flex System Gehäuse.
AMM	Advanced Management Module verwaltet das BladeCenter®-Gehäuse.
SNMP	Simple Network Management Protocol.
(Lenovo) XClarity® Integrator (LXCI)	Eine Toolsuite, mit der IT-Administratoren die Verwaltungsfunktionen des System x in Microsoft System Center integrieren können.
(Lenovo) XClarity Integrator Service	Die Hintergrundkomponente von Lenovo XClarity Integrator, mit der der Lenovo XClarity Integrator auf Lenovo Server zugreifen und diese verwalten kann.
(Lenovo) XClarity Administrator (LXCA)	Eine Lösung für die zentrale Ressourcenverwaltung, die für eine einfachere Infrastrukturverwaltung, schnellere Antworten und eine bessere Verfügbarkeit der Serversysteme und Lösungen von Lenovo sorgt.
Operations Manager	Microsoft System Center Operations Manager.
Verwalteter Server oder verwalteter Knoten	Eine physische Maschine, die von Operations Manager verwaltet wird.

Webressourcen

Die folgenden Webseiten enthalten die Ressourcen zum Verständnis, zur Verwendung und zur Fehlerbehebung der BladeCenter-Gehäuse, der Flex System-Gehäuse, der ThinkServer®-Server, der ThinkSystem®-Server, der System x-Server und der Systemverwaltungstools.

Lenovo-Webseite für Microsoft Systems Management Solutions für Lenovo-Server

Diese Webseite ermittelt die neuesten Downloads für die XClarity Integrator-Angebote für Microsoft System Center-Verwaltungslösungen:

- [Webseite „Lenovo XClarity Integrator for Microsoft System Center“](#)

Systemverwaltung mit Lenovo XClarity-Lösungen

Diese Webseite bietet eine Übersicht über die Lenovo XClarity-Lösungen, die System x- und Flex System-Hardware integrieren, um Systemverwaltungsfunktionen bereitzustellen:

- [Webseite „System Management with Lenovo XClarity Solution“](#)

Lenovo XClarity Forum und Ideation

Die folgenden Webseiten stellen das Forum und die Ideation aller Lenovo XClarity-Produkte bereit:

- [Webseite „Lenovo XClarity Community Forum“](#)
- [Webseite „Lenovo XClarity Ideation“](#)

Lenovo Technical Support Portal

Diese Webseite hilft Ihnen, wenn Sie Unterstützung für Hardware und Software suchen:

- [Webseite „Lenovo Support Portal“](#)

Lenovo ServerProven

Diese Webseite enthält Informationen zur Hardwarekompatibilität mit Lenovo ThinkSystem-Servern, System x-Servern, BladeCenter-Servern und Flex System-Servern:

- [Webseite „Lenovo ServerProven Compatibility“](#)

Webseite „Microsoft System Center Operations Manager“

Diese Webseite bietet eine Übersicht über Microsoft System Center Operations Manager:

- [Webseite „Microsoft System Center Operations Manager“](#)

Kapitel 1. Übersicht

Das Lenovo Hardware Management Pack verwaltet den Integritätsstatus der ThinkSystem-Server, der System x-Server, die ThinkServer-Server, der BladeCenter-Gehäuse und der Flex System Gehäuse mit den erweiterten Funktionen des Operations Manager. Das Lenovo Hardware Management Pack bietet eine ganzheitliche Ansicht Ihrer IT-Infrastrukturen und minimiert die durch Hardwareprobleme verursachte Ausfallzeit.

Produktmerkmale

Das Lenovo Hardware Management Pack enthält die folgenden wichtigen Funktionen:

- Verwalten von System x-Servern, ThinkSystem-Servern, BladeCenter-Servern und Flex System-Servern über den XClarity Integrator Service (Out-of-band-Modus).
- Verwalten von ThinkServer-Servern über XClarity Administrator (Out-of-band-Modus).
- Verwalten des BladeCenter-Gehäuses und des Flex System Gehäuses über SNMP.
- Verwalten von System x-Servern, BladeCenter-Servern und Flex System-Servern mit installierten Windows® Betriebssystemen über IBM® Platform Agent (In-band-Modus).

Anmerkung: Der IBM Platform Agent unterstützt nicht die Verwaltung von ThinkSystem-Servern und anderen BMC-basierten Servern mit installiertem Windows 2016-Betriebssystem oder neueren Versionen. Daher wird nicht empfohlen, IBM Platform Agent zur Verwaltung von Servern zu verwenden.

Das Lenovo Hardware Management Pack enthält mehrere Management Packs. Die folgende Tabelle enthält die Namen, die IDs und die entsprechenden Hauptfunktionen der Management Packs.

Tabelle 1. Lenovo Hardware Management Pack Funktionsliste

Lenovo Hardware Management Pack		Hauptfunktionen			
Management Pack-Name	Management Pack-ID	Verwalten von System x-Servern, ThinkSystem-, BladeCenter- und Flex System-Servern über den XClarity Integrator Service (Out-of-band-Modus)	Verwalten von ThinkServer-Servern über XClarity Administrator (Out-of-band-Modus)	Verwalten von System x-, BladeCenter-, und Flex System-Servern über den IBM Platform Agent (In-band-Modus)	Verwalten des Flex System Gehäuses und des BladeCenter-Gehäuses über SNMP
Lenovo Hardware Management Pack – Allgemeine Bibliothek	Lenovo.HardwareMgmt-Pack.Common	√	√	√	√
Lenovo Hardware Management Pack – Hardware-ID-Bibliothek	Lenovo.HardwareMgmt-Pack.HardwareIDs			√	

Tabelle 1. Lenovo Hardware Management Pack Funktionsliste (Forts.)

Lenovo Hardware Management Pack – Beziehungsbibliothek	Lenovo. HardwareMgmt-Pack.Relation.v2			√	√
Lenovo Hardware Management Pack – Flex Beziehungsbibliothek	Lenovo. HardwareMgmt-Pack. RelationCMM.v2			√	√
Lenovo Hardware Management Pack für Integrated Management Module	Lenovo. HardwareMgmt-Pack.IMM2.v2	√			
Lenovo Hardware Management Pack für Gehäuse und Module des Lenovo BladeCenter Systems	Lenovo. HardwareMgmt-Pack. BladeCenter.v2				√
Lenovo Hardware Management Pack für Gehäuse und Module des Lenovo Flex Systems	Lenovo. HardwareMgmt-Pack. FlexSystem.v2				√
Lenovo Hardware Management Pack für Lenovo System x- und x86/x64 Blade-Systeme	Lenovo. HardwareMgmt-Pack.xSystems			√	

Tabelle 1. Lenovo Hardware Management Pack Funktionsliste (Forts.)

Lenovo Hardware Management Pack für ThinkServer BMC	Lenovo. ThinkServer. BMC.Module		√		
Lenovo Hardware Management Pack für den XClarity Integrator Service	Lenovo.XClarity. Integrator. Service.Module	√	√		

Anmerkungen:

- Das Lenovo Hardware Management Pack für Lenovo System x- und x86/x64 Blade-Systeme ist für die automatische BMC-Ermittlung und -Authentifizierungsfunktion erforderlich.
- Das Lenovo Hardware Management Pack für das Überschreiben der automatischen BMC-Ermittlung ist in der vorherigen Tabelle nicht enthalten. Es wird während der Laufzeit generiert.

Die folgende Tabelle enthält die unterstützten Servermodelle und Funktionen des Lenovo Hardware Management Pack.

Tabelle 2. Unterstützte Servermodelle und Funktionen

System	Servermodelle	Unterstützte Funktionen			
		Verwalten von System x-Servern, ThinkSystem-, BladeCenter- und Flex System-Servern über den XClarity Integrator Service (Out-of-band-Modus)	Verwalten von ThinkServer-Servern über XClarity Administrator (Out-of-band-Modus)	Verwalten von System x-, BladeCenter-, und Flex System-Servern über den IBM Platform Agent (In-band-Modus)	Verwalten des Flex System Gehäuses und des BladeCenter-Gehäuses über SNMP

Tabelle 2. Unterstützte Servermodelle und Funktionen (Forts.)

Lenovo ThinkSystem	<ul style="list-style-type: none"> • ST250 (7Y45, 7Y46) • ST258 (7Y47) • SR250 (7Y51, 7Y52, 7Y72, 7Y73) • SR258 (7Y53) • SR150 (7Y54) • SR158 (7Y55) • SD530 (7X20, 7X21, 7X22) • SN550 (7X16, 7X17) • SN850 (7X15) • SR530 (7X07, 7X08) • SR550 (7X03, 7X04) • SR570 (7Y02, 7Y03) • SR590 (7X98, 7X99) • SR630 (7X01, 7X02) • SR650 (7X05, 7X06) • SR850 (7X18, 7X19) • SR860 (7X69, 7X70) • SR950 (7X11, 7X12, 7X13) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) (nur China) 	√			
Lenovo System x	<ul style="list-style-type: none"> • x240 M5 (2591, 9532) • x3250 M6 (3633, 3943) • x3500 M5 (5464) • x3550 M4 (7914) • x3550 M5 (5463) • x3630 M4 (7158) • x3650 M4 (7915) • x3650 M5 (5462, 8871) • x3750 M4 (8753) • x3850 X6 (6241) • x3950 X6 (6241) • x440 (7167, 2590) 	√		√	
Lenovo Flex System	<ul style="list-style-type: none"> • x280, x480, x880 X6 Rechenknoten (7196, 4258) • x240 Rechenknoten (7162, 2588) 	√		√	
Lenovo NeXtScale System®	<ul style="list-style-type: none"> • sd350 M5 (5493) • nx360 M5 (5465) • nx360 M5 DWC (5467, 5468, 5469) 	√		√	
Lenovo ThinkServer	<ul style="list-style-type: none"> • RD350 • RD450 • RD550 • RD650 • RS160 • TD350 • TS460 		√		

Tabelle 2. Unterstützte Servermodelle und Funktionen (Forts.)

IBM-System x	<ul style="list-style-type: none"> • x3100 M4 (2582, 2586) • x3100 M5 (5457) • x3200 M2 (4367, 4368) • x3200 M3 (7327, 7328) • x3250 M2 (4190, 4191, 4194) • x3250 M3 (4251, 4252, 4261) • x3250 M4 (2583, 2587) • x3250 M5 (5458) • x3300 M4 (7382) • x3350 (4192, 4193) • x3400 M2 (7836, 7837) • x3400 M3 (7378, 7379) • x3450 (7948, 7949, 4197) • x3455 (7940, 7941) • x3500 M2 (7839) • x3500 M3 (7380) • x3500 M4 (7383) • x3530 M4 (7160) • x3550 (7978) • x3550 M2 (7946) • x3550 M3 (4254, 7944) • x3550 M4 (7914) • x3620 M3 (7376) • x3630 M3 (7377) • x3630 M4 (7158) • x3650 (7979) • x3650 M2 (7947) • x3650 M3 (4255, 7945) • x3650 M4 (7915) • x3650 M4 HD (5460) • x3650 T (7980, 8837) • x3655 (7985) • x3690 X5 (7147, 7148, 7149, 7192) • x3750 M4 (8722, 8733) • x3755 (7163, 8877) • x3755 M3 (7164) • x3850 M2 (7141, 7144, 7233, 7234) • x3850 X5 (7143, 7145, 7146, 7191) • x3850 MAX5 (7145, 7146) • x3950 M2 (7141, 7144, 7233, 7234) • x3950 X5 (7143, 7145, 7146) 	✓		✓	
--------------	--	---	--	---	--

Tabelle 2. Unterstützte Servermodelle und Funktionen (Forts.)

	<ul style="list-style-type: none"> • x3950 MAX5 (7145, 7146) • x3850 X6/x3950 X6 (3837, 3839) • iDataPlex dx360 M2 (6380, 7323, 7321) • iDataPlex dx360 M3 (6391) • iDataPlex dx360 M4 (7912, 7913) 				
IBM Flex System	<ul style="list-style-type: none"> • x240 Rechenknoten (7906, 2585) • x222 Rechenknoten (7916) • x240 Rechenknoten (8737, 8738, 7863) • x440 Rechenknoten (7917) 	√		√	
IBM BladeCenter	<ul style="list-style-type: none"> • HS12 (8014, 8028) • HS21 (8853) • HS22 (7870, 1911) • HS22V (7871) • HS23 (7875, 1929) • HS23E (8038, 8039) • HX5 (7872) • LS21 (7971) • LS22 (7901) • LS41 (7972) • LS42 (7902) 	√		√	
IBM NeXtScale	5455	√		√	
BladeCenter-Gehäuse	7967, 8677, 8852, 7989, 8886, 7779, 8720, 8730, 8740, 8750				√
Flex System-Gehäuse	7893, 8721, 8724				√

Vorteile

Im Folgenden sind die Vorteile des Lenovo Hardware Management Pack aufgelistet.

- Einfache Ermittlung des allgemeinen Integritätsstatus von Servern über den Ordner „Lenovo Windows System Group“.
- Überwachung des Gesamtenergieverbrauchs der System x-Server, der BladeCenter-Server und der Flex System-Server über das Energieverbrauchsdatendiagramm und Generierung von Alerts, wenn der Energieverbrauch vordefinierte Schwellenwerte überschreitet.
- Überwachung der Integrität der Gehäusemodule des BladeCenter-Gehäuses in der Windows Integritäts-Exploreransicht.
- Hoch- oder Herunterfahren eines Bladeservers oder Rechenknotens per Fernzugriff.
- Herunterfahren des auf einem Bladeserver oder Rechenknoten installierten Windows-Betriebssystems per Fernzugriff.

- Festlegen des maximalen Werts für die Energieverbrauchsbeschränkung und des Energieverbrauchsschwellenwerts.
- Starten einer CMM-Webkonsole des BladeCenter-Gehäuses und des Flex System Gehäuses.
- Automatisches Ermitteln und Verwalten von BMC-Knoten.
- Migrieren der Daten von der PostgreSQL-Datenbank zur SQL Server-Datenbank.
- Konfigurieren des XClarity Integrator-Service vom Operations Manager aus.
- Unterstützung für mehrere Operations Manager in derselben Verwaltungsgruppe.

Hard- und Softwareanforderungen des Verwaltungsservers

In diesem Abschnitt wird beschrieben, wie Sie bestimmen, ob ein Server vom Lenovo Hardware Management Pack als Verwaltungsserver unterstützt wird. Der Verwaltungsserver muss die folgenden Hard- und Softwareanforderungen erfüllen. Wenn der XClarity Integrator Service auf einem separaten System installiert ist, muss das System auch die folgenden Hardware- und Softwarevoraussetzungen erfüllen.

Hardwarevoraussetzungen

In diesem Thema sind die Hardwareanforderungen des Verwaltungsservers je nach Anzahl der verwalteten Server aufgelistet.

Verwaltung von bis zu 100 Lenovo Servern

	Minimum	Empfohlen
Prozessor	Prozessor mit vier Kernen und 2,66 GHz	Prozessor mit vier Kernen und 2,66 GHz
Hauptspeicher	16 GB	32 GB
Freier Festplattenspeicherplatz	20 GB	40 GB
Netzwerkkarte	100 Mb/s	10 Gb/s

Verwaltung von bis zu 300 Lenovo Servern

	Minimum	Empfohlen
Prozessor	Prozessor mit vier Kernen und 2,66 GHz	Prozessor mit acht Kernen und 2,66 GHz
Hauptspeicher	16 GB	64 GB
Freier Festplattenspeicherplatz	20 GB	40 GB
Netzwerkkarte	100 Mb/s	10 Gb/s

Verwaltung von bis zu 500 Lenovo Servern

	Minimum	Empfohlen
Prozessor	Prozessor mit vier Kernen und 2,66 GHz	Prozessor mit acht Kernen und 2,66 GHz
Hauptspeicher	32 GB	64 GB
Freier Festplattenspeicherplatz	20 GB	40 GB
Netzwerkkarte	100 Mb/s	10 Gb/s

Softwarevoraussetzungen

In diesem Thema sind die Softwareanforderungen des Verwaltungsservers aufgelistet.

- Microsoft .NET Framework v3.5
- Microsoft .NET Framework v4.5 oder höhere Versionen
- PowerShell 3.0 oder höhere Versionen
- Internet Explorer® 11 oder höher
- Um die SQL Server-Datenbank als Datenbank im XClarity Integrator Service zu verwenden, stellen Sie sicher, dass der SQL Server die folgenden Voraussetzungen erfüllt:
 - Version: SQL server 2008 R2 SP3 oder höhere Versionen
 - Authentifizierungsmodus: SQL Server und Windows Authentifizierungsmodus
 - Festplattengröße: 10 GB freier Speicher für 100 verwaltete Server, 30 GB freier Speicher für 500 verwaltete Server
 - CPU- und Hauptspeicher: Four-Core-Prozessor 2,66 GHz und 16 GB Speicher sind empfohlen

Anmerkung: Um eine Verbindung zu einem entfernten SQL-Server herzustellen, installieren Sie das Programm SQL-Client-tools-connectivity auf demselben Server, der mit dem XClarity Integrator Service installiert ist. Dieses Programm ist im Installationsabbild des SQL-Servers verfügbar.

- Um die PostgreSQL-Datenbank als Datenbank im XClarity Integrator Service zu verwenden, stellen Sie sicher, dass der PostgreSQL-Server die folgenden Voraussetzungen erfüllt:
 - Version: 9.2, 9.3, 9.4, 9.5, 9.6, 10.6 oder 11.1
 - Festplattengröße: 10 GB freier Speicher für 100 verwaltete Server, 30 GB freier Speicher für 500 verwaltete Server
 - CPU- und Hauptspeicher: Four-Core-Prozessor 2,66 GHz und 16 GB Speicher sind empfohlen

Unterstützte Versionen von Operations Manager

Die folgenden Versionen von Operations Manager werden unterstützt:

- Microsoft System Center Operations Manager 2019
- Microsoft System Center Operations Manager 2016
- Microsoft System Center Operations Manager 2012
- Microsoft System Center Operations Manager 2012 R2
- Microsoft System Center Operations Manager 2012 SP1

Unterstützte Windows-Betriebssysteme für den Verwaltungsserver

Die folgenden Windows-Betriebssysteme werden für den Verwaltungsserver unterstützt:

- Windows 2008 R2 oder höher
- Windows Server 2012 SP1, R2
- Windows Server 2016
- Windows Server 2019

Der Lenovo Hardware Ordner im Operations Manager

Das Lenovo Hardware Management Pack fügt dem Operations Manager den Ordner Lenovo Hardware hinzu. Dieser Ordner stellt aktive Alerts, Taskstatus und Gesamtziele für alle ermittelten Lenovo Server und Hardwarekomponenten bereit.

Der Ordner Lenovo Hardware enthält die folgenden Ansichten und Ordner:

- **Ansichten:**

- **Lenovo System x und ThinkSystem BMC:** Diese Ansicht stellt den Status der BMC-basierten Server (außer der ThinkServer-Server) bereit.
 - **Lenovo ThinkServer BMC:** Diese Ansicht stellt den Status der ThinkServer Server bereit.
 - **Lenovo ThinkServer Windows-Computer:** Diese Ansicht stellt den Status der ThinkServer-Server, die gleichzeitig die zwei folgenden Voraussetzungen erfüllen, bereit:
 - Das Windows-Betriebssystem ist installiert.
 - Ermittelt vom Microsoft System Center Operations Manager 2007 Ermittlungs-Assistenten (nachfolgend Ermittlungsassistent genannt).
 - **Lenovo Windows System Group (Lenovo Windows-Systemgruppe):** Diese Ansicht zeigt den Status der BMC-basierten Server an, auf denen das Windows-Betriebssystem installiert ist.
- **Ordner:**
 - **Lenovo BladeCenter(s) and Modules (Lenovo BladeCenter und Module):** Dieser Ordner enthält die aktiven Alerts, den Task-Status, den Status der Windows-Computer, der das BladeCenter-Gehäuse verwalten und den allgemeinen Status aller BladeCenter-Gehäuse. Der Unterordner „Lenovo BladeCenter Module“ unter diesem Ordner enthält die zusammengefassten Ansichten von Blade-, Gehäuse-, Kühlungsmodulen, E/A-Modulen, Verwaltungsmodulen, Einschubmodulen, Stromversorgungsmodulen und Speichermodulen.
 - **Lenovo Flex System Chassis and Modules (Gehäuse und Module des Lenovo Flex Systems):** Dieser Ordner enthält die aktiven Alerts, den Task-Status, den Status der Windows-Computer, die das Flex System Gehäuse verwalten und den allgemeinen Status aller Flex System Gehäuse. Der Unterordner „Lenovo Flex System Chassis and Modules (Gehäuse und Module des Lenovo Flex Systems)“ unter diesem Ordner enthält die zusammengefassten Ansichten von Rechenknoten, Kühlungsmodulen, Mux-Lüfter-Modulen, FSM, E/A-Modulen, Verwaltungsmodulen, Stromversorgungsmodulen, Rückseiten-LED-Modulen und Speichermodulen.
 - **Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC):** Dieser Ordner enthält die zusammengefassten Ansichten von aktiven Alerts, Kühlgeräten, Fibre Channel, Firmware/VPD, InfiniBand, Netzwerkadaptern, numerischen Sensoren, PCI-Einheiten, physischen Speichern, Prozessoren und RAID-Controllern für Lenovo BMC-basierte Server (außer der ThinkServer-Server).
 - **Lenovo ThinkServer BMC:** Dieser Ordner enthält die zusammengefassten Ansichten von aktiven Alerts, Kühlgeräten, Fibre Channel, Firmware/VPD, InfiniBand, numerischen Sensoren, PCI-Einheiten, physischen Speichern und Prozessoren für die ThinkServer-Server.
 - **Lenovo Windows System Group (Lenovo Windows-Systemgruppe):** Dieser Ordner enthält die zusammengefassten Ansichten der BMC-basierten Server, auf denen das Windows-Betriebssystem installiert ist. Diese Server sind nach Typen, z. B. Tower, Rack, Blade, Enterprise Server usw. gruppiert. Die Hardwarekomponenten des Ordners „Lenovo Windows System Servers“ unter diesem Ordner enthalten die zusammengefassten Ansichten von Lüftern, Management-Controllern, Netzwerkadaptern, physischen Speichern, physischen Prozessoren, Netzteilen, Speichern (nicht spezifischen), Speichern (ServeRAID-8x/7x/6x), Speichern (ServeRAID-BR oder integrierte RAID), Speicher (ServeRAID-MR oder MegaRAID), Temperatursensoren, Spannungssensoren und nicht klassifizierter Hardware.
 - **Lenovo XClarity Integrator Service:** Dieser Ordner enthält die Zusammenfassung des Lenovo XClarity Integrator Service.

Lenovo Systemgruppen im Operations Manager

Das Lenovo Hardware Management Pack definiert einige Lenovo Systemgruppen im Operations Manager. Sie finden die Gruppen, indem Sie **Authoring (Erstellung) → Groups (Gruppen)** auswählen.

- **Lenovo Windows System Group (Lenovo Windows-Systemgruppe):** Diese Gruppe enthält die Server, auf denen das Windows-Betriebssystem installiert ist.

- **Lenovo System x and ThinkSystem Group (Lenovo System x und ThinkSystem Gruppe):** Diese Gruppe enthält die System x-Server und die ThinkSystem-Server.
- **Lenovo ThinkServer Group (Lenovo ThinkServer Gruppe):** Diese Gruppe enthält die ThinkServer-Server.
- **Lenovo Flex System Chassis Group (Lenovo Flex System Gehäusegruppe):** Diese Gruppe enthält die Flex System Gehäuse.
- **Lenovo BladeCenter Chassis Group (Lenovo Flex System-BladeCenter-Gruppe):** Diese Gruppe enthält die BladeCenter-Gehäuse.

Kapitel 2. Lenovo Hardware Management Pack installieren

In diesem Abschnitt wird beschrieben, wie Sie das Lenovo Hardware Management Pack installieren, aktualisieren und deinstallieren.

Lenovo Hardware Management Pack installieren

Im folgenden Verfahren wird beschrieben, wie Sie das Lenovo Hardware Management Pack installieren.

Vorbereitende Schritte

Stellen Sie vor dem Installieren des Lenovo Hardware Management Packs Folgendes sicher:

- Der aktuelle Benutzer hat Administratorrechte.
- Die Firewall blockiert nicht die Netzwerkanschlüsse des XClarity Integrator Service (Standardwert: 9500). Weitere Informationen finden Sie im Abschnitt Anhang C „Systemfirewalleinstellungen“ auf Seite 59.
- Wenn Sie beabsichtigen, XClarity Integrator Service auf separaten Systemen zu installieren, stellen Sie sicher, dass das System und Operations Manager sich in der gleichen Domäne befinden.

Um das Lenovo Hardware Management Pack erfolgreich zu installieren, stellen Sie sicher, dass die Management Packs für den Operations Manager die in der folgenden Tabelle aufgeführten Versionsanforderungen erfüllen.

Tabelle 3. Versionsanforderungen für die Management Packs von Operations Manager

Management Pack-Name	Management Pack-ID	Management Pack
Statusbibliothek	System.Health.Library	6.0.5000.0 oder höher
Systembibliothek	System.Library	6.0.5000.0 oder höher
Leistungsbibliothek	System.Performance.Library	6.0.5000.0 oder höher
SNMP-Bibliothek	System.Snmp.Library	6.0.6278.0 oder höher
Data Warehouse-Bibliothek	Microsoft.SystemCenter. Datawarehouse.Library	6.0.6278.0 oder höher
System Center-Kernbibliothek	Microsoft.SystemCenter.Library	6.0.5000.0 oder höher
Netzwerkeinheit-Bibliothek	System.NetworkManagement.Library	7.0.8107.0 oder höher
Windows-Kernbibliothek	Microsoft.Windows.Library	6.0.5000.0 oder höher

Vorgehensweise

Schritt 1. Laden Sie das Lenovo Hardware Management Pack-Installationsprogramm von der [XClarity Integrator-Downloadseite](#) herunter.

Schritt 2. Doppelklicken Sie auf die Installationsdatei. Der Begrüßungsbildschirm wird angezeigt.

Schritt 3. Lesen Sie die Lizenzvereinbarung, wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen von Lenovo und alle weiteren Bedingungen** aus und klicken Sie auf **Weiter**.

Schritt 4. Wählen Sie die zu installierenden Komponenten aus:

- **Lenovo Hardware Management Pack für Microsoft SCOM**

Diese Komponente umfasst das Management Pack und andere unterstützte Tools und sollte auf jedem SCOM-Server und jeder SCOM-Konsole installiert werden, mit der Sie zu arbeiten beabsichtigen.

- **Lenovo XClarity Integrator Service**

Lenovo XClarity Integrator Service ist in dieser Komponente enthalten. Er kann auf dem SCOM-Server oder auf einem separaten Windows-Betriebssystem installiert werden.

Anmerkung: In einer Managementgruppe wird nur eine XClarity Integrator Service-Instanz benötigt.

Schritt 5. Installieren Sie das Paket gemäß den Eingabeaufforderungen im Installationsassistenten.

Schritt 6. Installieren Sie das Hardware Management Pack, wenn es in Schritt 4 ausgewählt wurde.

Schritt 7. Installieren Sie den XClarity Integrator Service, wenn er in Schritt 4 ausgewählt wurde, und legen Sie das Passwort und den Netzwerkport (Standardwert: 9500) des XClarity Integrator Service fest. Konfigurieren Sie dann die Datenbank.

- **SQL-Server-Datenbank**

Geben Sie auf der Seite „SQL Server configuration (SQL Server-Konfiguration)“ den SQL Server-Namen (mit Port) ein, stellen Sie die Windows-Authentifizierung oder den SQL Server-Anmeldeaccount bereit und klicken Sie dann auf **Next** (Weiter). Der SQL Server-Name kann ein Computernamen oder eine IP-Adresse sein. Der Standardport ist 1433.

Anmerkungen:

- Bevor Sie den XClarity Integrator Service installieren, stellen Sie sicher, dass Sie die Windows-Authentifizierung und die SQL-Server-Authentifizierung auf dem SQL-Server aktivieren.
- Während der Datenbankkonfiguration ist eine Windows-Authentifizierung oder ein SQL-Server-Anmeldekonto erforderlich, damit Sie über den XClarity Integrator Service eine Datenbank und ein neues Anmeldekonto erstellen können, um die Datenbank auf dem SQL-Server zu verwalten. Stellen Sie sicher, dass das angegebene Konto über ausreichende Berechtigungen verfügt, um sich am SQL-Server anzumelden und Datenbanken und Benutzerkonten auf dem SQL-Server zu erstellen. Die Anmeldeinformationen des neuen Kontos werden in der Konfigurationsdatei des Lenovo XClarity Integrator Service gespeichert.
- Um eine Verbindung zu einem entfernten SQL-Server herzustellen, installieren Sie das Programm SQL-Client-tools-connectivity auf demselben Server, der mit dem XClarity Integrator Service installiert ist. Dieses Programm ist im Installationsabbild des SQL-Servers verfügbar.

- **PostgreSQL-Datenbank**

Geben Sie auf der PostgreSQL-Konfigurationsseite den PostgreSQL-Benutzernamen, das Passwort und den Port ein. Klicken Sie anschließend auf **Next** (Weiter).

Anmerkungen:

- Bevor Sie die PostgreSQL-Datenbank konfigurieren, stellen Sie sicher, dass eine lokale PostgreSQL-Datenbank auf demselben Server installiert ist, der mit dem XClarity Integrator Service installiert ist.
- Wenn Sie eine PostgreSQL-Datenbank verwenden und auf dem gleichen Windows-Betriebssystem zu einer SQL-Server-Datenbank wechseln möchten, können Sie die Daten aus der PostgreSQL-Datenbank in die SQL-Server-Datenbank migrieren. Informationen hierzu finden Sie im Abschnitt „Daten von der PostgreSQL-Datenbank zur SQL Server-Datenbank migrieren“ auf Seite 13.

Schritt 8. Importieren Sie die Management Packs auf den Operations Manager entsprechend den Eingabeaufforderungen im Installationsassistenten.

Anmerkungen:

- Die Management Packs werden automatisch aktualisiert.
- Wenn der Importvorgang fehlgeschlagen ist, entfernen Sie die alten Management Packs aus dem Operation Manager und importieren Sie die neuen Management Packs manuell. Standardmäßig werden die Management Packs im Ordner %Program Files%\Lenovo \Lenovo Hardware Management Pack\Management Packs installiert.

Schritt 9. Klicken Sie auf **Finish** (Fertigstellen).

Schritt 10. Starten Sie die Operations Manager-Konsole neu, wenn Sie sie während des Setups geöffnet haben.

Daten von der PostgreSQL-Datenbank zur SQL Server-Datenbank migrieren

Im folgenden Verfahren wird beschrieben, wie Sie die Daten von der PostgreSQL-Datenbank auf die SQL-Serverdatenbank migrieren.

Stellen Sie sicher, dass die PostgreSQL-Datenbank und der XClarity Integrator Service auf demselben Windows-System installiert sind.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie links auf der Seite auf die Registerkarte **Migrate Data (Daten migrieren)**.

Schritt 3. Klicken Sie auf **Migrate Data (Daten migrieren)**.

Schritt 4. Klicken Sie auf **OK**. Der Migrationsprozess startet.

Schritt 5. Klicken Sie erneut auf **OK**, sobald der Migrationsprozess abgeschlossen ist.

Anmerkungen:

- Deinstallieren Sie die PostgreSQL-Datenbank nicht und löschen Sie nicht die Konfigurationsdatei des XClarity Integrator Service, bevor die Datenmigration abgeschlossen ist.
- Die alten Daten in der SQL Server-Datenbank werden nach dem Migrationsprozess mit den migrierten Daten überschrieben.

Datenbankinformationen anzeigen

Im folgenden Verfahren wird beschrieben, wie Sie die Datenbankinformationen anzeigen.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Um die Datenbankinformationen anzuzeigen, klicken Sie im linken Navigationsbereich auf die Registerkarte **Database Information (Datenbankinformationen)**.

Lenovo Hardware Management Pack deinstallieren

Im folgenden Verfahren wird beschrieben, wie Sie das Lenovo Hardware Management Pack deinstallieren.

Vorbereitende Schritte

Stellen Sie vor dem Deinstallieren des Lenovo Hardware Management Pack vom Verwaltungsserver sicher, dass sich der Verwaltungsserver, auf dem das Lenovo Hardware Management Pack installiert ist, im Wartungsmodus befindet.

Vorgehensweise

- Schritt 1. Klicken Sie auf den Windows-Betriebssystem auf **Control Panel (Systemsteuerung) → Uninstall a program (Programme deinstallieren)**. Die Seite **Uninstall or change a program (Programme deinstallieren oder ändern)** wird geöffnet.
- Schritt 2. Klicken Sie mit der rechten Maustaste auf **Lenovo Hardware Management Pack**, und klicken Sie auf **Uninstall** (Deinstallieren).
- Schritt 3. Löschen Sie Lenovo Management Packs aus Operations Manager. Überspringen Sie diesen Schritt, wenn Sie das Lenovo Hardware Management Pack auf eine neue Version aktualisieren möchten.

Lenovo XClarity Integrator Service deinstallieren

Im folgenden Verfahren wird beschrieben, wie Sie den Lenovo XClarity Integrator Service deinstallieren.

Vorbereitende Schritte

Bevor Sie Lenovo XClarity Integrator Service deinstallieren, sollten Sie sicherstellen, dass sich der Verwaltungsserver mit installiertem Lenovo XClarity Integrator Service im Wartungsmodus befindet.

Vorgehensweise

- Schritt 1. Klicken Sie auf den Windows-Betriebssystem auf **Control Panel (Systemsteuerung) → Uninstall a program (Programme deinstallieren)**. Die Seite **Uninstall or change a program (Programme deinstallieren oder ändern)** wird geöffnet.
 - Schritt 2. Klicken Sie mit der rechten Maustaste auf **Lenovo XClarity Integrator Service** und klicken Sie auf **Uninstall** (Deinstallieren).
- Anmerkung:** Für Lenovo Hardware Management Pack v7.3.0 oder frühere Versionen lautet der Name der Anwendung „Lenovo XClarity Integrator Unified Service“.
- Schritt 3. Klicken Sie mit der rechten Maustaste auf **PostgreSQL database (PostgreSQL Datenbank)**, und klicken Sie auf **Uninstall** (Deinstallieren).
 - Schritt 4.

Anmerkung: Überspringen Sie diesen Schritt, wenn Sie auf eine neue Version aktualisieren möchten.

Falls erforderlich, löschen Sie alle Daten dauerhaft wie folgt:

- a. Löschen Sie die Datenbankdateien:
 - Für die SQL-Server-Datenbank löschen Sie die %hostname%\XCIDB-Datenbank aus dem SQL-Server.
 - Für die PostgreSQL-Datenbank löschen Sie den %USERPROFILE%\postgresql_data-Ordner auf Windows 2012 oder einer früheren Version bzw. den %SystemDrive%\ProgramData\Lenovo\postgresql_data-Ordner aus Windows 2016 oder einer höheren Version.
- b. Löschen Sie den Anwendungsordner %SystemDrive%\Program Files (x86)\Lenovo\Lenovo XClarity Integrator XClarity Integrator Service.

- c. Löschen Sie die Konfigurationsdateien im Ordner %SystemDrive%\ProgramData\Lenovo\LXCI\UUS.

Lenovo Hardware Management Pack aktualisieren

Zum Aktualisieren des Lenovo Hardware Management Pack müssen Sie es zuerst deinstallieren und anschließend die aktualisierte Version installieren.

Vorbereitende Schritte

Stellen Sie vor der Aktualisierung des Lenovo Hardware Management Pack sicher, dass sich der Verwaltungsserver, auf dem das Lenovo Hardware Management Pack installiert ist, in Wartungsmodus befindet.

Anmerkung: Nur Lenovo Hardware Management Pack v6.3.0 und höher wird unterstützt.

Vorgehensweise

Schritt 1. Deinstallieren Sie das Lenovo Hardware Management Pack. Siehe „Lenovo Hardware Management Pack deinstallieren“ auf Seite 13.

Anmerkung: Lenovo Management Packs sollten nicht aus Operations Manager gelöscht werden.

Schritt 2. Deinstallieren Sie Lenovo XClarity Integrator Service. Siehe „Lenovo XClarity Integrator Service deinstallieren“ auf Seite 14.

Anmerkung: Der Ordner %SystemDrive%\ProgramData\Lenovo\LXCI\UUS und die Datenbankdateien sollten nicht gelöscht werden.

Schritt 3. Installieren Sie das aktualisierte Lenovo Hardware Management Pack und Lenovo XClarity Integrator Service auf dem Verwaltungsserver.

Anmerkung: Für die aktualisierte Version und die vorherige Version von Lenovo XClarity Integrator Service ist dasselbe Windows-Betriebssystem erforderlich.

Kapitel 3. Server über den XClarity Integrator Service verwalten

Das Lenovo Hardware Management Pack unterstützt die Verwaltung von BMC-basierten Servern über den XClarity Integrator Service im Out-of-band-Modus, einschließlich der Systems x-Server, der ThinkSystem-Server, der BladeCenter-Server und der Flex System-Server.

Das Lenovo Hardware Management Pack bietet die folgenden Funktionen:

- Ermittlung und Authentifizierung der BMC-basierten Server
- Überwachung des Status der BMC-basierten Server und Anzeige der Ereignisse und Alerts
- Abrufen und Anzeige von Informationen zu den BMC-basierten Servern
- Verwalten der Energieverbrauchsbeschränkung
- Bereitstellung einer Option zum Löschen der BMC-basierten Server
- Unterstützung für mehrere Operations Manager in derselben Verwaltungsgruppe

Vorbereitende Schritte

Bevor Sie beginnen, stellen Sie Folgendes sicher:

- Der BMC-Zielknoten ist mit Port 5988 (HTTP) oder Port 5989 (HTTPS) über das CIM-Protokoll verbunden.
- Es gibt vier Services von Lenovo XClarity Integrator Service:
 - Lenovo XClarity Integrator-Verwaltungs-Webservice
 - Lenovo XClarity Integrator-Überwachung
 - Lenovo XClarity Integrator-Server
 - Lenovo XClarity Integrator-Service Starter
- Die Firewall blockiert nicht den Netzwerkport des XClarity Integrator Service (Standardwert: 9500) vom BMC-Knoten zum XClarity Integrator Service und vom Operations Manager bzw. von der Konsole zum XClarity Integrator Service.

Unterstützte Servermodelle

Siehe die Spalte „Manage System x, ThinkSystem, BladeCenter, and Flex System servers through XClarity Integrator Service (out-of-band mode)“ (Verwalten von System x-Servern, ThinkSystem-, BladeCenter- und Flex System-Servern über den XClarity Integrator Service (Out-of-band-Modus)) in Tabelle 2 „Unterstützte Servermodelle und Funktionen“ auf Seite 3.

Den XClarity Integrator Service konfigurieren

Zum Überwachen der BMC-basierten Server müssen Sie zunächst den XClarity Integrator Service konfigurieren. In diesem Abschnitt wird beschrieben, wie Sie den XClarity Integrator Service konfigurieren. Weitere Informationen hierzu finden Sie unter [Lenovo XClarity Integrator Service](#).

Bei XClarity Integrator Service anmelden

Im folgenden Verfahren wird beschrieben, wie Sie sich beim Lenovo XClarity Integrator Service anmelden.

Vorgehensweise

Schritt 1. Klicken Sie im **Start Menu (Startmenü) → Lenovo XClarity Integrator → Lenovo XClarity Integrator Management (Lenovo XClarity Integrator-Verwaltung)**.

Schritt 2. Führen Sie einen der folgenden Schritte aus:

- Melden Sie sich mit dem Benutzernamen und dem Kennwort des XClarity Integrator Service an, die während des Installierens generiert werden.
- Melden Sie sich von der Operations Manager-Konsole aus beim XClarity Integrator Service an.
 1. Öffnen Sie die Operations Manager-Konsole.
 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.
 3. Klicken Sie im Bereich **Task** auf **(Lenovo) XClarity Integrator Management ((Lenovo) XClarity Integrator-Verwaltung)**.
 4. Melden Sie sich mit dem Benutzernamen und dem Kennwort des XClarity Integrator Service an, die während des Installierens generiert werden.

Operations Management-Server registrieren

Im folgenden Verfahren wird beschrieben, wie Sie Operations Management Server registrieren.

Um mit Operations Management Server arbeiten zu können, sollten Sie den Verwaltungsserver in XClarity Integrator Service registrieren.

Sobald ein Verwaltungsserver registriert ist, führt XClarity Integrator Service automatisch alle Verwaltungsserver in derselben Verwaltungsgruppe auf. XClarity Integrator Service ist mit jeweils einem Verwaltungsserver verbunden. Wenn der verbundene Verwaltungsserver nicht mehr reagiert, stellt XClarity Integrator Service automatisch eine Verbindung mit einem anderen Verwaltungsserver her, der online ist.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Siehe „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie im Fenster **Lenovo XClarity Integrator Management** (Lenovo XClarity Integrator-Verwaltung) im linken Bereich auf **Management Server** (Verwaltungsserver).

Schritt 3. Führen Sie einen der folgenden Schritte aus:

- Wenn XClarity Integrator Service auf demselben Windows-Betriebssystem wie der Verwaltungsserver installiert ist, wird der Verwaltungsserver automatisch registriert. Andere Verwaltungsserver in derselben Verwaltungsgruppe sind in der Tabelle aufgeführt.
- Wenn XClarity Integrator Service auf einem anderen Windows-Betriebssystem als der Verwaltungsserver installiert ist, klicken Sie auf **Register** (Registrieren), um den Verwaltungsserver zu registrieren.

Schritt 4. Wählen Sie den Verwaltungsserver aus und klicken Sie auf **Credentials** (Anmeldeinformationen), um die Anmeldeinformationen gegebenenfalls zu bearbeiten.

Schritt 5. Der Verwaltungsserver, der mit XClarity Integrator Service verbunden ist, ist als **current** (aktuell) markiert. Wenn Sie mit einem anderen Verwaltungsserver eine Verbindung herstellen möchten, können Sie den Verwaltungsserver auswählen und auf **current** (aktuell) klicken.

Schritt 6. Klicken Sie auf **Refresh** (Aktualisieren), um den aktuellen Verwaltungsserverstatus anzuzeigen.

Anmerkung: Verbinden Sie nicht dieselbe Verwaltungsgruppe von verschiedenen XClarity Integrator Services, wenn es mehrere XClarity Integrator Services gibt.

Kennwort des XClarity Integrator Service ändern

Im folgenden Verfahren wird beschrieben, wie Sie das Kennwort des XClarity Integrator Service ändern.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie im Fenster **Lenovo XClarity Integrator Service** oben rechts auf **Change Password (Kennwort ändern)**.

Schritt 3. Geben Sie das vorhandene Kennwort und das neue Kennwort ein.

Anmerkung: Das neue Kennwort muss den Kennwortregeln entsprechen.

Schritt 4. Klicken Sie auf **Change (Ändern)**.

Den XClarity Integrator Service neu starten

Im folgenden Verfahren wird beschrieben, wie Sie den XClarity Integrator Service neu starten.

Starten Sie die folgenden vier Dienste neu, um den Lenovo XClarity Integrator Service neu zu starten:

- Lenovo XClarity Integrator-Verwaltungs-Webservice
- Lenovo XClarity Integrator-Überwachung
- Lenovo XClarity Integrator-Server
- Lenovo XClarity Integrator-Service Starter

XClarity Integrator Service auf dem Operations Manager Server überwachen

Die folgende Vorgehensweise beschreibt, wie Sie den XClarity Integrator Service auf dem Operations Manager Server überwachen.

Vorbereitende Schritte

Bevor Sie den XClarity Integrator Service im Operations Manager Server überwachen, stellen Sie Folgendes sicher:

- Die Lenovo Hardware Management Packs wurden in Operations Manager importiert.
- Der Operations Manager-Server wurde beim XClarity Integrator Service registriert.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware → Lenovo XClarity Integrator Service**.

Schritt 3. Zeigt den Status des XClarity Integrator Service an, der mit dem Operations Manager-Server verbunden ist.

Hohe Verfügbarkeit des XClarity Integrator Service

Wenn hohe Verfügbarkeit für den XClarity Integrator Service verlangt wird, wird Windows oder VMWare HA-Technologie nicht empfohlen. Im folgenden Verfahren wird beschrieben, wie Sie XClarity Integrator Service mit Windows HA-Technologie unterstützen.

Vorgehensweise

- Schritt 1. Bereiten Sie die Windows HA Umgebung vor und richten Sie zwei Hosts mit Hyper-v-FailOver-Cluster ein. Stellen Sie sicher, dass die beiden Hosts denselben Speicher verwenden.
- Schritt 2. Erstellen Sie eine virtuelle Windows-Maschine im gemeinsam genutzten Speicher.
- Schritt 3. Installieren Sie XClarity Integrator Service separat auf der virtuellen Maschine.
- Schritt 4. Konfigurieren und registrieren Sie Operations Manager auf dem XClarity Integrator-Service.

Anmerkungen:

- Wenn der Host verwaltet werden muss, kann die virtuelle Maschine mit installiertem XClarity Integrator Service auf einen anderen Host migriert werden.
- Wenn der Host nicht mehr reagiert und Fehler anzeigt, wird die virtuelle Maschine mit installiertem XClarity Integrator Service automatisch auf einem anderen Host neu gestartet.
- Ausführliche Informationen zum Einrichten der HA-Umgebung finden Sie in der Dokumentation zur Windows/VMWare HA-Technologie.

Den BMC-Knoten ermitteln

Nach der Konfiguration des XClarity Integrator Service können Sie den BMC-Knoten ermitteln. In diesem Abschnitt wird beschrieben, wie Sie den BMC-Knoten ermitteln.

BMC-Knotenermittlung und -Authentifizierung

Im folgenden Verfahren wird beschrieben, wie Sie den BMC-Knoten vom Verwaltungsserver ermitteln und authentifizieren.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.
- Schritt 3. Klicken Sie im Bereich **Task** (Aufgabe) auf der rechten Seite auf **(Lenovo) Discover/Authenticate BMC** ((Lenovo) BMC ermitteln/authentifizieren). Die Seite **BMC Discovery** (BMC-Ermittlung) wird geöffnet.
- Schritt 4. Melden Sie sich beim XClarity Integrator Service an. In der Regel sind der XClarity Integrator Service und der Operations Manager auf dem gleichen Server installiert.
- Schritt 5. Machen Sie in folgenden Feldern die erforderlichen Angaben:
 - **Host:** Dies ist die Adresse des Lenovo XClarity Integrator Service.
 - **Port:** Dies ist die Portnummer vom Lenovo XClarity Integrator Service, die bei der Installation festgelegt wird. Der Standardwert lautet 9500.
 - **Password (Kennwort):** Dies ist das Kennwort vom Lenovo XClarity Integrator Service, das bei der Installation festgelegt wird.
- Schritt 6. Wenn eine Zertifikatwarnung angezeigt wird, klicken Sie auf **Next (Weiter)**, um dieses Zertifikat als vertrauenswürdig einzustufen.

Anmerkung: Wenn Sie dem Zertifikat nicht vertrauen, wird ein Alert angezeigt, der auf ein Problem mit dem Sicherheitszertifikat der Webseite hinweist. Klicken Sie auf **Continue (Fortfahren)**, um diesen Alert zu überspringen.
- Schritt 7. Wählen Sie in der BMC-Ermittlungsliste einen BMC Knoten aus, der ermittelt werden soll, geben Sie die Adresse oder den Adressbereich in das Feld **IP Address (IP-Adresse)** ein, und klicken Sie auf **Add (Hinzufügen) → OK**.

Anmerkung: Der Ermittlungsvorgang kann einige Minuten dauern.

Schritt 8. Wählen Sie einen BMC-Knoten aus, der authentifiziert werden soll, und klicken Sie auf **Authenticate (Authentifizieren)**.

Schritt 9. Geben Sie im Eingabeaufforderungsfenster den Benutzernamen und das Kennwort ein und klicken Sie auf **OK**.

Anmerkung: Wenn Sie zweimal den falschen Benutzernamen oder das falsche Kennwort eingeben, wird der Account für einen bestimmten Zeitraum gesperrt.

Schritt 10. Klicken Sie auf **Monitor (Überwachen) → Lenovo Hardware → Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC)**. Der neue BMC-Knoten wird im Operations Manager angezeigt.

Anmerkung: Dieser Vorgang kann einige Minuten dauern.

Automatische Ermittlung und Authentifizierung von BMC-Knoten

Das Lenovo Hardware Management Pack kann den BMC Knoten automatisch ermitteln und authentifizieren, wenn der Zielservers von Operations Manager verwaltet wird.

Anmerkungen:

- Die automatische Ermittlung und Authentifizierung von BMC-Knoten ist für Flex System-Server und BladeCenter-Server nicht zugänglich.
- In der IPv6-Umgebung ist die automatische Ermittlung und Authentifizierung von BMC-Knoten nur für ThinkSystem-Server zugänglich. Die unterstützten Lenovo ThinkSystem-Servermodelle finden Sie unter Tabelle 2 „Unterstützte Servermodelle und Funktionen“ auf Seite 3.
- Standardmäßig ist die automatische Ermittlung und Authentifizierung von BMC-Knoten deaktiviert.

Vorbereitende Schritte

Stellen Sie Folgendes sicher, bevor Sie die automatische Ermittlungs- und Authentifizierungsfunktion für BMC-Knoten verwenden:

- Windows 2008 oder höher, PowerShell 3.0 oder eine neuere Version und .NET 4.5 oder eine neuere Version sind auf dem Zielservers installiert.
- Der Server wird von Operations Manager verwaltet.
- Der BMC-Knoten ist verbunden, und **IPMI over KCS Access** (IPMI über KCS-Zugriff) ist auf dem BMC-Knoten aktiviert.
- Ein lokales Konto ist auf BMC zulässig.
- Die automatische Erkennung und Authentifizierung des BMC-Knotens ist aktiviert.

Automatische Ermittlung und Authentifizierung für BMC-Knoten aktivieren oder deaktivieren

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie im Fenster **Lenovo XClarity Integrator Service** links auf **BMC Management Settings** (BMC Management-Einstellungen).

Schritt 3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Automatically manage the BMC of servers already managed by SCOM (System Center Operations Manager)** (BMC von Servern, die bereits von SCOM (System Center Operations Manager) verwaltet werden, automatisch verwalten), und klicken Sie dann auf **Save** (Speichern). Wenn die automatische Erkennung des BMC-Knotens fehlschlägt, werden Warnmeldungen auf den entsprechenden Windows-Servern gemeldet. Navigieren Sie zu **Lenovo Hardware → Lenovo Windows System Group**.

Anmerkungen:

- Wenn der Netzwerkanschluss des XClarity Integrator Service geändert wird, müssen Sie den UUServerIP- und UUSPort-Wert ändern. Der Wert kann im Objektermittlungsprogramm „Lenovo.HardwareMgmtPack.AutoOOB.Discovery“ im Operations Manager geändert werden.
- Standardmäßig beträgt das Intervall für die automatische Ermittlung und Authentifizierung vier Stunden (14400 Sekunden). Sie können das Intervall bei Bedarf in `Lenovo.HardwareMgmtPack.AutoOOB.Discovery` ändern.
- Überschreiben Sie nicht den Wert für UUSCert und UUSPbKey.
- Die automatische Ermittlung von BMC-Knoten funktioniert nicht, wenn auf dem BMC-Zielknoten nur LDAP-Authentifizierung aktiviert ist oder wenn der lokale Account deaktiviert ist.
- Während der automatischen Erkennung des BMC-Knotens werden im BMC-Knoten neue Anmeldeinformationen erstellt, einschließlich eines zufälligen Passworts für den XClarity Integrator Service.

Nur BMC von Servern verwalten, die bereits vom Operations Manager verwaltet werden

Standardmäßig kann der XClarity Integrator Service verwendet werden, um jeden unterstützten Lenovo-Server unabhängig vom Operations Manager zu verwalten. Wenn Sie das Kontrollkästchen **Only manage the BMC of servers already managed by SCOM** (Nur das BMC von Servern verwalten, die bereits von SCOM verwaltet werden) aktivieren, verwaltet der XClarity Integrator Service nur die Server, die von Operations Manager verwaltet werden. Um diese Funktion zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

Vorgehensweise

- Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.
- Schritt 2. Klicken Sie im Fenster **Lenovo XClarity Integrator Service** links auf **BMC Management Settings** (BMC Management-Einstellungen).
- Schritt 3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Only manage the BMC of servers already managed by SCOM** (Nur BMC der bereits von SCOM verwalteten Server verwalten), und klicken Sie dann auf **Save** (Speichern).

Anmerkung: Sobald Sie dieses Kontrollkästchen aktivieren, stoppt der XClarity Integrator Service automatisch die Verwaltung aller Server, die Operations Manager unbekannt sind.

Aktualisieren von BMC-Knotendaten

Die BMC-Knotendaten können automatisch auf Operations Manager synchronisiert werden.

XClarity Integrator Service erfasst BMC-Bestandsdaten standardmäßig alle 24 Stunden. Sie können in der Intervallwert (`Cim_collect_interval`) in `%SystemDrive%\ProgramData\Lenovo\LXCI\UUS\global.conf` auf dem Windows-Betriebssystem mit installiertem XClarity Integrator Service ändern. Die erfassten BMC-Bestandsdaten werden automatisch mit Operations Manager synchronisiert. Sie können die BMC-Daten in Operations Manager auch wie folgt manuell aktualisieren:

Vorgehensweise

- Schritt 1. Navigieren Sie zu **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.
- Schritt 2. Klicken Sie im **Task**-Bereich auf **(Lenovo) Refresh BMC** ((Lenovo) BMC aktualisieren).

Systemstatus überprüfen

In diesem Abschnitt wird beschrieben, wie Sie den Status des BMC-basierten Servers und dessen Hardwarekomponenten überwachen.

Die folgenden Hardwarekomponenten werden für die Überwachung des Integritätsstatus unterstützt:

- BMC-System
- Prozessor
- Kühlgerät
- Physischer Speicher
- PCI-Gerät
- Netzteil
- Speicher (Plattenlaufwerk)

Anmerkung: Lenovo Management Pack überwacht Ereignisse/Warnungen vom BMC. Diese Ereignisse/Warnungen können nicht überwacht werden, wenn Sie vor der Verwaltung des BMC generiert wurden.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware → Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC)**.
- Schritt 3. Um den allgemeinen Status der BMC-basierten Server anzuzeigen, wählen Sie die Ansicht **Lenovo System x and ThinkSystem BMC** (Lenovo System x und ThinkSystem BMC) aus.
- Schritt 4. Klicken Sie auf **Active Alerts (Aktive Alerts)**, um die kritischen oder Warnalerts für die Hardware anzuzeigen. Für weitere Informationen zu den Alerts siehe „Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden“ auf Seite 48.
- Schritt 5. Wählen Sie zum Anzeigen der Hardwarekomponenteninformationen die Hardwarekomponente aus, die Sie überprüfen möchten.

Anmerkungen:

- Der Ordner **Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC)** enthält die Ansichten der Kühlgeräte, Fibre Channel, Firmware/VPD, InfiniBand, Netzwerkadapter, numerischen Sensoren, PCI-Einheiten, physischen Speicher, Prozessoren, und RAID-Controller.
- Für Kühlgeräte, physischen Speicher und den Prozessor wird ein separater Monitor definiert. Auch wenn der Überwachungsstatus für andere Komponenten in der Komponentenansicht als **Nicht überwacht** angezeigt wird, werden sie tatsächlich überwacht. Wenn die Ereignisse/Warnungen dieser Hardwarekomponenten vom BMC empfangen werden, werden sie generiert und in der Ansicht **Aktive Alerts** angezeigt.

Energieverbrauchsbegrenzung festlegen

Im folgenden Verfahren wird beschrieben, wie Sie den maximalen Wert für die Energieverbrauchsbegrenzung für die BMC-basierten Server festlegen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.

- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**, und klicken Sie auf die Ansicht **Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC)**.
- Schritt 3. Wählen Sie den Server aus, für den Sie den Wert für die Energieverbrauchsbegrenzung festlegen möchten.
- Schritt 4. Klicken Sie im Bereich **Task** auf der rechten Seite auf **(Lenovo) Power Management ((Lenovo) Stromverbrauchssteuerung)**. Das Dialogfeld **Power Capping Management (Verwaltung der Energieverbrauchsbegrenzung)** wird geöffnet.
- Schritt 5. Geben Sie einen neuen Wert für die Energieverbrauchsbegrenzung ein und klicken Sie auf **OK**, um diesen Wert zu speichern.

Einen BMC-Knoten entfernen

Im folgenden Verfahren wird beschrieben, wie Sie einen BMC-Knoten entfernen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.
- Schritt 3. Klicken Sie auf **Lenovo System x and ThinkSystem BMC** (Lenovo System x und ThinkSystem BMC), wählen Sie einen BMC-Knoten aus und klicken Sie im Bereich **Task** (Aufgabe) auf der rechten Seite auf **(Lenovo) Remove BMC** ((Lenovo) BMC entfernen).

Einen oder mehrere BMC-Knoten entfernen

Im folgenden Verfahren wird beschrieben, wie Sie einen oder mehrere BMC-Knoten entfernen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.
- Schritt 3. Klicken Sie im Bereich **Task** (Aufgabe) auf der rechten Seite auf **(Lenovo) Discover/Authenticate BMC** ((Lenovo) BMC ermitteln/authentifizieren). Die Seite **BMC Discovery** (BMC-Ermittlung) wird geöffnet.
- Schritt 4. Wählen Sie einen oder mehrere BMC-Knoten aus und klicken Sie auf **Delete** (Löschen).

Kapitel 4. Server über XClarity Administrator verwalten

Das Lenovo Hardware Management Pack unterstützt die Verwaltung von ThinkServer-Servern über den XClarity Administrator im Out-of-band-Modus.

Das Lenovo Hardware Management Pack bietet die folgenden Funktionen:

- Ermittlung der ThinkServer-Server über den XClarity Administrator
- Überwachung des Status der ThinkServer-Server und Anzeige der Ereignisse und Alerts
- Abrufen und Anzeige von Informationen zu den ThinkServer-Servern
- Bereitstellung einer Option zum Löschen des BMC-Knotens

Vorbereitende Schritte

Stellen Sie vor der Verwaltung der ThinkServer-Server sicher, dass der ThinkServer-Zielserver vom XClarity Administrator verwaltet wird.

Anmerkung: Sie sollten XClarity Administrator nicht im XClarity Integrator registrieren, wenn sich in Ihrer Operations Manager-Umgebung kein ThinkServer-Server befindet.

Unterstützte Server

Siehe die Spalte „Manage ThinkServer servers through XClarity Administrator (out-of-band mode)“ (Verwalten von ThinkServer-Servern über XClarity Administrator (Out-of-band-Modus)) in Tabelle 2 „Unterstützte Servermodelle und Funktionen“ auf Seite 3.

XClarity Administrator konfigurieren

Zum Überwachen der ThinkServer-Server müssen Sie zunächst den XClarity Administrator konfigurieren. Die von Lenovo XClarity Administrator verwalteten ThinkServer-Server werden in Operations Manager nach der Konfiguration automatisch erkannt.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.

Schritt 3. Klicken Sie im Bereich **Task** auf der rechten Seite auf **(Lenovo) XClarity Administrator**. Die Seite **Registered Lenovo XClarity Administrator (Registrierter Lenovo XClarity Administrator)** wird geöffnet.

Schritt 4. Klicken Sie auf **Register (Registrieren)**. Geben Sie IP-Adresse, den Benutzernamen, das Kennwort und den Port für den XClarity Administrator ein. Klicken Sie anschließend auf **OK**. Führen Sie einen der folgenden Schritte aus:

- **Use an existing account** (Verwenden Sie einen vorhandenen Account):
 1. Stellen Sie sicher, dass dieser Account die Rollengruppe lxc-supervisor oder die kombinierten Rollengruppen lxc-operator, lxc-fw-admin, lxc-hw-admin und lxc-os-admin hat.
 2. Stellen Sie sicher, dass dieses Konto auf die Server zugreifen kann, wenn die Ressourcenzugriffssteuerung im XClarity Administrator aktiviert ist.

- **Create a new account by connecting with this administrative account** (Erstellen Sie einen neuen Benutzeraccount, indem Sie eine Verbindung mit diesem Administratoraccount herstellen):
 1. Ein eindeutiger Benutzername (LXCIUSER-Xxxx) mit einem sicheren, nach dem Zufallsprinzip generierten Kennwort wird in XClarity-Administrator erstellt und für die gesamte Kommunikation verwendet.
 2. Wenn die Ressourcenzugriffssteuerung aktiviert ist, müssen Sie sicherstellen, dass dieser neue Account auf die Server zugreifen kann.

Anmerkung: Wählen Sie diese Option nicht, wenn XClarity Administrator einen externen LDAP für die Authentifizierung verwendet.

Schritt 5. Wenn die Seite **View Certificate (Zertifikat anzeigen)** angezeigt wird, klicken Sie auf **Trust this certificate (Diesem Zertifikat vertrauen)**. Der neue Account wird erstellt.

Anmerkungen:

- Wenn Sie auswählen, einen neuen Account zu erstellen, stellen Sie sicher, dass der angegebene XClarity Administratoraccount über Supervisor-Berechtigungen verfügt und die Rollen „lxc-operator“, „lxc-fw-admin“, „lxc-hw-admin“, und „lxc-os-admin“ im XClarity Administrator ausübt.
- Sie können das XClarity Administrator-Zertifikat vom XClarity Administrator herunterladen. Klicken Sie auf **Manage trusted certificates (Vertrauenswürdige Zertifikate verwalten) → Add (Hinzufügen)**, um das XClarity Administrator-Zertifikat dem XClarity Integrator Service manuell hinzuzufügen.

ThinkServer-Daten aktualisieren

Die ThinkServer-Knotendaten können automatisch auf Operations Manager synchronisiert werden.

Standardmäßig erfasst XClarity Integrator Service ThinkServer-Bestandsdaten alle 60 Minuten. Sie können den Intervallwert (LXCA_collect_interval) in %SystemDrive%\ProgramData\Lenovo\LXCI\UUS\global.conf auf dem Windows-Betriebssystem mit installiertem XClarity Integrator Service ändern. Die erfassten ThinkServer-Bestandsdaten werden automatisch mit Operations Manager synchronisiert. Sie können die ThinkServer-Daten in Operations Manager auch wie folgt manuell aktualisieren:

Vorgehensweise

Schritt 1. Navigieren Sie zu **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.

Schritt 2. Klicken Sie im **Task**-Bereich auf **(Lenovo) Refresh BMC** ((Lenovo) BMC aktualisieren).

Systemstatus überprüfen

In diesem Abschnitt wird beschrieben, wie Sie den Status ThinkServer-Servers und dessen Hardwarekomponenten überwachen.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware → Lenovo ThinkServer BMC**.

Schritt 3. Um den Gesamtstatus der ThinkServer-Server anzuzeigen, wählen Sie die Ansicht **Lenovo ThinkServer BMC** aus.

- Schritt 4. Klicken Sie auf **Active Alerts (Aktive Alerts)**, um die kritischen oder Warnalerts für Ihre Hardware anzuzeigen. Für weitere Informationen zu den Alerts siehe „Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden“ auf Seite 48.
- Schritt 5. Wählen Sie zum Anzeigen der Hardwarekomponenteninformationen die Hardwarekomponente aus, die Sie überprüfen möchten.

Anmerkungen:

- Der Ordner **Lenovo ThinkServer BMC** enthält die Ansichten der Kühlgeräte, Fibre Channel, Firmware/VPD, InfiniBand, numerischen Sensoren, PCI-Einheiten, physischem Speicher und Prozessoren.
- Diese Hardwarekomponenten sind in der Ansicht als „Not monitored (Nicht überwacht)“ gekennzeichnet, obwohl sie tatsächlich überwacht werden. Wenn die Ereignisse dieser Hardwarekomponenten vom XClarity Administrator empfangen werden, werden Warnungen generiert und in der Ansicht **Active Alerts (Aktive Warnungen)** angezeigt.

Einen ThinkServer-Server entfernen

Im folgenden Verfahren wird beschrieben, wie Sie einen ThinkServer-Server aus dem Operations Manager entfernen.

Anmerkung: Entfernen Sie den ThinkServer-Server zuerst von XClarity Administrator, bevor Sie den Server von Operations Manager entfernen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.
- Schritt 3. Klicken Sie auf die Ansicht **Lenovo ThinkServer BMC**, wählen Sie den ThinkServer-Server aus und klicken Sie im Bereich **Task** auf der rechten Seite auf **(Lenovo) Remove BMC ((Lenovo) BMC entfernen)**.

Kapitel 5. Gehäuse über SNMP verwalten

Mit dem Lenovo Hardware Management Pack können Sie Gehäuse (einschließlich des BladeCenter-Gehäuses und des Flex System Gehäuses) sowie Gehäusemodule über SNMP verwalten.

Das Lenovo Hardware Management Pack bietet die folgenden Funktionen:

- Das Advanced Management Module (AMM) erkennen und authentifizieren
- Den Status des Gehäuses und der Gehäusemodule überwachen und die Ereignisse oder Alerts anzeigen
- Informationen für das Gehäuse abrufen und anzeigen
- Einen Bladeserver oder Rechenknoten per Fernzugriff hoch- oder herunterfahren
- Das auf einem Bladeserver oder Rechenknoten installierte Windows-Betriebssystem per Fernzugriff herunterfahren

Vorbereitende Schritte

Stellen Sie vor der Verwaltung des Gehäuses sicher, dass SNMP auf dem Gehäuse ordnungsgemäß konfiguriert ist.

Unterstützte Gehäuse

Siehe Spalte „Manage Flex System chassis and BladeCenter chassis through SNMP“ (BladeCenter-Gehäuse und Flex System Gehäuse über SNMP verwalten) in Tabelle 2 „Unterstützte Servermodelle und Funktionen“ auf Seite 3.

Den SNMP-Agenten konfigurieren

Konfigurieren Sie zum Überwachen des Gehäuses und der Gehäusemodule zunächst den SNMP-Agenten. Das BladeCenter-Gehäuse unterstützt nur den SNMPv1-Agenten, während das Flex System Gehäuse sowohl den SNMPv1-Agenten als auch den SNMPv3-Agenten unterstützt.

Anmerkung: SNMPv1 Agent unterstützt IPv6 nicht.

SNMPv1-Agent auf dem BladeCenter-Gehäuse konfigurieren

Im folgenden Verfahren wird beschrieben, wie Sie den SNMPv1-Agent auf dem BladeCenter-Gehäuse konfigurieren.

Vorgehensweise

Schritt 1. Melden Sie sich an der AMM-Webkonsole des BladeCenter-Gehäuses an. Informationen hierzu finden Sie im Abschnitt „AMM/CMM-Webkonsole starten“ auf Seite 35.

Schritt 2. Klicken Sie auf **MM Control (MM Steuerung) → Port Assignments (Portzuordnungen)**, um sicherzustellen, dass die Einstellung des SNMP-Agenten 161 und die Einstellung der SNMP-Traps 162 ist.

Anmerkung: Verwenden Sie die Standard-SNMP-Ports 161 für den Agenten (Abfragen) und 162 für das Trapping. Es ist wichtig, dass die SNMP-Porteinstellungen konsistent sind. Andernfalls kann der Operations Manager das BladeCenter-Gehäuse nicht ermitteln.

Schritt 3. Klicken Sie auf **MM Control (MM-Steuerung) → Network Protocols (Netzwerkprotokolle) → Simple Network Management Protocol (SNMP)** und führen Sie die folgenden Schritte aus:

- a. Wählen Sie **Enabled for SNMP Traps (Aktiviert für SNMP-Traps), SNMPv1 agent (SNMPv1-Agent)**.
- b. Geben Sie die folgenden Informationen für alle Operations Manager Programme ein, die das BladeCenter-Gehäuse verwalten:
 - Geben Sie im Feld **Community name (Community-Name)** den Community-Namen ein, der dem BladeCenter-Gehäuse zugeordnet ist, über das SNMP kommuniziert.
 - Wählen Sie in der Liste **Fully Qualified Hostnames or IP Addresses (Vollständig qualifizierte Hostnamen oder IP-Adressen)** die Adresse des Operations Manager aus.
- c. Wählen Sie in der Liste **Access Type (Zugriffstyp)** die Option **Set (Festlegen)** aus. **Set** ist der Zugriffstyp, der für das Aktivieren der Verwaltungstasks erforderlich ist. Ein Taskbeispiel ist das Hoch- oder Herunterfahren eines Bladeservers per Fernzugriff über die Operations Manager Console.

Anmerkungen:

- Wenn Sie nicht möchten, dass dieser Tasktyp über die Operations Manager Console läuft, können Sie den Zugriffstyp auf **Get** verringern. Der Zugriffstyp **Get** muss mindestens für den Operations Manager-Server festgelegt sein, damit die SNMP-Abfragen durchgeführt und die SNMP-Traps vom BladeCenter empfangen werden können.
- Stellen Sie sicher, dass die Werte für den SNMPv1-Agentenaccount im SCOM-Ermittlungs-Assistenten mit den im Operations Manager festgelegten Werten konsistent sind. Andernfalls kann der Operations Manager das BladeCenter-Gehäuse nicht ermitteln.

Schritt 4. Konfigurieren Sie die SNMP-Ereignisempfänger und das BladeCenter-Gehäuse.

- a. Klicken Sie auf **MM Control (MM Steuerung) → Alerts (Alerts)**. Klicken Sie im rechten Bereich unter **Remote Alert Recipients (Empfänger für ferne Alerts)** auf den Link **not used (nicht verwendet)**, um den Alertempfänger zu konfigurieren.

Anmerkung: Je nach Firmwareversion weicht das Menü möglicherweise geringfügig ab.

- b. Ändern Sie im neuen Fenster für den Empfänger der fernen Alerts den Status von **Disabled (Deaktiviert)** in **Enabled (Aktiviert)**.
- c. Geben Sie im Feld **Name** einen beschreibenden Namen für den Verwaltungsserver für Operations Manager ein, der für die Verwaltung des BladeCenter-Gehäuses verwendet wird.
- d. Wählen Sie aus der Liste **Notification method (Benachrichtigungsmethode) SNMP over LAN (SNMP über LAN)** aus.
- e. Klicken Sie auf **Save (Speichern)**.

Schritt 5. Konfigurieren Sie die überwachten Alerts.

- a. Klicken Sie auf **MM Control (MM Steuerung) → Alerts (Alerts)**.
- b. Klicken Sie im Kontextmenü auf **Monitor Alerts (Alerts überwachen)**.
- c. Wählen Sie die zu sendenden Alerts aus und klicken Sie auf **Save (Speichern)**.

SNMP auf dem Flex System Gehäuse konfigurieren

Im folgenden Verfahren wird beschrieben, wie Sie SNMP auf dem Flex System Gehäuse, einschließlich des SNMPv1-Agenten und des SNMPv3-Agenten konfigurieren.

Vorgehensweise

Schritt 1. Melden Sie sich an der CMM-Webkonsole an. Informationen hierzu finden Sie im Abschnitt „AMM/ CMM-Webkonsole starten“ auf Seite 35.

Schritt 2. Klicken Sie auf **Mgt Module Management (Mgt Modulverwaltung) → Network (Netzwerk) → Port Assignments (Portzuordnungen)**, um sicherzustellen, dass die Einstellung des SNMP-Agenten 161 und die Einstellung der SNMP-Traps 162 ist.

Anmerkung: Um die SNMP-Einstellungen zu ändern, wählen Sie **Enable SNMPv1 Agent (SNMPv1-Agenten aktivieren)** oder **Enable SNMPv3 Agent (SNMPv3-Agenten aktivieren)**. Siehe „Den SNMPv1-Agenten konfigurieren“ auf Seite 31 und „Den SNMPv3-Agenten konfigurieren“ auf Seite 32.

Schritt 3. Konfigurieren Sie die SNMP-Ereignisempfänger und das Flex System Gehäuse.

- a. Klicken Sie auf **Events (Ereignisse) → Event Recipients (Ereignisempfänger) → Create (Erstellen) → Create SNMP Recipient (SNMP-Empfänger erstellen)**.
- b. Geben Sie im Feld **Descriptive name (Beschreibender Name)** einen Namen ein.
- c. Wählen Sie in der Liste **Status** das Kontrollkästchen **Enable this recipient (Diesen Empfänger aktivieren)** aus.
- d. Wählen Sie in der Liste **Events to receive (Zu erhaltende Ereignisse)** das Kontrollkästchen **Use the global settings (Globale Einstellungen verwenden)** oder **Only receive critical alerts (Nur kritische Alerts empfangen)** aus und klicken Sie auf **OK**, um zur Seite **Event Recipients (Ereignisempfänger)** zurückzukehren.

Anmerkung: Wenn Sie das Kontrollkästchen **Use the global settings (Globale Einstellungen verwenden)** aktivieren, müssen Sie auf der Seite **Event Recipients (Ereignisempfänger)** auf **Global Settings (Globale Einstellungen)** klicken, um die Einstellungen zu ändern, und anschließend auf **OK** klicken, um die Änderungen zu übernehmen.

Den SNMPv1-Agenten konfigurieren

Im folgenden Verfahren wird beschrieben, wie Sie den SNMPv1-Agenten auf dem Flex System Gehäuse konfigurieren.

Vorgehensweise

Schritt 1. Klicken Sie auf **Mgt Module Management (Mgt Modulverwaltung) → Network (Netzwerk) → SNMP**, und wählen Sie das Kontrollkästchen **Enable SNMPv1 Agent (SNMPv1-Agenten aktivieren)** aus.

Schritt 2. Klicken Sie auf **Traps** und wählen Sie das Kontrollkästchen **Enable SNMP Traps (SNMP-Traps aktivieren)** aus.

Schritt 3. Wählen Sie **Communities (Communitys)** aus und geben Sie die folgenden Informationen ein:

- a. Geben Sie im Feld **Community name (Community-Name)** den Namen ein, der dem Flex System Gehäuse zugeordnet ist.
- b. Wählen Sie in der Liste **Access Type (Zugriffstyp)** die Option **Set (Festlegen)** aus.
- c. Wählen Sie in der Liste **Fully Qualified Hostnames or IP Addresses (Vollständig qualifizierte Hostnamen oder IP-Adressen)** die entsprechende Adresse aus.

Anmerkungen:

- Standardmäßig ist die Sicherheitsrichtlinienebene des Gehäusemoduls „Secure (Sicher)“. Auf dieser Ebene kann der SNMPv1-Agent nicht aktiviert werden. Um den SNMPv1-Agenten zu aktivieren, klicken Sie auf **Mgt Module Management (Mgt Modulverwaltung) → Security (Sicherheit) → Security Policies (Sicherheitsrichtlinien) → Legacy → Apply (Übernehmen)**.

- Stellen Sie sicher, dass die Werte für den SNMPv1-Agentenaccount im SCOM-Ermittlungs-Assistenten mit den im Operations Manager festgelegten Werten konsistent sind. Andernfalls kann der Operations Manager das Flex System Gehäuse nicht ermitteln.

Den SNMPv3-Agenten konfigurieren

Im folgenden Verfahren wird beschrieben, wie Sie den SNMPv3-Agenten auf dem Flex System Gehäuse konfigurieren. Sie müssen einen neuen Benutzeraccount erstellen, bevor Sie den SNMPv3-Agenten oder den Standard-Benutzeraccount verwenden.

Vorgehensweise

- Schritt 1. Klicken Sie auf **Mgt Module Management (Mgt Modulverwaltung) → User Accounts (Benutzeraccounts)**, wählen Sie einen vorhandenen Benutzeraccount aus der Liste aus oder erstellen Sie einen neuen SNMPv3-Benutzeraccount.
- Schritt 2. Doppelklicken Sie auf einen Benutzernamen, um die Seite **User Properties (Benutzereigenschaften)** zu öffnen. Klicken Sie anschließend auf die Registerkarte **General (Allgemein)** und legen Sie ein Benutzerkennwort für den neuen Account fest.
- Schritt 3. Klicken Sie auf **SNMPv3** und geben Sie die folgenden Informationen ein:
 - a. Wählen Sie in der Liste **Authentication Protocol (Authentifizierungsprotokoll) Hash-based Message Authentication Code (HMAC) – Secure Hash Algorithm (SHA) (Keyed-Hash Message Authentication Code (HMAC) – Sicherer Hash-Algorithmus (SHA))** aus.
 - b. Wählen Sie das Kontrollkästchen **Use a privacy protocol (Datenschutzprotokoll verwenden)** aus.
 - c. Wählen Sie in der Liste **Encryption Method (Verschlüsselungsverfahren) Advanced Encryption Standard (AES)** aus.
 - d. Geben Sie im Feld **Privacy password (Datenschutzkennwort)** und im Feld **Confirm privacy password (Datenschutzkennwort bestätigen)** den Authentifizierungsschlüssel ein.
 - e. Ändern Sie den Zugriffstyp in **Set (Festlegen)**.
 - f. Geben Sie im Feld **IP address or host name for traps (IP-Adresse oder Hostname für Traps)** die Operations Manager IP-Adresse ein.
- Schritt 4. Klicken Sie auf **OK**.

Ein Gehäuse ermitteln

Im folgenden Verfahren wird beschrieben, wie Sie ein Gehäuse ermitteln.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Administration (Verwaltung) → Network Management (Netzmanagement) → Discovery Rules (Ermittlungsregeln) → Discover Network Device (Netzwerkeinheit ermitteln)** um den **Network Device Discovery Wizard (Ermittlungs-Assistent für Netzwerkeinheiten)** zu starten.
- Schritt 3. Führen Sie auf der Seite **General Properties (Allgemeine Eigenschaften)** die folgenden Schritte aus:
 - a. Geben Sie im Feld **Name** den Namen der Ermittlungsregel ein.
 - b. Wählen Sie einen Verwaltungs- oder Gateway-Server aus.
 - c. Wählen Sie einen Ressourcenpool aus.

Anmerkung: Wenn mehrere Server vorhanden sind, stellen Sie sicher, dass das Lenovo Hardware Management Pack auf allen Servern im Ressourcenpool installiert ist.

- d. Klicken Sie auf **Next (Weiter)**.
- Schritt 4. Wählen Sie auf der Seite **Discovery Method (Ermittlungsmethode) Explicit Discovery** (Explizite Ermittlung), und klicken Sie auf **Next (Weiter)**.
- Schritt 5. Wählen Sie auf der Seite **Default Accounts (Standardaccounts)** die Option **Next (Weiter)** aus. Die Seite **Devices (Geräte)** wird geöffnet.
- Schritt 6. Klicken Sie auf der Seite **Devices (Geräte)** auf **Add (Hinzufügen)**. Das Dialogfenster **Add a Device (Einheit hinzufügen)** wird geöffnet.
- Schritt 7. Gehen Sie im Dialogfeld **Add a Device (Einheit hinzufügen)** wie folgt vor:
- Geben Sie in das Feld **Name or IP address (Name oder IP-Adresse)** die IP-Adresse des Gehäuses ein.
 - Wählen Sie in der Liste **Access Mode (Zugriffsmodus)** die Option **SNMP** aus.
 - Behalten Sie die Portnummer als Standardwert 161 bei.
 - Wählen Sie die entsprechende SNMP-Version aus.
 - Führen Sie einen der folgenden Schritte aus:
 - Um den vorhandenen Account auszuwählen, klicken Sie auf **SNMP V3 Run As Account (Ausführender SNMPv3-Account)** oder **SNMP V1 or V2 Run As account (Ausführender SNMPv1- oder v2-Account)**.
 - Um einen neuen Account hinzuzufügen, klicken Sie auf **Add SNMP V3 Run As Account (Ausführenden SNMP-V3-Account hinzufügen)** oder **Add SNMP V1 or V2 Run As account (Ausführenden SNMP-V1- oder V2-Account hinzufügen)**.
- Anmerkung:** Stellen Sie sicher, dass die Werte für den SNMPv1-Agent-Account oder den SNMPv3 Agent-Account mit den im Gehäuse-Account festgelegten Werten konsistent sind.
- Klicken Sie auf **OK**, um zum **Network Device Discovery Wizard (Ermittlungs-Assistent für Netzwerkeinheiten)** zurückzukehren.
- Schritt 8. Klicken Sie auf **Next (Weiter)**. Stellen Sie danach die Uhrzeit für die Ausführung der Ermittlungsregel ein, und klicken Sie auf **Save (Speichern)**. Wenn sich ein Fenster öffnet und Sie dazu auffordert, die Accounts zu verteilen, klicken Sie auf **Yes (Ja)**.
- Schritt 9. Klicken Sie auf **Discovery Rule (Ermittlungsregel) → Run (Ausführen)**.
- Schritt 10. Warten Sie eine Weile, und klicken Sie auf **Network Management (Netzmanagement) → Network Devices (Netzwerkeinheiten)**. Das ermittelte Gehäuse wird angezeigt.

Gehäuse-Status überwachen

In diesem Abschnitt wird beschrieben, wie Sie den Status der Gehäuse und Gehäusemodule überwachen.

Status des BladeCenter-Gehäuses überwachen

Das folgende Verfahren beschreibt, wie Sie die Integrität des BladeCenter-Gehäuses und der Gehäusemodule überwachen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware → Lenovo BladeCenter(s) and Modules (Lenovo BladeCenter und Module)**.
- Schritt 3. Um den Gesamtstatus des BladeCenter-Gehäuses anzuzeigen, wählen Sie die Ansicht **Lenovo BladeCenter(s)** aus.

- Schritt 4. Klicken Sie auf **Active Alerts (Aktive Alerts)**, um die kritischen oder Warnalerts für die Hardware anzuzeigen. Für weitere Informationen zu den Alerts siehe „Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden“ auf Seite 48.
- Schritt 5. Klicken Sie zum Anzeigen der Informationen zu den Gehäusemodulen auf **Lenovo BladeCenter Modules (Lenovo BladeCenter-Module)**, und wählen Sie das Gehäusemodul aus, das Sie überprüfen möchten.

Die Ansichten im Unterordner **Lenovo BladeCenter Modules (Lenovo BladeCenter-Module)** enthalten Folgendes:

- Lenovo BladeCenter Blades
- Lenovo BladeCenter-Gehäuse
- Lenovo BladeCenter-Kühlungsmodule
- Lenovo BladeCenter-E/A-Module
- Lenovo BladeCenter-Verwaltungsmodule
- Lenovo BladeCenter-Einschubmodule
- Lenovo BladeCenter-Stromversorgungsmodule
- Lenovo BladeCenter-Speichermodule

Status des Flex System Gehäuses überwachen

Das folgende Verfahren beschreibt, wie Sie die Integrität des Flex System Gehäuses und der Gehäusemodule überwachen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware → Lenovo Flex System Chassis and Modules (Gehäuse und Module des Lenovo Flex Systems)**.
- Schritt 3. Um den Gesamtstatus des Flex System Gehäuses anzuzeigen, wählen Sie die Ansicht **Lenovo Flex System chassis (Lenovo Flex System Gehäuse)** aus.
- Schritt 4. Klicken Sie auf **Active Alerts (Aktive Alerts)**, um die kritischen oder Warnalerts für die Hardware anzuzeigen. Für weitere Informationen zu den Alerts siehe „Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden“ auf Seite 48.
- Schritt 5. Klicken Sie zum Anzeigen der Informationen zu den Gehäusemodulen auf **Lenovo Flex System chassis and Modules (Gehäuse und Module des Lenovo Flex Systems)**, und wählen Sie das Gehäusemodul aus, das Sie überprüfen möchten.

Die Ansichten im Unterordner **Lenovo Flex System Chassis Modules (Lenovo Flex System Gehäusemodule)** enthalten Folgendes:

- Lenovo Flex System Gehäuse-Rechenknoten
- Lenovo Flex System Gehäuse-Kühlungsmodule
- Lenovo Flex System Gehäuse-Mux-Lüfter-Module
- Lenovo Flex System Gehäuse-FSM
- Lenovo Flex System Gehäuse-E/A-Module
- Lenovo Flex System Gehäuseverwaltungsmodule
- Lenovo Flex System Gehäuse-Stromversorgungsmodule
- Lenovo Flex System Gehäuse-Rückseiten-LED-Module
- Lenovo Flex System Gehäuse-Speicher

Die neuesten Informationen zum Gehäuse abrufen

Im folgenden Verfahren wird beschrieben, wie Sie die neuesten Informationen für das Gehäuse, einschließlich des Bestands und des Status von Gehäusen und Gehäusemodulen abrufen.

Die Informationen zum Gehäuse werden alle vier Stunden automatisch aktualisiert. Gehen Sie wie folgt vor, um die Informationen manuell zu aktualisieren:

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.

Schritt 3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Lenovo BladeCenter(s) and Modules (Lenovo BladeCenter und Module) → Lenovo BladeCenters**, und wählen Sie im Bereich **Lenovo BladeCenter(s)** ein BladeCenter-Gehäuse aus.
- Klicken Sie auf **Lenovo Flex System Chassis and Modules (Gehäuse und Module des Lenovo Flex Systems) → Lenovo Flex System Chassis (Lenovo Flex System Gehäuse)**, und wählen Sie im Bereich **Lenovo Flex System Chassis (Lenovo Flex System Gehäuse)** ein Flex System Gehäuse aus.

Schritt 4. Klicken Sie im Bereich **Task** auf der rechten Seite auf **(Lenovo) Refresh this Chassis Modules ((Lenovo) Module dieses Gehäuses aktualisieren)**. Anschließend werden die neuesten Informationen für das Gehäuse angezeigt.

AMM/CMM-Webkonsole starten

Das erweiterte Verwaltungsmodul (AMM, Advanced Management Module) ist ein Modul, mit dem Sie das BladeCenter-Gehäuse konfigurieren und verwalten können, während das Chassis Management Module (CMM) ein Modul ist, das zum Konfigurieren und Verwalten des Flex System Gehäuses verwendet wird. Im folgenden Verfahren wird beschrieben, wie Sie die AMM/CMM-Webkonsole starten.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.

Schritt 3. Führen Sie einen der folgenden Schritte aus:

- Für das BladeCenter-Gehäuse klicken Sie auf den Ordner **Lenovo BladeCenter(s) and Modules** (Lenovo BladeCenter und Module) und wählen Sie die Ansicht **Lenovo BladeCenter (s)** (Lenovo BladeCenter) aus.
- Für das Flex System Gehäuse klicken Sie auf den Ordner **Lenovo Flex System Chassis and Modules** (Gehäuse und Module des Lenovo Flex Systems) und wählen Sie die Ansicht **Lenovo Flex System Chassis** (Lenovo Flex System Gehäuse) aus.

Schritt 4. Wählen Sie ein BladeCenter- oder Flex System Gehäuse aus.

Schritt 5. Klicken Sie im Bereich **Task** auf der rechten Seite je nach Ihrem Gehäuse auf **Lenovo BladeCenter Chassis Management Web Console (Lenovo BladeCenter Gehäuseverwaltungs-Webkonsole)** oder **Lenovo Flex System Chassis Management Web Console (Lenovo Flex System Gehäuseverwaltungs-Webkonsole)**.

Einen Bladeserver oder Rechenknoten hoch- oder herunterfahren

Im folgenden Verfahren wird beschrieben, wie Sie einen Bladeserver oder einer Rechenknoten starten und wie Sie das Windows-Betriebssystem, das auf einem Bladeserver oder einem Rechenknoten installiert ist, herunterfahren.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.

Schritt 3. Führen Sie einen der folgenden Schritte aus:

- Für das BladeCenter-Gehäuse, klicken Sie auf den Ordner **Lenovo BladeCenter(s) and Modules** (Lenovo BladeCenter und Module) und klicken Sie auf die Ansicht **Lenovo BladeCenter Blades** im Unterordner **Lenovo BladeCenter Modules** (Lenovo BladeCenter Module).
- Für das Flex System Gehäuse, klicken Sie auf den Ordner **Lenovo Flex System Chassis and Modules** (Gehäuse und Module des Lenovo Flex Systems) und klicken Sie auf die Ansicht **Lenovo Flex System chassis Compute Nodes (Lenovo Flex System Gehäuse-Rechenknoten)** im Unterordner **Lenovo Flex System Chassis Modules** (Lenovo Flex System Gehäusemodule).

Schritt 4. Wählen Sie einen Bladeserver oder einen Rechenknoten aus.

Schritt 5. Klicken Sie entsprechend Ihren Anforderungen auf die entsprechende Task-Schaltfläche.

Ein ermitteltes Gehäuse entfernen

Im folgenden Verfahren wird beschrieben, wie Sie ein ermitteltes Gehäuse aus der Liste der Gehäuse entfernen.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Administration (Verwaltung) → Network Management (Netzmanagement) → Network Devices (Netzwerkeinheiten)**.

Schritt 3. Wählen Sie im Ergebnisbereich ein Gehäuse, das entfernt werden soll.

Schritt 4. Klicken Sie auf **Delete (Löschen)**. Das Gehäuse und die zugehörigen Gehäusemodule werden entfernt.

Kapitel 6. Server über IBM Platform Agent verwalten

Mit dem Lenovo Hardware Management Pack können Sie den IBM Platform Agent verwenden, um Lenovo Server zu verwalten, auf denen das Windows-Betriebssystem im In-band-Modus installiert ist. Die Lenovo Server enthalten die System x-Server, die BladeCenter-Server und die Flex System-Server.

Anmerkungen:

- Der IBM Platform Agent unterstützt nicht die ThinkSystem-Server.
- Der IBM Platform Agent unterstützt nicht Windows 2016 oder neuere Versionen.
- Der IBM Platform Agent wird nicht mehr unterstützt.
- Es wird empfohlen, Server über den XClarity Integrator Service zu verwalten.

Vorbereitende Schritte

Stellen Sie vor der Verwaltung der Lenovo Server Folgendes sicher:

- Eines der folgenden Windows-Betriebssysteme auf dem Zielsystem installiert ist: Windows 2008, Windows 2008 R2, Windows 2012 oder Windows 2012 R2.

Anmerkung: Windows 2016 oder neuere Versionen werden nicht unterstützt.

- Der Zielsystem wird von Operations Manager verwaltet.
- IBM Platform Agent v.6.3.3 oder höher ist auf dem Zielsystem installiert. Sie können Platform Agent von [IBM Fix Central](#) herunterladen. Weitere Informationen finden Sie in der [IBM Systems Director- Onlinedokumentation](#). Der Befehl für die automatische Installation ist `dir6.3.7_platformagent_windows.exe /s /a silent`.
- IBM Remote Supervisor Adapter II (RSA-II Daemon) v5.4.6 oder höher ist auf dem Zielsystem installiert.

Anmerkungen: Der RSA-II Daemon für das Windows-Betriebssystem steht unter den folgenden Adressen zur Verfügung:

- [RSA-II Daemon v5.46 für Microsoft Windows IA32](#)
- [RSA-II Daemon v5.44 für Microsoft Windows Server 2003/2008 \(x64\)](#)

Unterstützte Servermodelle

Siehe die Spalte „Manage System x, BladeCenter, and Flex System servers through IBM Platform Agent (in-band mode)“ in Tabelle 2 „Unterstützte Servermodelle und Funktionen“ auf Seite 3.

Einen Lenovo Server ermitteln

Im folgenden Verfahren wird beschrieben, wie Sie einen Lenovo Server mithilfe des **Microsoft System Center Operations Manager Ermittlungs-Assistenten** (nachfolgend **Ermittlungs-Assistent** genannt) ermitteln. Der **Ermittlungs-Assistent** implementiert das Lenovo Hardware Management Pack auf dem erkannten Server.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie auf **Administration (Verwaltung) → Device Management (Einheitenverwaltung) → Agent Managed (Mit Agents verwaltet) → Discovery Wizard (Ermittlungs-Assistent)**. Der **Computer and Device Management Wizard (Computer- und Einheitenverwaltungs-Assistent)** wird gestartet.

- Schritt 3. Klicken Sie auf **Discovery Type (Ermittlungstyp) → Windows computers (Windows Computer)**, und klicken Sie auf **Next (Weiter)**.
- Schritt 4. Wählen Sie das Kontrollkästchen **Advanced discovery (Erweiterte Ermittlung)** aus.
- Schritt 5. Wählen Sie in der Liste **Computer and Device Classes (Computer- und Einheitenklassen) Servers and Clients (Server und Clients)** aus, und wählen Sie einen Lenovo Server aus, der hinzugefügt werden soll.
- Schritt 6. Aktivieren Sie das Kontrollkästchen **Verify discovered computers can be contacted (Überprüfen, ob ermittelte Computer kontaktiert werden können)** und klicken Sie auf **Next (Weiter)**.
- Schritt 7. Aktivieren Sie das Kontrollkästchen **Browse for, or type-in computer names (Computernamen suchen oder eingeben)**.
- Schritt 8. Klicken Sie auf **Browse (Durchsuchen)**, um den Lenovo Server zu erkennen oder geben Sie den Namen des Lenovo Servers manuell in das Eingabefeld ein und klicken Sie auf **Next (Weiter)**.
- Schritt 9. Wählen Sie auf der Seite **Administrator Account (Administratoraccount)** eine der folgenden Optionen:
- Um einen vorhandenen Server auszuwählen, aktivieren Sie das Kontrollkästchen **Use selected Management Server Action Account (Ausgewählten Aktionsaccount von Verwaltungsserver verwenden)** und klicken Sie auf **Next (Weiter)**.
 - Um einen neuen Server hinzuzufügen, aktivieren Sie das Kontrollkästchen **Other user account (Anderer Benutzeraccount)** und geben Sie den neuen Lenovo Servernamen ein.
- Schritt 10. Klicken Sie auf **Discover (Ermitteln)**, um den Ermittlungsvorgang zu starten. Wenn die Ermittlung abgeschlossen ist, werden die Ermittlungsergebnisse auf der Seite **Summary (Zusammenfassung)** angezeigt.
- Anmerkung:** Die für die Ermittlung erforderliche Zeit hängt von der Anzahl der Lenovo Server im Netzwerk ab.
- Schritt 11. Klicken Sie auf der Seite **Summary (Zusammenfassung)** auf **Finish (Fertigstellen)**. Die Seite **Agent Management Task Status (Status des Agentverwaltungstasks)** wird geöffnet.
- Schritt 12. Klicken Sie auf **Monitoring (Überwachung) → Task Status (Taskstatus)**, um den Status des Verwaltungstasks zu überprüfen. Der Lenovo Server wird ermittelt, wenn der Status von **Queued (In Warteschlange)** auf **Success (Erfolg)** geändert wird.

Serverstatus überwachen

In diesem Abschnitt wird beschrieben, wie Sie die Integrität der Lenovo Server und der Hardwarekomponenten überwachen, einschließlich Lüfter, Hauptspeicher, Management-Controller, Netzwerkkarte, Netzteile, Prozessoren, Speicher, Temperatursensoren und Spannungssensoren.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.
- Schritt 3. Um den gesamten Status der Lenovo Server anzuzeigen, wählen Sie eine der folgenden Ansichten:
- **Lenovo Windows System Group (Lenovo Windows-Systemgruppe):** Diese Ansicht stellt den Hardwarestatus aller Lenovo Server bereit.
 - **Windows Computer on Lenovo Windows System Group (Windows-Computer in der Lenovo Windows-Systemgruppe):** Diese Ansicht listet die Statusanzeigen in der ersten Spalte des System-Dashboards und das Hardwarekomponenten-Dashboard auf.

- Schritt 4. Um die kritischen oder Warnalerts im Zusammenhang mit der Hardware anzuzeigen, klicken Sie auf den Ordner **Lenovo Windows System Group (Lenovo Windows-Systemgruppe)** und klicken Sie auf **Active Alerts (Aktive Alerts)**. Für weitere Informationen zu den Alerts siehe „Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden“ auf Seite 48.
- Schritt 5. Klicken Sie zum Anzeigen der Hardwarekomponenteninformationen auf den Ordner **Lenovo Windows System Group (Lenovo Windows-Systemgruppe)** und wählen Sie die Hardwarekomponente aus, die Sie überprüfen möchten.

Anmerkung: Hardwarekomponenten, die nicht ermittelt werden können, können weder überwacht noch verwaltet werden.

Energieverbrauchsdaten der Client System x-Server anzeigen

Im folgenden Verfahren wird beschrieben, wie Sie die Energieverbrauchsdaten der Client System x-Server im Lenovo System x Energieverbrauchsdatendiagramm anzuzeigen. Dieses Diagramm ist nur auf System x-Servern verfügbar.

Vorbereitende Schritte

Stellen Sie sicher, dass das Windows-Betriebssystem auf mehreren verwalteten System x-Servern installiert ist.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware → Lenovo System x Power Data Chart (Lenovo System x Energieverbrauchsdatendiagramm)**.
- Schritt 3. Aktivieren Sie das Kontrollkästchen **Show (Anzeigen)**. Das Energieverbrauchsdatendiagramm wird angezeigt.

Anmerkung: Die als gerade Linie angezeigten Energieverbrauchsdaten bedeuten, dass der Energieverbrauch in einem bestimmten Zeitraum konstant ist.

Energieverbrauchsbegrenzung festlegen

Im folgenden Verfahren wird beschrieben, wie Sie den maximalen Wert für die Energieverbrauchsbegrenzung für die Lenovo Server festlegen.

Vorbereitende Schritte

Stellen Sie Folgendes sicher, bevor Sie den maximalen Wert für die Energieverbrauchsbegrenzung festlegen:

- Der Zielsystem verfügt über Funktionen zur Energieverbrauchsbegrenzung.
- Die Benutzerkontensteuerung wird auf dem Zielsystem heruntergefahren.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**, und klicken Sie auf die Ansicht **Lenovo Windows System Group (Lenovo Windows-Systemgruppe)**.
- Schritt 3. Wählen Sie den Server aus, für den Sie den Wert für die Energieverbrauchsbegrenzung festlegen möchten.

Anmerkung: Sie können die aktuellen Werte für die Energieverbrauchsbeschränkung von **CappingCapable**, **CappingEnabled**, **PowerMax**, **PowerMin**, und **PowerCap** eines Servers in der **Detail View (Detailansicht)** anzeigen.

- Schritt 4. Klicken Sie im Bereich **Task** auf der rechten Seite auf **(Lenovo) Set Power Capping ((Lenovo) Energieverbrauchsbeschränkung festlegen)**. Der Bereich **Run the task on these targets (Task für diese Ziele ausführen)** wird angezeigt.
- Schritt 5. Geben Sie einen neuen Wert für die Energieverbrauchsbeschränkung ein und klicken Sie auf **Override (Überschreiben)**.
- Schritt 6. Klicken Sie auf **Run (Ausführen)**. Das Fenster „Taskstatus“ wird geöffnet und zeigt an, ob der Wert überschrieben wurde.

Energieverbrauchsschwellenwert festlegen

Das folgende Verfahren beschreibt, wie Sie eine Warnung oder einen kritischen Energieverbrauchsschwellenwert für den Lenovo Server festlegen.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**, und klicken Sie auf die Ansicht **Lenovo Windows System Group (Lenovo Windows-Systemgruppe)**.
- Schritt 3. Wählen Sie den Server aus, für den Sie den Energieverbrauchsschwellenwert festlegen möchten.

Anmerkung: Sie können die aktuellen Schwellenwerte und die Überwachungsleistungseigenschaft des Servers in der **Detail View (Detailansicht)** anzeigen.

- Schritt 4. Klicken Sie im Bereich **Task** auf der rechten Seite auf **(Lenovo) Set/Unset Power Threshold ((Lenovo) Energieverbrauchsschwellenwert festlegen/aufheben)**. Der Bereich **Run the task on these targets (Task für diese Ziele ausführen)** wird angezeigt.
- Schritt 5. Geben Sie einen neuen Energieverbrauchsschwellenwert ein und klicken Sie auf **Override (Überschreiben)**.
Anmerkung: Wenn Sie keinen Wert oder Null angeben, wird der Schwellenwert auf seinen Standardwert zurückgesetzt.
- Schritt 6. Klicken Sie auf **Run (Ausführen)**. Das Fenster „Taskstatus“ wird geöffnet und zeigt an, ob der Wert überschrieben wurde.

Die neuesten Informationen für die Lenovo Server abrufen

Im folgenden Verfahren wird beschrieben, wie Sie die neuesten Informationen für die Lenovo Server, einschließlich des Bestands und des Status von Servern und Hardwarekomponenten abrufen.

Die Informationen zu den Lenovo Servern werden alle vier Stunden automatisch aktualisiert. Gehen Sie wie folgt vor, um die Informationen manuell zu aktualisieren:

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Windows Computers (Windows-Computer)**.
- Schritt 3. Klicken Sie im Bereich **Task** auf der rechten Seite auf **Refresh Lenovo Windows Computer (Informationen zum Lenovo Windows-Computer aktualisieren)**. Die neuesten Informationen werden angezeigt.

Kapitel 7. Mit XClarity Integrator Service-Sicherheitszertifikaten arbeiten

XClarity Integrator Service unterstützt das HTTPS-Protokoll für die ein- und ausgehende Kommunikation. In Lenovo XClarity Integrator Service werden standardmäßig die selbst generierten Zertifikate verwendet, die von einer internen Zertifizierungsstelle (CA) ausgestellt und selbst signiert sind. In diesem Abschnitt wird beschrieben, wie Sie die Zertifikate festlegen, generieren, neu generieren und herunterladen.

Anmerkung: Standardmäßig unterstützen XClarity Integrator Service 7.6.0 und spätere Versionen nur Transport Layer Security (TLS) 1.2.

BMC-Kommunikationsprotokoll festlegen

Im folgenden Verfahren wird beschrieben, wie Sie das BMC-Kommunikationsprotokoll festlegen.

Vorbereitende Schritte

Stellen Sie sicher, dass das HTTPS-Protokoll auf allen BMC-Knoten aktiviert ist, wenn Sie nur das HTTPS-Protokoll verwenden, um mit BMC Knoten zu kommunizieren.

Anmerkung: Wenn Sie das Kontrollkästchen **Only use HTTPS protocol to communicate with BMC nodes (Nur das HTTPS-Protokoll zur Kommunikation mit BMC-Knoten verwenden)** nicht aktivieren, werden das HTTPS-Protokoll und das HTTP-Protokoll nacheinander probiert.

Vorgehensweise

- Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Security Settings** (Sicherheitseinstellungen). Die Seite **Security Settings (Sicherheitseinstellungen)** wird geöffnet.
- Schritt 3. Klicken Sie auf die Registerkarte **Security Settings** (Sicherheitseinstellungen).
- Schritt 4. Wählen Sie das Kontrollkästchen **Only use HTTPS protocol to communicate with BMC nodes (Nur das HTTPS-Protokoll zur Kommunikation mit BMC-Knoten verwenden)** aus.
- Schritt 5. Klicken Sie auf **Save** (Speichern).

Zertifikate generieren und hochladen

Beim Generieren des angepassten Serverzertifikats in Lenovo XClarity Integrator Service müssen Sie das Zertifikatpaket bereitstellen, das die vollständige CA-Signierungskette enthält.

Vorgehensweise

- Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.
- Schritt 2. Verbinden Sie einen Server mit dem XClarity Integrator Service.

Anmerkung: Wenn das Serverzertifikat nicht von einer vertrauenswürdigen internationalen Zertifizierungsstelle signiert ist, wird eine Sicherheitsnachricht angezeigt. Um diese Sicherheitsnachricht zu vermeiden, wählen Sie das Kontrollkästchen **Trust the certificate permanently (Dem Zertifikat dauerhaft vertrauen)** aus und klicken Sie auf **Next (Weiter)**.

- Schritt 3. Generieren Sie die Zertifikatssignieranforderung (CSR) für den XClarity Integrator Service.

- a. Klicken Sie auf **Security Settings** (Sicherheitseinstellungen). Die Seite **Security Settings (Sicherheitseinstellungen)** wird geöffnet.
- b. Klicken Sie auf **Server Certificate (Serverzertifikat)**.
- c. Klicken Sie auf **Generate Certificate Signing Request (CSR) (Zertifikatssignieranforderung (CSR) generieren)**.
- d. Füllen Sie alle Felder auf der Seite **Generate Certificate Signing Request (CSR) (Zertifikatssignieranforderung (CSR) generieren)** aus: Land, Bundesstaat/Bundesland, Stadt/Gemeinde, Organisation, Organisationseinheit (optional) und Allgemeiner Name.

Anmerkung: Sie können den allgemeinen Namen automatisch vom XClarity Integrator Service generieren lassen, indem Sie den Standardwert **Generated by LXCI (Generiert von LXCI)** behalten.
- e. Wählen Sie den richtigen Hostnamen aus. Wenn ein falscher Name ausgewählt ist, kann der Server keine Verbindung mit dem XClarity Integrator Service herstellen.
- f. Klicken Sie auf **Generate CSR File (CSR-Datei generieren)**. Die CSRs werden automatisch heruntergeladen.

Schritt 4. Senden Sie alle CSRs an die vertrauenswürdige Zertifizierungsstelle. Die vertrauenswürdige Zertifizierungsstelle ordnet jeder CSR ein Zertifikatspaket zu. Das Zertifikatspaket enthält die angepassten Zertifikate und die vollständige vertrauenswürdige CA-Zertifikatkette.

Schritt 5. Laden Sie die angepassten Zertifikate und generierten Serverzertifikate zum XClarity Integrator Service hoch.

- a. Klicken Sie auf der Seite **Security Settings (Sicherheitseinstellungen)** auf **Server Certificate (Serverzertifikat)**.
- b. Klicken Sie auf **Upload Certificate (Zertifikat hochladen)**, um die Zertifikatsdatei (mit der Erweiterung .cer) hochzuladen.

Anmerkungen:

- Die angepassten Zertifikate müssen die vollständige Zertifikatskette einschließlich des Stammzertifikats und der Zwischenzertifikate enthalten.
- Die Zertifikate müssen in folgender Reihenfolge hochgeladen werden: Serverzertifikate, Zwischenzertifikate, Stammzertifikate.

Zertifikate neu generieren

Wenn das vorhandene Zertifikat ungültig ist oder die Zertifikatsversion nicht die neueste ist, können Sie ein neues Serverzertifikat oder ein Stammzertifikat für den XClarity Integrator Service neu generieren, um das alte zu ersetzen.

Serverzertifikat neu generieren

Im folgenden Verfahren wird beschrieben, wie Sie das neue Serverzertifikat für den XClarity Integrator Service neu generieren.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie auf **Security Settings** (Sicherheitseinstellungen). Die Seite **Security Settings (Sicherheitseinstellungen)** wird geöffnet.

Schritt 3. Klicken Sie auf **Server Certificate (Serverzertifikat)**.

Schritt 4. Klicken Sie auf die Registerkarte **Regenerate Server Certificate (Serverzertifikat neu generieren)**.

Schritt 5. Füllen Sie alle Felder auf der Seite **Regenerate Server Certificate (Serverzertifikat neu generieren)** aus: Land, Bundesstaat/Bundesland, Stadt/Gemeinde, Organisation, Organisationseinheit (optional), und Allgemeiner Name.

Anmerkung: Sie können den allgemeinen Namen automatisch vom XClarity Integrator Service generieren lassen, indem Sie den Standardwert **Generated by LXCI (Generiert von LXCI)** behalten.

Schritt 6. Wählen Sie einen richtigen Hostnamen aus. Wenn ein falscher Name ausgewählt ist, kann der Server keine Verbindung mit dem XClarity Integrator Service herstellen.

Schritt 7. Klicken Sie auf **Regenerate Certificate (Zertifikat neu generieren)**.

Stammzertifikat neu generieren

Im folgenden Verfahren wird beschrieben, wie Sie das neue Stammzertifikat für den XClarity Integrator Service neu generieren.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie auf **Security Settings (Sicherheitseinstellungen)**. Die Seite **Security Settings (Sicherheitseinstellungen)** wird geöffnet.

Schritt 3. Klicken Sie auf **Certificate Authority (Zertifizierungsstelle)**.

Schritt 4. Wählen Sie **Regenerate Certificate Authority Root Certificate (Stammzertifikat der Zertifizierungsstelle neu generieren)** aus.

Schritt 5. Lesen Sie die Informationen und klicken Sie auf **OK**.

Anmerkungen:

- Wenn die angepassten Zertifikate ungültig sind, generiert der XClarity Integrator Service die neuen Zertifikate und ersetzt die alten Zertifikate automatisch durch diese neuen.
- Wenn die angepassten Zertifikate gültig sind, generiert der XClarity Integrator Service nur ein neues Stammzertifikat neu.

Zertifikate herunterladen

Sie können das Serverzertifikat und das Stammzertifikat herunterladen.

Das Serverzertifikat herunterladen

Im folgenden Verfahren wird beschrieben, wie Sie das Serverzertifikat herunterladen.

Vorgehensweise

Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.

Schritt 2. Klicken Sie auf **Security Settings (Sicherheitseinstellungen)**. Die Seite **Security Settings (Sicherheitseinstellungen)** wird geöffnet.

Schritt 3. Klicken Sie auf **Server Certificate (Serverzertifikat)**.

Schritt 4. Wechseln Sie auf die Registerkarte **Download Certificate (Zertifikat herunterladen)**.

Schritt 5. Klicken Sie auf **Download Certificate (Zertifikat herunterladen)**.

Stammzertifikat herunterladen

Im folgenden Verfahren wird beschrieben, wie Sie das Stammzertifikat herunterladen.

Vorgehensweise

- Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.
- Schritt 2. Klicken Sie auf **Security Settings** (Sicherheitseinstellungen). Die Seite **Security Settings (Sicherheitseinstellungen)** wird geöffnet.
- Schritt 3. Klicken Sie auf **Certificate Authority (Zertifizierungsstelle)**.
- Schritt 4. Wählen Sie **Download Certificate Authority Root Certificate (Stammzertifikat der Zertifizierungsstelle herunterladen)** aus.

Kapitel 8. Protokolldaten

Dieser Abschnitt enthält Anweisungen zum Festlegen der Protokollierungsstufe und wie Protokolle erfasst bzw. angezeigt werden.

Protokolle für den XClarity Integrator Service

Sie können die Protokolldateien erfassen und die Protokollierungsstufe für den XClarity Integrator Service festlegen.

Protokollierungsstufe festlegen

Im folgenden Verfahren wird beschrieben, wie Sie die Protokollierungsstufe für den XClarity Integrator Service festlegen.

Vorgehensweise

- Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Service Data (Servicedaten)**.
- Schritt 3. Klicken Sie auf das Dropdown-Menü, um die Protokollierungsstufe festzulegen.
 - **Fehlerstufe:** Nur Fehlernachrichten aufzeichnen.
 - **Warnstufe:** Warnnachrichten und Fehlernachrichten aufzeichnen.
 - **Informationsstufe:** Fehler-, Warn- und Informationsnachrichten aufzeichnen.
 - **Debug-Stufe:** Fehler-, Warn- und Informationsnachrichten sowie Debug-Nachrichten aufzeichnen.

Protokolldateien erfassen

Im folgenden Verfahren wird beschrieben, wie Sie die Protokolldateien für den XClarity Integrator Service erfassen.

Vorgehensweise

- Schritt 1. Melden Sie sich beim XClarity Integrator Service an. Informationen hierzu finden Sie im Abschnitt „Bei XClarity Integrator Service anmelden“ auf Seite 17.
- Schritt 2. Klicken Sie im linken Navigationsbereich auf **Service Data (Servicedaten)**.
- Schritt 3. Klicken Sie auf **Collect Log (Protokoll erfassen) → Download Log (Protokoll herunterladen)**. Die Protokolle für den XClarity Integrator Service werden heruntergeladen.

Protokolle für das Lenovo Hardware Management Pack

Sie können die Protokollierungsstufe festlegen und das Protokoll des Lenovo Hardware Management Packs anzeigen.

Protokollierungsstufe festlegen

Im folgenden Verfahren wird beschrieben, wie Sie die Protokollierungsstufe für das Lenovo Hardware Management Pack festlegen.

Vorgehensweise

Schritt 1. Öffnen Sie im Windows-Betriebssystem im Programm **regedit.exe** den REG-Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\Lenovo SCOM MP\Debug.

Schritt 2. Doppelklicken Sie im REG-Schlüssel auf **Level (Stufe)**, und geben Sie abhängig von Ihren Anforderungen einen der folgenden Werte ein:

- Fehlerstufe: Stufe = 1
- Warnstufe: Stufe = 3
- Informationsstufe: Stufe = 5
- Debug-Stufe: Stufe = 7

Anmerkung: Stellen Sie sicher, dass der Wertetyp des Werts „Stufe“ „Zeichenfolge“ ist.

Das Protokoll in der Windows-Ereignisanzeige anzeigen

Im folgenden Verfahren wird beschrieben, wie Sie die Protokolle für das Lenovo Hardware Management Pack in der Windows-Ereignisanzeige anzeigen.

Vorgehensweise

Schritt 1. Starten Sie im Windows-Betriebssystem die Windows-Ereignisanzeige.

Schritt 2. Klicken Sie auf **Applications and Services Logs (Anwendungs- und Dienstprotokolle) → Operations Manager**. Die Protokolle des Lenovo Hardware Management Packs werden angezeigt.

Schritt 3. Klicken Sie im Bereich **Actions (Aktionen)** auf der rechten Seite auf **Filter Current Log (Aktuelles Protokoll filtern)**.

Schritt 4. Aktivieren Sie in der Dropdown-Liste **Event sources (Ereignisquellen)** die Kontrollkästchen **Health Service Script (Integritätsdienst-Skript)** und **Lenovo.EventLogSource**. Die Protokolle des Lenovo Hardware Management Packs werden im Fenster angezeigt.

Anmerkung: Wenn LXCI Management Pack-Ereignisse vorhanden sind, wird in der Dropdown-Liste **Event sources (Ereignisquellen)** nur das Kontrollkästchen **Lenovo.EventLogSource** angezeigt.

Kapitel 9. Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Ihnen bei der Behebung von Problemen helfen, die Sie möglicherweise mit dem Lenovo Hardware Management Pack haben.

Fehlerbehebung nach Symptom

Dieser Abschnitt enthält Informationen zu allgemeinen Fehlerbehebungs- und Diagnosemethoden, mit deren Hilfe Sie Probleme beheben können, die möglicherweise bei Servern, auf denen das Lenovo Hardware Management Pack installiert ist, auftreten. Wenn Sie ein Problem anhand der folgenden Informationen nicht diagnostizieren und beheben können, finden Sie unter „Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden“ auf Seite 48 oder „Lenovo XClarity Forum und Lenovo XClarity Ideation verwenden“ auf Seite 49 weitere Informationen.

Symptom	Aktion
XClarity Integrator-Service kann keine Verbindung zum Operations Manager herstellen.	<ol style="list-style-type: none">1. Vergewissern Sie sich, dass die Anmeldeinformationen korrekt sind.2. Vergewissern Sie sich, dass die Firewall XClarity Integrator Service → Operations Manager (Port 5724) zulässt.3. Stellen Sie sicher, dass der SDK Service auf Operations Manager ausgeführt wird.
BMC wird in XClarity Integrator Service nicht erkannt.	<ol style="list-style-type: none">1. Stellen Sie sicher, dass die BMC-IP-Adresse verbunden werden kann.2. Stellen Sie sicher, dass die Firewall XClarity Integrator Service → BMC (SLP-Port 427) zulässt.
BMC wird in XClarity Integrator Service nicht authentifiziert.	<ol style="list-style-type: none">1. Stellen Sie sicher, dass der BMC-Account korrekt ist, damit Sie sich bei der BMC-Webseite anmelden können.2. Starten Sie BMC erneut und authentifizieren Sie sich nochmals.
Ereignis/Warnung wird von BMC nicht empfangen. Es gibt eine Warnung auf der BMC-Webseite, aber es wurde keine Warnung im Operations Manager ausgelöst.	<ol style="list-style-type: none">1. Stellen Sie sicher, dass BMC in XClarity Integrator Service authentifiziert wird.2. Stellen Sie sicher, dass die Warnung nach der Authentifizierung von BMC generiert wird.3. Stellen Sie sicher, dass die BMC → XClarity Integrator Service (Port 9500) zulässt.4. Stellen Sie sicher, dass der Verbindungsstatus des Operation Manager auf der XClarity Integrator-Service-Webseite online ist.
Der Status einiger BMC Hardwarekomponenten wird in Operations Manager als Not monitored (Nicht überwacht) angezeigt.	Die Hardwarekomponenten werden jedoch tatsächlich überwacht. Siehe „Systemstatus überprüfen“ auf Seite 23.
Es liegt keine BMC-IP-Adresse im XClarity Integrator Service und Operations Manager vor.	<ol style="list-style-type: none">1. Stellen Sie sicher, dass die BMC-IP-Adresse nicht geändert wurde.2. Ermitteln und authentifizieren Sie BMC erneut.

<p>Das erkannte Gehäuse installiert mit Windows Server 2012 wird in der Ansicht Network Devices Pending Management (Netzwerkgeräte mit ausstehender Verwaltung) angezeigt.</p>	<ol style="list-style-type: none"> 1. Starten Sie den Operations Manager. 2. Starten Sie die ein- und ausgehenden Regeln und starten Sie die Ermittlungsregel neu. <p>Anmerkung: Einige Regeln sind möglicherweise standardmäßig deaktiviert.</p> <ol style="list-style-type: none"> 3. Warten Sie, bis die Regeln in die geplante Aufgabe in der Operations Manager Console konvertiert werden.
<p>Die AMM/CMM-Webkonsole kann nicht über die Operations Manager Console auf einem Server mit installiertem Windows Server 2012 geöffnet werden.</p>	<ol style="list-style-type: none"> 1. Klicken Sie auf Server Manager (Server-Manager) → Configure this local server (Lokalen Server konfigurieren). Die Seite Local Server Configuration (Lokale Serverkonfiguration) wird geöffnet. 2. Klicken Sie auf On (Ein) im Bereich Properties (Eigenschaften). Das Dialogfeld Internet Explorer Enhanced Security Configuration (Verstärkte Sicherheitskonfiguration für Internet Explorer) wird geöffnet. <p>Anmerkung: Wenn sich auch ein Mitglied der lokalen Administratorengruppe anmeldet, klicken Sie auf Off (Aus). Anschließend können Sie die verstärkte Sicherheitskonfiguration für Internet Explorer weiterhin verwenden.</p> <ol style="list-style-type: none"> 3. Klicken Sie auf OK, um die Änderungen anzuwenden.
<p>Die Fehlermeldung „Could not locate automation class named IBM.SystemsManagement.SCOMHelper.SCOMServer (Automatisierungsklasse IBM wurde nicht gefunden. SystemsManagement.SCOMHelper.SCOMServer)“ wird angezeigt.</p>	<p>Führen Sie einen der folgenden Schritte aus:</p> <ul style="list-style-type: none"> • Wählen Sie einen Ressourcenpool, der nur die Server enthält, auf denen das Lenovo Hardware Management Pack installiert ist. • Erstellen Sie einen neuen Ressourcenpool, der nur die Server enthält, auf denen das Lenovo Hardware Management Pack installiert ist.

Integritäts-Explorer zum Anzeigen und Beheben von Problemen verwenden

Das folgende Verfahren beschreibt, wie Sie die Alerts mithilfe des Integritäts-Explorers anzeigen, mehr über sie erfahren, und beheben.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.

Schritt 3. Führen Sie abhängig von Ihren Servermodellen einen der folgenden Schritte aus:

- Für die Lenovo Server klicken Sie auf die Ansicht **Lenovo Windows System Group (Lenovo Windows-Systemgruppe)**
- Klicken Sie für die BMC-basierten Server auf die Ansicht **Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC)**
- Für die ThinkServer-Server klicken Sie auf die Ansicht **Lenovo ThinkServer BMC**
- Für das BladeCenter-Gehäuse klicken Sie auf die Ansicht **Lenovo BladeCenter(s)** im Ordner **Lenovo BladeCenter(s) and Modules (Lenovo BladeCenter und Module)**

- Für das Flex System Gehäuse klicken Sie auf die Ansicht **Lenovo Flex System Chassis (Lenovo Flex System Gehäuse)** im Ordner **Lenovo Flex System Chassis and Modules (Gehäuse und Module des Lenovo Flex Systems)**

Anmerkung: Standardmäßig werden beim Öffnen des Health Explorer (Integritäts-Explorer) alle Überwachungsprogramme mit Fehlern in einer erweiterten Ansicht angezeigt.

Schritt 4. Wählen Sie einen Alert aus und doppelklicken Sie auf **State (Status)**, um den Integritäts-Explorer zu öffnen. Alle Überwachungsprogramme der ersten Stufe, die die Fehler anzeigen, werden auf der Seite **Health Explorer (Integritäts-Explorer)** angezeigt.

Schritt 5. Führen Sie je nach Bedarf eine der folgenden Aktionen aus:

- a. Klicken Sie auf **State Change Events (Statusänderungsereignisse)**, um die aktuellen Statusänderungsereignisse anzuzeigen.
- b. Klicken Sie auf **Knowledge (Wissen)**, um die Erläuterungen zu und Lösungen für Alerts anzuzeigen. Führen Sie bei Bedarf die auf den **Knowledge (Wissen)**-Seiten beschriebenen Schritte durch, um den Fehler zu beheben, und setzen Sie den Statussensor zurück.

Anmerkung: Sie können die Seite **Knowledge (Wissen)** auch anzeigen, indem Sie auf die Ansicht **Active Alerts (Aktive Alerts)** in der Operations Manager Console oder auf den Link in der Registerkarte **Produkt Knowledge (Produktwissen)** klicken.

- c. Doppelklicken Sie auf einen Alert, um die Alerteigenschaften anzuzeigen. Die Alerteigenschaften werden auf der Registerkarte **General (Allgemein)** angezeigt.

Lenovo XClarity Forum und Lenovo XClarity Ideation verwenden

Im folgenden Verfahren wird beschrieben, wie Sie Fragen, Vorschläge oder Ideen mit Lenovo XClarity Forum und Lenovo XClarity Ideation übermitteln.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Monitoring (Überwachung) → Lenovo Hardware**.

Schritt 3. Führen Sie abhängig von Ihren Servermodellen einen der folgenden Schritte aus:

- Für die Lenovo Server klicken Sie auf die Ansicht **Lenovo Windows System Group (Lenovo Windows-Systemgruppe)**
- Klicken Sie für die BMC-basierten Server auf die Ansicht **Lenovo System x and ThinkSystem BMC (Lenovo System x und ThinkSystem BMC)**
- Für die ThinkServer-Server klicken Sie auf die Ansicht **Lenovo ThinkServer BMC**
- Für das BladeCenter-Gehäuse klicken Sie auf die Ansicht **Lenovo BladeCenter(s)** im Ordner **Lenovo BladeCenter(s) and Modules (Lenovo BladeCenter und Module)**
- Für das Flex System Gehäuse klicken Sie auf die Ansicht **Lenovo Flex System Chassis (Lenovo Flex System Gehäuse)** im Ordner **Lenovo Flex System Chassis and Modules (Gehäuse und Module des Lenovo Flex Systems)**

Schritt 4. Wählen Sie einen Server oder ein Gehäuse aus.

Schritt 5. Um eine Frage zu übermitteln, klicken Sie auf **Lenovo XClarity Forum**; um Vorschläge oder Ideen zu übermitteln, klicken Sie auf **Lenovo XClarity Forum** oder auf **Lenovo XClarity Ideation**.

Schritt 6. Befolgen Sie die angezeigten Anweisungen.

Anhang A. Funktionen zur barrierefreien Bedienung

Funktionen zur barrierefreien Bedienung helfen Benutzern mit körperlichen Behinderungen wie etwa mit eingeschränkter Beweglichkeit oder eingeschränktem Sehvermögen dabei, Softwareprodukte erfolgreich einzusetzen.

Lenovo möchte Produkte anbieten, die Zugriff für alle, unabhängig von Alter oder Fähigkeit, ermöglichen.

Das Lenovo Hardware Management Pack unterstützt die Funktionen zur barrierefreien Bedienung der integrierten Systemverwaltungssoftware. Die spezifischen Angaben zu Funktionen zur barrierefreien Bedienung und Tastaturnavigation finden Sie in der Dokumentation Ihrer Systemverwaltungssoftware.

Die Themensammlung zu Lenovo Hardware Management Pack und die verwandten Veröffentlichungen sind für den Lenovo-Home Page Reader zugänglich. Sie können alle Funktionen über die Tastatur anstatt über die Maus ausführen.

Sie können die Veröffentlichungen für Lenovo Hardware Management Pack im Adobe PDF-Format (Portable Document Format) mit Adobe Acrobat Reader anzeigen. Sie können über die Lenovo Hardware Management Pack-Download-Webseiten auf die PDFs zugreifen.

Lenovo und behindertengerechte Bedienung

Weitere Informationen darüber, wie sich [Webseite „Lenovo Accessibility“](#) für barrierefreie Bedienung einsetzt, finden Sie unter [Lenovo](#).

Anhang B. Bewährte Verfahren

Die Themen in diesem Abschnitt bieten vorgeschlagene Methoden für das Abschließen von Tasks.

Die Ursache eines Fehlers bestimmen

Verwenden Sie das folgende Diagnoseverfahren, um Probleme zu identifizieren und zu beheben, die möglicherweise in einer verwalteten Umgebung auftreten.

Vorgehensweise

Schritt 1. Melden Sie sich an der Operations Manager Console an.

Schritt 2. Klicken Sie auf **Monitoring** (Überwachung).

Schritt 3. Um den Status all Ihrer verwalteten Systeme anzuzeigen, auf denen Windows-Betriebssysteme installiert sind, klicken Sie auf **Lenovo Hardware → Windows Computers on Lenovo Windows Systems Group (Windows-Computer in der Lenovo Windows-Systemgruppe)**.

Schritt 4. Überprüfen Sie die Status der Systeme, die im oberen Ergebnisbereich angezeigt werden. Alle neu erkannten Objekte sind standardmäßig in einem fehlerfreien Zustand. Der Task zur Überwachung des Zustands aktualisiert den Status eines Objekts in regelmäßigen Abständen, entsprechend der Standardintervalleinstellung. Sie können die Überwachungshäufigkeit konfigurieren, indem Sie den Parameter **override-controlled** verwenden. Weitere Informationen über den Parameter **override-controlled** finden Sie in der Microsoft System Center Operations Manager-Dokumentation.

Schritt 5. Wählen Sie ein System aus, das den Status *Critical* oder *Warning* anzeigt.

Schritt 6. Überprüfen Sie, ob der Fehler von der Hardware oder Software verursacht wird.

- **Hardwarebezogene Fehler:** Überprüfen Sie den Bereich Lenovo-Hardwarekomponenten vom **System x-Server oder von x86-/x64 Bladeservern**, um das System auszuwählen. Blättern Sie nach rechts, um alle Komponentenstatus und Daten anzuzeigen. Sie können diese Ansicht personalisieren.

Dieser Bereich enthält Statusansichten auf Grundlage der Klasse der Hardwarekomponentenbasis. Der Zweck dieser Ansicht ist, Zugriff auf detaillierte Eigenschaften jeder Komponenteninstanz zu ermöglichen. Suchen Sie nach zusätzlichen Systeminformationen in der **Detail View (Detailansicht)**.

- **Softwarebezogene Fehler:** Überprüfen Sie den Bereich Windows-Computer auf dem **System x-Server oder den x86/x64 Bladeservern**. Dieser Bereich enthält Statusansichten und Informationen auf einer Pro-Softwarekomponentenklasse-Basis. Wählen Sie ein System aus, das entweder den Integritätsstatus *Critical* oder *Warning* anzeigt.

Der Zweck dieser Ansichten ist, Zugriff auf detaillierte Eigenschaften jeder Komponenteninstanz zu ermöglichen. Die **Detail View (Detailansicht)** zeigt alle Instanzen der Systemsoftware mit einem Integritätstatus für jeden der vier Integritätsaspekte an.

Schritt 7. Um weitere Informationen und Details zu einem Fehler zu erhalten, rufen Sie die Hardwareinformationen des gewünschten BladeCenter-Moduls oder der gewünschten Hardwaresystemkomponente auf, indem Sie **Lenovo BladeCenter Modules** (Lenovo BladeCenter-Module) klicken.

Schritt 8. Wenn Sie bereits wissen, dass zum Beispiel eine Netzteilkomponente fehlgeschlagen ist, wählen Sie die zugehörige Ansicht **Lenovo BladeCenter Power Modules** (Lenovo BladeCenter Stromversorgungsmodule), um den Fehler am Netzteil zu bestimmen.

Schritt 9. Klicken Sie auf ein Stromversorgungsmodul mit dem Status **Critical** (Kritisch) und überprüfen Sie die zugeordneten Daten.

- Schritt 10. Lesen Sie die Informationen und Daten, die im Bereich **Detail View (Detailansicht)** dargestellt werden. Überprüfen Sie alle Instanzen des Modultyps und jeden der vier Integritätsaspekte.
- Schritt 11. Klicken Sie mit der rechten Maustaste auf das ausgewählte Modul, und anschließend auf **Open (Öffnen) → Health Explorer (Integritäts-Explorer)**.
- Schritt 12. Wählen Sie den Alert, und überprüfen Sie die Informationen auf der Seite **State Change Events (Statusänderungsereignisse)**.
- Schritt 13. Abhängig vom Typ des Alerts erhalten Sie weitere Informationen durch Klicken auf **View Alert** (Alert anzeigen).
- Schritt 14. Klicken Sie auf die Registerkarte **Knowledge (Wissen)**, um die Seite **Knowledge (Wissen)** und einen oder mehrere Wissensartikel zu Ihrem Alert zu lesen.

Wichtig: Zusätzlich zu den für jedes Objekt verfügbaren Integritätsinformationen sind möglicherweise weitere Informationen von anderen Objekte verfügbar, die die verschiedenen Perspektiven der Integrität beleuchten. Beispielsweise zeigt ein Bladeserver, der in-band über seinen Plattformagenten überwacht wird, einen Integritätsstatus, das BladeCenter-Chassis Management Module zeigt aber auch einen Integritätsstatus für den Bladeserver.

Andere BladeCenter-Gehäusemodule wirken sich möglicherweise auf die Integrität des Bladeservers aus, wie ein Netzteil, das den Bladeserver mit Strom versorgt. Ebenso kann der Status eines Bladeservers aus der Perspektive des Verwaltungsmoduls den Status und andere Informationen über das Betriebssystem, das auf dem Bladeserver ausgeführt wird, enthalten.

Beispielsweise hat der folgende BladeCenter Simple Network Management Protocol(SNMP)-Alert ein Ereignisbeschreibungsfeld *1.3.6.1.4.1.2.6.158.3.1.1.8* und eine Ereignis-ID *1.3.6.1.4.1.2.6.158.3.1.1.14*. Wandeln Sie den Dezimal-Ereignis-ID-Wert in eine Hexadezimalzahl um, um die Nachricht im *Handbuch mit den Nachrichten des erweiterten Managementmoduls* zu suchen.

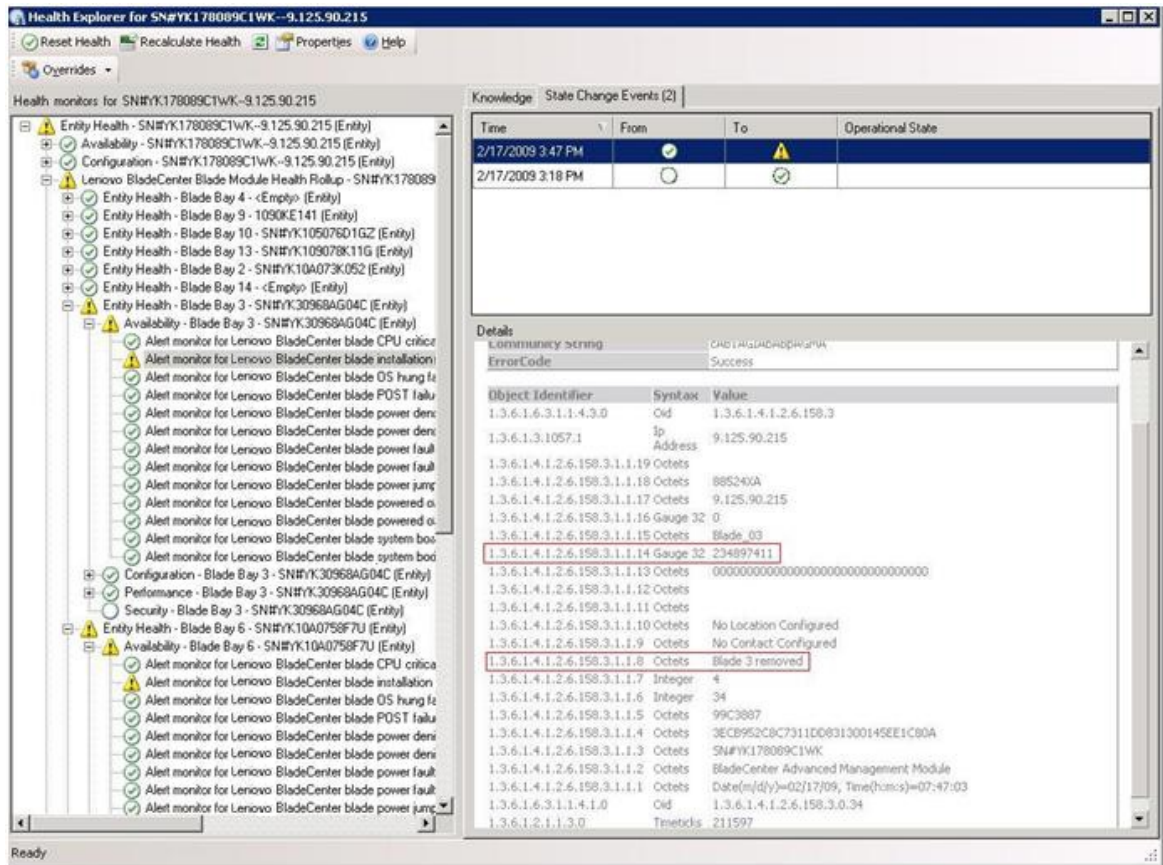


Abbildung 1. System x Windows Management Instrumentation(WMI)-Ereignis

Bei einem System x-WMI-Ereignis enthält der Bereich **Details** die Ereignis-ID und eine Beschreibung.

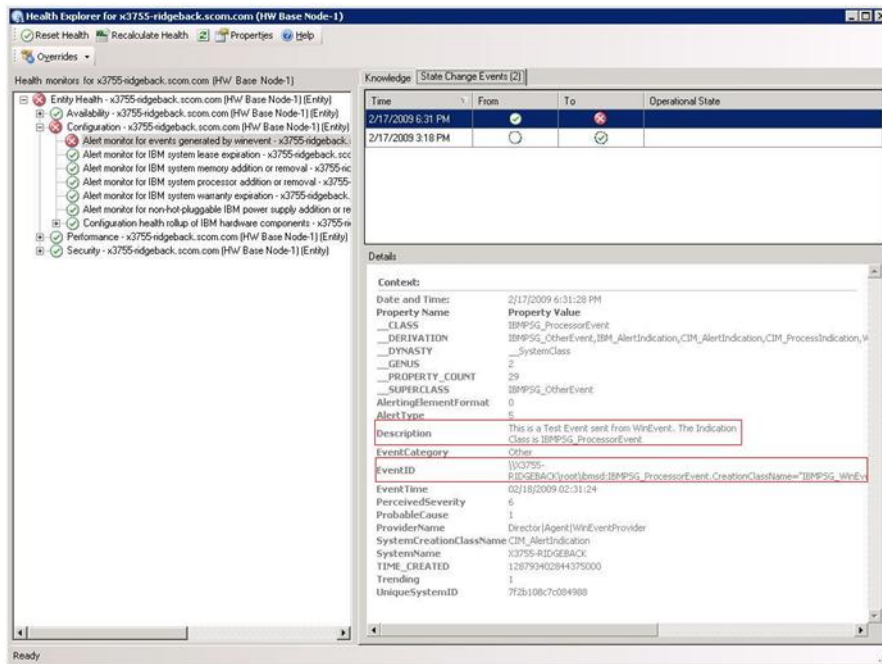


Abbildung 2. Beispiel für ausführliche Informationen auf der Registerkarte „Statusänderungsereignisse“

Alle BladeCenters erneut erkennen

Die BladeCenter-Überwachung gibt eine Warnung aus, wenn die gleiche Version von Lenovo Hardware Management Pack gelöscht und erneut importiert wird.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie auf **Administration (Verwaltung) → Device Management (Einheitenverwaltung) → Network Devices (Netzwerkeinheiten)**.
- Schritt 3. Notieren Sie sich die IP-Adressen, die in der Ansicht **Network Devices (Netzwerkeinheiten)** des Ergebnisbereichs angezeigt werden. Sie werden diese Informationen später für die Erkennungsnetzwerkeinheiten-Informationen benötigen.
- Schritt 4. Wählen Sie die **IP Address (IP-Adresse)** des BladeCenter, den Sie erneut erkennen möchten, im Bereich **Actions (Aktionen)** und wählen Sie **Delete (Löschen)** aus.
- Schritt 5. Verwenden Sie die notierte IP-Adresse, um den Umfang der Netzwerkeinheiten einzuschränken, und ermitteln Sie die BladeCenter erneut.

Einen umbenannten Server erneut erkennen

Wenn ein Windows-Server umbenannt wird, ist der Windows-Serverinstanzeintrag, der von Operations Manager überwacht wird, ausgeblendet. Dies ist ein Zeichen dafür, dass der Windows-Server nicht mehr von der Operations Manager überwacht wird.

Um einen umbenannten Server erneut zu erkennen und zu überwachen, löschen Sie zuerst den ursprünglichen Servernamen aus der Liste **Operations Manager Agent Managed server** (Mit Operations Manager Agent verwalteter Server) und erkennen Sie den umbenannten Server mithilfe des folgenden Verfahrens erneut.

Vorgehensweise

- Schritt 1. Melden Sie sich an der Operations Manager Console an.
- Schritt 2. Klicken Sie auf **Administration (Verwaltung)** → **Device Management (Einheitenverwaltung)** → **Agent Managed (Mit Agents verwaltet)**.

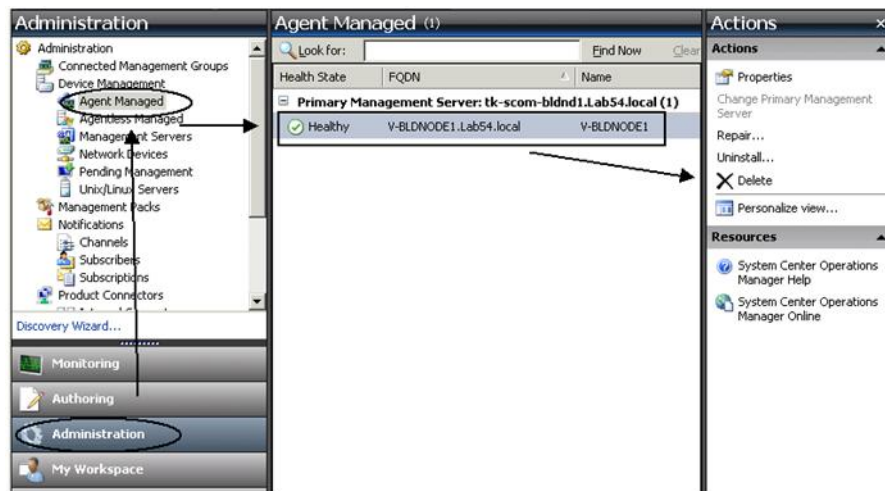


Abbildung 3. Einen umbenannten Server löschen

- Schritt 3. Wählen Sie den ursprünglichen Namen in der Ansicht **Agent Managed (Mit Agents verwaltet)** des Ergebnisbereichs aus. Dieser Eintrag hat den ursprünglichen Namen, bevor er umbenannt wurde.
- Schritt 4. Klicken Sie im Bereich **Actions (Aktionen)** auf der rechten Seite der Operations Manager Console auf **Delete (Löschen)**. Diese Aktion entfernt den umbenannten Server aus der Ansicht.
- Schritt 5. Fügen Sie den neuen Servernamen hinzu.

Anhang C. Systemfirewalleinstellungen

In diesem Abschnitt wird beschrieben, wie Sie Firewallausnahmen festlegen.

Diese Tabelle ist eine Referenz zur Bestimmung der Ports, die für die angegebenen Lenovo XClarity Integrator-Produkte verwendet werden.

Tabelle 4. Von Lenovo XClarity Integrator-Produkten verwendete Ports.

Projekt	Quelle			Ziel			Protokoll	Hinweise
	Port	Position	Komponente	Port	Position	Komponente		
SCVMM-Add-in	nicht angegeben	Verwaltungs-server	SCVMM Add-in-Konsole (localhost/127.0.0.1)	TCP 9500*	Verwaltungs-server	Lenovo XClarity Integrator XClarity Integrator Service	HTTPS	Sie können den Ziel-Port ändern, wenn Lenovo XClarity Integrator installiert ist.
		verwalteter Server	Hyper-V-/Windows-Clients, die mit SCVMM verwaltet werden					
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Service (localhost/127.0.0.1)	TCP 5432*	Verwaltungs-server	PostgreSQL	nicht zutreffend	Sie können den Ziel-Port ändern, wenn Lenovo XClarity Integrator installiert ist.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Service	TCP 5988 TCP 5989 UDP 427	verwalteter Server	BMC	HTTP, CIM	Sie können die BMC-HTTP/HTTPS-Ports im BMC-Portal ändern.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Service	TCP 80 TCP 443	externe Ressource	Webseite „IBM/Lenovo“	HTTP HTTPS	Sie können Firmware von der Webseite „IBM/Lenovo“ über HTTP-Proxy herunterladen.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Service	TCP 443	externe Ressource	Lenovo XClarity Administrator	HTTPS	Der Port hängt von der Lenovo XClarity Administrator-Konfiguration ab. Sie müssen dem richtigen Port eingeben, wenn Sie den Lenovo XClarity Administrator in Lenovo XClarity Integrator registrieren.

Tabelle 4. Von Lenovo XClarity Integrator-Produkten verwendete Ports. (Forts.)

Projekt	Quelle			Ziel			Protokoll	Hinweise
	Port	Position	Komponente	Port	Position	Komponente		
	nicht angegeben	Verwaltungs- server	Lenovo XClarity Integrator Service	TCP 135	verwalteter Server	Host-BS – WMI- Server	CIM	nicht zutreffend
	nicht angegeben	Verwaltungs- server	Lenovo XClarity Integrator Service	UDP 137	verwalteter Server	Host-BS – Samba- Server	NetBIOS- Namens- dienst (NMBD)	nicht zutreffend
				UDP 138			SMB	
				TCP 139			LDAP	
				TCP 389			NetBIOS	
				TCP 445			SWAT	
				TCP 901				
				UDP 137	Verwaltungs- server	BS – Samba-Server	NetBIOS- Namens- dienst (NMBD)	nicht zutreffend
				UDP 138			SMB	
				TCP 139			LDAP	
			TCP 389			NetBIOS		
			TCP 445			SWAT		
			TCP 901					
SCOM HWMIP	nicht angegeben	Lenovo XClarity Integrator	Lenovo XClarity Integrator Service	TCP 5724	Verwaltungs- server	SDK-Service	nicht zutreffend	Stellen Sie eine Verbindung zum Operations Manager SDK-Service her.
	nicht angegeben	Verwaltungs- server, BMC- Knoten	Lenovo Hardware, MP BMC-Knoten	TCP 9500*	Lenovo XClarity Integrator	Lenovo XClarity Integrator Service	HTTPS	Der Ziel-Port kann geändert werden, wenn Sie Lenovo XClarity Integrator installieren.

Tabelle 4. Von Lenovo XClarity Integrator-Produkten verwendete Ports. (Forts.)

Projekt	Quelle			Ziel			Protokoll	Hinweise
	Port	Position	Komponente	Port	Position	Komponente		
SCCM OSD	nicht angegeben	verwalteter Host	Lenovo Hardware MP	TCP 9500*	Lenovo XClarity Integrator	Lenovo XClarity Integrator Service	HTTPS	Ist für die automatische Ermittlung von BMC erforderlich.
	nicht angegeben	Lenovo XClarity Integrator	Lenovo XClarity Integrator Service (localhost/127.0.0.1)	TCP 5432*	Lenovo XClarity Integrator	PostgreSQL	nicht zutreffend	Der Ziel-Port kann geändert werden, wenn die PostgreSQL-Datenbank installiert ist.
	nicht angegeben	Lenovo XClarity Integrator	Lenovo XClarity Integrator Service	TCP 5988 TCP 5989 UDP 427	BMC-Knoten	BMC-Knoten	HTTP, CIM HTTPS, CIM SLP	Die BMC-HTTP/HTTPS-Ports können in das BMC-Portal geändert werden. SLP wird zum Ermitteln von BMC verwendet.
	nicht angegeben	Verwaltungs-server	Lenovo Hardware MP	TCP 161 TCP 162	Gehäuse	CMM oder AMM	SNMP SNMP-Traps	Die Ports können in das CMM-Portal geändert werden.
	nicht angegeben	Verwaltungs-server	SCCM OSD-Konsole	UDP 137 UDP 138 TCP 139 TCP 389 TCP 445 TCP 901	verwalteter Server	Preboot-BS und Host-BS – Samba-Server	NetBIOS-Namensdienst (NMBD) SMB LDAP NetBIOS SWAT	nicht zutreffend
	nicht angegeben	verwalteter Server	PXE-Client	UDP 67 UDP 68 UDP 69	Verwaltungs-server	DHCP-Server TFTP-Server	DHCP TFTP	nicht zutreffend

Tabelle 4. Von Lenovo XClarity Integrator-Produkten verwendete Ports. (Forts.)

Projekt	Quelle		Ziel			Hinweise		
	Port	Position	Komponente	Port	Position		Komponente	
SCCM-Aktualisierung	nicht angegeben	Verwaltungs-server	SCCM-Update-Tool	TCP 80	externe Ressource	WSUS-Server	HTTP	nicht zutreffend
				TCP 443			HTTPS	
				TCP 8530	externe Ressource	WSUS-Server (Windows Server 2012 und höhere Version)	HTTP	nicht zutreffend
				TCP 8531			HTTPS	
SCCM Inventory				UDP 137	verwalteter Server	Host-BS – Samba-Server	NetBIOS-Namensdienst (NMBD)	nicht zutreffend
				UDP 138			SMB	
				TCP 139			LDAP	
				TCP 389			NetBIOS	
				TCP 445			SWAT	
				TCP 901				
SCCM Inventory	nicht angegeben	Verwaltungs-server	SCCM Inventory Tool	TCP 5988	verwalteter Server	BMC	HTTP, CIM, SLP	Die BMC-HTTP/HTTPS-Ports können in das BMC-Portal geändert werden.
				TCP 5989			HTTPS, CIM, SLP	
SCCM-Konfiguration	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend

*Die mit einem Stern gekennzeichneten Ports werden von Lenovo XClarity Integrator registriert. Die anderen werden nur verwendet, um auf bestimmte Services in Lenovo XClarity Integrator zuzugreifen.

Anhang D. Hinweise

Möglicherweise bietet Lenovo die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim Lenovo Ansprechpartner erhältlich.

Hinweise auf Lenovo Lizenzprogramme oder andere Lenovo Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von Lenovo verwendet werden können. Anstelle der Lenovo Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von Lenovo verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es Lenovo Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an die nachstehende Adresse zu richten. Anfragen an diese Adresse müssen auf Englisch formuliert werden.

*Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing*

Lenovo stellt diese Veröffentlichung in der vorliegenden Form (auf „as-is“-Basis) zur Verfügung und übernimmt keine Garantie für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck und die Freiheit der Rechte Dritter. Einige Rechtsordnungen erlauben keine Garantieausschlüsse bei bestimmten Transaktionen, sodass dieser Hinweis möglicherweise nicht zutreffend ist.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Lenovo kann ohne weitere Mitteilung jederzeit Verbesserungen oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten oder Programmen vornehmen.

Die in diesem Dokument beschriebenen Produkte sind nicht zur Verwendung bei Implantationen oder anderen lebenserhaltenden Anwendungen, bei denen ein Nichtfunktionieren zu Verletzungen oder zum Tode führen könnte, vorgesehen. Die Informationen in diesem Dokument beeinflussen oder ändern nicht die Lenovo Produktspezifikationen oder Garantien. Keine Passagen in dieser Dokumentation stellen eine ausdrückliche oder stillschweigende Lizenz oder Anspruchsgrundlage bezüglich der gewerblichen Schutzrechte von Lenovo oder von anderen Firmen dar. Alle Informationen in dieser Dokumentation beziehen sich auf eine bestimmte Betriebsumgebung und dienen zur Veranschaulichung. In anderen Betriebsumgebungen werden möglicherweise andere Ergebnisse erzielt.

Werden an Lenovo Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Verweise in diesen Informationen auf Webseiten anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Webseiten dar. Das über diese Webseiten verfügbare Material ist nicht Bestandteil des Materials für dieses Lenovo Produkt. Die Verwendung dieser Webseiten geschieht auf eigene Verantwortung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier

erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments müssen überprüfen, welche Daten für ihre jeweilige Umgebung maßgeblich sind.

Marken

LENOVO, BLADECENTER, THINKSERVER, THINKSYSTEM, SYSTEM X, XCLARITY und NEXTSCALE SYSTEM sind Marken von Lenovo.

Internet Explorer, Microsoft und Windows sind Marken der Microsoft Group.

IBM ist eine Marke der International Business Machines Corporation, die in vielen Ländern weltweit registriert ist.

Alle anderen Marken sind Eigentum der jeweiligen Inhaber. © 2019 Lenovo.

Wichtige Anmerkungen

Die Prozessorgeschwindigkeit bezieht sich auf die interne Taktgeschwindigkeit des Mikroprozessors. Das Leistungsverhalten der Anwendung ist außerdem von anderen Faktoren abhängig.

Bei Angaben in Bezug auf Hauptspeicher, realen/virtuellen Speicher oder Kanalvolumen steht die Abkürzung KB für 1.024 Bytes, MB für 1.048.576 Bytes und GB für 1.073.741.824 Bytes.

Bei Angaben zur Kapazität von Festplattenlaufwerken oder zu Übertragungsgeschwindigkeiten steht MB für 1.000.000 Bytes und GB für 1.000.000.000 Bytes. Die gesamte für den Benutzer verfügbare Speicherkapazität kann je nach Betriebsumgebung variieren.

Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen. Eine eventuelle Unterstützung für Produkte anderer Hersteller erfolgt durch Drittanbieter, nicht durch Lenovo.

Manche Software kann sich von der im Einzelhandel erhältlichen Version (falls verfügbar) unterscheiden und enthält möglicherweise keine Benutzerhandbücher bzw. nicht alle Programmfunktionen.

Lenovo