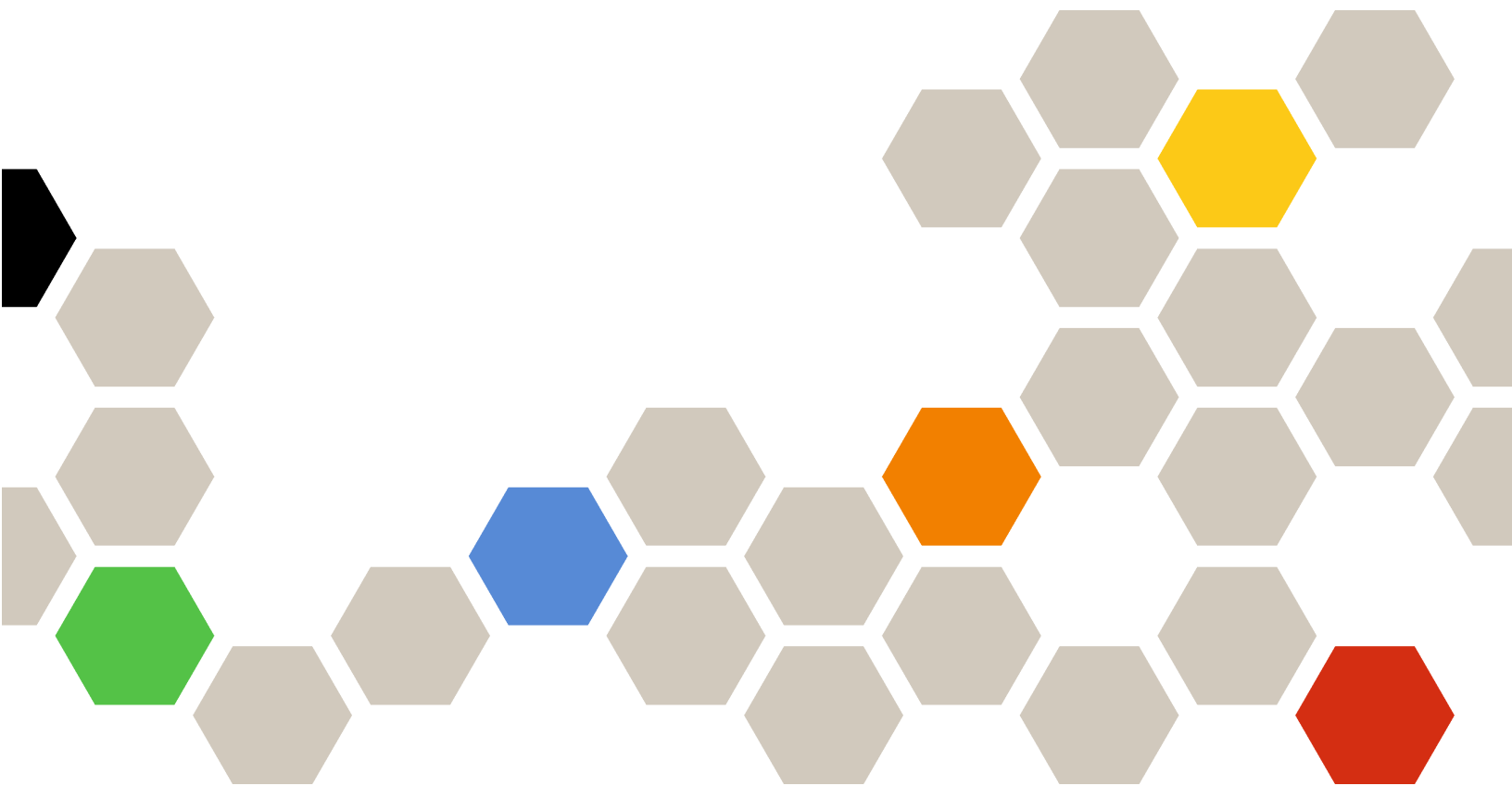




Lenovo Add-in für Microsoft System Center Virtual Machine Manager Installations- und Benutzerhandbuch



Version 3.3.0

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter Anhang B „Hinweise“ auf Seite 59 gelesen werden.

Zwölfte Ausgabe (November 2017)

© Copyright Lenovo 2014, 2017.

Portions © Copyright IBM Corporation 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	iv

Kapitel 1. Lenovo-Add-In 1

Kapitel 2. Systemvoraussetzungen 3

Hardwarevoraussetzungen	3
Softwarevoraussetzungen	6

Kapitel 3. Lenovo-Add-In installieren 7

Lenovo-Add-In deinstallieren	7
Lenovo-Add-In aus SCVMM entfernen	8

Kapitel 4. Lenovo-Add-In verwenden 11

Lenovo-Add-In importieren	11
Lenovo-Add-In starten	12
Bei Unified Service anmelden	13
Zertifizierung	14
Hostauthentifizierung einrichten	14
Einstellungen für laufende Systemaktualisierung festlegen	16
Ein Baseboard Management Controller (BMC) hinzufügen	16
BMC-Ermittlung	17
BMC-Authentifizierung	17
Lenovo XClarity Administrator hinzufügen	17
Lenovo XClarity Administrator-Serverzertifikat herunterladen	18
Vertrauenswürdige Zertifikate verwalten	19

Kapitel 5. Mit Funktionen arbeiten 21

Informationen sammeln	21
Hostinformationen anzeigen	21
Allgemeine Informationen zu Lenovo XClarity Administrator anzeigen	21
Eine Gehäuseübersicht anzeigen	22
Nach Ressourcen suchen	25
Überwachung	26
PFA-Verwaltung	27
Server aktualisieren	28
Laufende Systemaktualisierung	28
Laufender Systemneustart	33
Lenovo-Add-In konfigurieren	34
Konfigurationsmuster	34

Kapitel 6. Lenovo-Add-In konfigurieren 41

Lenovo XClarity Integrator-Verwaltung öffnen	41
Kennwort für Unified Service ändern	41
Servicedaten erfassen	41
Protokolldateien erfassen	41
Protokollierungsstufe ändern	41
Sicherheit verwalten	42
BMC-Kommunikationsprotokoll festlegen	42
Datenbankinformationen anzeigen	42
Daten von PostgreSQL zu SQL migrieren	42
Mit Sicherheitszertifikaten arbeiten	43
Ein angepasstes, extern signiertes Serverzertifikat generieren	43
Das von Lenovo XClarity Integrator generierte Serverzertifikat wiederherstellen	44
Stammzertifikat neu generieren	44
Stammzertifikat herunterladen	45

Kapitel 7. Fehlerbehebung 47

Scanjob für laufende Systemaktualisierung aufgrund von Systemfehler 22029 fehlgeschlagen	47
Fehler beim Speichern der Einstellungen für laufende Systemaktualisierung aufgrund von Systemfehler 1219	47
Die Lenovo XClarity Integrator Unified Service-Sitzung wird ungültig	47
Vorauthentifiziertes IMM verliert möglicherweise nach der Verwaltung durch Lenovo XClarity Administrator die Verbindung	48
Funktionen sind nicht für einen System x-Server verfügbar, wenn sie aus der Ressourcenbaumstruktur ausgewählt werden	48
Registrierung von Lenovo XClarity Administrator mit IPv6-Adresse fehlgeschlagen	49
Host wird in der SCVMM-Hostliste angezeigt, allerdings nicht im Lenovo-Add-In	49
Installationsprogramm zeigt Fehlernachricht an	50
Microsoft Internet Explorer-Update KB3087038 installieren	50
Lenovo XClarity Administrator-Zertifikat kann nicht importiert werden, wenn Internet Explorer 10 verwendet wird	50

Anhang A. Systemfirewalleinrichtungen 53

Anhang B. Hinweise 59

Marken	60
Wichtige Anmerkungen	60

Informationen über diese Veröffentlichung

Dieses Buch enthält Anweisungen für die Installation und Verwendung des Lenovo Add-in für Microsoft System Center Virtual Machine Manager.

Eine Übersicht über die neue Funktionalität in Version v3.3.0 sowie wichtige Informationen zu bekannten Einschränkungen und Lösungsstrategien finden Sie in den *Versionshinweisen Lenovo Add-in für Microsoft System Center Virtual Machine Manager*.

Das Lenovo Add-in für Microsoft System Center Virtual Machine Manager ist eine Plug-in-Anwendung für Microsoft System Center Virtual Machine Manager, die für die Verwaltung von Lenovo System x und Flex System-Servern konzipiert wurde. Sie bietet Mehrwertfunktionen, über die die Hardware- und die virtuelle Infrastruktur verbunden werden.

Konventionen und Terminologie

Absätze, die mit den fettgedruckten Begriffen **Hinweis**, **Wichtig** oder **Achtung** 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.

Achtung: Diese Bemerkungen weisen auf eventuelle Schäden an Programmen, Geräten oder Daten hin. Der Hinweis „Achtung“ wird vor einer Anweisung oder Situation angezeigt, bei der es zu Beschädigungen kommen kann.

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

Tabelle 1. Definitionen für Begriffe, die in diesem Handbuch verwendet werden

Begriff, Akronym oder Abkürzung	Bedeutung
Baseboard Management Controller (BMC)	Ein Serviceprozessor, der Serviceprozessor-Funktionen und einen Videocontroller in einem einzigen Chip vereint.
Lenovo XClarity Administrator	Bietet einen einzelnen Elementmanager für x86-Knoten in Flex Systems und eigenständigen Racks.
Lenovo XClarity Integrator (LXCI)	Eine Toolsuite, mit der IT-Administratoren die Verwaltungsfunktionen des System x in Microsoft System Center integrieren können. Lenovo erweitert die Microsoft System Center-Serververwaltungsfunktionen, indem die Funktion zur Lenovo-Hardwareverwaltung integriert wird, die eine erschwingliche, grundlegende Verwaltung Ihrer physischen und virtuellen Umgebungen ermöglicht, um die Zeit und den Aufwand für die Routinesystemverwaltung zu reduzieren. Sie bietet Ermittlung, Konfiguration, Überwachung, Ereignisverwaltung und Stromüberwachung, die benötigt werden, um die Kosten und Komplexität durch Serverkonsolidierung und vereinfachte Verwaltung zu reduzieren.
Verwaltungsmodus	Eine physische oder virtuelle Maschine, auf der der SCVMM-Service, der Lenovo XClarity Integrator Unified Service und das Lenovo Add-in für Microsoft System Center Virtual Machine Manager installiert sind und ausgeführt werden

Tabelle 1. Definitionen für Begriffe, die in diesem Handbuch verwendet werden (Forts.)

Begriff, Akronym oder Abkürzung	Bedeutung
Verwalteter Knoten	Eine physische Maschine, die mit SCVMM verwaltet wird, auf dem der SCVMM-Agent installiert ist und ausgeführt wird
PFA	Fehlervoraussage-Alert
SCVMM	Microsoft System Center Virtual Machine Manager
UXSP	UpdateXpress System Pack
CA	Zertifizierungsstelle
FQDN	Vollständig qualifizierter Domänenname

Webressourcen

Die folgenden Websites enthalten Ressourcen zum Verständnis, zur Verwendung und zur Fehlerbehebung von System x-, Flex System-, BladeCenter-Servern und Systemverwaltungstools.

Lenovo-Website für Microsoft Systems Management Solutions für Lenovo-Servers

Suchen Sie die neuesten Downloads für das Lenovo Add-in für Microsoft System Center Virtual Machine Manager:

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

Systemverwaltung mit Lenovo XClarity-Lösungen

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

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

Lenovo Technical Support Portal

Diese Website kann Ihnen helfen, wenn Sie Unterstützung für Hardware und Software suchen:

- [Lenovo Support Portal-Website](#)

Lenovo ServerProven-Seiten

Rufen Sie Informationen zu Hardwarekompatibilität mit Lenovo System x, BladeCenter und IBM IntelliStation-Hardware ab.

- [Lenovo ServerProven: Compatibility for BladeCenter products](#)
- [Lenovo ServerProven: Compatibility for Flex System Chassis](#)
- [Lenovo ServerProven: Compatibility for System x hardware, applications, and middleware](#)

Microsoft System Center-Website

Diese Website kann Ihnen helfen, die Microsoft System Center-Produkte zu finden:

- [Microsoft System Center-Website](#)

Kapitel 1. Lenovo-Add-In

Das Lenovo Add-in für Microsoft System Center Virtual Machine Manager ist eine Plug-in-Anwendung für Microsoft System Center Virtual Machine Manager (SCVMM), das als Lenovo XClarity Integrator-Erweiterung bereitgestellt wird. Es ermöglicht die Verwaltung von Lenovo System x- und Flex-Servern und bietet Mehrwertfunktionen, um die Hardwareinfrastruktur und die virtuelle Infrastruktur zu verbinden.

Informationen zu Lenovo XClarity Integrator

Lenovo XClarity Integrator besteht aus Erweiterungen für Microsoft System Center und VMware vCenter. Diese Erweiterungen bieten IT-Administratoren verbesserte Verwaltungsfunktionen für Lenovo System x-Server, BladeCenter-Server und Flex-Systeme. Die Lenovo XClarity Integrator-Erweiterungen enthalten einen Satz an Plug-ins für Microsoft System Center und VMware vCenter, eigenständige Anwendungen und Service-Anwendungen.

Mit Lenovo XClarity Integrator erweitert Lenovo die Verwaltungsfunktionen von Microsoft System Center und VMware vCenter, indem die Funktion zur Lenovo-Hardwareverwaltung integriert wird, die eine erschwingliche, grundlegende Verwaltung Ihrer physischen und virtuellen Umgebungen ermöglicht, um die Zeit und den Aufwand für die Routinesystemverwaltung zu reduzieren. Diese Funktion bietet Ermittlung, Konfiguration, Überwachung, Ereignisverwaltung und Stromüberwachung, die benötigt werden, um die Kosten und Komplexität durch Serverkonsolidierung und vereinfachte Verwaltung zu reduzieren.

Lenovo Add-in für Microsoft System Center Virtual Machine Manager

Durch Funktionen, wie Laufende Systemaktualisierung, die dafür sorgt, dass Firmware ohne Unterbrechung der Wartbarkeit aktualisiert wird, erleichtert das Lenovo-Add-In die Verwaltung von Lenovo. Über eine integrierte Benutzerschnittstelle im SCVMM-Administratorbereich können Sie Lenovo-Hardwareressourcen wie Server verwalten. Lenovo Add-in für Microsoft System Center Virtual Machine Manager benötigt den Lenovo XClarity Integrator Unified Service als Backend.

Kapitel 2. Systemvoraussetzungen

Dieser Abschnitt enthält Informationen zu den speziellen Hardware- und Softwarevoraussetzungen für das Lenovo-Add-In.

Hardwarevoraussetzungen

In diesem Abschnitt werden die Mindest- und empfohlenen Hardwarevoraussetzungen für das Lenovo-Add-In sowie IBM- und Lenovo-Hardware aufgelistet, die vom Add-in verwaltet werden kann.

Hardwarevoraussetzungen für das Lenovo-Add-In

Tabelle 2. Mindest- und empfohlene Hardwarevoraussetzungen für das Lenovo-Add-In

Minimum	Empfohlen
Einzelner x86-64-Prozessor/Kern	4 x86-64-Prozessoren/Kerne
2 GB RAM	8 GB RAM
20 GB freier Speicherplatz auf dem Festplattenlaufwerk	40 GB freier Speicherplatz auf dem Festplattenlaufwerk
Netzwerkkarte mit 100 MB/s	Netzwerkkarte mit 10.000 MB/s

IBM und Lenovo-Hardware

Obwohl Lenovo Add-in für Microsoft System Center Virtual Machine Manager keine Hardwareeinschränkungen hat, ist die Hardware, die es verwaltet, auf die IBM und Lenovo System x und Bladeserver in den folgenden Tabellen beschränkt.

Tabelle 3. Von **Lenovo** unterstützte Hardware

Von Lenovo unterstützte Hardware	Servernummer
NeXtScale	<ul style="list-style-type: none">• nx360 M5 (5465)• nx360 M5 DWC (5467, 5468, 5469)
System x Server	<ul style="list-style-type: none">• x3250 M6 (3633)• x3500 M5 (5464) x3550 M4 (7914)• x3550 M5 (5463)• x3630 M4 (7158)• x3650 M4 (7915)• x3650 M5 (5462)• x3750 M4 (8753)• x3850 X6 / x3950 X6 (6241)
ThinkServer	<ul style="list-style-type: none">• RD350• RD450• RD550• RD650• RS160• SD530 (5493)• TD350• TS460

Tabelle 3. Von Lenovo unterstützte Hardware (Forts.)

Von Lenovo unterstützte Hardware	Servernummer
ThinkSystem	<ul style="list-style-type: none"> • SD530 (7X20, 7X21, 7X22) • SN550 (7X16) • 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) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) (nur China)
Flex-Rechenknoten	<ul style="list-style-type: none"> • Flex System x240 Rechenknoten (7162, 2588) • Flex System x240 M5 Rechenknoten (2591, 9532) • Flex System x440 Rechenknoten (7167, 2590) • Flex System x280, x480, x880 X6 Rechenknoten (7196, 4258)

Tabelle 4. Von **IBM** unterstützte Hardware

System	Servernummer
System x Server	<ul style="list-style-type: none"> • dx360 M2 (7321, 7323) • dx360 M3 (6391) • dx360 M4 (7912, 7913, 7918, 7919) • nx360 M4 (5455) • Smart Analytics System (7949) • x3100 M4 (2582) • x3200 M2 (4367, 4368) • x3200 M3 (7327, 7328) • x3250 M2 (7657, 4190, 4191, 4194) • x3250 M3 (4251,4252,4261) • x3250 M4 (2583) • x3250 M5 (5458) • x3300 M4 (7382) • x3400 M2 (7836, 7837) • x3400 M3 (7378, 7379) • x3500 M2 (7839) • x3500 M3 (7380) • x3500 M4 (7383) • x3530 M4 (7160) • x3550 M2 (7946, 4198) • x3550 M3 (7944, 4254) • x3550 M4 (7914) • x3620 M3 (7376) • x3630 M3 (7377) • x3630 M4 (7158, 7518, 7519) • x3650 M2 (7947, 4199) • x3650 M3 (7944, 7945, 4254, 4255, 5454) • x3650 M4 (7915) • x3650 M4 HD (5460) • x3650 M4 BD (5466) • x3650 M5 (8871) • x3750 M4 (8722, 8733) • x3755 M4 (7164) • x3690 X5 (7148, 7149, 7147, 7192) • x3850 X5/X3950 X5 (7145, 7146, 7143, 7191) • x3850 X6 (3837)
Flex-Rechenknoten	<ul style="list-style-type: none"> • Flex System x220 Rechenknoten (7906, 2585) • Flex System x222 Rechenknoten (7916) • Flex System x240 Rechenknoten (8956, 8737, 8738, 7863) • Flex System x440 Rechenknoten (7917)
Bladesystem	<ul style="list-style-type: none"> • HS22 (7870, 7809, 1911, 1936) • HS22V (7871, 1949) • HS23 (7875, 1882, 1929) • HS23E (8038, 8039) • HX5 (7872, 7873, 1909, 1910)

Softwarevoraussetzungen

Das Lenovo-Add-In benötigt die Software, die in diesem Abschnitt aufgelistet ist.

Verwaltungsknoten

- Windows Server 2016, 2012 SP1 (x64), 2012 R2 (x64)
- NET Framework 3.5 oder 4.0
- Microsoft System Center Virtual Machine Manager 2016, 2012 SP1, 2012 R2
- Microsoft Internet Explorer, Version 10.0.9200.17492 oder höher
- SQL Server Client Tools Connectivity (wenn SQL Server als Datenbank für den Unified Service verwendet wird).

Verwaltete Knoten

- Windows Server 2016, 2008 R2 (x64), 2012 SP1 (x64), 2012 R2 (x64)
- NET Framework 3.5 und 4.0
- Microsoft System Center Virtual Machine Manager 2016, 2012 SP1 , 2012 R2 Agent
- Hyper-V-Rolle
- Optional: SQL Server 2008 R2 SP3 oder höher

Kapitel 3. Lenovo-Add-In installieren

Informationen zum Installieren des Lenovo-Add-In werden angegeben.

Vorbereitende Schritte

Sie müssen als Benutzer mit Administratorberechtigungen angemeldet sein, um das Lenovo-Add-In zu installieren.

Vorgehensweise

- Schritt 1. Laden Sie das Lenovo-Add-In-Installationsprogramm von der XClarity Integrator-Downloadseite unter [„Lenovo XClarity Integrator for Microsoft System Center“](#) herunter.
- Schritt 2. Doppelklicken Sie auf die Lenovo-Add-In-Installationsdatei. Der Begrüßungsbildschirm wird angezeigt.
- Schritt 3. Wählen Sie einen der folgenden Installationsmodi aus:

Vollständige Installation

Diese Option installiert alle Komponenten, einschließlich Lenovo XClarity Integrator Unified Service und der Lenovo-Add-In-Konsole.

Nur Konsole

Diese Option installiert nur mit der Konsole verbundene Komponenten.

- Schritt 4. Installieren Sie das Paket entsprechend der Aufforderungen im InstallShield-Assistenten.
- Schritt 5. Wenn die Installation abgeschlossen ist, führen Sie die Schritte unter „Lenovo-Add-In importieren“ auf Seite 11 aus.

Anmerkung: Während der Installation müssen Sie die Datenbank für Lenovo XClarity Integrator Unified Service auswählen. Unified Service unterstützt PostgreSQL- und SQL-Datenbankserver. Wenn Sie sich für die Verwendung eines PostgreSQL-Servers entscheiden, wird eine neue PostgreSQL-Datenbank auf dem Server installiert. Wenn Sie sich für die Verwendung eines SQL Servers entscheiden, müssen Sie SQL Server-Informationen bereitstellen. Weitere Informationen zu diesen Datenbanken finden Sie unter [Lenovo XClarity Integrator Unified Service- Onlinedokumentation](#).

Lenovo-Add-In deinstallieren

Verwenden Sie dieses Verfahren, um das Lenovo-Add-In zu deinstallieren.

Vorgehensweise

- Schritt 1. Öffnen Sie in der Systemsteuerung das Fenster Programs and Features (Programme und Funktionen).

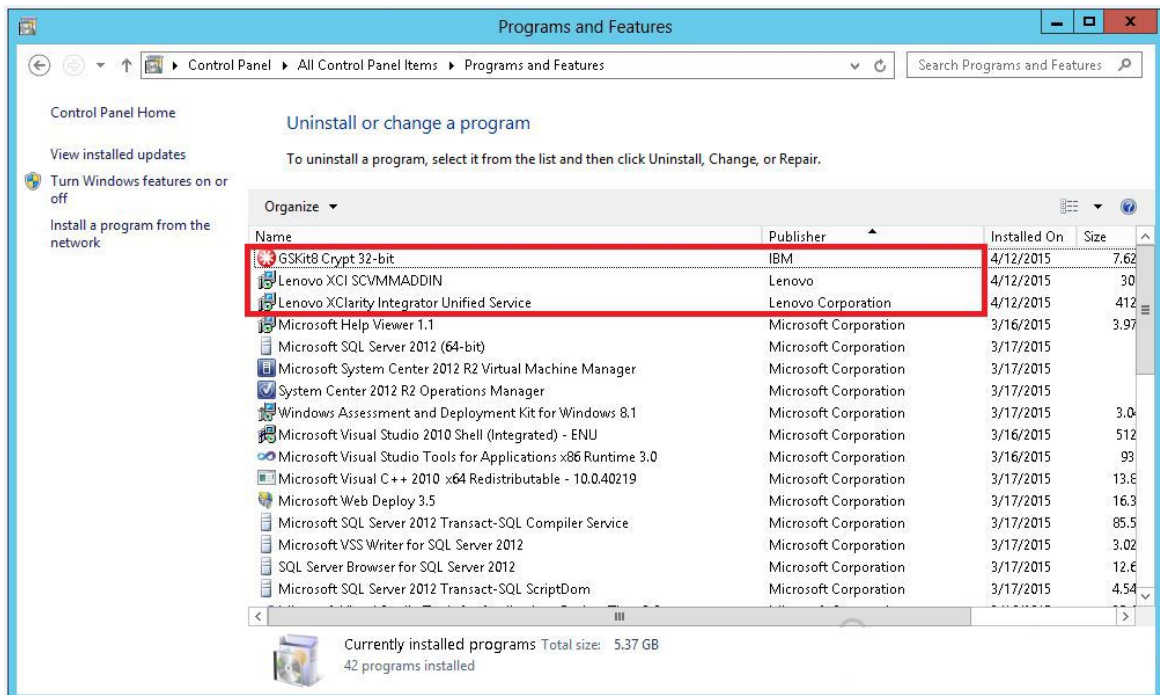


Abbildung 1. Fenster Programs and Features (Programme und Funktionen)

- Schritt 2. Deinstallieren Sie Lenovo XClarity Integrator SCVMMADDIN.
- Schritt 3. Deinstallieren Sie Lenovo XClarity Integrator Unified Service.
- Schritt 4. Entfernen Sie das Lenovo-Add-In manuell aus SCVMM. Ausführlichere Anweisungen zum Entfernen finden Sie unter „Lenovo-Add-In aus SCVMM entfernen“ auf Seite 8.
- Schritt 5. Entfernen Sie die SCVMMADDIN- und Unified Service-Installationsdateien %ProgramFiles(x86)%\Lenovo\Lenovo XClarity Integrator Unified Service und <installation path>\Lenovo\XCI ScvmmAddIn.
- Schritt 6. Entfernen Sie die Datenbankdateien (siehe [PostgreSQL deinstallieren – Unified Service-Installationsanweisung](#)).
- Schritt 7. Entfernen Sie die SCVMMADDIN- und Unified Service-Konfigurationsdateien %ProgramData%\Lenovo\LXCI und %Users%\<user>\Lenovo\LXCI.

Anmerkung: Das Entfernen der SCVMMADDIN- und Unified Service-Konfigurationsdateien wirkt sich auf verschiedenen Funktionen aus, wenn Sie SCVMMADDIN und Unified Service erneut installieren. Beispielsweise können Sie Daten in der Datenbank nicht wiederverwenden und Sie können keine Daten aus postgre zum SQL Server migrieren.

Lenovo-Add-In aus SCVMM entfernen

Sie müssen das Lenovo-Add-In manuell aus SCVMM entfernen, bevor Sie ein neu installiertes importieren oder bevor/nachdem Sie Lenovo-Add-In aus dem System deinstallieren.

Vorgehensweise

- Schritt 1. Öffnen Sie die Seite Settings category (Einstellungskategorie) unten links in SCVMM.
- Schritt 2. Wählen Sie das Lenovo-Add-In aus der Add-in-Liste aus.
- Schritt 3. Klicken Sie oben in der Symbolleiste von SCVMM auf **Remove (Entfernen)**. Ein Bestätigungsdialog wird angezeigt.

Schritt 4. Klicken Sie im Bestätigungsdialog auf **Yes (Ja)**.

Kapitel 4. Lenovo-Add-In verwenden

Dieser Abschnitt enthält Informationen zum Importieren und Starten des Lenovo Add-in für Microsoft System Center Virtual Machine Manager. Er enthält auch Verfahren zum Einstellen der Hostauthentifizierung, Festlegen von Anforderungen für das laufende System und Hinzufügen eines Baseboard Management Controller (BMC).

Lenovo-Add-In importieren

Sie müssen die Lenovo-Add-In-ZIP-Datei manuell in SCVMM importieren. Nachdem der InstallShield-Assistent abgeschlossen ist, wird die Lenovo-Add-In-ZIP-Datei in einen angegebenen Ordner kopiert. Gehen Sie wie folgt vor, um sie zu importieren.

Vorbereitende Schritte

Stellen Sie sicher, dass das Lenovo-Add-In nicht importiert oder entfernt wurde. Anweisungen zum Entfernen finden Sie unter „Lenovo-Add-In aus SCVMM entfernen“ auf Seite 8.

Vorgehensweise

Schritt 1. Klicken Sie in der SCVMM-Konsole auf der Seite Settings category (Einstellungskategorie) auf **Import Console Add-in (Konsolen-Add-in importieren)**. Das Fenster Import Console Add-in Wizard (Assistenten für Konsolen-Add-in importieren) wird angezeigt.

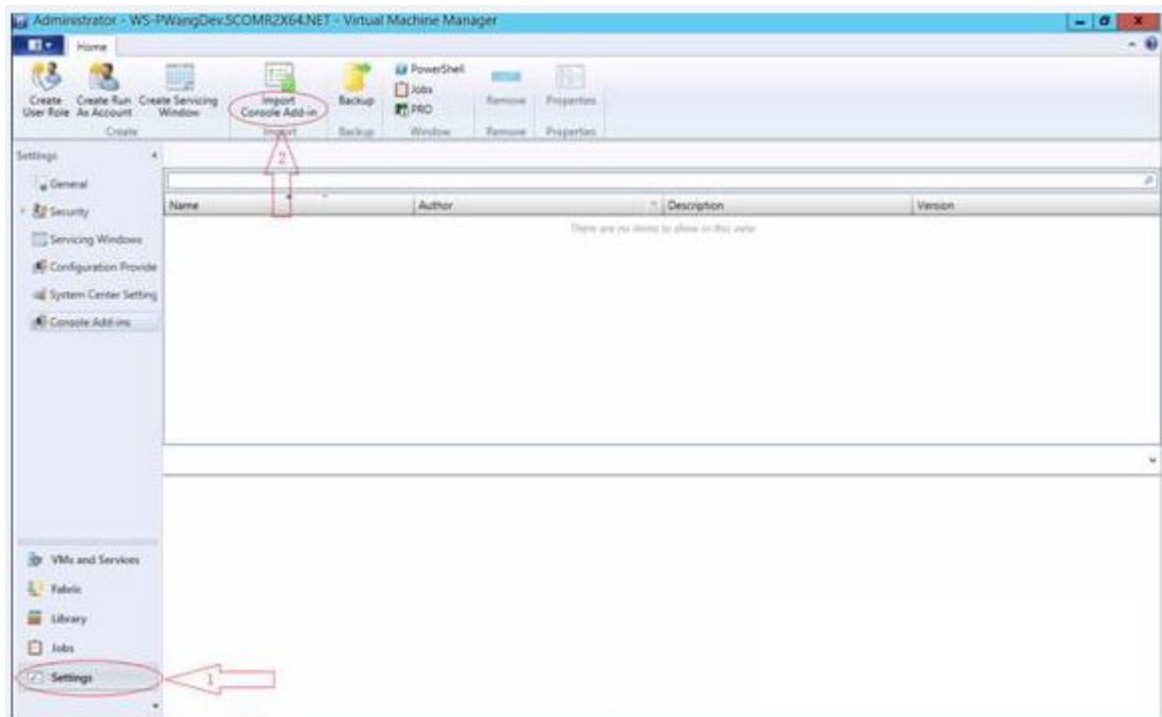
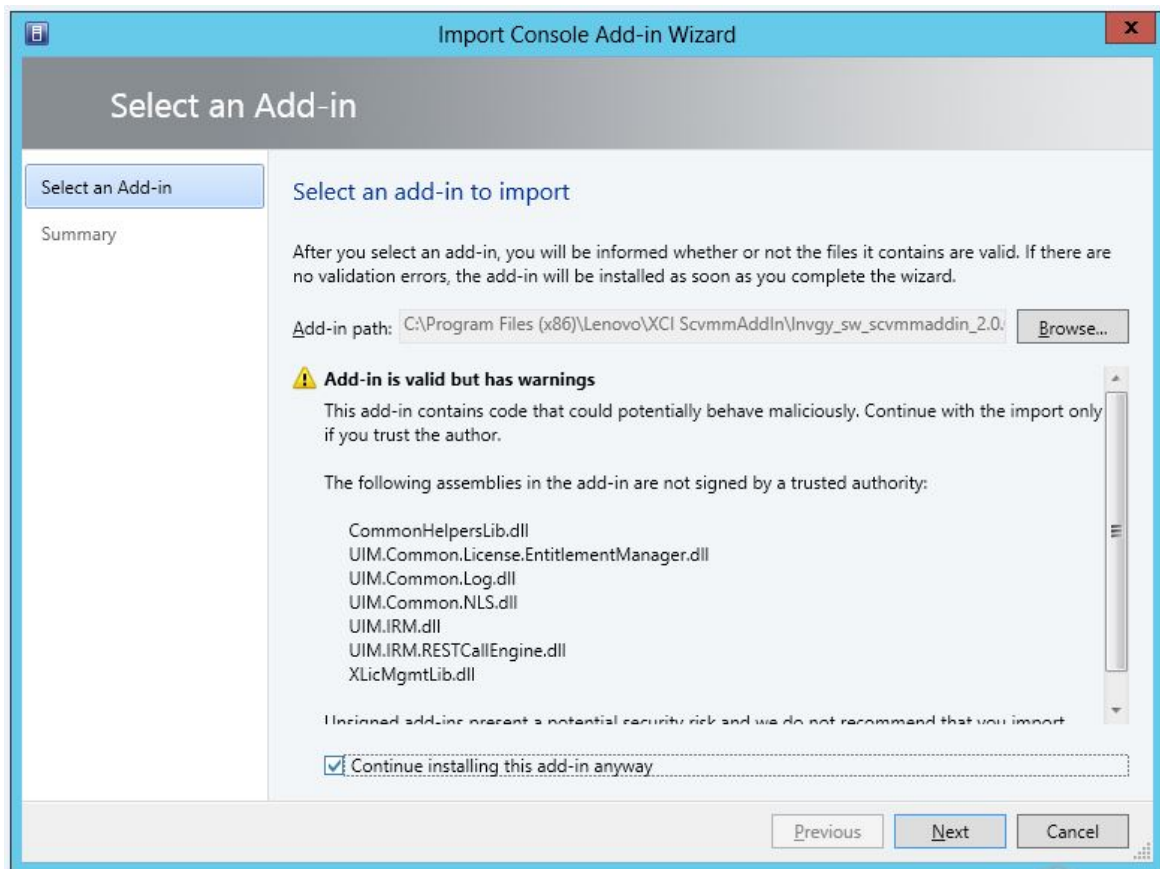


Abbildung 2. Auswahl von „Konsolen-Add-in importieren“

Schritt 2. Klicken Sie im Fenster Import Console Add-in Wizard (Assistenten für Konsolen-Add-in importieren) auf **Browse (Durchsuchen)**.



- Schritt 3. Navigieren Sie zur Datei `lnvgy_sw_scvmaddin_version_windows_32-64.zip`. Die ZIP-Datei befindet sich normalerweise im folgenden Pfad: `C:\Program Files (x86)\Lenovo\XCI ScvmmAddIn`.
- Schritt 4. Aktivieren Sie das Kontrollkästchen **Continue installing this add-in anyway (Add-in trotzdem installieren)**.
- Schritt 5. Klicken Sie zum Fortfahren auf **Next (Weiter)**.
- Schritt 6. Klicken Sie auf **Finish (Fertigstellen)**, um mit dem Importvorgang fortzufahren. Der Status des Importvorgang wird in der Berichtskonsole Jobs dargestellt.

Lenovo-Add-In starten

Nachdem Sie die ZIP-Datei Lenovo-Add-In importiert haben, gehen Sie wie in diesem Abschnitt beschrieben vor, um das Lenovo-Add-In zu starten.

Vorbereitende Schritte

Wichtig: Lenovo-Add-In enthält einige Funktionen, mit denen Sie Hosts, Cluster, Gehäuse, Racks und Lenovo XClarity Administrator betreiben können. Um den nicht genehmigten Betrieb zu verhindern, können nur Domänen-Administratoren und Konten mit einer delegierten Administratorbenutzerrolle auf das Lenovo-Add-In zugreifen.

Vorgehensweise

- Schritt 1. Öffnen Sie die SCVMM-Konsole.
- Schritt 2. Wählen Sie **VMs and Services (VMs und Services)** oder **Fabric** aus der unteren linken Ecke der SCVMM-Konsole. Ein Navigationsbereich wird angezeigt.

Schritt 3. Wählen Sie **All Hosts (Alle Hosts)**.

Schritt 4. Klicken Sie auf das Symbol **Lenovo XClarity Integrator** oben in SCVMM-Konsole.

Schritt 5. Klicken Sie entweder auf der Seite Fabric category (Fabric-Kategorie) oder auf der Seite VMs and Services (VMs und Services) auf das Symbol **Lenovo XClarity Integrator** oben im Fenster.

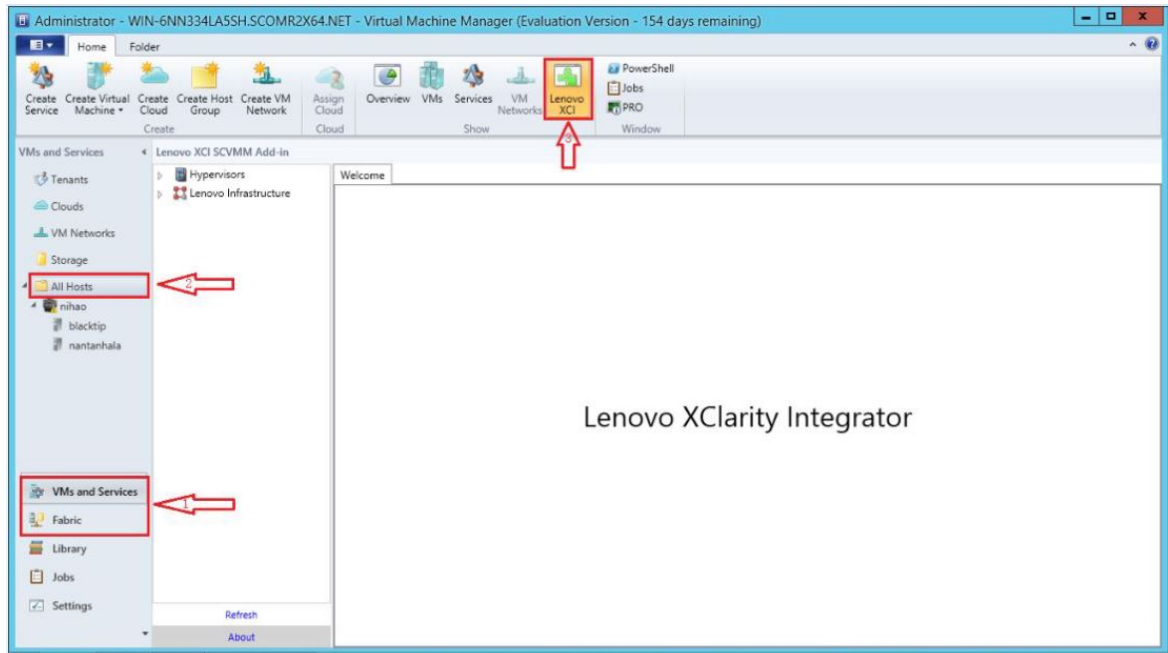


Abbildung 3. Lenovo XClarity Integrator-Add-in starten

Die Schnittstelle für die Lenovo Add-in für Microsoft System Center Virtual Machine Manager-Konsole weist zwei Bereiche auf. Auf der linken Seite ist ein Navigationsbereich, der verwaltete Ressourcen, einschließlich Hostcluster und deren verwaltete Hosts, enthält, die mit SCVMM synchronisiert werden, sowie Lenovo XClarity Administrator-Instanzen und ihre verwalteten Gehäuse. Auf der rechten Seite ist das Hauptbild, in dem die aktuelle Operation angezeigt wird, die für die in der linken Baumstruktur ausgewählte Ressource relevant ist. Um Ressourcen im linken Navigationsbereich zu aktualisieren oder neu zu laden, drücken Sie Strg+F5 oder klicken Sie auf **Refresh (Aktualisieren)** unten im Navigationsbereich.

Bei Unified Service anmelden

Nachdem Sie auf das Symbol **Lenovo XClarity Integrator** oben in der SCVMM-Konsole geklickt haben, wird die Unified Service-Anmeldeseite angezeigt. Sie können diese Seite verwenden, um sich von einem lokalen oder Fern-SCVMM-Server bei Unified Service anzumelden, um Vorgangshosts, Cluster, Gehäuse, Racks und Lenovo XClarity Administrator-Instanzen anzumelden, die vom Ziel-Unified Service verwaltet werden.

Servername

Geben Sie die FQDN des Zielservers an, auf dem Unified Service installiert ist und mit dem der SCVMM-Server verbunden ist. Sie können die FQDN nicht ändern oder sich mit einem anderen Server anmelden, es sei denn, Sie verbinden SCVMM mit einer anderen Adresse neu.

Port

Geben Sie den Port von Unified Service auf dem Zielserver an. Der Port wurde während der Installation von Unified Service festgelegt. Der Standardport ist 9500.

Kennwort

Geben Sie ein Kennwort an, um sich bei Unified Service auf dem Zielserver anzumelden. Dieses Kennwort wurde während der Installation von Unified Service festgelegt.

Kennwort speichern

Bei Auswahl dieser Option wird das Kennwort in der Konfigurationsdatei gespeichert und beim nächsten Mal automatisch eine Verbindung mit diesen Einstellungen hergestellt. Diese Einstellungen werden nur für den aktuellen Windows-Benutzer gespeichert und sind nur für ihn wirksam.

Konfigurationsdateipfad

system drive\users\current user\Lenovo\LXCI\ScvmmAddin\config.json.txt

Zertifizierung

Lenovo XClarity Integrator gewährleistet die Sicherheit der Verbindung mit dem Unified Service durch Überprüfung der Zertifikate. Wenn die Zertifikate nicht sicher sind, erhalten Sie eine Warnmeldung.

Anmerkungen: Lenovo XClarity Integrator verwendet in den Standardeinstellungen eine selbst signierte Zertifikatskette. Möglicherweise erhalten Sie bei der Anmeldung die Warnung, dass das CA-Stammzertifikat nicht vertrauenswürdig ist. Aktivieren Sie das Kontrollkästchen **Trust the certificate permanently (Dem Zertifikat dauerhaft vertrauen)**, wenn Sie sicher sind, dass die Zertifikate gültig sind, oder deaktivieren Sie es, um die Überprüfung dieser Verbindung zu ignorieren. Wenn Sie nicht auswählen, dem Zertifikat dauerhaft zu vertrauen, werden je nach die Sicherheitseinstellungen Ihres Systems mehrere Systemwarnungen angezeigt:

1. „Content within this application coming from the website listed below is being blocked by Internet Explorer Enhanced Security Configuration. (Inhalte in dieser Anwendung, die von der unten aufgeführten Website stammen, werden durch die verstärkte Sicherheitskonfiguration für Internet Explorer blockiert.)“
Folgende Website können aufgeführt sein: „about:blank“, „about:internet“ oder „security_VmmAdminUI.exe“.
 - Klicken Sie auf **Close (Schließen)**, um die Warnung zu unterdrücken, oder klicken Sie auf **Add... (Hinzufügen...)**, um eine dauerhafte Ausnahme hinzuzufügen.
2. „Navigation to the webpage was canceled. (Navigation zur Webseite wurde abgebrochen.)“
Klicken Sie mit der rechten Maustaste auf die Seite und wählen Sie **Refresh (Aktualisieren)** aus, oder drücken Sie die Taste F5.
3. „There is a problem with this website's security certificate. (Es ist ein Problem mit dem Sicherheitszertifikat der Website aufgetreten.)“
Klicken Sie auf **Continue to this website (not recommended) (Zu dieser Website wechseln [nicht empfohlen])**.

So können Sie überprüfen, ob Sie eine Verbindung zu Lenovo XClarity Integrator herstellen:

1. Rufen Sie auf dem SCVMM-Server das Verzeichnis %ProgramFiles(x86)%\Lenovo\Lenovo XClarity Integrator Unified Service\WebServer\conf auf.
 2. Doppelklicken Sie auf **ca.root** oder **ca.root.cer**.
 3. Vergleichen Sie den Zertifikatsfingerabdruck mit dem in der Warnung angezeigten. Sie sollten identisch sein.
-

Hostauthentifizierung einrichten

Verwenden Sie den Hypervisor-Knoten, um Informationen zum Host anzuzeigen.

Die Authentifizierungsdaten sind erforderlich, um ausführliche Systeminformationen, wie Maschinentyp, zu erfassen und einige XClarity Integrator-Funktionen, wie „Laufende Systemaktualisierung“ und „Laufender Systemneustart“, zu aktivieren. Um Host-Authentifizierungsdaten festzulegen, können Sie Hypervisor im

Navigationsbereich des Lenovo-Add-In erweitern und anschließend den Cluster erweitern und auf einen Host klicken. Auf der Seite Host General (Host allgemein) können Sie **Authentication OS (Authentifizierungs-BS)** sehen. Klicken Sie darauf, um das Dialogfenster Host Authentication Information (Host-Authentifizierungsdaten) zu öffnen. Sie müssen die folgenden Informationen festlegen, um die Hostauthentifizierung abzuschließen.

Ausführung als Konto

Geben Sie ein Domäne\Administrator-Konto als Konto für Lenovo XClarity Integrator an, damit Tasks über SCVMM auf dem Client-Host ausgeführt werden.

Das „Ausführung als“-Konto wird für den SCVMM-Service verwendet, um Scripts auf dem Zielhost auszuführen. Verwenden Sie das Domäne\Administrator-Konto, um sicherzustellen, dass alle Lenovo-Add-In-Funktionen ordnungsgemäß arbeiten.

Benutzername und Kennwort

Ein Benutzerkonto mit einer Berechtigung als Domänenadministrator ist erforderlich, um eine Verbindung zu einem bestimmten Host über WMI herzustellen, um Systeminformationen zu erfassen, Scripts und Anwendungen auszuführen, oder auf den freigegebenen SMB-Ordner (in der Regel C\$) eines bestimmten Hosts zuzugreifen.

Anmerkung: Stellen Sie sicher, dass die SMB- und WMI-Services der verwalteten Hosts aktiviert sind. Nach der Verschlüsselung werden die Authentifizierungsdaten in der Lenovo XClarity Integrator Unified Service-Datenbank gespeichert.

Klicken Sie auf **Set Auth Info (Authentifizierungsdaten festlegen)** unten auf der Registerkarte General (Allgemein) des Hosts. Füllen Sie dann die Felder im Fenster Set Authentication Information (Authentifizierungsdaten festlegen) aus. Die Informationen können auf den ausgewählten Host, die Hosts im selben Cluster oder auf alle Hosts angewendet werden, die im Navigationsbereich aufgeführt sind. Warten Sie, nachdem die Informationen angewendet wurden. Die Informationen werden überprüft und das Ergebnis wird in der Benutzerschnittstelle angezeigt.

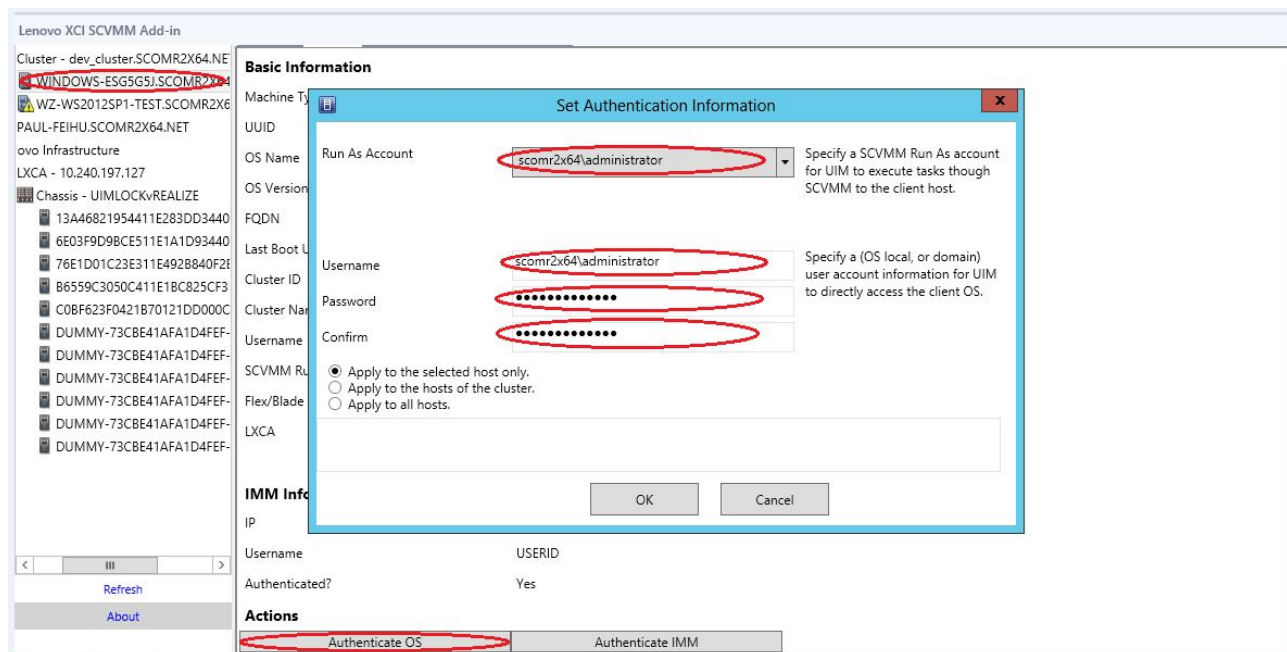


Abbildung 4. Hostauthentifizierung einrichten

Einstellungen für laufende Systemaktualisierung festlegen

Einstellungen für laufende Systemaktualisierung festzulegen, ist eine Vorbedingung der Funktionen „Laufende Systemaktualisierung ohne Richtlinie“. Verwenden Sie folgendes Verfahren.

Vorgehensweise

- Schritt 1. Erweitern Sie im Navigationsfenster des Lenovo-Add-In „Hypervisor“ und wählen Sie dann den Zielcluster aus.
- Schritt 2. Wählen Sie oben im Hauptbereich „Rolling System Update (Laufende Systemaktualisierung)“.
- Schritt 3. Klicken Sie auf die Verknüpfung Preferences (Einstellungen) auf der Seite Rolling System Update (Laufende Systemaktualisierung).
- Schritt 4. Weisen Sie einen **Local / Remote Repository Folder (Lokaler Ordner/Remote-Repository-Ordner)** zu, der zum Speichern oder Herunterladen von Firmware-Nutzdaten für Firmwareaktualisierungen verwendet wird.
- Schritt 5. Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Zugriff auf den Windows-Freigabenordner an (falls erforderlich). Wenn Sie einen lokalen Ordner verwenden, gibt das Lenovo Add-in diesen Ordner automatisch unter dem Namen `Repository` frei. Daher ist ein Windows-Account mit den passenden Berechtigungen erforderlich. Das Lenovo-Add-In unterstützt nur Windows-Ordnerfreigaben. Das Zuweisen von Linux-Freigaben oder anderen Freigaben kann bei einigen Lenovo-Add-In-Funktionen (z. B. laufende Systemaktualisierung) zu einem schwerwiegenden Fehler führen.
- Schritt 6. Führen Sie einen der folgenden Schritte aus:
 - Wenn Aktualisierungspakete vorhanden sind, kopieren Sie sie in den Pfad des lokalen Repository-Ordners.
 - Wenn keine Aktualisierungspakete verfügbar sind, legen Sie den Bereich „Check Updates from Lenovo Website (Aktualisierungen von Lenovo Website überprüfen)“ so fest, dass Aktualisierungspakete automatisch von der Lenovo-Website heruntergeladen werden:
 1. Aktivieren Sie das Kontrollkästchen **Download Updates from Lenovo Website (Aktualisierungen von Lenovo Website herunterladen)**.
 2. Konfigurieren Sie Ihre Interneteinstellungen.
 3. Wählen Sie die Frequenz für das automatische Herunterladen von Aktualisierungspaketen und speichern Sie die Änderungen. Wenn Sie ein Aktualisierungspaket sofort herunterladen möchten, klicken Sie auf **Check Now (Jetzt suchen)**. Der Downloadvorgang beginnt, nachdem Sie auf die Schaltfläche geklickt haben.
- Schritt 7. Klicken Sie auf **Save (Speichern)**, um die Einstellungen zu speichern. Wenn die Einstellungen erfolgreich gespeichert werden, geschieht nichts.
- Schritt 8. Klicken Sie auf den Link „Go Back (Zurück)“, um zur Seite Rolling System Update Task Manager (Task-Manager für laufenden Systemneustart) zurückzukehren.

Ein Baseboard Management Controller (BMC) hinzufügen

Das Hinzufügen eines Baseboard Management Controller (BMC) zum Lenovo-Add-In ist für einige Funktionen, wie die PFA-Funktion, Voraussetzung.

Ein BMC wird in zwei Schritten hinzugefügt:

1. BMC-Ermittlung
2. BMC-Authentifizierung

BMC-Ermittlung

Diese Funktion dient zur Ermittlung von BMC-Einträgen.

Vorgehensweise

- Schritt 1. Wählen Sie den **Hypervisors (Hypervisoren)-** oder **Lenovo Infrastructure (Lenovo Infrastruktur)-** Stammeintrag im Navigationsbereich des Lenovo-Add-In.
- Schritt 2. Wählen Sie die Seite BMC Management (BMC-Verwaltung) oben im Hauptbild aus.
- Schritt 3. Klicken Sie auf **Discover (Ermitteln)**.
Das Dialogfenster BMC Discovery (BMC-Ermittlung) wird angezeigt.
- Schritt 4. Geben Sie eine IP-Adresse oder ein Bereich von IP-Adressen ein. IPv4 und IPv6 werden unterstützt.
- Schritt 5. Klicken Sie im Dialogfenster BMC Discovery (BMC-Ermittlung) auf **OK**.

Das Dialogfenster wird unverzüglich geschlossen, wenn die Option **Run in the background (Im Hintergrund ausführen)** ausgewählt ist. Andernfalls wird das Dialogfenster geschlossen, wenn der Ermittlungsvorgang abgeschlossen ist. Ein erfolgreicher Abschluss bedeutet, dass die Anforderung unabhängig von der Anzahl der BMC-Einträge, die tatsächlich ermittelt wurden, verarbeitet wurde.

Wenn die Anforderung erfolgreich abgeschlossen wurde, werden die neu ermittelten BMC-Einträge in der BMC-Tabelle auf der Seite BMC Management (BMC-Verwaltung) aktualisiert.

Das Dialogfenster bleibt geöffnet, wenn ein Fehler bei der Verarbeitung der Anforderung auftritt. Dies kann vorkommen, wenn die Anforderung den Server aufgrund eines Kommunikationsfehlers nicht erreicht hat.

BMC-Authentifizierung

Diese Funktion dient zur Eingabe von Benutzernamen- und Kennwortinformationen für BMC-Einträge. Die Informationen werden in der XClarity Integrator-Datenbank für die zukünftige Verwendung in anderen Funktionen gespeichert.

Vorgehensweise

- Schritt 1. Wählen Sie den **Hypervisors (Hypervisoren)-** oder **Lenovo Infrastructure (Lenovo Infrastruktur)-** Stammeintrag im Navigationsbereich des Lenovo-Add-In.
- Schritt 2. Wählen Sie die Seite BMC Management (BMC-Verwaltung) oben im Hauptbild aus.
- Schritt 3. Aktivieren Sie die Kontrollkästchen neben den BMCs, die authentifiziert werden sollen.
- Schritt 4. Klicken Sie auf **Authenticate (Authentifizieren)**.
Das Dialogfenster BMC Authentication (BMC-Authentifizierung) wird angezeigt.
- Schritt 5. Geben Sie die Benutzernamen- und Kennwortinformationen ein.
- Schritt 6. Klicken Sie auf **OK**. Wenn die Anforderung erfolgreich abgeschlossen ist, wird die BMC-Tabelle auf der Seite BMC Management (BMC-Verwaltung) aktualisiert.

Lenovo XClarity Administrator hinzufügen

Das Hinzufügen von Lenovo XClarity Administrator zum Lenovo-Add-In ist für bestimmte Funktionen, wie das Anzeigen von allgemeinen Informationen zu Lenovo XClarity Administrator und das Anzeigen einer Gehäuseübersicht des verwalteten Gehäuses, erforderlich. Führen Sie die Schritte in diesem Abschnitt aus, um Lenovo XClarity Administrator zum Lenovo-Add-In hinzuzufügen.

Vorgehensweise

- Schritt 1. Klicken Sie im Navigationsbereich auf **Lenovo**.
- Schritt 2. Klicken Sie oben im Hauptbild auf die Registerkarte **LXCA Registration (LXCA-Registrierung)**. Die Seite Registered LXCA (Registriertes LXCA) wird auf dem Hauptbild angezeigt. Alle registrierten Lenovo XClarity Administrator-Instanzen werden auf der Seite angezeigt.
- Schritt 3. Klicken Sie auf **Register (Registrieren)**, um mit der Lenovo XClarity Administrator-Registrierung zu beginnen.
Ein Dialogfenster für die Lenovo XClarity Administrator-Registrierung wird angezeigt.
- Schritt 4. Geben Sie die IP-Adresse, den Benutzernamen, das Kennwort und den Anschluss für den Lenovo XClarity Administrator im Dialogfenster für die Lenovo XClarity Administrator-Registrierung ein. Nach der Übermittlung stellt das Lenovo-Add-In zu Authentifizierungszwecken eine Verbindung zum Lenovo XClarity Administrator her.
- Schritt 5. Wenn die Seite View Certificate (Zertifikat anzeigen) angezeigt wird, klicken Sie auf **Trust this certificate (Diesem Zertifikat vertrauen)**, um zu bestätigen, dass Lenovo XClarity Administrator vertrauenswürdig ist. Klicken Sie anschließend auf **Close (Schließen)**.
- Schritt 6. Klicken Sie nach der Registrierung auf **Refresh (Aktualisieren)**, um den Navigationsbereich zu aktualisieren.

Nächste Schritte

Anmerkungen:

- Stellen Sie sicher, dass das Benutzerauthentifizierungsverfahren in Lenovo XClarity Administrator *nicht* als **Allow logons from LDAP users (Anmeldung von LDAP-Benutzern zulassen)** konfiguriert ist.
- Stellen Sie sicher, dass der angegebene Lenovo XClarity Administrator Benutzeraccount über Supervisor-Berechtigungen verfügt.
- Wenn Sie eine Lenovo XClarity Administrator-Instanz mit einer früheren Version von Lenovo XClarity Integrator registriert haben, laden Sie das Serverzertifikat für die Lenovo XClarity Administrator-Instanz manuell herunter und importieren Sie es in Lenovo XClarity Integrator, indem Sie **Manage trusted certificates (Vertrauenswürdige Zertifikate verwalten) → Add (Hinzufügen)** auswählen. Wenn das Serverzertifikat nicht zu Lenovo XClarity Integrator hinzugefügt wird, wird keine Verbindung zwischen Lenovo XClarity Integrator und Lenovo XClarity Administrator hergestellt.
- Wenn Ihr Lenovo XClarity Administrator nur in einer IPv6-Umgebung funktioniert, können Sie das entsprechende Zertifikat manuell in Lenovo XClarity Integrator importieren, indem Sie auf **Manage trusted certificates (Vertrauenswürdige Zertifikate verwalten) → Add (Hinzufügen)** klicken. Anderenfalls wird Lenovo XClarity Administrator nicht registriert.

Andere Lenovo XClarity Administrator Registrierungsvorgänge:

Nach Abschluss der Registrierung können Sie die folgenden Aktionen ausführen:

- Bearbeiten Sie Lenovo XClarity Administrator, indem Sie auf **Edit (Bearbeiten)** klicken und alle erforderlichen Änderungen vornehmen.
- Heben Sie die Registrierung von Lenovo XClarity Administrator durch Klicken auf **Unregister (Registrierung aufheben)** auf.
- Verwalten Sie vertrauenswürdige Zertifikate, indem Sie **Manage trusted certificates (Vertrauenswürdige Zertifikate verwalten)** klicken.

Lenovo XClarity Administrator-Serverzertifikat herunterladen

Sie können eine Kopie des aktuellen Lenovo XClarity Administrator-Serverzertifikats im PEM-Format auf das lokale System herunterladen.

Vorgehensweise

Gehen Sie wie folgt vor, um das Serverzertifikat herunterzuladen.

Schritt 1. Melden Sie sich bei Lenovo XClarity Administrator an.

Schritt 2. Wählen Sie in der Lenovo XClarity Administrator-Menüleiste **Administration (Verwaltung)** → **Security (Sicherheit)** aus, um die Seite „Security“ (Sicherheit) anzuzeigen.

Schritt 3. Klicken Sie im Abschnitt für die Zertifikatsverwaltung auf **Server Certificate (Serverzertifikat)**. Die Seite „Serverzertifikat“ wird angezeigt.

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

Schritt 5. Klicken Sie auf **Download Certificate (Zertifikat herunterladen)**. Das Dialogfeld „Server Certificate“ (Serverzertifikat) wird angezeigt.

Schritt 6. Klicken Sie auf **Save to pem (Als PEM sichern)**, um das Serverzertifikat als PEM-Datei auf dem lokalen System zu speichern.

Anmerkung: Das DER-Format wird nicht unterstützt.

Vertrauenswürdige Zertifikate verwalten

Lenovo XClarity Integrator bietet eine integrierte Methode für die Verwaltung von vertrauenswürdigen Lenovo XClarity Administrator-Zertifikaten.

Vorgehensweise

Klicken Sie auf der Seite Lenovo XClarity Integrator Management (Lenovo XClarity Integrator-Verwaltung) auf **Manage trusted certificates (Vertrauenswürdige Zertifikate verwalten)**, um die Seite **Trusted Certificates (Vertrauenswürdige Zertifikate)** anzuzeigen. Über diese Seite können Sie die folgenden Aktionen ausführen:

- Fügen Sie manuell ein vertrauenswürdigen Lenovo XClarity Administrator-Zertifikat hinzu, indem Sie auf **Add (Hinzufügen)** klicken.
- Zeigen Sie detaillierte Informationen zu einem vertrauenswürdigen Zertifikat durch Klicken auf **View (Ansicht)** an.
- Löschen Sie ein vertrauenswürdigen Zertifikat durch Klicken auf **Delete (Löschen)**.
- Aktualisieren Sie die vertrauenswürdigen Zertifikate durch Klicken auf **Refresh (Aktualisieren)**.
- Kehren Sie zur Seite „Lenovo XClarity Integrator Management (Lenovo XClarity Integrator-Verwaltung)“ zurück, indem Sie auf **LXCA Registration (LXCA-Registrierung)** klicken.

Kapitel 5. Mit Funktionen arbeiten

In diesem Abschnitt werden die Lenovo-Add-In-Funktionen vorgestellt.

Informationen sammeln

Das Lenovo-Add-In sammelt Informationen zu Hosts, Gehäuse und Lenovo XClarity Administrator, die bei der Systemverwaltung hilfreich sind.

Hostinformationen anzeigen

Sie können allgemeine Informationen zu Hosts in einem Hostcluster abrufen, das in SCVMM konfiguriert ist.

Informationen dazu, wie Sie einen Hostcluster in SCVMM konfigurieren, finden Sie unter [Webseite „Microsoft System Center – Managing Host Clusters“](#).

Um Host-Authentifizierungsdaten anzuzeigen, können Sie Hypervisor im Navigationsbereich des Lenovo-Add-In erweitern und anschließend den Cluster erweitern und auf einen Host klicken.

Um allgemeine Informationen für einen Host innerhalb eines Clusters anzuzeigen, erweitern Sie den **Hypervisor**-Knoten aus dem Navigationsbereich der Lenovo Add-in für Microsoft System Center Virtual Machine Manager-Benutzeroberfläche, wählen Sie den Cluster, auf dem sich der Host befindet, und wählen Sie den Host.

Um die allgemeinen Informationen für einen Host außerhalb eines Clusters anzuzeigen, erweitern Sie den **Hypervisor**-Knoten aus dem Navigationsbereich der Lenovo Add-in für Microsoft System Center Virtual Machine Manager-Benutzeroberfläche und wählen Sie dann den Host.

Allgemeine Informationen zu Lenovo XClarity Administrator anzeigen

Sie können allgemeine Informationen zum Lenovo XClarity Administrator und das Gehäuse, das von Lenovo XClarity Administrator verwaltet wird, anzeigen.

Zum Anzeigen allgemeiner Informationen zu Lenovo XClarity Administrator, müssen Sie zunächst Lenovo XClarity Administrator registrieren. Weitere Informationen finden Sie in Kapitel 4.

Erweitern Sie dann Lenovo-Infrastruktur im Navigationsfenster und wählen eine der Lenovo XClarity Administrator-Instanzen aus, die Sie ausgewählt haben. Allgemeine Informationen zum Lenovo XClarity Administrator werden im Hauptbild in folgender Form angezeigt:

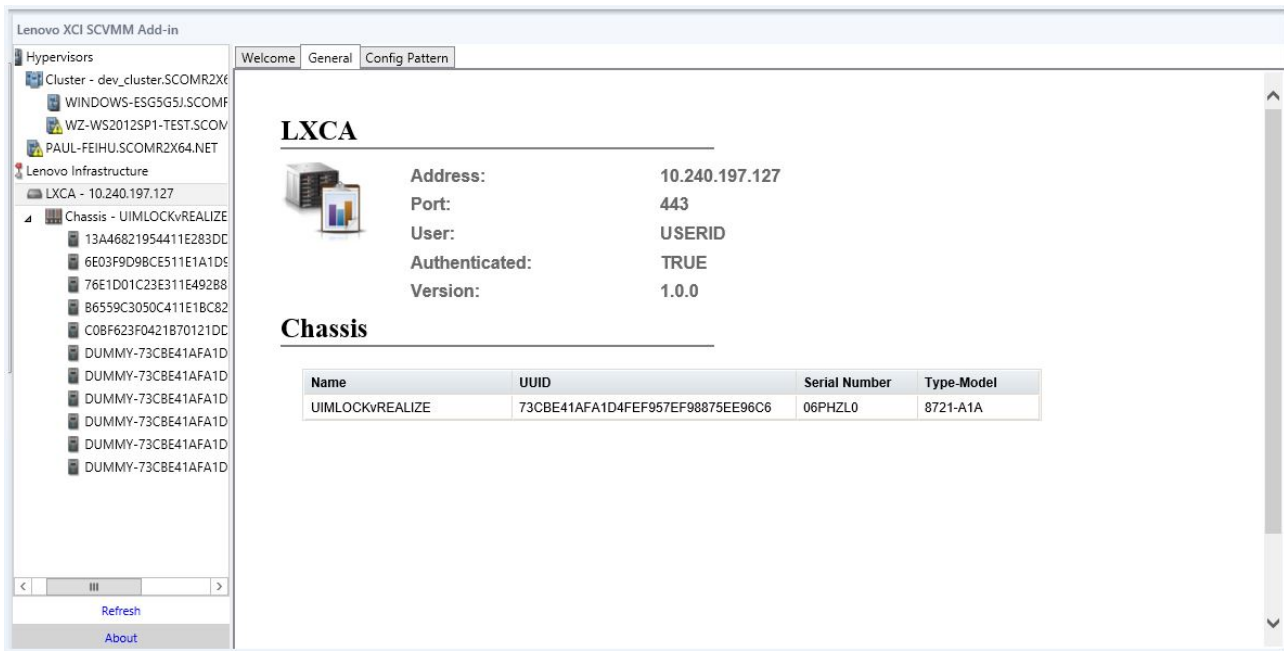


Abbildung 5. Lenovo XClarity Administrator Allgemeine Informationen

Eine Gehäuseübersicht anzeigen

Nachdem Lenovo XClarity Administrator im Lenovo-Add-In registriert wurde, können Sie Gehäuseübersicht für ein Gehäuse überprüfen, das vom Lenovo XClarity Administrator verwaltet wird.

Vorgehensweise

Schritt 1. Suchen Sie ein Gehäuse oder einen Server in einem bestimmten Gehäuse und wählen Sie es bzw. ihn aus dem Feld „Assetbaum“ in der Lenovo-Add-In-Konsole.

Das Gehäuse sollte vom Lenovo XClarity Administrator unter dem Lenovo-Infrastrukturknoten im Feld „Assetbaum“ der Lenovo-Add-In-Konsole verwaltet werden.

Schritt 2. Klicken Sie auf die Registerkarte mit der Gehäuseübersicht im Arbeitsbereich der Lenovo-Add-In-Konsole.

Sie haben folgende Möglichkeiten:

- Auf eine Komponente im Gehäuse klicken, um ihren grundlegenden Bestand und Statusinformationen von einer Eingabeaufforderung anzuzeigen.
- Wenden Sie verschiedene Overlays an, um unterschiedliche Informationen oder Status für Komponenten im Gehäuse anzuzeigen.
- Aktivieren Sie die Overlays, die für Sie interessant sind, in der Symbolleiste oben in der Ansicht „Gehäuseübersicht“. Die Tabelle Tabelle 5 „Hardware-Overlays-Übersicht“ auf Seite 24 enthält weitere Details zu den Overlays.



Abbildung 6. Gehäuseübersicht

Tabelle 5. Hardware-Overlays-Übersicht






Overlay	Symbol	Beschreibung
Hardwarestatus		<p>Verwenden Sie das Hardwarestatus-Overlay, um den Status jeder Komponente anzuzeigen. Sie können einen oder mehrere der folgenden Statuskriterien auswählen, um Folgendes anzuzeigen:</p> <ul style="list-style-type: none"> • Critical (Kritisch). Komponenten weisen einen oder mehrere kritische Alerts auf und eine sofortige ist Benutzeraktion erforderlich. • Warning (Warnung). Komponenten weisen eine oder mehrere Warnalerts auf. Eine Untersuchung durch den Benutzer ist erforderlich, um die Ursache der Warnungen zu ermitteln, aber es besteht kein unmittelbares Risiko eines Ausfalls. • Synchronizing (Synchronisation). Lenovo XClarity Administrator wartet darauf, dass die Komponenten einen aktualisierten Status bereitstellen. • Offline. Die Komponenten sind nicht online. • Unknown (Nicht bekannt). Lenovo XClarity Administrator kann den Status einer oder mehrerer Komponenten in einem Gehäuse nicht abrufen. Eine Untersuchung durch den Benutzer ist erforderlich. • Normal. Die Komponenten funktionieren ordnungsgemäß. Bewegen Sie den Mauszeiger über eine bestimmte Komponente, um weitere Informationen über den aktuellen Status abzurufen.
Hervorheben der LEDs im Bedienfeld		<p>Verwenden Sie das Overlay zur Hervorhebung der LEDs im Bedienfeld, um die für jede Komponente verfügbaren LEDs anzuzeigen. Sie können eine oder mehrere der folgenden LEDs auswählen, um Folgendes anzuzeigen:</p> <ul style="list-style-type: none"> • Power LED (Betriebsanzeige). Zeigt die aktuelle Betriebsanzeige für jede Komponente an. • Event Log LED (Anzeige für Ereignisprotokoll). Zeigt die Anzeige für Ereignisprotokoll an, die leuchtet, wenn für eine bestimmte Komponente Ereignisse im Ereignisprotokoll von Lenovo XClarity Administrator vorhanden sind. • Location LED (Positionsanzeige). Zeigen Sie die Positionsanzeige an, die Sie über das CMM einschalten können, um zu ermitteln, wo sich eine Komponente befindet. • Fault LED (Fehleranzeige). Zeigt den Status der Fehleranzeige für jede Komponente an. • Other LED (Andere Anzeige). Zeigt alle anderen Anzeigen an, die für jede Komponente verfügbar sind. • Only Active LEDs (Nur aktive Anzeigen). Zeigt nur die Anzeigen an, die derzeit leuchten. <p>Bewegen Sie den Mauszeiger über eine bestimmte Komponente, um weitere Informationen über alle Anzeigen für eine Komponente abzurufen. Ausführliche Informationen zu den Anzeigen, die für die jeweilige Komponente angezeigt werden können, finden Sie in der für diese Komponente verfügbaren Produktdokumentation.</p>
Komponentennamen und Eigenschaften		<p>Verwenden Sie das Overlay für Komponentennamen und Eigenschaften, um den Namen jeder Komponente im Gehäuse anzuzeigen. Wenn Sie den Mauszeiger über eine Komponente bewegen, werden weitere Eigenschaften zu der Komponente angezeigt (z. B. die IP-Adresse und UUID).</p>

Tabelle 5. Hardware-Overlays-Übersicht (Forts.)

Overlay	Symbol	Beschreibung
Konformität		Verwenden Sie diese Konformität, um festzustellen, ob die aktuell auf einer Komponente installierte Firmware der für diese Komponente definierten Konformitätsrichtlinie entspricht.
Konfigurationsmuster		Verwenden Sie das Konfigurationsmuster-Overlay, um zu ermitteln, welche Servermuster jedem Rechenknoten zugeordnet sind.

Die Details eines verwalteten Gehäuses anzeigen

Sie können detaillierte Informationen zum verwalteten Gehäuse über Lenovo XClarity Administrator anzeigen, wenn Sie auf den Link „Lenovo XClarity Administrator für Details öffnen“ klicken.

Diese Details enthalten Firmwareversionen, IP-Adressen und Universally Unique Identifiers (UUIDs).

Schaltfläche „Alle Aktionen“

Es gibt die Schaltfläche **All Actions (Alle Aktionen)** auf der Seite Chassis Map (Gehäuseübersicht). Wenn Sie auf diese Schaltfläche klicken, können Sie auf die BMC-Schnittstelle zugreifen und einen ausgewählten Host über Fernzugriff steuern.

Schnittstelle des Managementmoduls starten

Wenn Sie ein Gehäuse oder einen Host auf der Seite Chassis Map (Gehäuseübersicht) auswählen, können Sie eine BMC-Webseite im neuen Fenster öffnen.

Fernsteuerung starten

Sie können eine Fernsteuerung öffnen, wenn Sie einen Host in der Gehäuseübersicht auswählen.

Nach Ressourcen suchen

Die Funktion zum Suchen nach Ressourcen bietet die Suchfunktion, um schnell bestimmte Server, Cluster, Gehäuse und/oder Lenovo XClarity Administrator-Instanzen unter den Ressourcen aus der Lenovo-Add-In-Konsole mit einem Suchbegriff zu finden.

Suchbegriffe

Beim Suchbegriff muss die Groß-/Kleinschreibung beachtet werden. Ein Suchbegriff unterstützt keine Platzhalterzeichen oder regulären Ausdrücke.

Suchfelder

Suchfelder variieren entsprechend den Suchzielen. Eine Übereinstimmung ist gefunden, wenn der Suchtext in einem der Felder eines Suchziels enthalten ist.

Für Server sind die Suchfelder:

- **OS FQDN**
- **OS IP address (IP-Adresse des Betriebssystems)**
- **OS Name (Betriebssystemname)**
- **Machine type (Maschinentyp)**
- **Server UUID (Server-UUID)**
- **IMM IP address (IMM-IP-Adresse)**
- **IMM model (IMM-Modell)**
- **IMM part number (IMM-Teilenummer)**
- **IMM serial number (IMM-Seriennummer)**
- **IMM UUID (IMM-UUID)**

Für das Gehäuse sind die Suchfelder:

- **Domain name (Domänenname)**
- **Machine type (Maschinentyp)**
- **Model (Modell)**
- **Name**
- **Part number (Teilenummer)**
- **Serial number (Seriennummer)**
- **CMM IP address (CMM-IP-Adresse)**
- **Product name (Produktname)**
- **UUID**

Für Lenovo XClarity Administrator ist das Suchfeld:

- **IP address (IP-Adresse)**

Für Cluster sind die Suchfelder:

- **Cluster ID (Cluster-ID)**
- **Cluster Name (Clustername)**

Suchergebnisse

Die Suchergebnisse werden in der Baumstruktur in der hierarchischen Struktur angezeigt. Übereinstimmungen werden in Blau hervorgehoben. Die Knoten der oberen Ebene eines Übereinstimmungsknotens werden erweitert. Ein Übereinstimmungsknoten, der untergeordnete Knoten ohne Übereinstimmungen hat, wird reduziert.

Aus den Suchergebnissen können Sie einen Knoten auswählen und ihn wie gewohnt ausführen. Die Funktionen funktionieren auch normal.

Die Baumstruktur stoppt die Aktualisierung automatisch, während die Suchergebnisse angezeigt werden.

Eine Suche starten

Die Funktion zum „Starten einer Suche“ ermöglicht es Ihnen, nach bestimmten Ressourcen von Servern, Clustern, Gehäusen und/oder Lenovo XClarity Administrator-Instanzen zu suchen.

Vorgehensweise

Geben Sie den Suchbegriffstext in das Feld **Search (Suchen)** ein, das sich oben in der Lenovo-Add-In Baumstruktur befindet. Die Ergebnisse werden automatisch während der Eingabe angezeigt.

Suchergebnisse löschen

Die Funktion zum Löschen der Suchergebnisse ermöglicht es Ihnen, Ergebnisse einer Suche zu löschen, damit vollständige Ressourcen von Servern, Clustern, Gehäusen und/oder Lenovo XClarity Administrator-Instanzen angezeigt werden.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus:

1. Löschen Sie das Feld **Search (Suchen)**.
2. Drücken Sie die Esc-Taste.
3. Klicken Sie auf **Clear the Search (Suchfeld löschen)**.

Überwachung

In diesem Abschnitt wird das Verwalten von RAS, das Einstellen der Richtlinie, die Deaktivierung der Funktion „Automatische VM-Migration“ von Serverknoten und das Anzeigen des Ereignisverlaufs behandelt.

PFA-Verwaltung

Diese Funktion bietet die automatische Migrationsfunktion der virtuellen Maschine (VM) auf angegebenen Hardwareereignissen.

Vorbereitende Schritte

Diese Funktion ist Cluster-basiert. Bevor Sie mit den Vorgängen fortfahren, müssen Sie Cluster in SCVMM erstellen und Hosts in den Clustern hinzufügen. Das Cluster Shared Volume (CSV) ist ebenfalls erforderlich. Weitere Details finden Sie im Thema Microsoft System Center [Webseite „Microsoft System Center – Creating a Hyper-V Host Cluster in VMM Overview“](#).

Sie müssen auch die Schritte in „Ein Baseboard Management Controller (BMC) hinzufügen“ auf Seite 16 durchführen.

Eine Richtlinie festlegen

Mit der Funktion zum Festlegen von Richtlinien können Sie die Automatische VM-Migration auf ausgewählten Serverknoten mit besonderen Bedingungen und Ereigniskategorien aktivieren.

Vorbereitende Schritte

Schließen Sie die Voraussetzungen in „PFA-Verwaltung“ auf Seite 27 ab.

Vorgehensweise

- Schritt 1. Wählen Sie den **Hypervisors**-Stammeintrag oder einen Cluster oder einen Hypervisor-Knoten in einem Cluster im linken Hostnavigationsbereich.
- Schritt 2. Wählen Sie die Seite **PFA Management (PFA-Verwaltung)** oben im rechten Bereich aus. Die Seite RAS Management (RAS-Verwaltung) wird geöffnet.
- Schritt 3. Klicken Sie auf **Set Policy (Richtlinie festlegen)**. Das Dialogfenster Set Policy (Richtlinie festlegen) wird angezeigt.
- Schritt 4. Wählen Sie die Option „VM-Migration bei Hardwareereignissen aktivieren“ aus der Dropdown-Liste oben.
- Schritt 5. Wählen Sie bei Bedarf Bedingungen, Ereignis-Kategorien und Hosts bzw. heben Sie die Auswahl auf. Ein Host ist nicht auswählbar, wenn seine BMC nicht erkannt oder nicht authentifiziert wurde.
- Schritt 6. Klicken Sie auf **OK**. Eine Seite, auf der Sie aufgefordert werden, die Einstellungsanzeigen zu bestätigen.
- Schritt 7. Klicken Sie auf **OK**.
- Schritt 8. Klicken Sie auf den Zurück-Link unten, um zur Seite RAS Management (RAS-Verwaltung) zu wechseln.

Funktion „Automatische VM-Migration“ von Serverknoten deaktivieren

Diese Funktion ermöglicht es Ihnen, die automatische VM-Migration von ausgewählten Serverknoten zu deaktivieren.

Vorbereitende Schritte

Schließen Sie die Voraussetzungen in „PFA-Verwaltung“ auf Seite 27 ab.

Vorgehensweise

- Schritt 1. Wählen Sie den **Hypervisors**-Stammeintrag oder einen Cluster oder einen Hypervisor-Knoten in einem Cluster im linken Hostnavigationsbereich.
- Schritt 2. Wählen Sie die Seite **PFA Management (PFA-Verwaltung)** oben im rechten Bereich aus.

Die Seite RAS Management (RAS-Verwaltung) wird geöffnet.

Schritt 3. Klicken Sie auf **Set Policy (Richtlinie festlegen)**.

Das Dialogfenster Set Policy (Richtlinie festlegen) wird angezeigt.

Schritt 4. Wählen Sie die Option „VM-Migration bei Hardwareereignissen deaktivieren“ aus der Dropdown-Liste oben.

Schritt 5. Ändern Sie die Auswahl der Hosts, wenn dies notwendig ist.

Schritt 6. Klicken Sie auf **OK**.

Eine Seite, auf der Sie aufgefordert werden, die Einstellungsanzeigen zu bestätigen.

Schritt 7. Klicken Sie auf **OK**.

Schritt 8. Klicken Sie auf den Zurück-Link unten, um zur Seite RAS Management (RAS-Verwaltung) zu wechseln.

Ereignisprotokoll anzeigen

Die Funktion zum Anzeigen des Ereignisprotokolls ermöglicht Ihnen, Hardwareereignisse und die entsprechend durchgeführten Aktionen für diese Ereignisse anzuzeigen.

Vorbereitende Schritte

Schließen Sie die Voraussetzungen in „PFA-Verwaltung“ auf Seite 27 ab.

Vorgehensweise

Schritt 1. Wählen Sie den **Hypervisors**-Stammeintrag oder einen Cluster oder einen Hypervisor-Knoten in einem Cluster im linken Hostnavigationsbereich.

Schritt 2. Wählen Sie die Seite **PFA Management (PFA-Verwaltung)** oben im rechten Bereich aus. Die Seite RAS Management (RAS-Verwaltung) wird geöffnet.

Schritt 3. Klicken Sie auf **View Event History (Ereignisprotokoll anzeigen)**.

Die Seite **RAS Events (RAS-Ereignisse)** wird angezeigt. Sie enthält die RAS-Ereignisse und Vorgangsverlauf der Ereignisse, die für die Hosts vorhanden sind, die in der Tabelle auf der Seite PFA Management (PFA-Verwaltung) angezeigt werden.

Schritt 4. Klicken Sie auf den Zurück-Link unten, um zur Seite RAS Management (RAS-Verwaltung) zu wechseln.

Server aktualisieren

Dieses Kapitel enthält Informationen zum laufenden Systemneustart und zur laufenden Systemaktualisierung.

Laufende Systemaktualisierung

Die Funktion „Laufende Systemaktualisierung“ hilft Ihnen, die Server zu aktualisieren, während das System ausgeführt wird. Es gibt auf den betreffenden Serverhosts keine Unterbrechungen der Anwendungsdienste.

Vorbereitende Schritte

- Der Firmware-Download für IBM-Server wird nicht unterstützt.
- ThinkServer-Server werden nicht unterstützt.
- Die Funktion für die laufende Systemaktualisierung unterstützt die Server mit den folgenden Maschinentypen nicht, wenn das Betriebssystem Windows Server 2016 ist.

Maschinentypen: 7875,1929, 8038, 8039, 2582, 5457, 2583, 5458, 7382, 7383, 7160, 7914, 7158, 7159, 7915, 5460, 5466, 8722, 8733, 8752, 8718, 7145, 7146, 3837, 3839, 7143, 7191, 3837, 3839, 7918, 7919, 7912, 7913, 8737, 8738, 7863, 8956, 7906, 2585, 7916, 7917, 4259, 7903, 4259, 7903, 4259, 7903, 5455

- Installieren Sie das Microsoft Internet Explorer-Update KB3087038 mithilfe der Anweisungen in Microsoft Internet Explorer-Update KB3087038 installieren.

Task für laufende Systemaktualisierung erstellen

Sie können ein Update-Task erstellen und eine Firmwareaktualisierung für einen geplanten Zeitpunkt festlegen.

Zu dieser Aufgabe

Sie können Hostfirmware mit oder ohne eine Richtlinie aktualisieren.

- **Update with Policy (Aktualisierung mit Richtlinie)**

Sie können Firmwarekonformitätsrichtlinien erstellen und diese dann verwalteten Einheiten zuweisen. So können Sie sicherstellen, dass die Firmware auf diesen Einheiten konform bleibt. Folgende Voraussetzungen sind erforderlich:

- Hostmaschinen müssen zu Lenovo XClarity Administrator hinzugefügt und von diesem verwaltet werden.
- Firmwarekonformitätsrichtlinien müssen in Lenovo XClarity Administrator erstellt werden.
- Firmware wird in Lenovo XClarity Administrator heruntergeladen.
- Lenovo XClarity Administrator muss in Lenovo XClarity Integrator registriert werden.

Anmerkung: Wenn Sie Lenovo XClarity Administrator in Lenovo XClarity Integrator und neuer registriert haben, und später einen neuen Server zu Lenovo XClarity Administrator hinzugefügt haben, ist der Host beim Erstellen des Aktualisierungs-Tasks möglicherweise nicht zu sehen. Wenn dies auftritt, warten Sie eine Stunde vor einer Wiederholung.

- **Update without Policy (Aktualisierung ohne Richtlinie)**

Wenn Lenovo XClarity Administrator nicht in Ihrer Umgebung vorhanden ist, müssen Sie einzelne Firmwareaktualisierungen oder UXSP für jeden Server auswählen. Folgende Voraussetzungen sind erforderlich:

- Die Schritte im Hostauthentifizierung einrichten müssen abgeschlossen werden, wenn Sie eine Task vom Typ **Update without Policy (Aktualisierung ohne Richtlinie)** erstellen.
- Die Schritte in Einstellungen für laufende Systemaktualisierung festlegen müssen abgeschlossen werden, wenn Sie eine Task vom Typ **Update without Policy (Aktualisierung ohne Richtlinie)** erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Task für eine laufende Systemaktualisierung zu erstellen:

Schritt 1. Klicken Sie auf der Seite „Task-Manager“ auf **Create (Erstellen)**, um den Assistenten zum Erstellen von Tasks zu starten.

Schritt 2. Geben Sie einen Tasknamen an, wählen Sie den Tasktyp (**Update with Policy (Aktualisierung mit Richtlinie)** oder **Update without Policy (Aktualisierung ohne Richtlinie)**) aus und klicken Sie auf **Next (Weiter)**.

Anmerkung: Stellen Sie sicher, dass alle Voraussetzungen für jeden Tasktyp erfüllt sind.

Schritt 3. Wählen Sie Firmwareaktualisierungen und klicken Sie auf **Next (Weiter)**.

Wenn **Update with Policy (Aktualisierung mit Richtlinie)** ausgewählt ist, wählen Sie eine verfügbare Firmwarerichtlinie aus der Dropdown-Liste **Policy (Richtlinie)** für jeden Host aus. Sie können die Firmwareversion anzeigen, die in der Richtlinie definiert ist, und die Firmware-Auswahl anpassen.

Wenn **Update without Policy (Aktualisierung ohne Richtlinie)** ausgewählt ist, wählen Sie die bestimmte Firmware für jeden Host aus, den Sie aktualisieren möchten.

Schritt 4. Wählen Sie eine oder mehrere der folgenden Aktualisierungsoptionen aus und klicken Sie anschließend auf **Next (Weiter)**.

- **Update Parallelization (Parallele Aktualisierung).** Gibt an, wie viele Hosts gleichzeitig aktualisiert werden

- **Perform VM Evacuation (VM-Migration durchführen)**. Gibt an, ob virtuelle Maschinen vor der Aktualisierung des Hosts migriert werden.
- **Schedule (Zeitplan)**. Plant die Ausführung der Task zu einem geplanten Zeitpunkt.

Schritt 5. Zeigen Sie die Taskzusammenfassung an und klicken Sie auf **Save (Speichern)**.

Laufende Systemaktualisierung-Tasks verwalten

Sie können die Funktion „Laufende Systemaktualisierung“ verwenden, um Laufende Systemaktualisierung-Tasks zu verwalten.

Zu dieser Aufgabe

Die Funktion „Laufende Systemaktualisierung“ bietet einen Task-Manager zum Verwalten von Laufende Systemaktualisierung-Tasks. Eine Task enthält alle Informationen und Optionen für eine laufende Aktualisierung.

Mit dem Task-Manager können Sie die folgenden Tasks durchführen:

- Task für laufende Systemaktualisierung erstellen. Jeder Cluster kann nur eine aktive Task haben, wenn der Tasktyp **Update Only (Nur aktualisieren)**, **Update and Reboot (Aktualisieren und neu starten)** oder **Reboot Only (Nur neu starten)** lautet.
- Eine Task für laufende Systemaktualisierung bearbeiten, die noch nicht gestartet wurde.
- Eine Task für laufende Systemaktualisierung kopieren, die abgeschlossen wurde.
- Eine Task für laufende Systemaktualisierung aus der Taskliste entfernen.
- Eine Task für laufende Systemaktualisierung abbrechen, die bereits ausgeführt wird.
- Den Status einer Task für laufende Systemaktualisierung anzeigen.

Vorgehensweise

Schritt 1. Klicken Sie auf **Lenovo XClarity Integrator → Rolling System Update (Laufende Systemaktualisierung)**.

Schritt 2. Klicken Sie im Navigationsbereich auf **Task Manager (Task-Manager)**. Die Seite „Task-Manager“ wird angezeigt.

Wenn die Einstellungen nicht vorher festgelegt wurden, wird die Einstellungenseite angezeigt. Wenn bereits Einstellungen festgelegt wurden, wird die Task-Manager-Seite „Laufende Systemaktualisierung“ angezeigt und Sie können auf den Link **Preferences (Einstellung)** klicken, um die Einstellungenseite anzuzeigen.

Schritt 3. Führen Sie einen der folgenden Schritte aus:

- Task erstellen
- Task kopieren
- Task bearbeiten
- Task entfernen
- Task abbrechen
- Taskliste auf der Seite aktualisieren

Wenn Sie auf **Create (Erstellen)** oder **Edit (Bearbeiten)** klicken, können Sie den Assistenten „Task erstellen/bearbeiten“ verwenden, um eine Task zu erstellen oder zu bearbeiten.

Tabelle 6. **Rolling System Update-Taskstatus**

Ziel	Status	Beschreibung
Task für laufende Aktualisierung	Nicht gestartet	Die Task wurde nicht gestartet.
	Wird ausgeführt	Die Task wird ausgeführt.
	Abgebrochen	Die Task wird abgebrochen.
	Fehler	Das Herunterladen des Firmwarepakets ist fehlgeschlagen.
	Fertig	Die Task ist abgeschlossen.
Host	Nicht gestartet	Das Update für den Host wurde nicht gestartet.
	Migrieren	Der Host tritt in den Wartungsmodus ein.

Tabelle 6. Rolling System Update-Taskstatus (Forts.)

Ziel	Status	Beschreibung
	Wartung	Der Host befindet sich im Wartungsmodus.
	Aktualisieren	Die Firmware des Hosts wird aktualisiert.
	Neustart	Der Host wird neu gestartet, nachdem die Aktualisierung abgeschlossen wurde.
	Wartungsmodus beenden	Der Host verlässt den Wartungsmodus.
	Erfolg	Die Firmwareaktualisierung ist fehlgeschlagen.
	Fehler	Die Ursachen des Hostfehlers: <ul style="list-style-type: none"> • Das Aktualisierungspaket kann nicht abgerufen werden. • Der Wartungsmodus kann nicht aktiviert werden. • Die Firmware kann nicht aktualisiert werden. • Der Host kann nicht neu gestartet werden. • Der Wartungsmodus kann nicht beendet werden.
Firmware	Nicht gestartet	Die Firmwareaktualisierung wurde nicht gestartet.
	Wird ausgeführt	Die Firmwareaktualisierung wird ausgeführt.
	Erfolg	Die Firmwareaktualisierung ist fehlgeschlagen.
	Fehler	Die Firmwareaktualisierung ist fehlgeschlagen.

Laufender Systemneustart

Die Funktion „Laufender Systemneustart“ hilft Ihnen, die Server neu zu starten, während das System ausgeführt wird. Es gibt auf den betreffenden Serverhosts keine Unterbrechungen der Anwendungsdienste.

Vorbereitende Schritte

- Sie müssen die Informationen, die in „Hostauthentifizierung einrichten“ auf Seite 14 beschrieben werden, festlegen.
- Sie müssen die Schritte in „Einstellungen für laufende Systemaktualisierung festlegen“ auf Seite 16 durchführen.

Zu dieser Aufgabe

Der laufende Systemneustart stellt einen Task-Manager bereit, über den Sie Tasks für einen laufenden Systemneustart verwalten können. Eine Task enthält alle Informationen und Optionen für einen laufende Neustart.

Der Task-Manager hält die folgenden Taskoptionen bereit:

- Task für laufenden Systemneustart erstellen. Jeder Cluster kann nur eine aktive Task haben, wie auch immer der Tasktyp ist:
 - Nur Aktualisierung
 - Aktualisierung und Neustart
 - Nur Neustart
- Eine Task für laufenden Systemneustart bearbeiten, die noch nicht gestartet wurde
- Eine Task für laufenden Systemneustart aus der Taskliste entfernen
- Eine Task für laufenden Systemneustart abbrechen, die bereits ausgeführt wird
- Status des laufenden Systemneustarts anzeigen

Vorgehensweise

Schritt 1. Erweitern Sie im Navigationsfenster des Lenovo-Add-In „Hypervisor“ und wählen Sie dann Zielcluster aus.

Schritt 2. Wählen Sie „Laufender Systemneustart“ oben im Hauptbild.
Die Seite Task Management (Task-Verwaltung) wird angezeigt.

Schritt 3. Führen Sie eine der folgenden Aufgaben aus:

- Task erstellen
- Task bearbeiten
- Task entfernen
- Task abbrechen
- Taskliste auf der Seite aktualisieren

Wenn Sie auf **Create (Erstellen)** oder **Edit (Bearbeiten)** klicken, können Sie den Assistenten Create/Edit Task (Task erstellen/bearbeiten) verwenden, um eine Task zu erstellen oder zu bearbeiten.

Table 7. Status der Task für laufenden Systemneustart

Ziel	Status	Beschreibung
Laufender Neustart	Nicht gestartet	Die Task wurde nicht gestartet.
Aufgabe	Wird ausgeführt	Die Task wird ausgeführt.
	Abgebrochen	Die Task wird abgebrochen.
	Fehler	Ursachen des Taskfehlers: <ul style="list-style-type: none">• Neustarthost fehlgeschlagen• VIM-Migration fehlgeschlagen
	Fertig	Die Task ist abgeschlossen.
Host	Nicht gestartet	Der Neustart für den Host wurde nicht gestartet.
	Migrieren	Der Host tritt in den Wartungsmodus ein.
	Wartung	Der Host befindet sich im Wartungsmodus.
	Neustart	Der Host wird neu gestartet, nachdem die Aktualisierung abgeschlossen wurde.
	Wartungsmodus beenden	Der Host verlässt den Wartungsmodus.
	Erfolg	Der Neustart und das Beenden der Wartung waren erfolgreich.
	Fehler	Die Ursachen des Hostfehlers: <ul style="list-style-type: none">• Der Wartungsmodus kann nicht aktiviert werden.• Der Host kann nicht neu gestartet werden.• Der Wartungsmodus kann nicht beendet werden.

Lenovo-Add-In konfigurieren

Alle in diesem Abschnitt beschriebenen Funktionen basieren auf Lenovo XClarity Administrator und beschreiben, wie Sie mit Konfigurationsmustern arbeiten.

Konfigurationsmuster

Die Konfigurationsmusterfunktion hilft Ihnen, ein Konfigurationsmuster ganz einfach bereitzustellen. Konfigurationsmuster sind eine Serverkonfiguration, die vor Installation des Betriebssystems vorgenommen wird; dazu gehört die Konfiguration des lokalen Speichers, der E/A-Adapter, der Booteinstellungen sowie

anderer BMC- und uEFI-Firmwareeinstellungen. Ein Konfigurationsmuster ist ein Gesamtmuster für die schnelle Konfiguration mehrerer Server zur gleichen Zeit.

Vorbereitende Schritte

- Sie müssen die Schritte in „Lenovo XClarity Administrator hinzufügen“ auf Seite 17 durchführen.
- Sie müssen sich bei Lenovo XClarity Administrator anmelden und ein Konfigurationsmuster auf der Website erstellen.

Um die Seite Configuration Pattern (Konfigurationsmuster) aufzurufen, führen Sie die Schritte im Verfahren aus.

Vorgehensweise

- Schritt 1. Erweitern Sie im Navigationsbereich Lenovo Infrastruktur und klicken Sie anschließend auf einen Lenovo XClarity Administrator oder Elemente unter dem Lenovo XClarity Administrator.
- Schritt 2. Klicken Sie oben im Hauptbild auf die Registerkarte **Config Pattern (Konfigurationsmuster)**. Die Seite Config Pattern (Konfigurationsmuster) wird angezeigt.

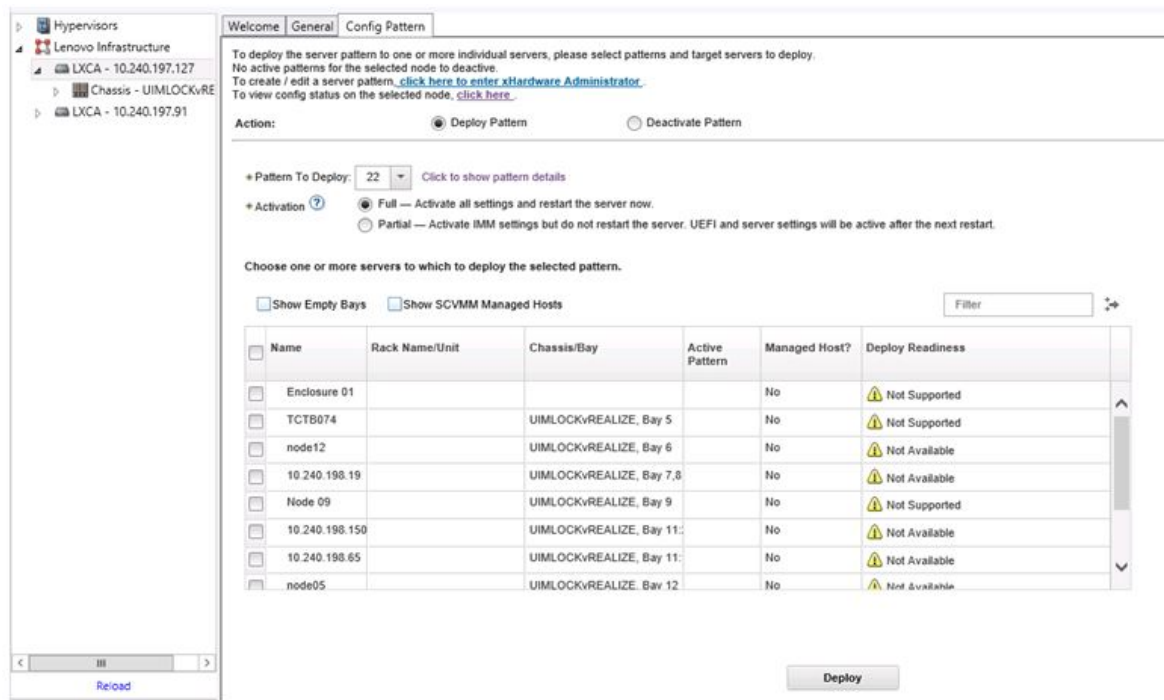


Abbildung 7. Seite Configuration Pattern (Konfigurationsmuster)

Konfigurationsmuster implementieren

Unter Verwendung der Seite Configuration Pattern (Konfigurationsmuster) können Sie die Schritte in diesem Abschnitt befolgen, um ein Konfigurationsmuster zu implementieren.

Vorgehensweise

- Schritt 1. Wählen Sie **Deploy Pattern (Muster bereitstellen)** als Aktion aus.
- Schritt 2. Wählen Sie das Muster aus, die Sie implementieren möchten. Wenn es keine Elemente in Liste **Pattern to Deploy (Zu implementierendes Muster)** gibt, müssen Sie bei Lenovo XClarity Administrator anmelden, um eines zu erstellen.
- Schritt 3. Treffen Sie Ihre Wahl dazu, wie Sie das Konfigurationsmuster aktivieren möchten.

- **Full (Vollständig):** Alle Einstellungen werden aktiviert und der Server wird nun neu gestartet.
- **Partial (Teilweise):** BMC-Einstellungen werden aktiviert, der Server wird jedoch nicht neu gestartet. uEFI- und Servereinstellungen werden nach dem nächsten Neustart übernommen.

Schritt 4. Wählen Sie die Systeme aus, auf die Sie abzielen möchten, um das Konfigurationsmuster zu implementieren.

Schritt 5. Klicken Sie auf **Deploy (Implementieren)**. Ein Dialogfenster mit einer Zusammenfassung wird angezeigt, in dem Sie Ihre Auswahl bestätigen können.

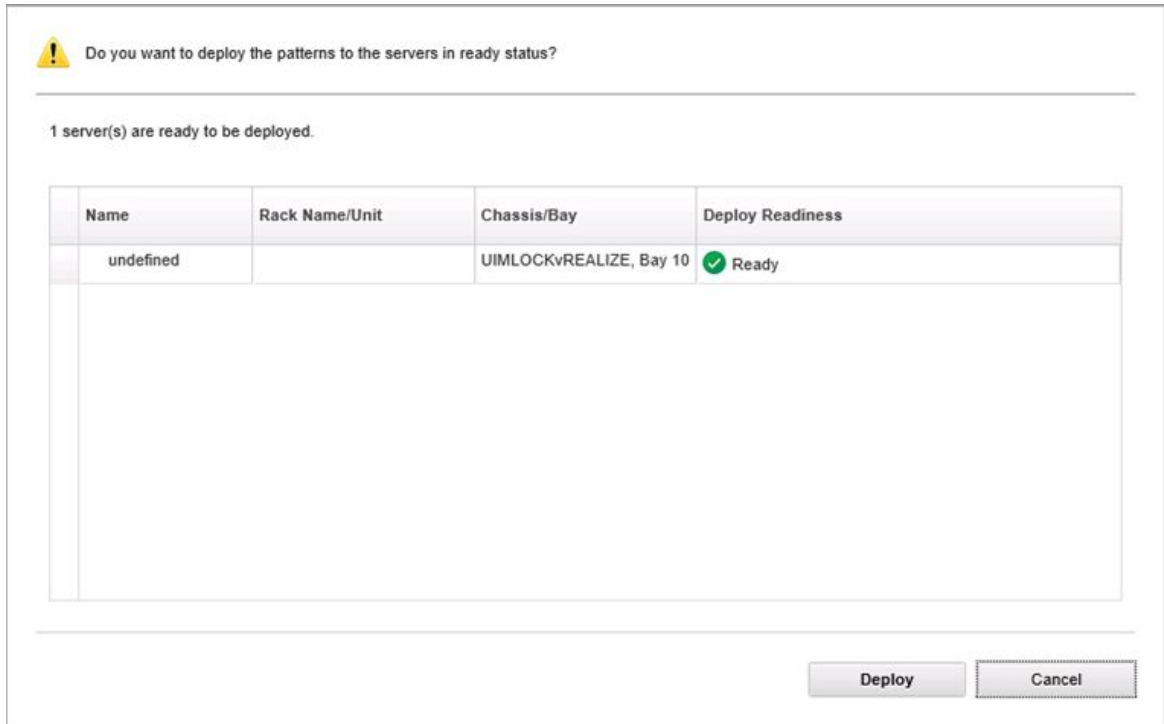


Abbildung 8. Dialogfenster mit einer Zusammenfassung der Konfigurationsmuster

Schritt 6. Klicken Sie auf **Deploy (Implementieren)**.

Ein Bestätigungsfenster, in dem gezeigt wird, dass die Bereitstellungsanforderung übermittelt wird.



Abbildung 9. Bestätigungsfenster mit der Bereitstellungsanforderung

Wenn die Übermittlung abgeschlossen ist, wird ein anderes Bestätigungsfenster angezeigt.

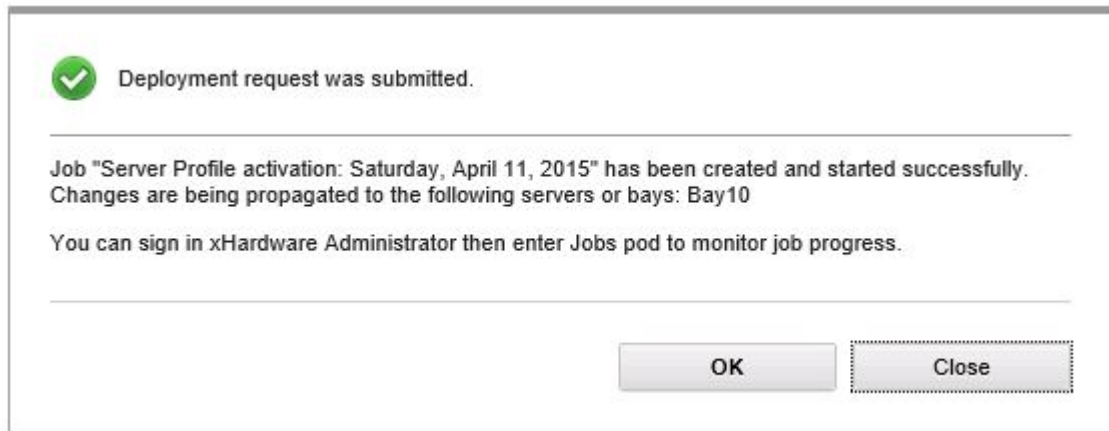


Abbildung 10. Bestätigungsfenster mit der übermittelten Bereitstellungsanforderung

Zum Anzeigen der Details eines Servermusters klicken Sie auf den Link zum Anzeigen der Musterdetails im Fenster Deploy Server Pattern (Servermuster implementieren). Die Details eines Servermusters werden ähnlich wie im Beispiel auf dem Bildschirm unten angezeigt.

angela01 - Details

Pattern type: Server
Description: Pattern created from server: IMM2-40f2e9b813 Learned on: Nov 1, 2015 8:02:49 PM

Configuration

Server Pattern Settings: angela01	
Form Factor: Rack 1 Bay Compute Node	
+ Local Storage	
+ I/O Adapters	
+ Boot	

Close

Abbildung 11. Servermusterdetails

Konfigurationsmuster deaktivieren

Unter Verwendung der Seite Configuration Pattern (Konfigurationsmuster) können Sie die Schritte in diesem Abschnitt befolgen, um ein Konfigurationsmuster zu deaktivieren.

Vorgehensweise

Schritt 1. Wählen Sie **Deactivate Pattern (Muster deaktivieren)** als Aktion aus.

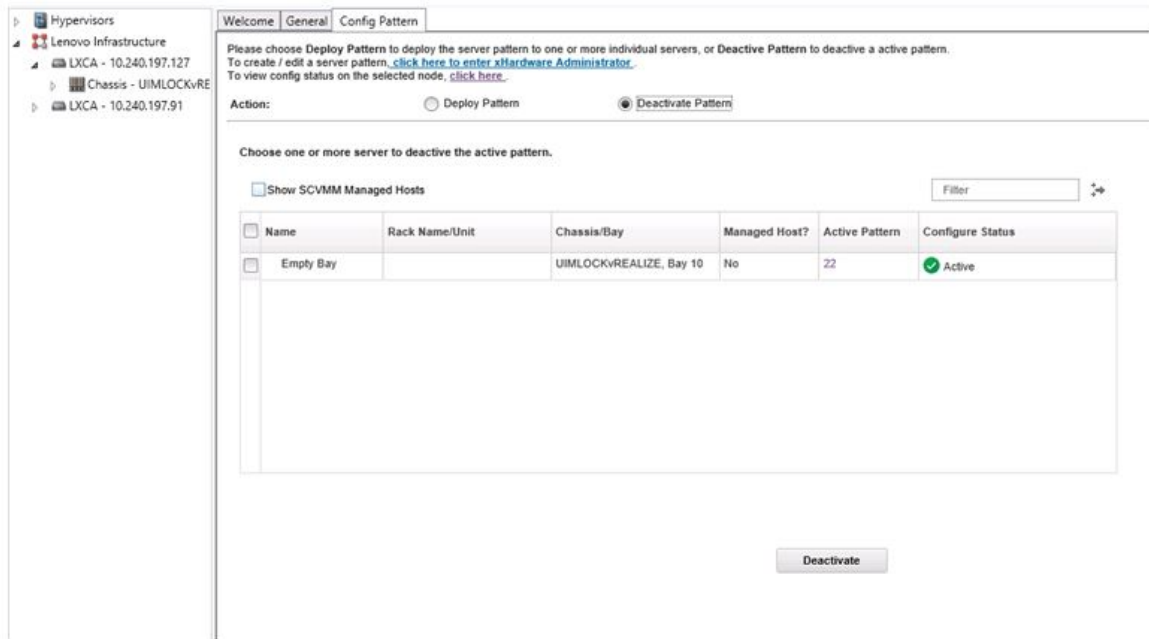


Abbildung 12. Konfigurationsmuster deaktivieren

- Schritt 2. Aktivieren Sie ein oder mehrere Kontrollkästchen neben den Konfigurationsmustern, die Sie deaktivieren möchten.
- Schritt 3. Klicken Sie auf **Deactivate (Deaktivieren)**.
Das Dialogfenster Deactivate Server Pattern (Servermuster deaktivieren) wird angezeigt.



Abbildung 13. Dialogfenster Deactivate Server Pattern (Servermuster deaktivieren)

- Schritt 4. Klicken Sie auf **Deactivate (Deaktivieren)**, um zu bestätigen, dass Sie das Konfigurationsmuster deaktivieren möchten.

Ein Statusdialog wird angezeigt, während das Konfigurationsmuster deaktiviert wird.



Abbildung 14. Statusdialogfeld deaktivieren

Wenn die Deaktivierung abgeschlossen ist, wird das Dialogfenster Pattern Deactivation Summary (Zusammenfassung der Musterdeaktivierung) angezeigt.

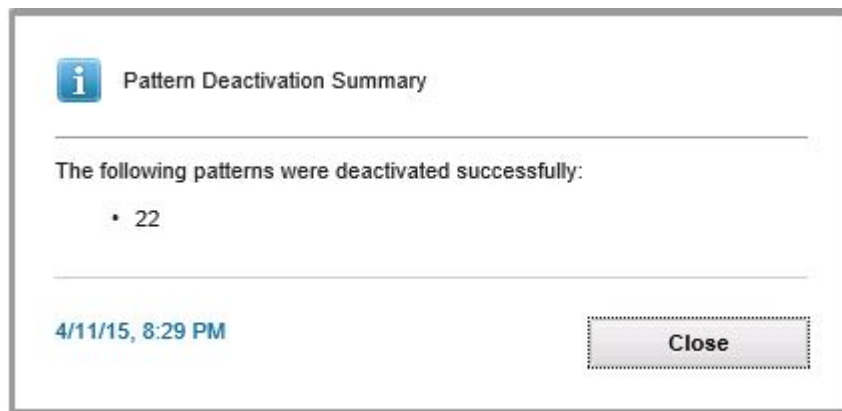


Abbildung 15. Dialogfenster „Zusammenfassung der Musterdeaktivierung“

Schritt 5. Klicken Sie auf **Close (Schließen)**, um zur Seite Configuration Pattern (Konfigurationsmuster) zurückzukehren.

Kapitel 6. Lenovo-Add-In konfigurieren

In diesem Abschnitt wird die Konfiguration von Lenovo-Add-In beschrieben.

Lenovo XClarity Integrator-Verwaltung öffnen

Vorbereitende Schritte

Stellen Sie sicher, dass Sie bei Lenovo XClarity Integrator Unified Service angemeldet sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Lenovo XClarity Integrator-Verwaltung zu öffnen.

Schritt 1. Erweitern Sie die Seitenleiste links von Lenovo-Add-In.

Schritt 2. Klicken Sie auf **Lenovo XClarity Integrator Management (Lenovo XClarity Integrator-Verwaltung)**.

Schritt 3. Melden Sie sich mit dem Benutzernamen und dem Kennwort für Unified Service an.

Kennwort für Unified Service ändern

Sie können das Kennwort für Unified Service ändern.

Vorgehensweise

Schließen Sie die folgenden Schritte ab, um das Kennwort für Unified Service zu ändern.

Schritt 1. Klicken Sie oben rechts auf **Change Password (Kennwort ändern)**.

Schritt 2. Geben Sie das vorhandene Kennwort und das neue Kennwort ein.

Anmerkung: Das neue Kennwort muss den Kennwortregeln entsprechen.

Schritt 3. Klicken Sie auf **Change (Ändern)**.

Servicedaten erfassen

Sie können Protokolldateien erfassen und die Protokollierungsstufe festlegen.

Protokolldateien erfassen

Sie können Protokolldateien erfassen und herunterladen.

Vorgehensweise

Schritt 1. Klicken Sie auf **Collect Log (Protokoll erfassen)**.

Schritt 2. Klicken Sie auf **Download Log (Protokoll herunterladen)**.

Protokollierungsstufe ändern

Sie können die Protokollierungsstufe ändern. Die Protokollierungsstufen umfassen Debug-Nachrichten, Informationen, Warnungen und Fehler.

Vorgehensweise

Klicken Sie auf das Dropdown-Menü, um die Protokollierungsstufe zu ändern.

- **Debug-Nachrichten.** Die Protokolldatei zeichnet Fehler, Warnungen, Informationen und Debug-Nachrichten auf.
- **Informationen.** Die Protokolldatei zeichnet Fehler, Warnungen und Informationsnachrichten auf.
- **Warnung.** Die Protokolldatei zeichnet Warnungen und Fehlernachrichten auf.
- **Fehler.** Die Protokolldatei zeichnet nur Fehlernachrichten auf.

Sicherheit verwalten

Sie können das BMC-Kommunikationsprotokoll festlegen und Stammzertifikate verwalten.

BMC-Kommunikationsprotokoll festlegen

Sie können sich dazu entscheiden, mit allen verwalteten Baseboard Management Controllern (BMCs) über das HTTPS-Protokoll zu kommunizieren.

Vorbereitende Schritte

Stellen Sie sicher, dass das HTTPS-Protokoll auf allen BMCs aktiviert ist. Falls es nicht aktiviert ist, erfolgt erst ein Versuch mit HTTPS und dann ein Versuch mit HTTP.

Vorgehensweise

Schritt 1. Klicken Sie auf die Registerkarte **Security Setting (Sicherheitseinstellung)**.

Schritt 2. Wählen Sie das Kontrollkästchen aus.

Schritt 3. Klicken Sie auf **Save (Speichern)**.

Datenbankinformationen anzeigen

Sie können die Datenbankinformationen anzeigen.

Vorgehensweise

Um Datenbankinformationen anzuzeigen, klicken Sie auf die Registerkarte **Database Information (Datenbankinformationen)**.

Daten von PostgreSQL zu SQL migrieren

Sie können vorhandene Daten von einem PostgreSQL- zu einem SQL-Datenbankserver migrieren.

Vorbereitende Schritte

Während der Deinstallation der alten Version darf die Konfigurationsdatei nicht gelöscht werden und der PostgreSQL-Server darf nicht deinstalliert sein.

Während der Installation der neuen Version müssen Sie den SQL Server als Datenbanklösung auswählen.

Nach erfolgreichem Abschluss der Migration werden die vorhandenen Daten in der neuen Datenbank durch die migrierten Daten überschrieben.

Vorgehensweise

Schließen Sie die folgenden Schritte ab, um das Kennwort für Unified Service zu ändern.

Schritt 1. Klicken Sie links auf der Seite auf die Registerkarte **Migrate Data (Daten migrieren)**.

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

Schritt 3. Klicken Sie auf **OK**.

Schritt 4. Klicken Sie nach erfolgreichem Abschluss der Migration auf **OK**.

Mit Sicherheitszertifikaten arbeiten

Lenovo XClarity Integrator und die unterstützende Software verwenden SSL-Zertifikate, um eine sichere Verbindungen miteinander einzurichten. In Lenovo XClarity Integrator werden standardmäßig von Lenovo XClarity Integrator generierte Zertifikate verwendet, die von einer internen Zertifizierungsstelle (CA) ausgestellt und selbst signiert sind.

Ein angepasstes, extern signiertes Serverzertifikat generieren

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

Vorbereitende Schritte

Wenn das neue Serverzertifikat nicht von einer vertrauenswürdigen internationalen Zertifizierungsstelle signiert ist, wird bei der nächsten Verbindung zum Add-in eine Sicherheitsnachricht angezeigt. Um die Sicherheitsnachricht zu vermeiden, aktivieren Sie das Kontrollkästchen **Trust the certificate permanently (Dem Zertifikat dauerhaft vertrauen)** und klicken Sie auf **Next (Weiter)**.

Vorgehensweise

Schritt 1. Generieren Sie die Zertifikatssignieranforderung (CSR) für Lenovo XClarity Integrator.

- a. Wählen Sie **Server Certificate (Serverzertifikat)** aus, um die Seite „Server Certificate (Serverzertifikat)“ anzuzeigen.
- b. Wählen Sie die Registerkarte **Generate Certificate Signing Request (CSR) (Zertifikatssignieranforderung (CSR) generieren)** aus.
- c. 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: Wählen Sie einen Allgemeinen Namen aus, der die IP-Adresse oder den Hostnamen von Lenovo XClarity Integrator enthält. Bei Auswahl eines falschen Werts wird die Verbindung nicht als vertrauenswürdig betrachtet. Wenn der allgemeine Name automatisch von Lenovo XClarity Integrator generiert werden soll, wählen Sie **Generated by LXCI (Generiert von Lenovo LXCI)** aus.

- d. Wählen Sie **Generate CSR File (CSR-Datei generieren)** aus, um die generierte Datei herunterzuladen.

Schritt 2. Senden Sie alle CSRs zum Signieren an die vertrauenswürdige Zertifizierungsstelle. Die vertrauenswürdige Zertifizierungsstelle gibt für jede CSR ein Zertifikatspaket zurück. Dieses enthält das signierte Zertifikat und eine vollständige vertrauenswürdige CA-Zertifikatkette.

Schritt 3. Laden Sie das extern signierte Serverzertifikat nach Lenovo XClarity Integrator hoch.

Anmerkung: Erstellen Sie das Zertifikat zum Hochladen in der CSR, die Sie zuvor durch Klicken auf die Schaltfläche **Generate CSR File (CSR-Datei generieren)** erzeugt haben. Die hochgeladene Datei muss die vollständige Zertifikatskette einschließlich des Stammzertifikats und der Zwischenzertifikate enthalten. Die Zertifikate müssen in folgender Reihenfolge aufgeführt sein: Serverzertifikat, Zwischenzertifikate, Stammzertifikat.

- a. Klicken Sie im Lenovo XClarity Integrator-Menü auf **Security Settings (Sicherheitseinstellungen)**.

- b. Klicken Sie auf der Seite „Settings“ (Einstellungen) auf **Server Certificate (Serverzertifikat)**.
- c. Klicken Sie auf **Upload Certificate (Zertifikat hochladen)**, um die Zertifikatsdatei (.cer) hochzuladen.

Anmerkung: Nachdem das neue Serverzertifikat hochgeladen wurde, starten Sie System Center Virtual Machine Manager neu.

Das von Lenovo XClarity Integrator generierte Serverzertifikat wiederherstellen

Wenn Lenovo XClarity Integrator ein angepasstes Serverzertifikat verwendet, können Sie das von Lenovo XClarity Integrator generierte Zertifikat wiederherstellen, indem Sie ein neues Serverzertifikat generieren. Das angepasste Serverzertifikat wird dann durch das neue selbst signierte Serverzertifikat ersetzt.

Vorgehensweise

Schritt 1. Generieren Sie ein neues CA-Stammzertifikat und ersetzen Sie alle Serverzertifikate, die in Lenovo XClarity Integrator generiert wurden.

- a. Klicken Sie auf der Seite „Settings (Einstellungen)“ auf **Certificate Authority (Zertifizierungsstelle)**.
- b. Wählen Sie **Regenerate Certificate Authority Root Certificate (Stammzertifikat der Zertifizierungsstelle neu generieren)** aus.

Schritt 2. Laden Sie das CA-Stammzertifikat herunter.

- a. Klicken Sie auf der Seite „Settings (Einstellungen)“ auf **Certificate Authority (Zertifizierungsstelle)**.
- b. Wählen Sie **Download Certificate Authority Root Certificate (Stammzertifikat der Zertifizierungsstelle herunterladen)** aus, um das Stammzertifikat herunterzuladen.

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

- a. Klicken Sie auf der Seite „Settings (Einstellungen)“ auf **Server Certificate (Serverzertifikat)**.
- b. Wählen Sie die Registerkarte **Regenerate Server Certificate (Serverzertifikat neu generieren)** aus.
- c. 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: Wählen Sie einen Allgemeinen Namen aus, der die IP-Adresse oder den Hostnamen von Lenovo XClarity Integrator enthält. Bei Auswahl eines falschen Werts wird die Verbindung nicht als vertrauenswürdig betrachtet. Wenn der allgemeine Name automatisch von Lenovo XClarity Integrator generiert werden soll, wählen Sie **Generated by LXCI (Generiert von Lenovo LXCI)** aus.

- d. Wählen Sie **Regenerate Certificate (Zertifikat neu generieren)** aus.

Stammzertifikat neu generieren

Sie können das Stammzertifikat neu generieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das Stammzertifikat neu zu generieren.

Schritt 1. Klicken Sie auf die Registerkarte **Certificate Authority (Zertifizierungsstelle)**.

Schritt 2. Klicken Sie auf **Regenerate Certificate Authority Root Certificate (Stammzertifikat der Zertifizierungsstelle neu generieren)**.

Schritt 3. Klicken Sie auf **OK**, um fortzufahren.

Schritt 4. Klicken Sie nach dem Neustart des Service auf **Refresh (Aktualisieren)**.

Stammzertifikat herunterladen

Sie können das Stammzertifikat herunterladen.

Vorgehensweise

Schritt 1. Klicken Sie auf die Registerkarte **Certificate Authority (Zertifizierungsstelle)**.

Schritt 2. Wählen Sie **Download Certificate Authority Root Certificate (Stammzertifikat der Zertifizierungsstelle herunterladen)** aus.

Kapitel 7. Fehlerbehebung

Dieser Abschnitt beschreibt Situationen, die gelegentlich mit auftreten, und wie Sie sie durch Scannen lösen können. Zudem gibt es eine ausführliche Tabelle zum Festlegen Ihrer Firewall-Einstellungen.

Scanjob für laufende Systemaktualisierung aufgrund von Systemfehler 22029 fehlgeschlagen

Verwenden Sie diese Informationen zur Fehlerbehebung bei der Fehlermeldung Error (22029) VMM could not create a process for the script command C:\UIM_RIM\UIM.IRM.OneCliManagement.exe. (Fehler (22029). Ein Prozess für den Skriptbefehl C:\UIM_RIM\UIM.IRM.OneCliManagement.exe konnte nicht erstellt werden.) im SCVMM-Job. Dieser Fehler bedeutet, dass die Funktion für eine laufende Aktualisierung ohne Richtlinie die installierte Version des Zielservers nicht abrufen kann.

Entweder wurde eine erforderliche Identitätswechselebene nicht bereitgestellt oder die bereitgestellte Identitätswechselebene ist ungültig (0x80070542).

Vorgehensweise

Führen Sie zur Lösung des Problems einen oder mehrere der folgenden Schritte aus.

- Verwenden Sie Domäne\Administrator als Konto zur Ausführung auf dem Zielserver
- Wenn sich das „Ausführen als“-Konto für SCVMM in der Gruppe „Administratoren“ befindet, jedoch kein Administrator ist, deaktivieren Sie die Sicherheitsoption **Run all administrators in Admin Approval Mode (Alle Administratoren im Administratorgenehmigungsmodus ausführen)** auf dem Zielserver. Wenn diese Richtlinieneinstellung deaktiviert ist, benachrichtigt Sie das Sicherheitscenter darüber, dass die Gesamtsicherheit des Betriebssystems reduziert wurde. Weitere Informationen finden Sie unter [Microsoft TechNet: „User Account Control: Run all administrators in Admin Approval Mode“](#)..

Fehler beim Speichern der Einstellungen für laufende Systemaktualisierung aufgrund von Systemfehler 1219

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlermeldung im SCVMM-Job: Error (1219) (Fehler (1219)). Dieser Fehler kann auftreten, wenn Sie versuchen, einen freigegebenen Netzwerkordner als Repository zu verwenden.

Vorgehensweise

Um dieses Problem zu beheben, installieren Sie die neueste Aktualisierung für Windows und wählen Sie einen anderen Ordner.

Die Lenovo XClarity Integrator Unified Service-Sitzung wird ungültig

Die Lenovo Add-in-Konsole meldet sich beim Hintergrund-Dämon, dem (Lenovo XClarity Integrator Unified Service) an, wenn die Konsole startet. Das heißt eine neue Sitzung wird erstellt.

Zu dieser Aufgabe

Die Sitzung läuft nicht aus, wenn die Konsole offen bleibt und der Dämon ohne Unterbrechung im Dienst bleibt.

Wenn der Dämon jedoch unterbrochen wird (zum Beispiel durch einen Neustart), wird die Sitzung ungültig.

Wenn eine Sitzung ungültig wird, treten die folgenden Symptome auf:

- Das Feld „Assetbaum“ im Lenovo Add-in zeigt nur Stammknoten an oder Ressourcenänderungen werden nicht im Feld „Assetbaum“ angezeigt.
- Die funktionalen Benutzeroberflächenseiten sind leer oder enthalten keine Daten, wenn Daten angezeigt werden sollen.

Um das Problem zu beheben, starten Sie die SCVMM-Konsole und die Lenovo-Add-in-Konsole erneut.

Anmerkung: Anweisungen dazu, wie der Anmeldeverlauf überprüft wird, finden Sie unter .

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die SCVMM-Konsole und die Lenovo-Add-in-Konsole erneut zu starten.

Schritt 1. Klicken Sie auf die Schaltfläche ganz links, um die Seitenleiste zu erweitern.

Schritt 2. Klicken Sie auf **Reload (Erneut laden)**.

Vorauthentifiziertes IMM verliert möglicherweise nach der Verwaltung durch Lenovo XClarity Administrator die Verbindung

Bei einem IMM, für den Sie vorher in Lenovo XClarity Integrator einen Zugriff über ein lokales IMM-Konto angefordert haben, verliert Lenovo XClarity Integrator den Zugriff auf den IMM, nachdem dieser mit Lenovo XClarity Administrator verwaltet wird.

Lenovo XClarity Administrator deaktiviert alle lokalen IMM-Konten bei der Übernahme der Verwaltung des IMM. Lenovo XClarity Integrator kann daher nicht über das vorher bereitgestellte lokale IMM-Konto auf den IMM zugreifen.

Vorgehensweise

Verwenden Sie den Account, das Sie in Lenovo XClarity Administrator konfigurieren haben, um den IMM-Zugriff in Lenovo XClarity Integrator erneut anzufordern.

Funktionen sind nicht für einen System x-Server verfügbar, wenn sie aus der Ressourcenbaumstruktur ausgewählt werden.

Funktionen sind nicht für System x-Server verfügbar, wenn sie aus der Ressourcenbaumstruktur von Lenovo XClarity Integrator-Add-in ausgewählt werden, wenn der Maschinentyp des Servers nicht bestimmt wurde.

Vorgehensweise

Gehen Sie wie folgt vor, um den Maschinentyp für einen Server aufzurufen:

- Lassen Sie den UUS-Serverservice mit einer Windows-/Domänenanmeldung ausführen, die die WMI-Leseberechtigung für das Ziel-Hyper-V-System hat. Um das Benutzeraccount eines Windows-Service zu ändern, verwenden Sie die Webseite „Microsoft TechNet: Configure How a Service Is Started“.
- Authentifizieren Sie einen Hypervisor-Knoten mit einer Windows-/Domänenanmeldung, die die WMI-Leseberechtigung für das Ziel-Hyper-V-System hat.
- Verwalten Sie den Server mit einem Lenovo XClarity Administrator und registrieren Sie den Lenovo XClarity Administrator im Lenovo XClarity Integrator-Add-in.
- Führen Sie die Erkennung des IMM für den bestimmten Server durch.

Registrierung von Lenovo XClarity Administrator mit IPv6-Adresse fehlgeschlagen

Wenn Sie eine IPv6-Adresse für die Registrierung von Lenovo XClarity Administrator verwenden, wird die Nachricht Loading, Please wait ... (Laden, bitte warten ...) angezeigt, doch es passiert nichts, da Lenovo XClarity Integrator Unified Service die Zertifikatskette nicht von der IPv6-Adresse abrufen konnte. Hierbei handelt es sich um eine Einschränkung von Lenovo XClarity Integrator.

Vorgehensweise

Strategie zur Problemlösung: Um das Problem zu beheben, laden Sie das Zertifikat manuell von Lenovo XClarity Administrator herunter und fügen Sie das Zertifikat zu Lenovo XClarity Integrator hinzu, indem Sie **Manage trusted certificates (Vertrauenswürdige Zertifikate verwalten)** → **Add (Hinzufügen)** auswählen.

Anmerkung: ThinkServer unterstützen nur den laufenden Neustart. Hierbei handelt es sich um eine Einschränkung des Lenovo XClarity Integrator-Add-ins.

Host wird in der SCVMM-Hostliste angezeigt, allerdings nicht im Lenovo-Add-In

Manchmal wird ein Host in der SCVMM-Hostliste angezeigt, allerdings nicht im Lenovo-Add-In. Sie können diesen Fehler umgehen, indem Sie den Host manuell zu SCVMM hinzufügen.

Gelegentlich fehlt ein Host in der Lenovo-Add-In-Hostliste, auch wenn er in der SCVMM-Hostliste angezeigt wird. Dies geschieht, wenn die SCVMM-Service-/Agenten-Anwendungen die Hardwaresystem-UUID nicht vom BIOS des Hosts erfassen. Es ist möglich, dass die SCVMM-Service-/Agenten-Anwendungen die Informationen später erfolgreich erfassen, aber ob dies der Fall ist und wie lange es dauert, kann nicht vorhergesehen werden. Um sicherzustellen, dass der Host im Lenovo-Add-In aufgelistet ist, können Sie ihn manuell hinzufügen, indem Sie wie folgt vorgehen.

1. Entfernen Sie auf der Seite SCVMM Admin (SCVMM-Admin) den Host manuell aus der SCVMM-Hostliste.
 - a. Wählen Sie den Host aus der Hostliste aus.
 - b. Klicken Sie auf **Host** und wählen Sie **Start Maintenance Mode (Wartungsmodus starten)** aus.
 - c. Abhängig davon, ob der Host in einem Cluster ist oder nicht, führen Sie einen der folgenden Schritte aus.
 - Wenn der Host nicht in einem Cluster ist, wählen Sie aus dem Menü **Host Remove (Entfernen)** aus.
 - Wenn der Host in einem Cluster ist, wählen Sie aus dem Menü **Host Remove Cluster Node (Clusterknoten entfernen)** aus.

Anmerkungen: Manchmal funktionieren die oben genannten Anweisungen in Schritt 1 nicht. Wenn das der Fall, führen Sie die folgenden PowerShell-Befehle aus:

- `import-module virtualmachinemanager $RunAsAccount = Get-SCRunAsAccount -Name "RunAsAccount01" Get-SCVMHost -ComputerName "VMHost01"`
 - `remove-SCVMHost -Credential $RunAsAccount`
2. Fügen Sie auf der Administrator-Benutzeroberfläche den Host manuell zu SCVMM oder zum Cluster hinzu.
 - a. Wählen Sie den Hypervisor-Knoten in der Lenovo-Add-In-Liste aus.
 - b. Klicken Sie auf **Synchronize (Synchronisieren)** über der Baumstruktur, um die Liste erneut zu laden.

3. Wenn der Host nicht in der Lenovo-Add-In-Hostliste angezeigt wird, starten Sie den Host neu und führen Sie anschließend die vorherigen Schritte erneut aus.

Installationsprogramm zeigt Fehlernachricht an

In seltenen Fällen schlägt das Lenovo-Add-In-Installationsprogramm fehl und zeigt eine Fehlernachricht an.

Der Fehler tritt normalerweise auf, wenn das Installationsprogramm zum ersten Mal auf dem System ausgeführt wird.

Wenn das Installationsprogramm fehlschlägt, führen Sie die folgenden Schritte aus:

1. Schließen Sie das Nachrichtenfenster, um die Installation zu stoppen.
2. Führen Sie das Installationsprogramm erneut aus.

Nachdem Sie das Installationsprogramm ein zweites Mal ausgeführt hat, funktioniert es ordnungsgemäß und das Lenovo-Add-In wird installiert.

Microsoft Internet Explorer-Update KB3087038 installieren

Für einige Lenovo Add-in für Microsoft System Center Virtual Machine Manager-Funktionen ist es erforderlich, dass der Microsoft Internet Explorer mit der Aktualisierung KB3087038 oder einer späteren Aktualisierung gepatcht wird.

Vorgehensweise

Schritt 1. Überprüfen Sie, ob Ihre Version von Microsoft Internet Explorer einen Patch erfordert.

- a. Öffnen Sie das Dialogfenster About Internet Explorer (Informationen zu Internet Explorer).

Anmerkung: Die Schritte, die Sie verwenden, um das Dialogfenster zu öffnen, variieren möglicherweise je nach Internet Explorer-Versionen.

- b. Prüfen Sie die Versionsnummer. Wenn die Versionsnummer niedriger als 10.0.9200.17492 ist, müssen Sie Internet Explorer mit dem Internet Explorer-Update KB3087038 patchen. Wenn der Wert gleich oder größer als 10.0.9200.17492 ist, benötigen Sie keinen Patch.
- c. Wenn Sie Internet Explorer patchen müssen, fahren Sie mit dem nächsten Schritt fort. Wenn Sie Internet Explorer nicht patchen müssen, stoppen Sie hier.

Schritt 2. Laden Sie den KB3087038-Patch herunter und installieren Sie ihn.

- a. Navigieren Sie zu der entsprechenden Microsoft-Webseite:
 - Für X64-basierte Systeme gehen Sie zu [Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 \(KB3087038\)](#).
 - Für X86-basierte Systeme gehen Sie zu [Kumulatives Sicherheitsupdate für Internet Explorer 11 unter Windows Embedded Standard 7 \(KB3087038\)](#).
- b. Befolgen Sie die Anweisungen auf der Seite, um den KB3087038-Patch herunterzuladen und zu installieren.

Lenovo XClarity Administrator-Zertifikat kann nicht importiert werden, wenn Internet Explorer 10 verwendet wird

Wenn Sie eine Lenovo XClarity Administrator-Zertifikatsdatei (PEM) manuell in Lenovo XClarity Integrator importieren, schlägt der Import möglicherweise mit der folgenden Nachricht fehl: Fail to upload certificate file (Hochladen der Zertifikatsdatei fehlgeschlagen). Dies ist ein bekanntes Problem von Internet Explorer 10.

Vorgehensweise

Führen Sie einen der folgenden Schritte zur Behebung dieses Problems aus:

- Aktualisieren Sie Internet Explorer auf eine spätere Version oder verwenden Sie einen anderen Web-Browser.
- Wenn Sie das Zertifikat importieren, wählen Sie **Paste certificate in PEM format (Zertifikat im PEM-Format einfügen)** aus. Verwenden Sie nicht **Add from a file (PEM) (Aus Datei hinzufügen)**, um das Zertifikat hinzuzufügen.

Anhang A. Systemfirewalleinstellungen

Mithilfe der Tabelle in diesem Abschnitt können Sie Firewallausnahmen festlegen.

Die Tabelle unten zeigt Ports, die vom Lenovo-Add-In und weiteren Lenovo XClarity Integrator-Produkten für Microsoft System Center verwendet werden.

Tabelle 8. Von Lenovo XClarity Integrator-Produkten verwendete Ports.

Projekt	Quelle		Ziel			Protokoll	Hinweise
	Port	Position	Komponente	Port	Position		
SCVMM-Add-in	nicht angegeben	Verwaltungs-server	SCVMM Add-in-Konsole (localhost/127.0.0.1)	TCP 9500*	Verwaltungs-server	Lenovo XClarity Integrator Unified Service	Der Ziel-Port kann geändert werden, wenn Lenovo XClarity Integrator installiert ist.
		verwalteter Server	Hyper-V-/Windows-Clients, die mit SCVMM verwaltet werden				
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Unified Service (localhost/127.0.0.1)	TCP 9501*	Verwaltungs-server	PostgreSQL	Der Ziel-Port kann geändert werden, wenn Lenovo XClarity Integrator installiert ist.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Unified Service	TCP 5988 TCP 5989	verwalteter Server	BMC	Die BMC-HTTP/HTTPS-Ports können in das BMC-Portal geändert werden.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Unified Service	TCP 80 TCP 443	externe Ressource	IBM/Lenovo-Website	Für das Herunterladen der Firmware von IBM/Lenovo-Websites wird HTTP-Proxy unterstützt.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Unified Service	TCP 443	externe Ressource	Lenovo XClarity Administrator	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.
	nicht angegeben	Verwaltungs-server	Lenovo XClarity Integrator Unified Service	TCP 135	verwalteter Server	Host-BS – WMI-Server	nicht zutreffend

Tabelle 8. Von Lenovo XClarity Integrator-Produkten verwendete Ports. (Forts.)

Projekt	Quelle		Ziel			Protokoll	Hinweise
	Port	Position	Komponente	Port	Position		
	nicht angegeben	Verwaltungs- server	Lenovo XClarity Integrator Unified Service	UDP 137	verwalteter Server	Host-BS – Samba-Server	NetBIOS-Namensdienst (NMBD)
				UDP 138			
				TCP 139			
				TCP 389			
				TCP 445			
				TCP 901			
SCOM HWMIP	nicht angegeben	Verwaltungs- server	Hyper-V-/Windows-Clients, die mit SCVMM verwaltet werden	UDP 137	Verwaltungs- server	BS – Samba-Server	NetBIOS-Namensdienst (NMBD)
				UDP 138			
				TCP 139			
				TCP 389			
				TCP 445			
				TCP 901			
SCOM HWMIP	nicht angegeben	Verwaltungs- server	SCOM-Hardware MP-Konsole (localhost/127.0.0.1)	TCP 9500*	Verwaltungs- server	Verwaltungsserver – (Lenovo XClarity Integrator) Unified Service	HTTPS
				TCP 9501*			
	nicht angegeben	Verwaltungs- server	Lenovo XClarity Integrator Unified Service (localhost/127.0.0.1)	TCP 9501*	Verwaltungs- server	PostgreSQL	nicht zutreffend

Tabelle 8. 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 Unified Service	TCP 5988 TCP 5989	verwalteter Server	BMC	HTTP, CIM, SLP HTTPS, CIM, SLP	Die BMC-HTTP/HTTPS-Ports können in das BMC-Portal geändert werden.	
	nicht angegeben	Verwaltungs-server	SCOM Hardware MP	TCP 161 TCP 162	verwalteter Server	CMIM und/oder AMM	SNMP-Agent SNMP-Traps	Die Ports können in das CMM-Portal geändert werden.	
SCCM OSD	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	DHCP TFTP-Server	nicht zutreffend	
	nicht angegeben	Verwaltungs-server	SCCM-Update-Tool	TCP 80 TCP 443 TCP 8530 TCP 8531	externe Ressource	WSUS-Server	HTTP HTTPS HTTP HTTPS	nicht zutreffend	
SCCM-Aktualisierung	nicht angegeben	Verwaltungs-server	SCCM-Update-Tool	UDP 137	verwalteter Server	Host-BS – Samba-Server	NetBIOS-Namensdienst (NMBD)	nicht zutreffend	

Tabelle 8. Von Lenovo XClarity Integrator-Produkten verwendete Ports. (Forts.)

Projekt	Quelle		Ziel			Protokoll	Hinweise
	Port	Position	Komponente	Port	Position		
				UDP 138		SMB	
				TCP 139			
				TCP 389		LDAP	
				TCP 445		NetBIOS	
				TCP 901		SWAT	
SCCM Inventory	nicht angegeben	Verwaltungs-server	SCCM Inventory Tool	TCP 5988	verwalteter Server	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

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

Anhang B. 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 jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

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

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

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

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

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

Marken

Lenovo, das Lenovo Logo, Flex System, System x und NeXtScale System sind Marken von Lenovo in den Vereinigten Staaten und anderen Ländern.

Intel und Intel Xeon sind Marken der Intel Corporation in den USA und/oder anderen Ländern.

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

Linux ist eine eingetragene Marke von Linus Torvalds.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

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.

